Management der Informationssicherheit in Unternehmen

DISSERTATION
DER WIRTSCHAFTSWISSENSCHAFTLICHEN
FAKULTÄT
DER UNIVERSITÄT ZÜRICH

zur Erlangung der Würde
eines Doktors der Informatik

vorgelegt von

MARCUS HOLTHAUS

von

Deutschland

genehmigt auf Antrag von

PROF. DR. K. BAUKNECHT
PROF. DR. ST. TEUFEL

August 2000

Die Wirtschaftswissenschaftliche Fakultät, Abteilung Informatik, gestattet hierdurch die Drucklegung der vorliegenden Dissertation, ohne damit zu den darin ausgesprochenen Anschauungen Stellung zu nehmen.

Zürich, den 3. Februar 1999*

Der Abteilungsvorsteher: Prof. Dr. P. Stucki

* Datum der Promotionsfeier

für Désirée

HAVE A GOAL.

A GOAL IS JUST A DREAM WITH A DEADLINE.

– MAJORIE BLANCHARD

Vorwort

Die Erarbeitung dieser Dissertation habe ich als Herausforderung empfunden, welche ich ohne die Unterstützung zahlreicher Personen aus meinem privaten und beruflichen Umfeld nicht hätte meistern können. Deshalb möchte ich hier all Jenen danken, auf deren Hilfe ich in dieser anspruchsvollen Zeit zählen konnte.

In erster Linie gilt mein Dank Herrn Prof. Dr. Kurt Bauknecht, der mir als Assistent am Institut für Informatik der Universität Zürich die Umgebung für die Erarbeitung dieser Dissertation zur Verfügung gestellt hat. Das kreative und aufgeschlossene Team, das moderne Umfeld und die gewährten Freiheiten erlaubten mir eine unabhängige Entwicklung und den Aufbau eines breiten Fachwissens, das im Rahmen von Aus- und Weiterbildung weitergeben werden konnte und das die Bildung einer eigenen Meinung über das von mir bearbeitete Fachgebiet erlaubte.

Die wohl wichtigste Zutat zum Gelingen dieser Dissertation war das Coaching durch Frau Prof. Dr. Stephanie Teufel. Ihre stets konstruktiv-kritische Begleitung dieser Arbeit hatte spürbare Einflüsse. Die von ihr vermittelten Kontakte in Wissenschaft und Praxis erwiesen sich sowohl als wertvolle Grundlage für diese Arbeit als auch für die Zeit danach.

Darüber hinaus gilt mein besonderer Dank Herrn Dr. Daniel von Stockar, der meine Dissertation während dreier Jahre unterstützte. Auch er gewährte mit bedeutende Freiräume in dem von ihm geleiteten Projekt und förderte mich bei der Weitergabe der im Projekt gewonnenen Erkenntnisse nach meinen Prioritäten.

Für viele interessante Diskussionen, die in der stets offenen Atmosphäre am Institut stattfinden konnten, danke ich Dr. Christian Tschudin, Thomas Kessler, Othmar Morger, Philipp Kirsch und Ulrich Nitsche. Ein ganz besonderer Dank für kritische Stellungnahmen gilt Harald Weidner, der die Grundlagen für konzeptionelles und technisches Know-how in den Bereichen *LINUX* und Internet Security einbrachte.

Ohne die Unterstützung durch Heinz Wyler wäre diese Dissertation kaum entstanden. Er war es, der die theoretische Betrachtung der hier behandelten praxisrelevanten Probleme anregte und sie mir in seinem Umfeld vor Augen führte.

Und schliesslich waren es vier Jahre, welche Désirée trotz der hohen Belastung als erlebnis- und ereignisreichen Lebensabschnitt zu gestalten verstanden hat. Auch Daniel Annen, Adolf Dörig, Thomas Gaugler, Rolph Haefelfinger, Bernhard M. Hämmerli, Markus Schilling, Hans-Rudolf Thomann, Stefan Thomer, Peter Trachsel, Dr. Markus Unternährer, Patrick Winter, Dr. Urs Zurfluh und den weiteren Vorstandsmitgliedern der Fachgruppe Security der Schweizer Informatiker Gesellschaft habe ich jeweils einen eigenen, besonderen privaten oder professionellen Anteil am Gelingen dieser Dissertation zu verdanken. Dass diese Arbeit weitgehend auf Orthographie- und Grammatikfehler verzichtet, ist der

unermüdlichen qualifizierten Arbeit mehrerer Lektoren – darunter meine Eltern – zu verdanken.

Ausserdem bedanke ich mich bei meinen Vorgängern am Institut für Informatik Dr. Brigitte Bailer, Dr. Thomas Barothy, Dr. Ralph Holbein, Dr. Andrew Hutchison, Dr. Christian Schatzmann, Dr. Walter Seitz und Dr. Volker Stadler, welche mir mit gutem Rat zur Seite standen und mich zum Abschluss dieser Dissertation ermunterten.

Marcus Holthaus

Zusammenfassung

Management der Informationssicherheit in Unternehmen

Eine informationsorientierte Betrachtung von Bezugsobjekt, Inhalten, Institutionen, Instrumenten und Prozessen der Informationssicherheit

Die Umsetzung der Informationssicherheit in einer Unternehmung ist komplex und aufwendig. Das Gelingen eines Informationssicherheitsprojektes hängt von vielen Voraussetzungen ab, die es im Rahmen eines Umsetzungsprojektes möglichst früh zu erkennen gilt. Ein Überblick über das Fachgebiet ist notwendig und wird in dieser Dissertation als *Rahmenwerk* definiert und in einem *Prozess* konkretisiert.

Wichtigste Voraussetzung für das erfolgreiche Management der Informationssicherheit ist die Unterstützung der obersten Unternehmungsführung und der Wille, dieses Thema in der eigenen Unternehmung konsequent zu betrachten und die dazu notwendigen Mittel bereitzustellen. Die Einigung auf eine entsprechende, eindeutig formulierte ***Ziel***setzung ist der erste Schritt dazu. Die spezifischen Ziele der Unternehmung bzgl. Informationssicherheit können dann aus den unternehmerischen Zielen hergeleitet und zu diesen in Beziehung gesetzt werden. Dabei werden Entwicklungen des unternehmerischen Umfeldes ebenso berücksichtigt wie interne Anforderungen. Aus diesen Zielen kann eine (zunächst informelle) Informationssicherheitspolitik formuliert werden. Diese Politik muss so früh und so konsequent wie möglich innerhalb der Unternehmung kommuniziert und vorbildlich gelebt werden.

Aufbauend auf der Politik wird eine unternehmensweite ***Organisation*** ins Leben gerufen, welche die Durchführung eines Projektes zur Umsetzung der Informationssicherheit innerhalb der Unternehmung vorantreibt. Diese Organisation – z.B. unter Leitung eines *Informationssicherheitsbeauftragten* – hat folgende Aufgaben:

- Formulierung, Formalisierung und Kommunikation der Informationssicherheitspolitik,
- Unterteilung des Gesamtprojektes in einzelne, handhabbare Blöcke und Bereiche, z.B. gemäss Abteilungsgrenzen,
- Förderung bzw. Festlegung der Integration der Sicherheitstätigkeiten in die bestehenden Stellen,
- Bereitstellung von strategischen und taktischen Vorgehensweisen und Verfahren, um Informationssicherheit in den einzelnen Bereichen umzusetzen,
- Koordination der Informationssicherheitsarbeiten, insbesondere bei Problemen, welche bereichsübergreifend gelöst werden müssen,

- Betreuung, Beratung und Förderung der einzelnen Informationssicherheitsprojekte,
- Aufbau und Weitergabe von Know-how,
- Bereitstellung von Hilfsmitteln für die Sicherheitsadministration, Sensibilisierung etc.,
- Kontrolle der Umsetzung und der Resultate.

Weiterhin kann ein ***Rollenmodell*** festgelegt werden, welches die Verantwortungen, Aufgaben und Kompetenzen jeder einzelnen Person in der Unternehmung hinsichtlich Informationssicherheit beschreibt. Jede Person erhält dann mindestens eine (evtl. mehrere) dieser Rollen.

Im hier beschriebenen Vorschlag koordiniert eine Person aus jeder Abteilung die Umsetzung der Informationssicherheit (Rolle des *Koordinators für Informationssicherheit*). Diese Person durchläuft einen ***Prozess***, der folgende Tätigkeiten umfasst:

- *Abgrenzung* des Untersuchungsobjektes bzgl. Breite und Tiefe. Die Abgrenzung in der Breite geschieht durch die ausdrückliche Zuordnung bzw. den Ausschluss von schützenswerten Objekten aus der Untersuchung. Die Abgrenzung der Tiefe geschieht durch Beschränkung auf einzelne Objektgruppen (Informationen, Hardware, Software, Personen etc.) und die Einschränkung der zu betrachtenden inhaltlichen Anforderungen an die Informationssicherheit (Verfügbarkeit, Vertraulichkeit etc.),
- *Identifikation* und Inventur der schützenswerten Objekte evtl. mit Erfassung aller relevanten Eigenschaften (konkrete Anforderungen an die einzelnen Objekte, Beschreibung wichtiger Risiken, Werte der Objekte etc.),
- *Allgemeine Risikoanalyse* zur Identifikation übergreifender Risiken, denen die Objekte unterliegen,
- *Spezifische Risikoanalyse* zur genaueren Betrachtung hoher Risiken,
- *Massnahmenauswahl* zur Reduktion der identifizierten Risiken,
- *Massnahmendiskussion und -beschluss* zur Bestimmung der Budgets, zur Festlegung der Umsetzungstermine und zur Vergabe der Aufträge (Realisierungsplan),
- *Koordination der Massnahmenumsetzung* gemäss festgelegtem Realisierungsplan,
- *Kontrolle* der Umsetzung durch die verantwortliche Person selbst, durch die Betroffenen, den Informationssicherheitsbeauftragten und weitere Stellen.

Diese Komponenten (*Ziel, Organisation, Rollenmodell, Prozess*) bilden gemeinsam das *Rahmenwerk der Informationssicherheit*, welches in dieser Dissertation in Kapitel 1 kurz vorgestellt, zu Beginn von Kapitel 3 gesamthaft und in den Kapiteln

3 bis 6 detailliert beschrieben wird. Das Rahmenwerk betrachtet Informationssicherheit als Managementaufgabe und leitet sie aus den Ansätzen von Rühli (Zürcher Führungsansatz [Rühli85]) und Heinrich (Grundlegung des Informationsmanagements [Heinrich93]) her. Teile I und II dieser Dissertation sind entsprechend der Unterteilung dieser Ansätze strukturiert:

- In den *Grundlagen* (Kapitel 2) werden die Begriffe und allgemeinen Ziele der Informationssicherheit identifiziert und beschrieben,
- das *Bezugsobjekt* (Kapitel 3) identifiziert, worauf sich Informationssicherheit bezieht, welcher Teil der Unternehmung für die Betrachtung der Informationssicherheit ausgewählt werden muss und wie er unterteilt werden kann,
- die *Elemente* der Informationssicherheit (Kapitel 4) umfassen die Betrachtung der Institutionen, der Motivationen, der Ziele und der Werkzeuge der Informationssicherheit,
- die *Tätigkeiten* der Informationssicherheit (Kapitel 5) umfassen die verschiedenen Sicherheitsfachgebiete, welche aus der Strukturierung des Bezugsobjekts gemäss Kapitel 3 hervorgehen und
- der *Prozess* der Informationssicherheit (Kapitel 6) umfasst die Vorgehensweise der Informationssicherheit in vier Zyklen mit je fünf Phasen.

Neu und einzigartig an der vorliegenden Arbeit ist die Definition eines derart breit abgestützten Rahmenwerks. Zur kritischen Beurteilung dieser Arbeit werden die bestehenden Verfahren, welche sich in der Praxis bewährt haben, einer eingehenden Analyse unterzogen, um ihre Stärken und Schwächen anhand von Vergleichen mit dem Rahmenwerk zu identifizieren. Aus dieser Analyse wird sodann ein neues Verfahren hergeleitet und hier beschrieben, wobei die Anforderungen an dieses neue Verfahren sich aus der Einbindung der erkannten Stärken und der Vermeidung der Schwächen der etablierten Verfahren ergeben.

Dieses neue Verfahren berücksichtigt die vier Komponenten des Rahmenwerks und wird in Kapitel 8 unter dem Namen *ISIWAY 4* Schritt für Schritt definiert. Es stellt die *erste Konkretisierung* des Rahmenwerks dar und definiert das Vorgehen zur Erreichung von Informationssicherheit in den vier Zyklen *Minimale Informationssicherheit*, *Angepasste Informationssicherheit, Risikogerechte Informationssicherheit* und *Umfassende Informationssicherheit* (daher die Bezeichnung *ISIWAY 4*). Es wird anschliessend kritisch beurteilt und an den zuvor gestellten Anforderungen gemessen.

Die Anforderungen an das neue Verfahren werden in die Bereiche *Auslösung, Organisation, Durchführung* und *Fachbereiche* unterteilt. *ISIWAY 4* wurde darauf angelegt, parametrisierbar und skalierbar zu sein. Bei der kritischen Beurteilung wurde festgestellt, dass im Teilkriterium *Erlernbarkeit* (als Teil des Kriteriums *Organisation*) die grösste Diskrepanz zwischen den Anforderungen an das neue Verfahren und der Bewertung dieses Verfahrens entstand. Deshalb wurde eine

vereinfachte Variante erstellt, die nicht nur leichter erlernbar ist, sondern sich zudem auch für kleinere Projekte und als Einstieg in *ISIWAY 4* eignen soll. Dieses Verfahren wird in Kapitel 10 beschrieben wird und stellt die *zweite Konkretisierung* des Rahmenwerkes dar. Es enthält nur noch einen Zyklus mit einigen Zusätzen und wird deshalb *ISIWAY 1.5* genannt. Zusätzlich wird dieses Verfahren vollumfänglich von einem Hilfsmittel namens *ISIGO 1.5* unterstützt. Dieses Werkzeug wird in Kapitel 9 erläutert und unterstützt den Durchführenden in jedem Schritt des Verfahrens *ISIWAY 1.5*. Darüber hinaus berücksichtigt es auch einige Elemente des allgemeinen, in Kapitel 8 vorgestellten *ISIWAY*-Verfahrens und baut auf einem übergreifenden Datenmodell auf, das in Kapitel 9 unter dem Titel *ISIGO CENTRAL* konzipiert wird. Insbesondere lässt sich *ISIWAY 1.5* in Verbindung mit *ISIGO 1.5* vollkommen unabhängig von dieser Dissertation einsetzen.

Gesamthaft bietet diese Dissertation also eine strukturierte, breit abgestützte und detaillierte Analyse des Problemfeldes Informationssicherheit, ein Rahmenwerk für die strategische, taktische und operative Umsetzung der Informationssicherheit in einer Unternehmung sowie zwei unterschiedlich komplexe Realisierungsvorschläge namens *ISIWAY 4* und *ISIWAY 1.5* mit einem dazu passenden Hilfsmittel namens *ISIGO 1.5*.

Es werden somit alle Bestandteile zur Verfügung gestellt, um Informationssicherheit im unternehmerischen Umfeld effizient und effektiv umzusetzen. Insbesondere kann das hier entwickelte Rahmenwerk (Teil II) als Grundlage für weitere Arbeiten im Bereich des Managements der Informationssicherheit verwendet werden.

Summary

Management of information security in enterprises

An Information-Oriented Examination of the Reference Object, the Subjects, Institutions, Instruments and Processes of Information Security

Implementing information security in a business environment is complex and time-consuming. Many forces and influences contribute to the positive outcome of an information security project. Therefore it is an advantage to know as many of them as early as possible. These influences are examined and formalised in this dissertation and have been arranged as a *framework*. They have been integrated as a *process*.

There is one most important prerequisite to successfully manage information security: Getting top management commitment to implement information security and to free the resources needed to do so. Initially, this requires management to agree on an appropriate, uniquely formulated information security ***goal***. Actual information security related goals can then be deduced from the general business policy. Business environment developments must be considered as well as internal requirements. An information security policy – informally in the beginning – begins to develop. This policy must be communicated within the enterprise as early and as consistently as possible and must be lived after exemplarily.

Based on this policy, an enterprise-wide ***organisation*** must be brought into life. It is needed to initialise and to support the execution of a corresponding information security project within the enterprise. This organisation, which can be lead by an *Information Security Delegate*, has the following tasks:

- To formulate, to formalise and to spread the information security policy,
- to split the overall project into individual, manageable parts and subjects, e.g. in accordance to department boundaries,
- to promote the co-operation of information security activities between existing institutions inside the enterprise and its integration into business processes,
- to supply strategic and tactical methodologies and procedures to implement information security within the individual departments,
- to co-ordinate the information security activities, most importantly when problems must be solved at a level superior to an individual project,
- to take care of, to provide advice for and to promote the individual information security projects,
- to collect know-how and to pass it on,

- to supply tools for information security administration, awareness promotion etc., and
- to check on implementation and results.

Furthermore, a ***role model*** has to be defined. It should describe the information security responsibilities, functions and authorities of each individual person in the enterprise. This model must be formulated in such a way that each person fits into at least one of the roles.

In the proposal formulated in this dissertation, it is the duty of one person per department to co-ordinate local implementation of information security (this role is called *Information Security Co-ordinator*). This person must guide a ***process*** covering the following activities:

- To set the boundaries of the investigation target, concerning width and depth. Setting the width boundary is done by the express inclusion or exclusion of parts of the object investigated. Setting the depth boundary is done by limiting the investigation to specified kinds of objects (information, hardware, software, co-workers etc.) and by restricting the requirements to be considered (availability, confidentiality, obligation etc.),
- to identify and to administer protection objects, possibly collecting additional characteristics (requirements on the individual objects, important risks, object values etc.),
- to carry out a general risk analysis to identify major risks which the protection objects are subject to,
- to carry out specific risk analyses for the more exact consideration of important risks,
- to select measures to reduce the identified risks,
- to discuss and to promote decisions on measures to reduce the identified risks, considering costs and setting deadlines,
- to co-ordinate the implementation of measures, and
- to check on implementation, done by the person in charge, by those affected, by the Information Security Delegate and by other parties.

These components (*goal, organisation, role model, process*) make up the *Information Security Management Framework*, which is presented in this dissertation. A short description can be found in chapter 1. A broad view is presented at the beginning of chapter 3 and it is described in detail in chapters 3 to 6. The framework looks at information security as a management function. It is deduced it from the approaches of Rühli [Rühli85] and Heinrich [Heinrich93]. Part I and II of this dissertation are structured according to these approaches:

- The *foundation* (chapter 2) identifies and defines terms an general information security goals and concepts,

- the *reference object* (chapter 3) defines which part of the enterprise must be selected for information security and how it must be split into parts,
- the *elements* of information security (chapter 4) cover institutions, motivations, specific goals and instruments,
- the *activities* of information security (chapter 5) describe the various information security subjects which can be applied to the parts of the reference model,
- the information security *process* (chapter 6) describes the procedure in four cycles with five phases each.

A framework like this has not been described yet in any known approach. The existing procedures, which have mostly proven useful in practice, are subjected to a detailed analysis nevertheless, in order to identify their strengths and weaknesses. Is it deduced from this analysis how a new procedure must be constituted, if it were to combine the strengths and to avoid the weaknesses.

This new procedure, called "*ISIWAY 4",* covers the four framework components and is defined step by step in chapter 8. *ISIWAY 4* is the first of two ways in which the framework is put into concrete form. It defines the procedure to reach information security in four cycles (hence the **4** in *ISIWAY 4*), called *Minimal Information Security, Appropriate Information Security, Risk-Related Information Security* and *Comprehensive Information Security*. *ISIWAY 4* will be subjected to the same detailed analysis as the existing procedures mentioned before, in order to explain how the requirements are fulfilled.

The requirements of the new procedure will are divided in the groups *Initiation, Organisation, Implementation* and *Content*. *ISIWAY 4* has been designed to be adaptable and scalable. Another required property of *ISIWAY* is ease of use. In order to achieve this, the procedure must not be too complex. The full *ISIWAY 4* procedure *is* complex, so a more simple version was designed, which can be applied in smaller projects, or which may serve as an introduction to the information security process and should be easier to learn. *ISIWAY 1.5* is such a simplification. It will be introduced in chapter 10 and is the second way described here to put the Information Security Framework in concrete. Additionally, this procedure is fully supported by a tool named *ISIGO 1.5*. This tool is presented in chapter 9 and supports the execution of each step of the *ISIWAY 1.5* procedure. In addition, it considers some items of the *ISIWAY 4* procedure presented in chapter 8 and is based on structures of an overall data model, which is presented in chapter 9 under the title of *ISIGO CENTRAL*.

Thus, this dissertation offers a structured, broadly supported and detailed analysis of the information security problem field, defines an information security management framework as a general solution, contains two procedures named

ISIWAY 4 and *ISIWAY 1.5* which differ in complexity, and it supplies a corresponding tool named *ISIGO 1.5*.

Therefore, all components necessary to implement information security efficiently and effectively in a business environment have been presented in this dissertation. In particular, the framework developed here (part II) can be used as a basis for further work in the information security management field.

Übersicht

TEIL I GRUNDLAGEN

1 PROBLEMSTELLUNG 1

2 GRUNDLAGEN UND BEGRIFFE 21

TEIL II RAHMENWERK DER INFORMATIONSSICHERHEIT

3 BEZUGSOBJEKT 59

4 ELEMENTE 101

5 TÄTIGKEITEN 141

6 PROZESS 167

TEIL III IMPLEMENTATION

7 VERGLEICHENDE EVALUATION 191

8 VERFAHREN ISIWAY 217

9 PROTOTYP ISIGO 241

TEIL IV UMSETZUNG

10 VERWENDUNG VON ISIWAY UND ISIGO 257

11 AUSBLICK 273

ANHÄNGE 279

Inhalt

1 PROBLEMSTELLUNG 1

1.1 Forschungskonzept und Beitrag 3
1.2 Terminologie 9
1.3 Methodik 14
1.4 Lesehinweise 19

2 GRUNDLAGEN UND BEGRIFFE 21

2.1 Informationsbegriffe 21
2.2 Sicherheitsbegriffe 25
2.3 Grundanforderungen und Grundbedrohungen 35
2.4 Typisierung von Bedrohungen und Risiken 38
2.5 Informationssicherheit 44
2.6 Unternehmerische Führung 48
2.6.1 Führungskonzeption 48
2.6.2 Strategisches Führungskonzept 50
2.6.3 Phasen der strategischen Führung 51
2.6.4 Aspekte der Führung 53
2.6.5 Verwendung in dieser Dissertation 56

3 BEZUGSOBJEKT 59

3.1 Rahmenwerk der Informationssicherheit 60
3.2 Bezugsobjekt der Informationssicherheit 66
3.3 Unternehmung 68
3.4 Informationssystem 75
3.5 Institutionen 81
3.6 Informationen 82
3.7 Instrumente 84
3.8 IT- / EDV-System 87
3.9 IT- / EDV-Ressourcen 89
3.10 Integration des Bezugsobjekts 92
3.11 Klassifikation der schützenswerten Objekte 97

4 ELEMENTE 101

4.1 Umsetzung und Kontrolle 101
4.1.1 Controlling 102
4.1.2 Überprüfung 103
4.1.3 Internes Kontrollsystem (IKS) 103
4.1.4 Revision / Audit 104
4.1.5 Interne Revision 105
4.1.6 Externe Revision 107
4.1.7 Zusammenarbeit zwischen interner und externer Revision 108

4.1.8 IT- / Informatik-Revision ... 108
4.1.9 IT- / Informatik-Controlling ... 110
4.1.10 Fazit ... 110
4.2 Strukturen der Informationssicherheit ... 113
4.2.1 Gestaltungsvorschlag Controlling ... 114
4.2.2 Gestaltungsvorschlag Revision ... 115
4.2.3 Rollenkonzept ... 116
4.3 Externe Einflüsse ... 121
4.3.1 Veränderungen des unternehmerischen Umfelds ... 121
4.3.2 Fazit ... 131
4.4 Informationssicherheit als Ziel ... 132
4.4.1 Zielsystem der Unternehmung ... 132
4.4.2 Einfluss der Informationssicherheit auf die unternehmerische Zielerreichung ... 133
4.4.3 Bewertungskonflikte ... 134
4.4.4 Wirkung von Informationen ... 135
4.4.5 Fazit ... 136
4.5 Instrumente ... 137
4.5.1 Externe Instrumente ... 137
4.5.2 Interne Instrumente ... 138

5 TÄTIGKEITEN ... 141

5.1 Unternehmerische Sicherheit ... 142
5.2 Informationssicherheit ... 144
5.3 Sicherheit der Rollenwahl ... 149
5.3.1 Sicherheitskultur ... 149
5.3.2 Personensicherheit ... 150
5.4 Sicherheit der Aufgabenbearbeitung ... 151
5.4.1 Sichere Informationsverwendung ... 154
5.4.2 Kongruenz ... 155
5.4.3 Inhaltliche Datensicherheit ... 155
5.4.4 Inhaltliche Kommunikationssicherheit ... 156
5.5 DV-Sicherheit ... 157
5.5.1 IT- / EDV-Sicherheit ... 157
5.5.2 Prozesssicherheit ... 161
5.5.3 IT- / EDV-Betriebssicherheit ... 161
5.5.4 Systemsicherheit ... 162
5.5.5 Anwendungssicherheit ... 162
5.5.6 Technische Kommunikationssicherheit ... 163
5.5.7 Sicherheit der nicht-digitalen Datenverarbeitung ... 164
5.6 Produktionssicherheit ... 164
5.7 Infrastruktursicherheit ... 165

6 PROZESS ... 167

6.1 Inhalt und Ablauf ... 167
6.2 Vorbereitungen ... 169

6.3 Inventur ... 170
6.4 Analyse ... 171
6.5 Massnahmen ... 180
6.6 Umsetzung und Kontrolle ... 184
6.7 Aufwand für Informationssicherheitsbetrachtungen ... 185
6.8 Fazit aus Teil II ... 186

7 VERGLEICHENDE EVALUATION ... 191

7.1 Bewertungsschema ... 192
7.2 Bewertete Informationssicherheitsverfahren ... 199
7.2.1 IT-Sicherheitshandbuch (BSI-D) ... 200
7.2.2 Grundschutz-Verfahren (BFI) ... 203
7.2.3 IT-Grundschutzhandbuch (BSI-D) ... 205
7.2.4 Code of Practice (BSI-GB) ... 208
7.2.5 COBIT (ISACF) ... 210
7.2.6 GMITS (ISO) ... 212
7.3 Vergleichende Bewertung und Beurteilung ... 213

8 VERFAHREN *ISiWAY* ... 217

8.1 *ISiWAY* Konzept ... 217
8.2 *ISiWAY* Struktur ... 220
8.3 Rollen ... 225
8.4 Projekt ... 228
8.5 Evaluation von *ISiWAY* ... 237

9 PROTOTYP *ISiGo* ... 241

9.1 Spezifikation ... 241
9.2 Architektur ... 244
9.3 Technologievarianten ... 249
9.4 Fazit aus Teil III ... 254

10 VERWENDUNG VON *ISiWAY* UND *ISiGo* ... 257

10.1 Situation und Zielsetzung ... 258
10.2 Auslöser ... 258
10.3 Anwendung von *ISiWAY* ... 259
10.4 Definition von *ISiWAY* 1.5 ... 266
10.5 Situationsbezogene Evaluation von *ISiWAY 1.5* ... 268

11 AUSBLICK ... 273

11.1 Erarbeitete Komponenten ... 273
11.2 Folgeprojekte ... 276
11.3 Fazit ... 278

A EXKURS: INFORMATIK, EDV UND IT ... 279

B TABELLEN ZUR VERGLEICHENDEN EVALUATION ... 281

B.1 Bewertung BSI (D) IT-Sicherheitshandbuch ... 287

B.2 Bewertung BFI Grundschutzverfahren 291
B.3 Bewertung BSI (D) IT-Grundschutzhandbuch 295
B.4 Bewertung BSI (GB) Code of Practice 299
B.5 Bewertung ISACF COBIT 303
B.6 Bewertung ISO GMITS 307
B.7 Anforderungen an *ISiWAY* 311
B.8 Bewertung ISiWay 315
B.9 Gegenüberstellung Auslösung 319
B.10 Gegenüberstellung Organisation 321
B.11 Gegenüberstellung Durchführung 323
B.12 Gegenüberstellung Fachbereiche 325
B.13 Differenzen zwischen Anforderungen an ISiWay und Bewertung von ISiWay 327

C DOKUMENTATION ZU *ISiWAY* 329

C.1 Detaillierte Beschreibung von ISiWAY 329
C.1.1 Aktivitätengruppen 329
C.1.2 Inhalte der Vorbereitung (Detaillierungsgrad 0) 333
C.1.3 Minimale Informationssicherheit (Detaillierungsgrad 1) 346
C.1.4 Angepasste Informationssicherheit (Detaillierungsgrad 2) 356
C.1.5 Risikogerechte Informationssicherheit (Detaillierungsgrad 3) 361
C.1.6 Umfassende Informationssicherheit (Detaillierungsgrad 4) 366
C.1.7 Krisenmanagement (Detaillierungsgrad 3.5) 370
C.2 Vollständige Beschreibung von ISiWAY 1.5 375

D DOKUMENTATION ZU *ISiGo* 427

D.1 Implementation 427
D.1.1 Priorität der Implementation 427
D.1.2 Datenmodell 428
D.1.3 Funktionsbeschreibung 445
D.1.4 Erklärung der implementierten Funktionen 452
D.2 Beispiele 457

E GLOSSAR 465

F LITERATUR 471

G CURRICULUM VITAE 479

Abbildungen

Abbildung 1-1: Beziehungen zwischen Rühlis und Heinrichs Terminologie 11
Abbildung 1-2: Terminologie zur Strukturierung dieser Dissertation 13
Abbildung 1-3: Gliederung dieser Dissertation 14
Abbildung 1-4: Grundlagen und Begriffe 16
Abbildung 1-5: Gliederung des Rahmenwerks der Informationssicherheit und dieser Dissertation 17
Abbildung 2-1: Verhältnis zwischen Aufwand und Sicherheit [in Anlehnung an BSI-IT-GSHB97, T1, K1, S.7] 28
Abbildung 2-2: Darstellung der Risikobegriffe [in Anlehnung an ISO13335-1, S. 15] 32
Abbildung 2-3: Sicherheits- / Schutzziel [in Anlehnung an Winterthur90, S. 3] 33
Abbildung 2-4: Typisierung nach Ursache / Urheber 39
Abbildung 2-5: Typisierung nach Motivation 40
Abbildung 2-6: Dimensionen einer Führungskonzeption [Rühli91a, S. 16, Abb. 1] 49
Abbildung 2-7: Dimensionen eines strategischen Führungskonzeptes [Rühli91a, S. 24] 51
Abbildung 2-8: Gliederung der Führungskonzeption 53
Abbildung 3-1: Formelle Betrachtung der Elemente und Management-Tätigkeiten des Bezugsobjekts 60
Abbildung 3-2: Formelle Betrachtung der Elemente und Management-Tätigkeiten der Informationssicherheit 62
Abbildung 3-3: Statische und dynamische Betrachtung mit generischer Unterteilung der Managementprozesse 65
Abbildung 3-4: Rahmenwerk der Informationssicherheit 66
Abbildung 3-5: Elemente, Tätigkeiten und Sicherheitsfachgebiete der Unternehmung 74
Abbildung 3-6: Elemente, Tätigkeiten und Sicherheitsfachgebiete des Informationssystems 81
Abbildung 3-7: Elemente, Prozesse und Sicherheitsfachgebiete von Institutionen 82
Abbildung 3-8: Elemente, Tätigkeiten und Sicherheitsfachgebiete der Information 84
Abbildung 3-9: Elemente, Tätigkeiten und Sicherheitsfachgebiete des Informationssystems 87

Abbildung 3-10: Elemente, Prozesse und Sicherheitsfachgebiete des IT- / EDV-Systems 89
Abbildung 3-11: Elemente, Prozesse und Sicherheitsfachgebiete der IT- / EDV-Ressourcen 92
Abbildung 3-12: Zusammenfassende Darstellung der Elemente, Tätigkeiten und Sicherheitsfachgebiete des Bezugsobjekts der Informationssicherheit 95
Abbildung 4-1: Kontrollbegriffe, -stellen / -institutionen und -tätigkeiten (basierend auf [Rühli93, Korber93]) 111
Abbildung 4-2: Kontrollstrukturen der Unternehmung 113
Abbildung 5-1: Sicherheitsfachgebiete des Bezugsobjekts der Informationssicherheit 142
Abbildung 6-1: Risikomatrix mit Risiken 176
Abbildung 6-2: Risikomatrix mit Sicherheitsziel 177
Abbildung 6-3: Sicherheitsdispositiv [in Anlehnung an Winterthur90, S. 10] 182
Abbildung 6-4: IT-Sicherheitsarchitektur [Sherwood96] 183
Abbildung 7-1: Schema für Informationssicherheitsverfahren mit den vier Bewertungsbereichen 195
Abbildung 7-2: Verfahren zur Gewährleistung der IT-Sicherheit [BSI-IT-SHB92, S. 35] 201
Abbildung 7-3: Abhängigkeiten zwischen den 12 Schritten [BSI-IT-SHB92, S. 37] 202
Abbildung 7-4: BFI-Verfahren 204
Abbildung 7-5: Aktionsplan für den IT-Sicherheitsprozess 206
Abbildung 7-6: Beispiel zur Organisation des IT-Sicherheitsmanagements 207
Abbildung 8-1: *ISiWAY* DG0 bis DG4 221
Abbildung 8-2: *ISiWAY* DG0 bis DG4 mit Phasenbezeichnungen 222
Abbildung 8-3: Zusammenarbeit der Rollen 228
Abbildung 8-4: *ISiWAY*-Projekthierarchie 231
Abbildung 9-1: Blockdiagramm der *ISiGO*-Architektur 244
Abbildung 9-2: Funktionenmodell der *ISiGO*-Architektur mit Ebenen 246
Abbildung C-1: Detaillierungsgrad 0 334
Abbildung C-2: Detaillierungsgrad 1 346
Abbildung C-3: Detaillierungsgrad 2 356
Abbildung C-4: Detaillierungsgrad 3 361
Abbildung C-5: Detaillierungsgrad 4 366
Abbildung C-6: Detaillierungsgrad 3.5 370
Abbildung D-1: Personen, Adressen, Telefonnummern und E-Mail-Adressen 429
Abbildung D-2: Projekte, Untersuchungsobjekte und Teilnahme 430
Abbildung D-3: Prozesse 431

Abbildung D-4: Informationssammlungen 432
Abbildung D-5: Bewertungskriterien, Werte und Bewertung von Informationssammlungen 433
Abbildung D-6: Anforderungen der Informationssammlungen 433
Abbildung D-7: Informationssysteme aus technischer und benutzerorientierter Sicht, deren Verknüpfung und Bewertung 434
Abbildung D-8: Sicherheitsleistung der Systeme 435
Abbildung D-9: Verknüpfung von Informationssammlungen und Informationssystemen (Bearbeitung) 435
Abbildung D-10: Herleitung der Diskrepanzen 436
Abbildung D-11: Bedrohungen 436
Abbildung D-12: Massnahmen und ihre Beeinflussung der Sicherheitsleistung der Systeme 437
Abbildung D-13: Zusammenfassung der Beeinflussung der Sicherheitsleistung des Systems 437
Abbildung D-14: *ISIGO* Tabelle "Willkommen" 447
Abbildung D-15: Steuerungsfunktion von *ISIGO* (Menu) 448
Abbildung D-16: Bildschirmdarstellung des Zyklus *ISIWAY1.5* 448
Abbildung D-17: Darstellung der Aufgabe der aktuellen Aktivität 449
Abbildung D-18: Tabelle "Informationssammlungen", linker Teil 450
Abbildung D-19: Tabelle "Informationssammlungen", rechter Teil 450

Tabellen

Tabelle 2-1: Elemente und Aspekte der Führung [Rühli85, S. 28] 50
Tabelle 2-2: Phasen der strategischen Führung [Rühli91a, S. 27] 51
Tabelle 3-1: Elemente der Unternehmung 73
Tabelle 3-2: Kategorisierung der schützenswerten Objekte in Gruppen gemäss [BSI-IT-SHB92, S.43] 97
Tabelle 3-3: Klassifikation nach hier vorgeschlagener Gliederung des Bezugsobjekts 98
Tabelle 7-1: Bedeutungen der Werte bei quantitativen Fragestellungen 198
Tabelle 7-2: Bedeutungen der Werte bei qualitativen Fragestellungen 198
Tabelle 7-3: Bedeutungen der Werte bei spekulativen Fragestellungen 199
Tabelle 7-4: Massnahmen des COP 210
Tabelle 9-1: Beschreibung der *ISiGo*-Basisfunktionen 248
Tabelle A-1: Informatik, EDV und IT in Deutschland 280
Tabelle A-2: Informatik, EDV und IT in der Schweiz 280
Tabelle B-1: Bewertung BSI (D) IT-Sicherheitshandbuch 290
Tabelle B-2: Bewertung BFI Grundschutzverfahren 293
Tabelle B-3: Bewertung BSI (D) IT-Grundschutzhandbuch 297
Tabelle B-4: Bewertung BSI (GB) Code of Practice 301
Tabelle B-5: Bewertung ISACF COBIT 305
Tabelle B-6: Bewertung ISO GMITS 309
Tabelle B-7: Anforderungen an ISiWay 314
Tabelle B-8: Bewertung ISiWay 318
Tabelle B-9: Gegenüberstellung der Profile: Variable 1 (Auslösung) 319
Tabelle B-10: Gegenüberstellung der Profile: Variable 2 (Organisation) 321
Tabelle B-11: Gegenüberstellung der Profile: Variable 3 (Durchführung) 323
Tabelle B-12: Gegenüberstellung der Profile: Variable 4 (Fachbereiche) 325
Tabelle B-13: Differenzen zwischen Anforderungen an ISiWay und Bewertung von ISiWay 327
Tabelle C-1: Beispiel für Stellenbeschreibung des ISiBE 337
Tabelle C-2: Elemente der Informationssicherheitspolitik 340
Tabelle D-1: Zuordnung von *ISiGo 1.5*-Tabellen und *ISiGo Central*-Abfragen 438
Tabelle D-2: Infosammlungen 459
Tabelle D-3: Statistik 463

Abkürzungen

ACM	Association of Computing Machinery
AG	Aktiengesellschaft
API	Application Program Interface (= Programmierschnittstelle für Applikationen)
AppSec	Application Security (= Anwendungssicherheit)
BFI	Schweizerisches Bundesamt für Informatik
BS	British Standard
BSI	steht je nach Zusammenhang für BSI (D) oder BSI (GB)
BSI (D)	Deutsches Bundesamt für Sicherheit in der Informationstechnik
BSI (GB)	British Standards Institution
CAAT	Computer-Aided Audit Tool
CAIS	Computer-Aided Information Security
CERT	Computer Emergency Response Team
CIA	Akronym für die drei Grundanforderungen Vertraulichkeit (*c*onfidentiality), Integrität (*i*ntegrity) und Verfügbarkeit (*a*vailability)
COBIT	Control Objectives for Information and Related Technology, bezieht sich auf [COBIT96.1 bis .5]
CompSec	Computer Security (= Computersicherheit)
COP	Code of Practice
CSO/CSSO	Chief (Safety &) Security Officer (= Oberster Sicherheitsverantwortlicher)
Ctr.	Controller
Ctrl.	Control
Ctrlg.	Controlling
DataSec	Data Security (= Datensicherheit)
DIN	Deutsches Institut für Normung
DPSec	Data Processing Security (= Sicherheit der Datenverarbeitung)
DS	Datenschutz
DSG	Datenschutzgesetz
EDV	Elektronische Datenverarbeitung
ERev	Externe Revision
GAN	Global Area Network
GL	Geschäftsleitung, oberstes aktives Führungsgremium einer Unternehmung
GMITS	General Management of IT-Security, bezieht sich auf [ISO13335-1 bis –5]
GSHB	Grundschutzhandbuch, bezieht sich i.d.R. auf [BSI-IT-GSHB97]
GV	Generalversammlung
HTML	Hypertext Markup Language
i.e.S.	im engeren Sinne
IEC	International Electrotechnical Commission
IKS	Internes Kontrollsystem
IP	Information Processing (= Informationsverarbeitung)
IPSec	Information Processing Security (= Sicherheit der Informationsverarbeitung)
IRev	Interne Revision
ISec	Information Security (= Informationssicherheit)
IT	Informationstechnik, Informationstechnologie, informationstechnologisch

ITSec	Information Technology Security (= IT-Sicherheit = Sicherheit der Informationstechnik)
IS	Informationssystem
ISi	Informationssicherheit
ISiBe	Informationssicherheitsbeauftragter
ISiGo	In dieser Dissertation entwickeltes IT-System zur Unterstützung von *ISiWAY*
ISiKo	Koordinator für Informationssicherheit
ISiM	Management der Informationssicherheit
ISiPol	Informationssicherheitspolitik
ISiStrat	Informationssicherheitsstrategie
ISiVA	Verantwortlicher für Informationssicherheit
ISiWay, ISiWay 4	In dieser Dissertation entwickelter Prozess der Informationssicherheit mit vier Zyklen
ISiWay 1.5	In dieser Dissertation entwickelter Prozess der Informationssicherheit mit einem Zyklus und Zusätzen
ISO	International Organisation for Standardisation
i.w.S.	im weiteren Sinne
Kat.	Kategorie
LAMP	*LINUX-APACHE-MYSQL-PHP*
LAN	Local Area Network
MAN	Metropolitan Area Network
NetSec	Network Security (= Netzwerksicherheit)
OSI	Open Systems Interconnection
PEAK	Akronym für die vier konzeptionellen Führungsphasen Planung, Entscheidung, Anordnung und Kontrolle
Rev	Revision
S&S	Safety & Security
S&SO, SSO	Safety & Security Officer (Sicherheitsbeauftragter oder Sicherheits-verantwortlicher)
SHB	Sicherheitshandbuch
Si	Sicherheit
SiBe	Sicherheitsbeauftragter
SQL	Structured Query Language
TÜV	Technischer Überwachungsverein
ÜM	Übergeordneter Manager
WAN	Wide Area Network
ZSI	Zentralstelle für Sicherheit in der Informatik, nachmalig BSI (D)

Schlagwörter

Management der Informationssicherheit, Verfahren, Ressource Information, Sicherheitsmassnahmen, Unternehmung, Information Security, Information Security Management, Informationssicherheitsprozess, Information Security Process, Awareness, Process, Technology, Information Technology Security, IT-Sicherheit, IT Security, Information System Security, Information Management, ISec, ITSec, InfoSec, *ISIWAY*, *ISIGO*

LIKE ANY POWERFUL TOOL, COMPUTERS CAN BE A FORCE FOR GOOD OR HARM. [...] BECAUSE THE COMPUTER GIVES US FUNDAMENTALLY NEW POWER, WE ARE FACED WITH DECISIONS FOR WHICH OUR EXPERIENCES MAY GIVE US LITTLE GUIDANCE.

– MARY B. WILLIAMS,
PROFESSOR FOR PHILOSOPHY, UNIV. OF DELAWARE
IN: COMPUTER, ETHICS, AND SOCIETY, [ERMANN97 S. 3]

Teil I: Grundlagen

Im ersten Teil wird die Problemstellung dieser Dissertation behandelt (Kapitel 1). Dies umfasst Forschungskonzept und Beitrag, Terminologie und Methodik. In Abbildung 1-3 (Seite 14) wird die Gliederung gesamthaft dargestellt. In Kapitel 2 werden notwendige Grundlagen identifiziert und Begriffe definiert, bevor im Teil II mit der inhaltlichen Erarbeitung des Rahmenwerks der Informationssicherheit begonnen wird.

1 Problemstellung

In den vergangenen ca. 40 Jahren wurde *"das Organisationsmodell der Industrialisierung mit den Mitteln des Informationszeitalters zur letzten Perfektion entwickelt."* [Lutz95, S. 111]. Die technische Informatik, welche dies ermöglichte, geht dabei mehr und mehr in die Grundlage einer neuen Informations- und Kommunikationsinfrastruktur über, die gesellschaftlichen und sozialen Wandel auszulösen scheint. Gemäss [Peters96, S. 22] befinden wir uns am Beginn einer digitalen Revolution, dem Übergang ins Informationszeitalter. [Tapscott96, S. xv] schreibt:

> *"[...] today we are witnessing the early, turbulent days of a revolution as significant as any other in human history. A new medium of human communications is emerging, one that may prove to surpass all previous revolutions. The computer is expanding from a tool for information management to a tool for communications. Interactive multimedia and the so-called information highway, and its exemplar the Internet, are enabling a new economy based on the networking of human intelligence."*

Müller und Pfitzmann erwarten, *"dass dieses komfortable Kommunikations-instrument zu einem internationalen, elektronischen Feld der Begegnung zwischen Menschen, aber auch zu einem Kanal zu den Menschen werden wird."* [Müller97a, S. 11].

Die veränderte Sichtweise der Informationsverarbeitung, welche mit diesem Wandel einhergeht, betrifft die Gesellschaft als Ganzes. Die Globalisierung von rechtlichen und wirtschaftlichen Systemen wird durch die Vereinfachung der Kommunikation gefördert. Durch konsequente Digitalisierung ist eine Neu-organisation der Arbeit mit veränderter Arbeitsteilung möglich, was jedem der daran teilhabenden „Informationsarbeiter“[1] vermehrte zeit- und ortsunabhängige Leistungserbringung erlaubt. Die zunehmend leistungsfähige Informationstechnik und die konstante unternehmerische Forderung nach höherer Effizienz bilden einen sich selbst antreibenden Prozess. [2]

Wer in welchem Masse von diesen Entwicklungen profitieren wird, ist heute noch offen. Es ist jedoch absehbar, dass das *„nächste Jahrtausend [...] den Missbrauch geistigen Eigentums und einen Einbruch in unsere Privatsphäre [bringen wird]. Wir werden Digitalvandalismus, Softwarepiraterie und Datendiebstahl kennenlernen.“* [Negroponte95, S. 275]. Wie können sich die Informationsarbeiter in den Unternehmungen oder als Privatpersonen vor derartigen Beeinträchtigungen schützen, ohne auf die Potentiale der Entwicklung verzichten zu müssen? Wie müssen sie sich verhalten, um die Technologie-Folgerisiken zu minimieren?

Hier werden drei Forderungen genannt, die von ihnen erfüllt werden müssen:

- Es muss ein *Informationsbewusstsein* entstehen: Die Erkenntnis, dass im Zentrum jeder Informationsverarbeitung die *Information* steht, und dass ein technik- und datenzentrierter Ansatz, wie er noch heute üblich ist, nicht alle Aspekte informationsbezogener Risiken abdecken kann, muss sich bei den an Informationsverarbeitungsprozessen Beteiligten durchsetzen, so dass sie sich tatsächlich von Mitgliedern einer Organisation des Industriezeitalters zu *Informationsarbeitern* wandeln.
- Die Informationsarbeiter müssen die *besonderen Eigenschaften von Information* als neuem Produktionsfaktor erkennen. Information umfasst gemäss Definition (vgl. Kapitel 2) alle Aspekte von Wissen, Daten und Nachrichten unabhängig von Speicher- und Übertragungsmedium. Auch alle organisatorischen Tätigkeiten einer Unternehmung lassen sich der Informationsverarbeitung zuordnen, selbst wenn sie mündlich kommuniziert

---

1 Der Begriff des „Information Workers“ oder „Informationsarbeiters“ beschreibt alle Personen, welche Teil eines Informationsverarbeitungsprozesses sind.

2 Weitere erwartete Entwicklungen sind in [Negroponte95], [Lutz95, S. 84ff, S. 111ff], [Davidson97, S. 139ff], [Peters96, S.17ff] und [Popcorn96, S. 52ff, S. 124ff, S. 239ff] beschrieben.

und nicht auf Papier festgehalten werden. Deshalb gelten für die Verarbeitung von Information besondere Regeln.

- Die Informationsarbeiter müssen sich *über die Anforderungen*, welche sie an die von ihnen verarbeitete Information stellen, *klar werden*. Information hat für jede Person einen subjektiven Wert, der um so höher ist, je mehr die Anforderungen dieser Person an die Information erfüllt werden. Um den Wert der Information zu erhöhen, muss eine Person also die Erfüllung ihrer Anforderungen fordern und die Anwendung von Massnahmen verlangen, die diese Wertsteigerung zulässt.

Diese Dissertation beschäftigt sich mit der dritten Forderung. Um ihre Erfüllung zu erlauben, müssen Vorgehensweisen erstellt und angewendet werden, welche eine Identifikation der schützenswerten Information unabhängig vom verwendeten Medium erlauben. Diese Vorgehensweisen müssen die Beurteilung von Sicherheitsanforderungen ermöglichen. Massnahmen müssen bereitgestellt werden, mit deren Hilfe sich Information effizient schützen lässt. So kann ein sicherer Zustand von Informationen erreicht werden: *Informationssicherheit*.

1.1 Forschungskonzept und Beitrag

Zielsetzung

Der Begriff der Informationssicherheit ist mehrfach belegt und mit anderen Begriffen (z.B. IT-Sicherheit) verbunden. Es bestehen vielfältige Beiträge zur Informationssicherheit aus Forschung und Praxis. Hier soll deshalb ein Rahmenwerk definiert werden, in welches sich die vielen verschiedenen Aspekte einordnen lassen, die mit dem Begriff Informationssicherheit verbunden werden. Informationssicherheit wird dabei im unternehmerischen Umfeld betrachtet und die Unternehmung als Element einer sich verändernden Gesellschaft gesehen. Es wird eine Vorgehensweise vorgeschlagen, wie Informationssicherheit im unternehmerischen Umfeld erreicht werden kann. Dabei werden die unternehmerischen Ziele und die bestehenden Steuerungsstrukturen der Unternehmung berücksichtigt. Diese Vorgehensweise wird durch ein Werkzeug unterstützt und ihre Anwendung anschliessend in einem konkreten Umfeld exemplarisch beschrieben.

Forschungskonzept

Das Konzept der Forschung, welche mit dieser Dissertation dokumentiert wird, beruht auf einem empirischen Ansatz, der hier gemäss Atteslander in fünf Phasen des Forschungsablaufs gegliedert wird: *Problembenennung, Gegenstandsbenennung, Durchführung, Analyse* und *Verwendung von Ergebnissen* [Atteslander92, S. 32].

Problembenennung

Am Anfang der Forschung zu dieser Dissertation stand ein als soziales Problem wahrgenommener Zustand[3]: Die Durchführung von Informationssicherheits-projekten innerhalb von Unternehmungen ist oftmals unstrukturiert, erfolglos oder kurzfristig orientiert. Dies wird auf folgende Faktoren zurückgeführt:

- Der Wandel vieler Unternehmungen von einer industriellen Organisation der Arbeitsabläufe zu einer Informationsorientierung hat erst begonnen. Informationsorientierung bedingt die Anerkennung von Information als wichtige unternehmerische, und deshalb schützenswerte Ressource. Die Informationsorientierung einer Unternehmung kann beispielsweise an einer entsprechenden schriftlichen Formulierung der Unternehmungsleitung erkannt werden (z.B. in der Unternehmenspolitik oder in der unternehmerischen Sicherheitspolitik), oder durch Analyse der internen Abläufe oder durch Beobachtung des individuellen Verhaltens. Es bestehen heute noch viele Unternehmungen, in denen nur auf den Schutz der technischen Systeme zur Informationsverarbeitung (IT-Systeme, Informatik) fokussiert wird, die Informationsorientierung jedoch noch nicht begonnen oder abgeschlossen ist und in denen die Information selbst noch nicht als schützenswerte Ressource anerkannt wird. Auf sie bezieht sich diese Arbeit.
- Das Verständnis der grundlegenden Begriffe der Informationssicherheit oder ihrer gegenseitigen Ein- bzw. Unterordnung ist in diesen Unternehmungen nicht einheitlich[4], da diese Grundbegriffe in der bestehenden Literatur ebenfalls noch uneinheitlich verwendet werden, und die darauf aufbauenden Verfahren deshalb ebenfalls uneinheitlich sind. Als grundlegende Begriffe werden hier angesehen: *Informationen, Daten, Sicherheit, Informations-sicherheit, Management der Informationssicherheit, Informatik-Sicherheit, IT-Sicherheit, Datensicherheit*.
- Mit dem beginnenden, vom marktwirtschaftlichen Umfeld bestimmten Wandel dieser Unternehmungen hin zur Informationsorientierung, entsteht die Notwendigkeit, die Anforderungen an die verarbeitete Ressource Information zu erkennen und zu formulieren und die Erfüllung dieser Anforderungen zu ermöglichen. Dazu werden in diesen Unternehmungen Projekte der Infor-

---

3 Gemäss [Atteslander92, S. 52] wird in der Problembenennung zunächst eine Theorie formuliert, welche verschiedenen Kriterien genügen muss; unter anderem muss sie empirisch überprüfbar sein. Eine Theorie stellt jedoch nicht unbedingt "*den Anfangspunkt des Forschungsablaufes dar, sondern ist in sich selbst ein Prozess und wird* [...] *durch den Forschungsverlauf selber beeinflusst.*" [ebd., S.44]. Die Problembenennung identifiziert den Entdeckungszusammenhang der Forschung, den Anlass, der zum Forschungsprojekt geführt hat. Friedrichs nennt drei mögliche Anlässe: die *Untersuchung eines sozialen Problems*, ein *Problem der Theoriebildung* oder einen *Auftrag* [vgl. Friedrichs90, S. 50].

4 Das bedeutet, dass keine Teilmenge von mehr als der Hälfte dieser Unternehmungen gebildet werden kann, in welcher dieselben Definitionen dieser Grundbegriffe gelten.

mationssicherheit durchgeführt. Aufgrund des noch nicht vollzogenen Wandels zur Informationsorientierung und aufgrund des uneinheitlichen Verständnisses der Grundbegriffe sind diese Projekte zum Teil unstrukturiert oder erfolglos. Ein Projekt gilt als unstrukturiert, wenn es nicht in Phasen und Aktivitäten mit klaren Zielen, Verantwortlichkeiten und Terminen aufgeteilt ist. Darüber hinaus wird keine Frequenz für die Durchführung der Projekte vorgesehen (einmalige Aktivität) und es wird bei erneuter (nicht aufgrund einer Frequenz durchgeführten) Durchführung eines Projektes eine von der vorherigen Durchführung unterschiedliche Vorgehensweise gewählt. Ein Projekt gilt als erfolglos, wenn es ein Ergebnis erzielt, welches nach Aussage der Mehrheit der davon Betroffenen die Zielsetzung des Projektes nicht erfüllt.

Die dieser Arbeit zugrundeliegende Theorie lässt sich zusammenfassend also wie folgt formulieren:

- In nicht informationsorientierten Unternehmungen wird Informationssicherheit uneinheitlich umgesetzt, da die begrifflichen Grundlagen inkonsistent sind und die bestehenden Verfahren inkonsequent angewendet werden und entsprechende Projekte deshalb zumindest zum Teil erfolglos sind.

Die Erkennung dieses Problems beruht auf Beobachtungen von einzelnen derartigen Situationen durch den Autor, kann jedoch prinzipiell auch empirisch bestätigt (oder widerlegt) werden[5].

In der hier dokumentierten Forschung wird ein Beitrag zur Beseitigung dieses Problems vorgelegt.

Gegenstandsbenennung

Es wird hier folgende Hypothese formuliert[6]:

---

5 Den empirischen Nachweis des Problems zu erbringen, ist schwierig, aber prinzipiell möglich: Dazu müsste (nach geeigneter Auswahl einer genügenden Anzahl von Unternehmungen) die Durchführung von Projekten der Informationssicherheit empirisch begleitet oder die Dokumentation derartiger Durchführungen empirisch ausgewertet werden. Die empirische Begleitung bedingt hohen Aufwand: Projekte der Informationssicherheit erstrecken sich typischerweise über einen Zeitraum mehrerer Wochen bis Monate. Um valide Aussagen generieren zu können, müssten mehrere derartige Projekte parallel beobachtet werden. Die Auswertung von Projektdokumentationen ist schwierig, weil sie in der veröffentlichten, referenzierbaren Literatur kaum zu finden sind. In beiden Fällen müsste eine solche empirische Untersuchung unterschiedliche Ansätze berücksichtigen, welche in den verschiedenen Projekten verwendet werden, da mehrere vorherrschende Meinungen zur Methodik der Durchführung derartiger Projekte besteht. Ausserdem unterliegen die Resultate und zum Teil auch die Vorgehensweisen derartiger Projekte oft einer Vertraulichkeitsanforderung von der durchführenden Unternehmung selbst, was die Beschaffung der Dokumentation und ihre Referenzierung erschwert.

6 "*Die Gegenstandsbenennung ist ein Vorgang, bei dem beobachtbare Erscheinungen, aber auch abstrakte Vorstellungen und Elemente im Zusammenhang, d.h. in eine systematische Ordnung*

- Das in der Problembenennung als Theorie beschriebene Verhalten von Unternehmungen ist eine Folge der Nichtverfügbarkeit eines Rahmenwerks der Informationssicherheit, welches alle relevanten Komponenten der Informationssicherheit definiert und eines Verfahrens, welche diese Komponenten in eine eindeutige Ordnung stellt. Bestünde ein solches Rahmenwerk mit Verfahren, so könnte die Theorie bei denjenigen Unternehmen empirisch falsifiziert werden, die dieses Rahmenwerk anwendeten.

Um die empirische Überprüfbarkeit dieser Hypothese zu erlauben, muss also zunächst ein derartiges Rahmenwerk mit Verfahren geschaffen werden. Dabei muss einerseits Vollständigkeit angestrebt werden ("alle relevanten Komponenten"), andererseits müssen die bestehenden Ansätze (z.B. Grundschutzansatz) in dieses Rahmenwerk integriert werden. Weitere relevante Kriterien müssen hergeleitet und berücksichtigt werden.

Zunächst ist jedoch zu prüfen, in wie weit die schon bestehenden, in der Literatur dokumentierten Verfahren „vollständig“ sind. Dazu wird das Rahmenwerk als Referenz definiert, an welcher diese Vollständigkeit gemessen werden kann. Diese Referenz bildet die Basis für die Erstellung des Verfahrens *ISIWAY* (Kapitel 8).

Als *Betrachtungsobjekt* der Informationssicherheit wird hier das *unternehmerische Informationssystem* und die darin stattfindende *Informationsverarbeitung* ausgewählt, welche „sicher“ zu gestalten sind. Dazu gehört beispielsweise auch die unternehmerische Nutzung von Informationen über Privatpersonen und ihre Tätigkeiten. Private Nutzung von Information sowie alle anderen Aspekte der Informationsverarbeitung, welche im unternehmerischen Kontext nicht relevant sind, werden hier nicht näher betrachtet.

Durchführung

Die Durchführung[7] der in dieser Dissertation dokumentierten Untersuchung der Hypothese geschah durch teilnehmende Beobachtung an den Projekten der Informationssicherheit in einem Teilbereich eines international tätigen Konzerns und durch gezielte, kontrollierte Beeinflussung dieser Projekte. Der Ablauf dieser

---

gebracht werden sollen." [Atteslander92, S. 59]. Dazu werden Klassifikationen entworfen und Begriffe definiert. Schliesslich wird eine Hypothese formuliert, welche eine Aussage über eine "Wenn-Dann"-Beziehung zwischen zwei "semantisch gehaltvollen Begriffen" enthält [ebd., S. 62]. "*Hypothesen beziehen sich dabei nicht unbedingt auf einzelne Fragen, sondern auf ganze Fragenkomplexe*". [ebd., S. 64]. Die Hypothese soll empirisch überprüfbar sein.

7 In der Durchführung werden die Hypothesen überprüft. Die Art und Weise des Einsatzes der dabei verwendeten Forschungsinstrumente wird als Forschungsdesign bezeichnet. Ein möglicher Forschungstypus ist die *Aktionsforschung*, bei welcher " *der Forscher nicht nur einen Teil des Untersuchungsgegenstandes dar[stellt], sondern [...] ganz bewusst und kontrolliert diesen Gegenstand im Verlauf der Forschung zu verändern [sucht].*" [Atteslander92, S. 77].

Projekte wurde spezifiziert und auf dem hier definierten Rahmenwerk aufgebaut. Im konkreten Fall war der Autor als interimistischer Beauftragter für Informationssicherheit des Konzerns tätig. Er nahm damit einerseits eine der in dieser Dissertation definierten Rollen wahr, andererseits wurden die Definitionen von Rahmenwerk und Verfahren im Laufe dieser Projektmitarbeit verfeinert.

Als Forschungsmethoden wurden eine teilnehmende Beobachtung und eine strukturierte Befragung vorbereitet. Die Untersuchung wurde Ende 1997 und Mitte 1998 in zwei weitgehend voneinander unabhängigen Organisationseinheiten des Konzerns begonnen und war auf sechs zu untersuchende Einheiten (Teiluntersuchungen) ausgelegt. Als Dauer wurde ein halbes Jahr vorgesehen. Dazu wurde eine zusätzliche, reduzierte Version des definierten Verfahrens erstellt (vgl. Kapitel 10.4).

Analyse

Die empirische Untersuchung, die als Teil der Durchführung vorgesehen war, konnte nicht abgeschlossen werden. Die Erkenntnis der Konzernleitung, dass die mit dem "Jahr-2000-Problem" verbundenen Risiken zu massiven Störungen der unternehmerischen Leistungserbringung führen könnten, resultierte in einer anderen Vergabe der für die empirische Untersuchung vorgesehenen und notwendigen Ressourcen. Die beiden angefangenen Teiluntersuchungen konnten bis zu ihrem Abbruch keine verwendbaren Ergebnisse produzieren, so dass keine empirischen Daten zur Verifikation der Hypothese gewonnen werden konnten. Die Auswahl eines anderen Projektpartners für die empirische Untersuchung wurde fallengelassen, da auch bei anderen Unternehmungen ähnliche Prioritäten vermutet wurden.

Verwendung von Ergebnissen

Trotz des Abbruchs der empirischen Untersuchung ist es möglich, über die durchgeführten Teile der Untersuchungen zu berichten und Aussagen über den Wahrheitsgehalt der Hypothese zu postulieren. Die erarbeiteten Teilergebnisse und die für die Untersuchung zur Verfügung gestellten Hilfsmittel (insbesondere das Werkzeug *ISIGO*) stehen auch für andere Anwendungsumgebungen zur Verfügung.

Beitrag

Der wissenschaftliche Beitrag dieser Dissertation besteht aus einem *Rahmenwerk der Informationssicherheit*, einer strukturierten *Evaluation bestehender Verfahren*, dem *normativen Entwurf eines neuen Verfahrens* und der Implementation eines *Werkzeugs* als Demonstrator der elektronischen Unterstützbarkeit des Verfahrens.

- *Rahmenwerk der Informationssicherheit*

Das Rahmenwerk integriert Konzepte der unternehmerischen Führung, des Informationsmanagements und der Informatik-Sicherheit, um das unternehmerische Management der Informationssicherheit umfassend als Führungsaufgabe zu definieren. Die Unterteilung des Rahmenwerks in Institutionen, Informationen, Instrumente und Prozesse entspricht Erkenntnissen aus dem Zürcher Managementansatzes nach Rühli [vgl. Rühli85, Rühli88, Rühli93a] und dem Informationsmanagement nach Heinrich [vgl. Heinrich 93 und Heinrich95]. Die Umsetzung von Informationssicherheit wird als Projekt organisiert. Das Verständnis von Controlling und Revision als Teil der Führungsaufgabe wurde erweitert und in das Rahmenwerk und die Projektorganisation eingebunden. Der wissenschaftliche Beitrag besteht in der auf die Zielsetzung „Informationssicherheit" ausgerichteten Integration dieser Konzepte und der damit erfolgten theoretischen Grundlegung des Managements der Informationssicherheit.

- *Evaluation bestehender Verfahren*

  Mehrere gebräuchliche Verfahren zum Management von Informationssicherheit wurden evaluiert, indem für jedes Verfahren die Berücksichtigung der einzelnen Elemente des Rahmenwerkes geprüft wurden. Es konnte gezeigt werden, dass jedes der betrachteten Verfahren das Rahmenwerk nur unvollständig berücksichtigt. In einer vergleichenden Bewertung und Beurteilung wurde weiterhin festgestellt, welche Stärken und Schwächen die einzelnen Verfahren aufweisen. Dieser Vergleich dient zur Definition eines *Anforderungsprofils* an ein idealisiertes Verfahren, welches alle Elemente des Rahmenwerks umfassen und einige weitere Anforderungen erfüllen soll. Das Rahmenwerk wurde hier also als *Zertifizierungsschema* für Informationssicherheitsverfahren verwendet An diesem Profil könnten auch Verfahren gemessen werden, die hier nicht berücksichtigt wurden, um so ihre Vollständigkeit bzgl. des definierten Rahmenwerks zu bestimmen.

- *Verfahren ISIWAY*

  Dem *Anforderungsprofil* entsprechend wurde ein neues Verfahren *ISIWAY 4* [8] mit vier Zyklen definiert und detailliert dokumentiert. Die Erfüllung der einzelnen Anforderungen wurde separat beurteilt und mit den Evaluationen der anderen Verfahren verglichen. Zur besonderen Berücksichtigung der Anforderung „einfache Erlernbarkeit" wurde zusätzlich ein reduziertes Verfahren *ISIWAY 1.5* erstellt, welches sich auf prioritäre Inhalte der Informationssicherheit beschränkt. Es kann als Vorbereitung für das ausführliche Verfahren gelten. Es konnte gezeigt werden, dass die Definition

---

8 Im gesamten Text steht die Bezeichnung *ISIWAY* für das zyklisch aufgebaute Verfahren, welches in dieser Dissertation beschrieben wird. *ISIWAY 4* stellt die erste Konkretisierung mit vier Zyklen dar, *ISIWAY 1.5* bezeichnet die zweite Konkretisierung mit einem Zyklus und Zusätzen. Falls im Text nur auf *ISIWAY* verwiesen wird, ist damit i.d.R. *ISIWAY 4* gemeint.

von anforderungsgerechten und gemäss Rahmenwerk vollständigen Verfahren möglich ist.

- *Werkzeug ISIGO*

  Als Demonstrator zur elektronischen Unterstützung des Verfahrens *ISIWAY* wurde das Datenmodell des Verfahrens *ISIWAY* als relationales Modell definiert und ein darauf zugeschnittenes Werkzeug *ISIGO* auf Basis eines Tabellenkalkulationsprogramms implementiert und für den praktischen Einsatz vorbereitet. Auf diese Weise wurde die Definition des Verfahrens um einen Prototypen zur Computer-Aided Information Security (CAIS) erweitert.

1.2 Terminologie

Diese Dissertation basiert begrifflich auf zwei verschiedenen anerkannten und gut dokumentierten Ansätzen:

- dem von Rühli entwickelten *Zürcher Management-Ansatz* [Rühli85] und
- der *Grundlegung des Informationsmanagements und der Wirtschafts-informatik* von Heinrich [Heinrich93].

Beide Ansätze werden im Verlauf des Textes noch genauer beschrieben und hier in erster Linie zur Strukturierung und zur Bestimmung der Terminologie verwendet. Da beide jedoch unabhängig voneinander eine Strukturierung der unternehmerischen Tätigkeiten vornehmen – Ersterer mit Fokus auf die Strukturen und Abläufe der Führung, Letzterer mit Fokus auf die computergestützte Informationsverarbeitung – führt dies dazu, dass die Terminologie zunächst uneinheitlich ist, obwohl die beiden genannten Autoren jeweils eine in sich geschlossene Begriffsbasis verwenden. Die Lösung dieses Terminologieproblems liegt in der Entwicklung einer eigenen Terminologie, deren einzelne Begriffe möglichst weit auf Begriffen der beiden Ansätze basieren. Dazu werden die Schlüsselbegriffe hier kurz zusammengefasst und geordnet.

Zürcher Management-Ansatz

Wie in Abschnitt 2.6 ausgeführt wird (vgl. linker Teil von Abbildung 1-1 (Seite 11) sowie Abbildung 2-6 (Seite 49) und Abbildung 2-8 (Seite 53)), kann Führung *formell* und *inhaltlich* betrachtet werden.

- Auf der *formellen* Seite werden *Führungstechnik* und *Menschenführung* behandelt.
  - Die *Führungstechnik* umfasst die *Phasen Planung, Entscheidung, Anordnung* und *Kontrolle* als konstitutive Elemente der Problemlösung, und die *Aspekte* der dazu notwendigen *Institutionen, Funktionen* und *Instrumente* innerhalb der Unternehmung.

Unter *Institutionen* versteht Rühli die Anordnung von Stellen, Gremien und anderen mit Personen besetzten Einheiten, denen die Führung obliegt. *Funktionen* stellen für ihn die Bearbeitung der unternehmerischen Inhalte dar. Dazu werden *Instrumente* verwendet, welche einerseits technische und abstrakte Werkzeuge umfassen (z.B. Computer, Sitzungen, Publikationen), andererseits auch Inhalte beschreiben können (z.B. eine Personalpolitik als Instrument zur Beeinflussung der Unternehmungskultur).

  - Die *Menschenführung* umfasst Betrachtungen der Verhaltensweisen von Personen als aktive Individuen innerhalb und ausserhalb der Unternehmung (*individuelles Verhalten*) sowie Betrachtungen von kollektivem Verhalten und die Übertragung dieses Verhaltens zwischen Personen in *dualistischen* und *gruppenorientierten* Beziehungen (sog. *Kultur*).

- Auf der *inhaltlichen* Seite werden allgemeine und situative Aufgaben mit Innen- und Aussenvertretung der Unternehmung betrachtet, wobei Grundlagen, Ziele, Strategien (Massnahmen) und Werkzeuge (Mittel, Potentiale) zur Funktionsweise der Unternehmung (Innenverhältnis) und zur Teilnahme der Unternehmung in ihrer Umwelt (Aussenverhältnis) betrachtet werden.

Grundlegung von Heinrich

Heinrich betrachtet das Informationssystem und unterteilt es in *Mensch*, *Technik, Aufgaben* und *Beziehungen zwischen diesen drei Komponenten*. Dabei stellt er das Informationssystem ins Zentrum der unternehmerischen Tätigkeiten unter der Annahme, dass keine moderne Unternehmung ohne ein solches Informationssystem überlebensfähig wäre und dass das Informationssystem das zentrale Element aller unternehmerischen Tätigkeiten bildet. *Technik* ist bei ihm identisch mit *Informations- und Kommunikationstechnik* vgl. rechter Teil von Abbildung 1-1).

Verknüpfung der Ansätze

Beide Ansätze nehmen eine Strukturierung der Unternehmung und der darin stattfindenden Abläufe vor. Hier wird folgende Verknüpfung der einzelnen Komponenten und Aspekte vorgeschlagen (vgl. Abbildung 1-1):

- Die *Menschen* aus Heinrichs Kontext lassen sich vereinfacht mit Rühlis *Institutionen* gleichsetzen, da jede Institution durch eine oder mehrere Personen (Menschen) repräsentiert wird, sowie mit Rühlis *Menschenführung*.
- Heinrichs *Technik* kann mit den technischen *Instrumenten* von Rühli gleichgesetzt werden.
- Heinrichs *Aufgaben* werden bei Rühli in der *inhaltlichen Betrachtung* und teilweise über die nicht-technischen *Instrumente* behandelt.

- Die eigentliche Verarbeitung der Inhalte, welche bei Rühli in den *Funktionen* festgelegt ist und durch den *Führungsprozess* gesteuert wird, ordnet Heinrich als *Beziehungen* zwischen den drei Komponenten Mensch, Technik und Aufgaben ein.

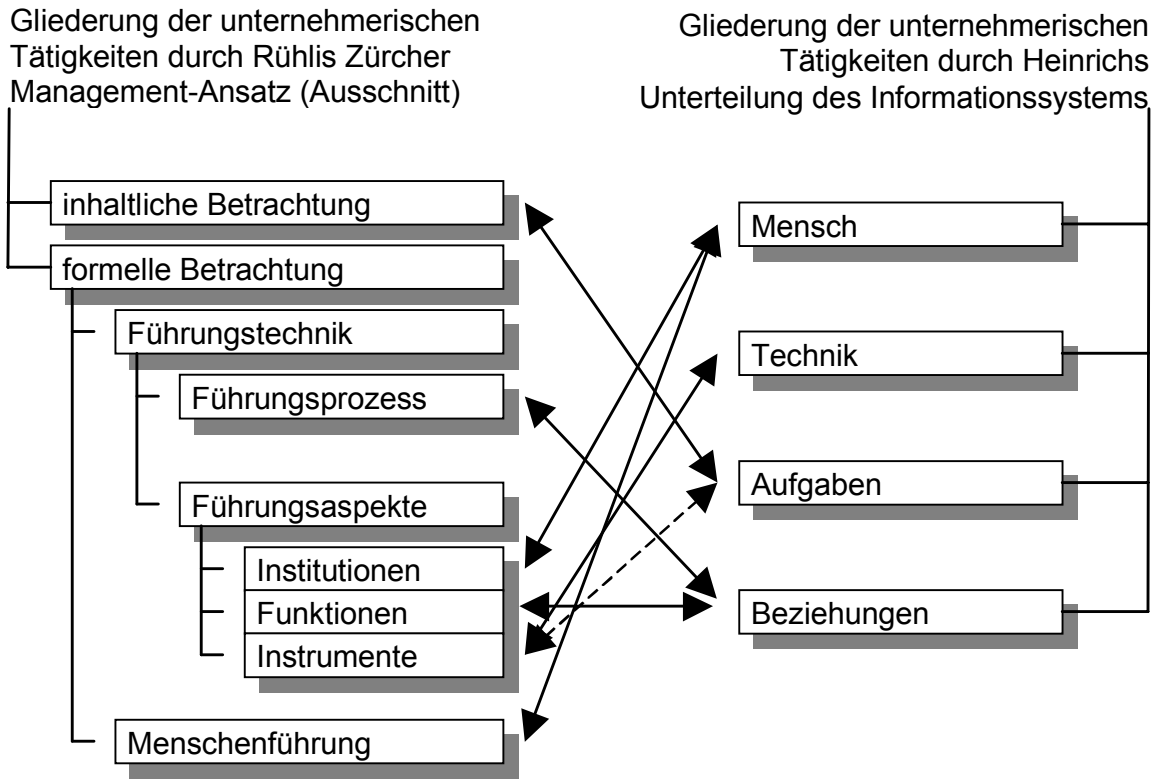


Abbildung 1-1: Beziehungen zwischen Rühlis und Heinrichs Terminologie

Es kann hier also eine vollständige, wenngleich nicht eindeutige Zuordnung zwischen den Begriffen der beiden Terminologien hergestellt werden. Hier wird dies nur aufgezählt, um die Terminologieprobleme zu verdeutlichen. Es dient hier dazu, ein eigenes Begriffssystem festzulegen, welches zur Strukturierung dieser Arbeit verwendet wird.

Begriffsverständnis und Terminologie

Es soll im folgenden davon ausgegangen werden, dass bei der Betrachtung einer Unternehmung und der Unternehmungsführung prinzipiell eine *formelle* und eine *inhaltliche* Betrachtung möglich ist.

- Bei der formellen Betrachtung soll unterschieden werden zwischen *Institutionen, Informationen, Instrumenten (statische Betrachtung)* und *Prozessen (dynamische Betrachtung).* Gemeinsam werden sie als statische und dynamische *Elemente* der Unternehmung bezeichnet.
  - Unter *Institutionen* werden alle Stellen und Gremien verstanden, welche gesamthaft die Aufbau*struktur* der Unternehmung ausmachen und durch

Personen (Menschen) besetzt sind. Institutionen zeichnen sich durch Aufgaben, Kompetenzen und Verantwortungen aus, welche beispielsweise in einer Stellen- oder Rollenbeschreibung festgehalten werden können und jeweils *Rollen* definieren. Die Begriffe *Institutionen, Instanzen, Aufbauorganisation* und *Struktur der Unternehmung* werden in der Folge weitgehend synonym verwendet und es wird immer davon ausgegangen, dass damit die Rollen von *Personen* bezeichnet werden.

- Die *Informationen* umfassen in der formellen Betrachtung all diejenigen Formen, welche für die Kommunikation der Inhalte verwendet werden. Im informationstechnologischen Kontext stellen Informationen die Inhalte dar (Wissen, Informationsverwendung) und umfassen *Aufgaben* und *Ziele*, während Daten und Nachrichten die *Formen der Kommunikation* dieser Informationen sind. Die formelle Betrachtung der Inhalte wird unter anderem benötigt, um technische Anforderungen an Informationen (Daten) festlegen zu können, z.B. Integritätsforderungen.
- *Instrumente* umfassen alle konkreten Hilfsmittel, welche die Institutionen bei ihren Tätigkeiten verwenden. Dazu gehören digitale und nicht-digitale Werkzeuge zur Informationsverarbeitung, aber auch abstrakte Instrumente wie Sitzungen und Gespräche. *Instrument* wird synonym zu *Werkzeug* und *Hilfsmittel* verwendet. Inhaltlich definierte Werkzeuge wie beispielsweise eine Informationssicherheitspolitik werden allerdings der inhaltlichen Betrachtung zugeordnet.
- *Prozesse* verbinden die Bearbeitung von *Informationen* durch *Institutionen* mit Hilfe von *Instrumenten.* Ein Prozess umfasst also die *Funktion* der Umwandlung einer Ein- in eine Ausgabe und soll in der hier zu verwendenden Bedeutung ausserdem in Phasen unterteilbar sein. Diese Phasen umfassen verschiedene Aktivitäten, die in einem *Ablauf* untereinander stehen und einzelnen Institutionen (Rollen) innerhalb des Prozesses zugeordnet werden können. Der Prozess ist das dynamische Element und beschreibt die Abfolge der Tätigkeiten, nicht jedoch deren Inhalte.

- Auf der inhaltlichen Seite werden Grundlagen, Ziele, Strategien (Massnahmen) und Werkzeuge (Mittel, Potentiale) zur Aufgabenbearbeitung der Unternehmung betrachtet. Die Aufgabenbearbeitung in einzelne inhaltliche Fachbereiche aufgeteilt. Gesamthaft werden die Inhalte deshalb hier als *Tätigkeiten* der Unternehmungsführung bezeichnet.

Alle nachfolgenden Betrachtungen werden also in formelle und inhaltliche Betrachtungen unterteilt. Formell wird zwischen Institutionen, Informationen, Instrumenten und Prozessen unterschieden (vgl. Abbildung 1-2).

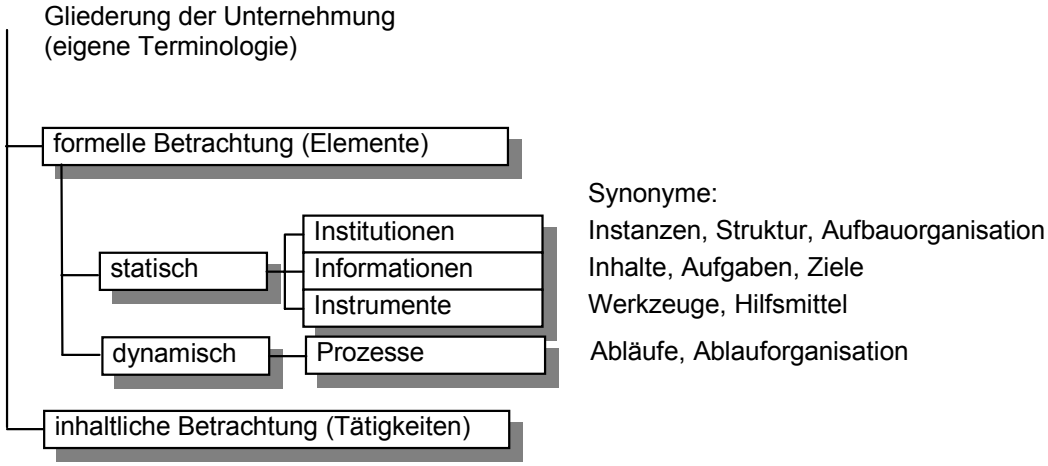


Abbildung 1-2: Terminologie zur Strukturierung dieser Dissertation

1.3 Methodik

Gliederung dieser Dissertation

Diese Dissertation ist folgendermassen aufgebaut (vgl. Abbildung 1-3):

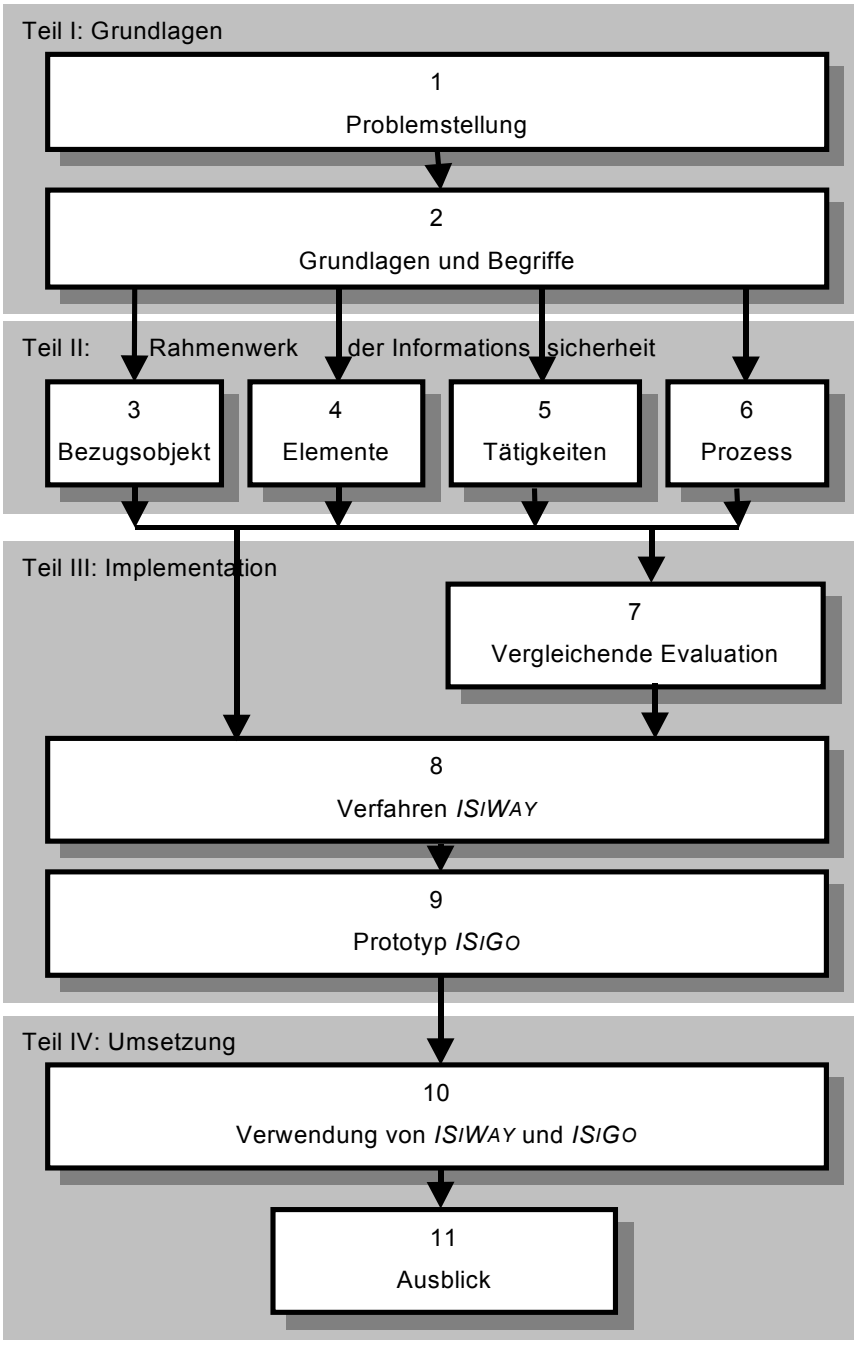


Abbildung 1-3: Gliederung dieser Dissertation

Teil I: Konzeption

In diesem ersten Teil werden zunächst Ausgangslage und Problemstellung, Ziel, Beitrag und Vorgehensweise dieser Dissertation in einer Einleitung erläutert und in einem Überblick dargestellt (**Kapitel 1**).

Daran anschliessend wird in den Kapiteln 2 bis 6 die Definition des *Rahmenwerks der Informationssicherheit* wiedergegeben. Dies beginnt mit der Beschreibung der Grundlagen und der Festlegung der Begriffe.

Bei der wissenschaftlichen Betrachtung der Informationssicherheit fällt die Vielfalt an Begriffen auf, welche in Theorie und Praxis verwendet werden. Sie stehen in verschiedenartigem Bezug zueinander und die Begriffsbasis ist nicht einheitlich. Als eine der Voraussetzungen für diesen Text muss eine einheitliche Begriffsbasis im Bereich Informationssicherheit geschaffen werden. Ausserdem muss das Verständnis der Informationssicherheit derart erweitert werden, dass dieser Begriff alle notwendigen Aspekte des unternehmerischen Umfeldes abdeckt.

Die in **Kapitel 2** beschriebenen *Grundlagen und Begriffe* (vgl. Abbildung 1-4) umfassen die Definition der Grundbegriffe der Informationssicherheit, darunter vor allem die Schlüsselbegriffe *Information, Sicherheit* und ihre Kombination zur *Informationssicherheit*, die *Ziele und die Motivation* der Informationssicherheit, die *Grundanforderungen* sowie eine Erklärung der *Führungskonzeption* nach Rühli.

Information wird als Oberbegriff für die voneinander verschiedenen Konzepte *Daten*, *Wissen, Nachrichten* und *Informationsverwendung* definiert. Es wird festgelegt, dass Informationssicherheit sich auf alle vier Konzepte zu beziehen hat,

Sicherheit wird als subjektiv wahrgenommener Zustand eines Objektes dargestellt und festgestellt, dass die Sicherheit eines Objektes sich umgekehrt proportional zum Risiko verhält, welchem dieses Objekt unterliegt. Der Begriff Risiko wird dabei unter verschiedenen Aspekten betrachtet (Gefahr, Bedrohung, Gefährdung, Wahrscheinlichkeit, Schaden), die hier erklärt und in einen eindeutigen Zusammenhang gestellt werden, und welche hier weiter typisiert werden.

Sicherheit im unternehmerischen Umfeld wird als *Ziel* definiert, welches anderen unternehmerischen Zielen untergeordnet wird und dessen Erreichung Aufgabe des Sicherheitsmanagements ist. Dazu wird ein abstraktes Sicherheitsniveau festgelegt.

Informationssicherheit soll als Anforderung an Informationen verstanden und in verschiedene einzelne *Grundanforderungen* unterteilt werden, welche in technische (Verfügbarkeit, Interne Integrität, Verfügbarkeit), ökonomische (Effektivität, Effizienz, Zuverlässigkeit, beabsichtigte Verwendung) und soziale Ebenen (Ordnungsmässigkeit, Verbindlichkeit, Externe Integrität) eingeteilt werden können.

Abschliessend wird der von Rühli entwickelte Zürcher Management-Ansatz mit der darin definierten *Führungskonzeption* vorgestellt und erklärt. Dies dient als Grundlage für die Strukturierung der Informationssicherheit als Führungsaufgabe.

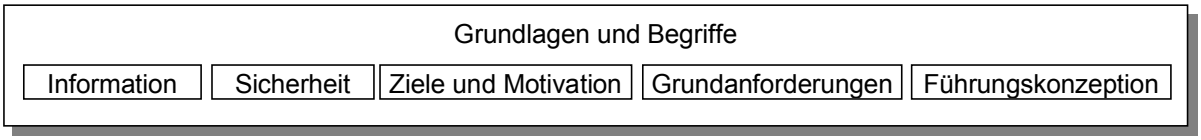


Abbildung 1-4: Grundlagen und Begriffe

Teil II: Rahmenwerk der Informationssicherheit

Das Rahmenwerk der Informationssicherheit basiert auf dem Stand der Forschung in diesem Bereich und verwendet die in Abschnitt 1.2 eingeführte Terminologie und Strukturierung. Für die Erarbeitung dieses Rahmenwerks und später für den Entwurf eines Verfahrens wird die Informationssicherheit als *Führungsaufgabe* betrachtet.

Das Rahmenwerk geht über die Beschreibung des Stands der Forschung hinaus: Es beschreibt das bestehende Wissen nicht nur, sondern ordnet es und stellt es in einen gesamtheitlichen Zusammenhang.

Dazu unterteilt das Rahmenwerk (vgl. Abbildung 1-5) Informationssicherheit in *Grundlagen und Begriffe* (Kapitel 2), *statische* (**Kapitel 3 bis 5**) und *dynamische Betrachtung* (Kapitel 6)[9]. Die statische Betrachtung umfasst die *Elemente* und *Tätigkeiten* der Informationssicherheit. Sie wird weiter unterteilt in eine *formelle Betrachtung* (Kapitel 3), in welcher die Institutionen, Informationen und Instrumente der Informationssicherheit behandelt werden, und in eine *inhaltliche Betrachtung* (Kapitel 4 und 5), welche die Ziele, Aufgaben und Fachgebiete der Informationssicherheit abdeckt. Die dynamische Betrachtung in Kapitel 6 umfasst die generische Definition des Informationssicherheitsprozesses und bildet die Grundlage für dessen spezifische Betrachtung in Teil III dieser Dissertation.

[9] Die Grundlagen werden hier als notwendige Voraussetzung für das Rahmenwerk betrachtet und können deshalb als Bestandteil des Rahmenwerks gesehen werden.

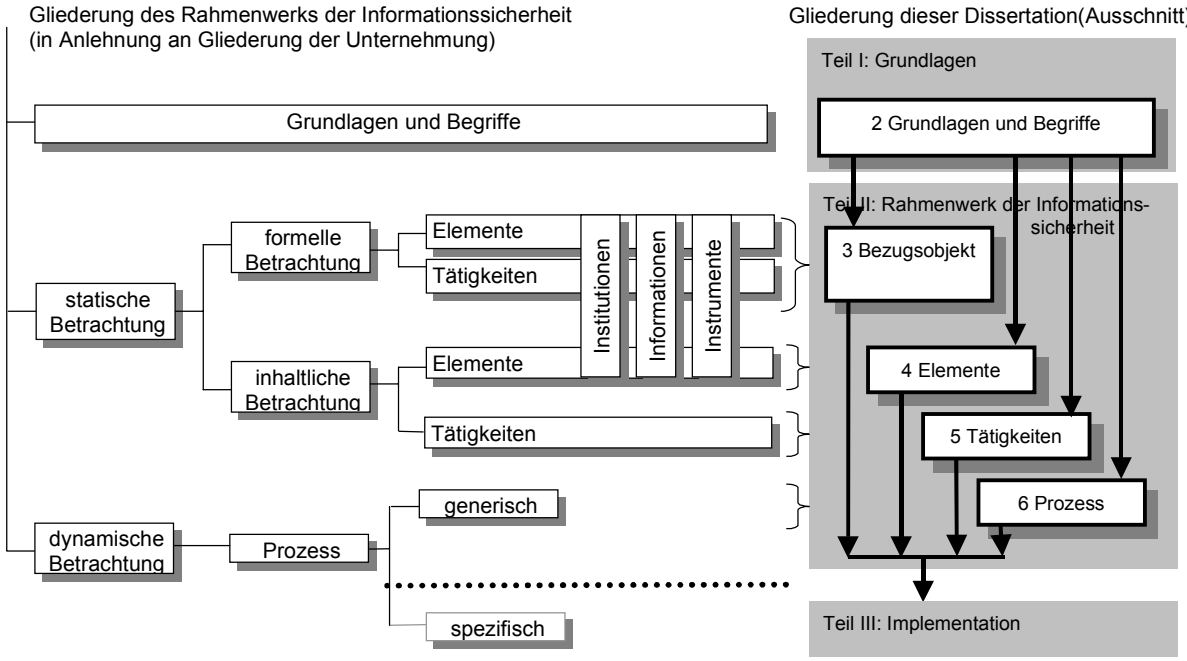


Abbildung 1-5: Gliederung des Rahmenwerks der Informationssicherheit und dieser Dissertation

Das Rahmenwerk der Informationssicherheit wird in Teil II detailliert beschrieben. Ein Überblick findet sich zu Beginn von Teil II in Abschnitt 3.1.

Teil III: Implementation

Teil III beinhaltet die Definition eines eigenen Verfahrens (*ISiWAY*) und eines dazu passenden Werkzeugs.

Dazu werden in **Kapitel 7** zunächst die *bestehenden* und verbreiteten *Verfahren* zur Erreichung unternehmerischer Informationssicherheit identifiziert und kurz beschrieben. Ein Bewertungsschema wird entwickelt, mit welchem die bestehenden Verfahren dann bewertet und miteinander verglichen werden. Daraus werden Anforderungen an das hier zu definierende Verfahren hergeleitet, wodurch auch eine Beurteilung der untersuchten Verfahren entsteht.

In **Kapitel 8** wird das Verfahren *ISiWAY* auf Basis der hergeleiteten Anforderungen definiert. Dabei werden die vorher identifizierten Grundlagen, Informationen, Instrumente, Institutionen und generischen Prozesse berücksichtigt. Das *neue Verfahren* zur Erreichung von Informationssicherheit besteht aus einem zyklischen Vorgehen mit vier Zyklen und einer von Zyklus zu Zyklus zunehmenden Betrachtungstiefe. Die Strukturierung des Verfahrens geschieht wieder mit Hilfe der oben vorgestellten Unterteilung. Diese Erstellung eines eigenen Vorschlages wird hier als *erste Konkretisierung* bezeichnet.

Die in Kapitel 7 hergeleiteten Anforderungen waren Ziele bei der Entwicklung von *ISiWAY*. Vorrangige Ziele waren

- die Integration der bestehenden Ansätze der Informationssicherheit,

- Einfachheit des Verfahrens, so dass es auch durch Personen angewendet werden kann, welche sich nicht primär mit Informationssicherheit beschäftigen. Dies bedingt die Erstellung konkreter, in spezifischer Reihenfolge stehender Handlungsanweisungen für die durchführenden Personen sowie die Definition eines Rollenmodells (Definition von Institutionen der Informationssicherheit), denen die Durchführung obliegt,
- die konkrete Festlegung von Datenstrukturen für die Verwaltung der bei der Durchführung anfallenden Informationen über das betrachtete Bezugsobjekt,
- die Skalierbarkeit zur möglichst flexiblen Anpassung von Verfahrensbreite und -tiefe an die konkreten Anforderungen der Unternehmung,
- die Unterstützung von Kommunikation, Koordination und Kooperation zur Ermöglichung gemeinsamer, verteilter Erarbeitung der Informationssicherheit und Erreichung von Vergleichbarkeit.

Das Verfahren *ISIWAY* umfasst den Informationssicherheitsprozess vollständig. Dazu definiert es vier Detaillierungsgrade (DG 1 bis 4), welche die verschiedenen Ansätze der Analysephase des Ablaufs repräsentieren und zyklisch angeordnet sind. Zusätzlich wird ein Vorbereitungszyklus (DG 0) definiert sowie ein Zyklus für das Krisenmanagement (DG 3.5). Jeder der Zyklen wird im Detail beschrieben, wobei konkrete Handlungsanweisungen für die durchführenden Institutionen abgegeben werden.

Eine der identifizierten Schwächen der bestehenden Verfahren ist die fehlende Unterstützung durch ein jeweils darauf zugeschnittenes internes Instrument (computergestütztes Hilfsmittel). Ein solches Werkzeug wurde hier entwickelt und zur einfachen Erlernbarkeit und guten Portierbarkeit auf dem Tabellenkalkulationssystem *EXCEL* von *MICROSOFT* aufgebaut. Es unterstützt die einzelnen Detaillierungsgrade von *ISIWAY* und wird *ISIGO* genannt. Die Implementation konzentriert sich auf die Anforderungen der zweiten Konkretisierung.

Kapitel 9 enthält die Spezifikation und Entwicklung des Prototypen *ISIGO*, welcher den in Kapitel 8 definierten Prozess unterstützt und einfach handhabbar macht. Dieser wird speziell für den Einsatz mit der in Kapitel 10 entwickelten reduzierten Version von *ISIWAY (ISIWAY 1.5)* entwickelt.

Teil IV: Anwendung

In **Kapitel 10** wird schliesslich theoretisch betrachtet, wie die Anwendung von *ISIWAY* in einer konkreten Situation aussehen könnte. Dazu wird das Verfahren zunächst auf einen geringeren Umfang reduziert, indem ein Subset der Aufgaben gebildet wird, dessen Beschreibung wiedergegeben wird. Dies wird als *zweite Konkretisierung* bezeichnet. Sie zeichnet sich durch eine Vereinfachung aus, welche vor allem für das erstmalige Durchlaufen des Verfahrens *ISIWAY* gedacht ist. Dazu wurde das Verfahren weiter integriert, so dass nur *ein* Zyklus (DG 1.5) verbleibt,

welcher Aktivitäten der DGs 0 (Vorbereitungen), 1 (Grundschutz) und 2 (Wertekonzept) vereint. Dies stellt gleichzeitig eine einfache Ausgangsbasis für die Untersuchung der Anwendbarkeit des Verfahrens dar. *ISiWAY 1.5* kann vollkommen unabhängig vom vollständigen *ISiWAY*-Verfahren eingesetzt werden, weist allerdings Schnittstellen für einen einfachen Wechsel auf. Das Werkzeug *ISiGO* unterstützt beide Verfahren und erzeugt dadurch eine einheitliche Schnittstelle für die Datenerfassung und -weitergabe.

Die Anwendung dieses reduzierten Verfahrens wird sodann auf einen konkreten Bereich einer Unternehmung bezogen, welcher detailliert beschrieben wird. Das Vorgehen und die dabei zu erwartenden Probleme werden geschildert und Lösungen vorgeschlagen. Das Verfahren wird also auf den angestrebten Einsatzbereich projiziert. Zusätzlich werden die Rahmenbedingungen für eine empirische Studie definiert und erklärt, warum die Durchführung einer derartigen Studie im Rahmen dieser Dissertation nicht möglich war.

Abschliessend werden in **Kapitel 11** die Informationssicherheit, das Verfahren *ISiWAY* und seine Anwendung nochmals kritisch gewürdigt. Es wird ein Rückblick auf die geleistete Arbeit, eine Einschätzung des Beitrags für die Praxis und ein Ausblick auf mögliche Erweiterungen des Ansatzes, notwendige Ergänzungen und Anpassungen abgegeben. Ausserdem wird versucht, den Einfluss zukünftiger Entwicklungen abzuschätzen.

Anhänge

Die Anhänge enthalten einen Exkurs, Tabellen zur vergleichenden Evaluation von Kapitel 7, Detailbeschreibungen zu *ISiWAY*, die Dokumentation zu *ISiWAY* 1.5, Abbildungen und Erklärungen zum Datenmodell von *ISiGO*, SQL-Selektionsbefehle zur Verknüpfung von *ISiGO 1.5* und *ISiGO CENTRAL,* ein Glossar, das Literaturverzeichnis, Beispiele für Tabellen und Module von *ISiGO 1.5* mit Kurzbeschreibung sowie den Lebenslauf des Autors.

1.4 Lesehinweise

Es besteht vor allem *ein* Lesepfad, der sequentiell durch die Dissertation führt. Dennoch wurden die Teile und Kapitel so zusammengestellt, dass auch eine jeweils separate Lektüre möglich ist.

- Abschnitt 3.1 enthält die komplette Beschreibung des Rahmenwerks der Informationssicherheit, so dass praxisorientierte Leser den Rest des eher theoretischen Teils II überspringen können.
- Leser, die an den Grundlagen der Informationssicherheit und an dem darauf aufbauenden Rahmenwerk interessiert sind, können ihre Lektüre auf Teil I und II der Dissertation beschränken.

- Wer nur an den bestehenden Verfahren und ihrer Beurteilung interessiert ist, kann die Lektüre auf Kapitel 7 beschränken.
- Das Verfahren *ISIWAY 1.5* kann losgelöst von dieser Dissertation betrachtet und verwendet werden, da es als vollkommen eigenständiges Verfahren formuliert wurde (wiedergegeben in Anhang C.2). Im Verbund mit dem Werkzeug *ISIGO 1.5* stehen die wichtigsten Hilfsmittel bereit, um das Management der Informationssicherheit in einer Unternehmung zu beginnen.

2 Grundlagen und Begriffe

In diesem Kapitel werden zunächst die begrifflichen Grundlagen bereitgestellt, indem grundlegende Konzepte wie *Information*, *Sicherheit* und *Management* erklärt werden. Es werden vier Ausprägungen von *Information* unterschieden: *Wissen*, *Daten*, *Nachrichten* und *Informationsverwendung*. Darauf aufbauend werden *Informationssammlungen* und *Dokumente* als gebräuchliche unternehmerische Informationseinheiten identifiziert. *Sicherheit* und *Risiko* werden allgemein definiert und in die einzelnen Komponenten *Gefahr, Bedrohung, Schwachstelle* etc. unterteilt. Die verschiedenen *Grundbedrohungen* werden identifiziert. Weiterhin wird eine allgemeine Klassifikation von Bedrohungen vorgenommen. Darauf aufbauend wird *Informationssicherheit* als unternehmerisches Ziel beschrieben. Abschliessend wird die von Rühli entwickelte *Führungskonzeption* gemäss Zürcher Führungsansatz vorgestellt.

2.1 Informationsbegriffe

Information

Information dient als Oberbegriff für alle Erscheinungsformen von Wissen. Informationswissenschaftlich besteht für *Information (im weiteren Sinne)* eine anerkannte Definition [Kuhlen89, Kuhlen95], welche die vier Komponenten *Daten*, *Wissen*, *Nachricht* und *Information (im engeren Sinne)* beschreibt. Es wird in der Herleitung dieser Definition davon ausgegangen, dass jegliches vorhandenes Wissen sich mit Hilfe von Abbildungsprozessen (Aufzeichnung etc.) als Daten darstellen lässt und durch Anwendung weiteren Wissens wieder von Daten zu Wissen reformieren lässt (Interpretation). Nur die *Verwendung* dieses Wissens durch eine Person macht daraus Information (oder gemäss Kuhlen: *„Information ist Wissen in Aktion"*) [Kuhlen95, S. 34][10]. Zur Übermittlung von Wissen von einer Person zu einer anderen werden Nachrichten verwendet, welche allerdings eine Abbildung in Daten voraussetzen, die der Übermittlungsart angemessen ist. Der Begriff Information wird im allgemeinen als Oberbegriff für diese vier Aspekte verwendet. Im Folgenden wird diese weite Bedeutung verwendet.

> *Def.:* Wissen *umfasst den Bestand an Kenntnissen in einem bestimmten Sachgebiet.*

---

10 Dies impliziert, dass Informationsverarbeitung ohne menschliche Beteiligung nicht möglich ist. Datenverarbeitung hingegen ist nicht auf menschliche Interaktion angewiesen.

Wissen ist abhängig von der Interpretation durch ein Individuum. Es wird Sachwissen, konzeptionelles Wissen und Metawissen unterschieden. Von "Wissen" besteht im deutschen keine Mehrzahl. Englische Entsprechungen: *knowledge*, *know-how*.

> *Def.:* Information (i.e.S.) *ist die Verwendung von Wissen für einen speziellen Zweck, für ein sich dem Individuum stellendes Problem.*

Die Einzahl von "Information" wird normalerweise synonym zur Mehrzahl "*Informationen"* benutzt, weil die kleinstmögliche "atomare" Informationseinheit (das *Bit*) bei der Verarbeitung durch bzw. bei der Kommunikation zwischen Personen selten identifiziert werden kann. Engl. Entsprechung: *information* (nur Einzahl, Mehrzahl *informations* nicht gebräuchlich).

> *Def.:* Daten *sind die Repräsentation von Wissen mit Zeichen aus einem Zeichensatz.*

Daten werden auf Medien gespeichert und / oder übertragen, indem sie physische Phänomene von Medien benutzen, um die Zeichen abzubilden. Die Zeichen gehören einer Sprache an, auf welche sich die Kommunikationspartner geeinigt haben. Daten können auf den Medien Zeit und Raum überwinden.

Die Einzahl von "Daten" wird im deutschen Sprachgebrauch nicht verwendet. Die korrekte Form "Datum" hat eindeutigen temporalen Bezug, der in diesem Zusammenhang nicht interessiert. Engl. Entsprechung: *data* (nur Mehrzahl, Einzahl *datum* nicht gebräuchlich, *data* wird mitunter auch als Einzahl verwendet).

> *Def.:* Nachrichten *sind Daten, welche von einem Individuum an ein anderes übertragen werden.*

Dazu können technische Systeme benutzt werden, welche die Nachrichten gemäss Anforderung von Empfänger oder Sender sammeln, zusammenfassen oder auswerten.

Die Einzahl *Nachricht* bezeichnet meist eine klar abgrenzbare Übermittlung zwischen zwei Personen oder Systemen mit allen notwendigen Steuerungs-informationen (Übertragungsanforderung, Empfangsbestätigung etc.). Die Mehrzahl bezeichnet demnach Sammlungen solcher Übermittlungen. Engl. Entsprechung: *message, messages.*

Konvention:
Der Begriff Information *wird hier als Oberbegriff für Wissen, Information (i.e.S.), Daten und Nachrichten verwendet.*[11]

Informationseinheiten im unternehmerischen Umfeld

Im unternehmerischen Umfeld, d.h. im Bereich der Informationsverarbeitung in der Sachbearbeitung oder bei steuernden Abläufen, nicht bei der technischen Datenverarbeitung, ist das Bit als kleinste Informationseinheit ungeeignet. Als kleine Informationseinheiten haben sich die Begriffe *Dokument* und *Datensatz* etabliert.

Konvention:
Zur Bezeichnung der kleinsten Informationseinheit im unternehmerischen Umfeld wird der Begriff Dokument *für unstrukturierte und der Begriff* Datensatz *für strukturierte Inhalte verwendet.*

Def.: Ein Dokument *umfasst unstrukturierte Daten über eine einzelne oder einige wenige zusammengehörende geschäftliche Transaktionen oder beschreibt eines oder einige wenige Objekte aus dem Umfeld der unternehmerischen Tätigkeit.*

Bei einem Dokument kann es sich um einen Text handeln, der beispielsweise mit einem Textverarbeitungsprogramm erstellt wurde oder um jede andere Art von Information, welche typischerweise in einer Datei für sich alleine gespeichert wird. Englische Entsprechung: *document*. Beispiele für Dokumente sind *Mitteilung* (*message)*, *Brief* (*letter*), *Auftrag* (*order*), *Protokoll* (*protocol*), *Hinweis* (*note*), *Liste* (*list*) etc.

Def.: Ein Datensatz *umfasst strukturierte, inhaltlich zusammengehörende Daten über eine einzelne geschäftliche Transaktion oder beschreibt ein Objekt aus dem Umfeld der Unternehmung.*

---

11 Zum Verhältnis zwischen Wissen, Sprache und Interpretation vgl. auch [Schneider86, insbes. S. 81ff und S.185ff]

Ein Datensatz ist zusammen mit weiteren gleichartigen (gleichformatigen) in einer Datei gespeichert. Engl. Entsprechung: *record*. Der Begriff „Informationssatz" ist nicht gebräuchlich.

> *Def.:* Informationssammlungen *sind Sammlungen von Informationseinheiten, welche gemeinsam einem Zweck dienen, oder die inhaltlich ähnlich sind, oder die zu denselben Prozessen gehören.*

Informationssammlungen können Dokumente, Datensätze oder beides umfassen. Englische Entsprechung: *information collections.* Beispiele für Informationssammlungen sind *Korrespondenz* (*correspondence*), *Aufträge* (*orders*), *Sitzungsprotokolle* (*meeting protocols*), *Kundenstamm* (*client base*) etc.

Daten

Analog zur Information wird die kleinste *Daten*einheit meist auch aus dem Gebrauch in der Unternehmung hergeleitet und stellt die Abbildung der oben genannten Informationseinheiten auf ein bestimmtes Medium dar. Gesamthaft handelt es sich dann um *Datensammlungen* (engl.: *data collections*). Beispiele für Datensammlungen sind *Ordner* (*binder*), *Archiv* (*archive*), *Datenbank* (*data base*), *E-Mail* (*e-mail*), *Dossier* (*folder*) etc.

Wenn Datensammlungen eine Struktur aufweisen, welche das schnelle Auffinden einzelner Elemente erlaubt oder eine Ordnung, Zusammenfassung etc. der Daten auf einfache Weise unterstützt, wird von einer *Datenbank* (engl.: *data base*) und einem darauf zugreifenden *Datenbanksystem* (*data base system*) gesprochen.

Es ist schwierig, bei der Bezeichnung von Informations- und Datensammlungen eine Vermischung von Bezeichnungen des Inhalts, der Form, der Übertragung und der Speicherung zu vermeiden. Beispiele:

- Ein *Datensatz* bezeichnet eine Form, sagt aber nichts über den Inhalt aus, nur teilweise etwas über die Speicherung (digital, im Gegensatz zur analogen "Karteikarte").
- Ein *Auftrag* ist ein Spezialfall eines Dokuments. Der Begriff kann Form und Inhalt bezeichnen: Zum Ersten beschreibt er eine inhaltliche *Beziehung* zwischen Auftraggeber und Auftragnehmer (konzeptionelles Element). Aufgrund der üblichen Verwendung des Begriffs bezeichnet er zweitens die *damit beschriebenen Transaktionen* (Auftragsvergabe als Tätigkeit) und schliesslich drittens die *schriftliche Niederlegung* der Auftragsinhalte auf Papier und das *Papier* selbst, auf welchem diese Inhalte abgebildet sind (Auftragsdokument).

- *Brief* (als Spezialfall eines Dokuments) bezieht sich v.a. auf die Form und die Übertragung per Post, die Speicherung auf Papier und die Form der Darstellung und lässt teilweise unstrukturierte Inhalte vermuten.
- *Fax* oder *Express-Sendung* (als Spezialfälle von Dokumenten) bezeichnen *Übertragungsformen*, aber beispielsweise auch das dem Faxgerät entnommene Stück *Papier*, welches wiederum als Dokument betrachtet wird.
- Ein *Dokument* bezeichnet allgemein Form (Text mit Formatierungen und Anordnung der Textelemente) und Speicherung (auf Papier). Seit der durch die Textverarbeitung eingeführten Verwendung kann die Speicherung auch digital erfolgen, und verbreitete Textverarbeitungssysteme bezeichnen die bearbeitete Datei als Dokument (z.B. durch Kennzeichnung mit der Dateinamenendung *.doc). Ob das Dokument auch dann noch so bezeichnet wird, wenn es über E-Mail versendet und empfangen wird, wenn es komprimiert oder verschlüsselt wird, wenn es in Inter- und Intranetsystemen abgelegt oder wenn es laut vorgelesen wird, ist nicht eindeutig, aber zumindest teilweise üblich.

Der Begriff der *unternehmerischen Informationseinheit* ist deshalb vorsichtig und im Bewusstsein unscharfer Begrenzungen zu verwenden, ist aber eine sinnvolle Basis für die Betrachtung der Sicherheit unternehmerischer Information.

Fazit

Der Begriff *Information* beschreibt die vier Ausprägungen *Daten, Wissen, Nachrichten* und *Information (i.e.S.)* und wird in der Regel als Oberbegriff dieser vier Ausprägungen verwendet. Die Verarbeitung von *Information* benötigt Interpretation und Verwendung und kann deshalb nur durch Personen geschehen, während Geräte lediglich *Daten* verarbeiten können. Im unternehmerischen Umfeld stellen *Dokumente* und *Datensätze* gebräuchliche Informationseinheiten dar. Sie werden zu *Informationssammlungen* zusammengefasst.

2.2 Sicherheitsbegriffe

Sicherheit und Risiko

Sicherheit wird im Duden als *"Sichersein vor Gefahr oder Schaden"*, als *"sicheres, keinen Zweifel aufkommen lassendes Gefühl, Wissen"*[12], als *"Freisein von Fehlern oder Irrtümern"* definiert. [Duden85, S. 584].

---

12 Der möglicherweise bestehende Bezug zwischen Sicherheit als Wissen und dem Wissensbegriff der Informationswissenschaft soll hier nicht weiter betrachtet werden.

> *Def.:* Sicherheit *(security) ist ein Zustand eines Objekts, in welchem das Verhalten des Objektes und das von einem Betrachter erwartete Verhalten dieses Objekts übereinstimmen.*
>
> *Def.:* Das Risiko *(risk) ist umgekehrt der Zustand, in welchem die Erwartungen nicht mit dem Verhalten übereinstimmen.*

Sicherheit und Risiko spiegeln also Annahmen wider, welche letztendlich nicht beweisbar sind; absolute Sicherheit existiert deshalb weder im Sinne von *vollständiger* noch im Sinne von *neutral oder objektiv feststellbarer* Sicherheit.

Anforderungen

Sicherheit und Risiko sind abstrakte subjektive Beurteilungen. Im hier betrachteten Kontext bezieht sich Sicherheit immer auf ein Objekt, dessen Schutz im Interesse des Individuums liegt, und welches deshalb als *schützenswertes Objekt* (auch: Schutzobjekt, *protection object*) bezeichnet wird. Da es sich bei diesen Objekten oft um Ressourcen der Unternehmung handelt, werden sie im Englischen auch als *assets* bezeichnet.

Sicherheit ist eine subjektive Qualität des schützenswerten Objektes. Diese Qualität wird aus Anforderungen des Betrachters hergeleitet: Die Erfüllung der Anforderungen erzeugt die Qualität. Ein Objekt ist beispielsweise sicher, wenn es genau dann verfügbar ist, wenn es von einer Person benötigt wird (Verfügbarkeitsanforderung), oder wenn sein Wert erhalten bleibt (Werterhaltungsanforderung). Die Anforderungen können voneinander unabhängig oder abhängig sein, und die Abhängigkeit kann direkt oder invers sein. Beispiele: Wenn eine Information verfügbar ist, sagt dies nichts über ihre Integrität aus, umgekehrt sagt die korrekte Integrität einer Information nichts über ihre Verfügbarkeit aus. Wenn eine Information allerdings nicht zum gewünschten Zeitpunkt verfügbar ist, sondern erst später, sinkt ihr Wert, z.B. bei Börsenkursen (der Wert ist direkt abhängig von der Verfügbarkeit). Wenn eine Information der Person A für eine Person B verfügbar ist, obwohl sie ihr nicht zugänglich sein sollte, wird die Verfügbarkeitsanforderung von B erfüllt, die Vertraulichkeitsanforderung von A jedoch nicht (umgekehrte Abhängigkeit zwischen Verfügbarkeit und Vertraulichkeit). Es ist angebracht, möglichst *unabhängige* Anforderungen zu definieren, sog. Grundanforderungen.

Der *Wert* einer Information hängt oft von anderen Anforderungen ab. Es können jedoch völlig unterschiedliche Anforderungen gestellt und unterschiedliche Grundanforderungen formuliert werden. Zwei Betrachter werden also i.d.R. die Sicherheit eines Objektes unterschiedlich beurteilen.

Einflüsse der Umwelt

Die Sicherheit (und das Risiko) eines Objekts ist von Veränderungen der Umgebung des Objekts und des beurteilenden Individuums abhängig. Einflüsse aus dieser Umwelt können Eigenschaften des Objektes verändern oder dazu führen, dass ein einmal als sicher angenommener Zustand anders beurteilt wird. Sicherheit muss also immer wieder neu beurteilt werden. Es existieren Einflüsse aus der Umgebung, welche die Sicherheit dieses Objekts erhöhen oder senken, indem sie das Objekt verändern.

Risikomanagement und Sicherheitsmanagement

Risiko und Sicherheit beziehen sich immer auf ein Objekt und sind gegenseitig voneinander abhängig. Auf eine Formel gebracht: Risiko ist nicht vorhandene Sicherheit und umgekehrt. Die Absenz von Sicherheit ist demnach vollständiges Risiko, die Absenz von Risiko stellt vollkommene Sicherheit dar. Beide Extremwerte sind in der Praxis nicht möglich.

"Risikomanagement ist eine Führungsfunktion, welche sämtliche Zustände und Aktivitäten eines System überprüft und steuert, um möglichst zu verhindern, dass das Erreichen der gesetzten Ziele durch Störprozesse gefährdet wird." [Winterthur90, S. 5] Risikomanagement betrachtet also die möglichen sicherheitssenkenden Einflüsse. Sicherheitsmanagement verfolgt denselben Ansatz, indem es die Sicherheit erhöht. Die Begriffe Risiko- und Sicherheitsmanagement sind also synonym.

> *Def.: Sicherheit ist in einem konkreten Umfeld immer ein* Ziel*, da vollständige Sicherheit in der Praxis nicht erreicht werden kann.*
>
> *Def.: Sicherheitsmanagement umfasst die Tätigkeiten zur Erreichung von Sicherheit.*

Im Folgenden soll Sicherheit als *Ziel und* als *Zustand* aufgefasst werden. Der Zustand hat für den Beurteilenden einen Wert, der aus der Erfüllung von Anforderungen (z.B. "das Objekt ist verfügbar, wenn es benötigt wird") hergeleitet werden kann. Zu Erreichung dieses sicheren Zustandes (also zur Werterhöhung) werden Aktionen durchgeführt, welche unter dem Begriff *Sicherung* oder *Schutz* (*protection*) zusammengefasst werden und Verminderung des Risikos und Erhöhung der Sicherheit anstreben. Sicherung und Schutz sind teilweise synonym, indem beide die Sicherheit eines Objektes erhöhen. Die Adjektive *sicher* und *geschützt* unterscheiden sich jedoch: das erste beschreibt einen sicheren Zustand, das zweite beschreibt lediglich, dass etwas zur Erreichung dieses Zustandes unternommen wurde.

Schutz geschieht durch die Anwendung von *Schutz-* oder *Sicherheitsmassnahmen* (diese Begriffe sind synonym; engl. *safeguards, protection measures*). Die Massnahmen haben zum Ziel, die Sicherheit des Objekts zu erhöhen. Sie erfordern jedoch Aufwand, der mit der Annäherung an vollständige Sicherheit überproportional steigt (vgl. Kurve in Abbildung 2-1). Dieser Aufwand umfasst nicht nur die einmaligen Anstrengungen zur Einrichtung der Massnahme, sondern auch den kontinuierlich zu leistenden Mehraufwand.

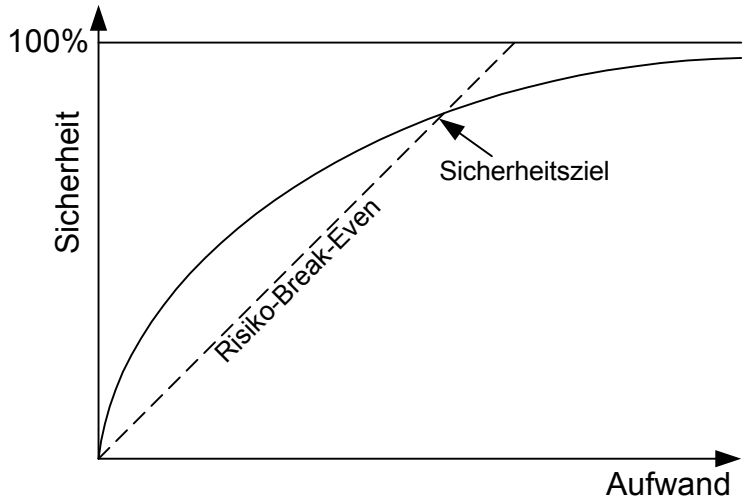


Abbildung 2-1: Verhältnis zwischen Aufwand und Sicherheit
[in Anlehnung an BSI-IT-GSHB97, T1, K1, S.7]

Im Idealfall kann deshalb ein bestmögliches Verhältnis von Sicherheit und Schutzaufwand (Punkt *Sicherheitsziel* in Abbildung 2-1) gefunden werden. Die gestrichelte Linie in Abbildung 2-1 stellt ein ausgewogenes Kosten-Nutzen-Verhältnis dar: Links davon überwiegt der Nutzen von Sicherheitsmassnahmen, rechts davon überwiegen die Kosten. Wenn der Wert des Objektes durch eine Sicherheitsmassnahme nicht über die Kosten (den Aufwand) dieser Sicherheitsmassnahme hinaus gesteigert werden kann, stellt diese Massnahme keine Werterhöhung dar und sollte nicht angewendet werden. Vollständige Sicherheit ist deshalb nicht erreichbar; es bleibt immer ein Risiko, welches als *Restrisiko (residual risk)* bezeichnet wird.

Risiko als sicherheitssenkender Einfluss

Der Begriff Risiko wird auch verwendet, um eine unerwünschte Veränderung des Zustands eines Objekts zu bezeichnen, welche nicht immer eintritt (einer *Wahrscheinlichkeit* (*probability*) unterliegt) und einen *Schaden* (*damage*) zur Folge

hat[13]. Beide Komponenten (Wahrscheinlichkeit und Höhe des Schadens) können idealerweise numerisch angegeben werden, was eine quantitative Bestimmung des Risikos erlaubt. Die Gesamtheit der einzelnen Risiken bildet *das* Risiko in der erstgenannten, abstrakten Bedeutung.

> *Def.:* Ein Risiko *ist ein sicherheitssenkender Einfluss.*

Wenn ein Schaden eintritt, so ist er auf eine *Ursache* (*source, cause*) zurückzuführen (wenngleich diese nicht immer bestimmbar ist) und hat direkte und indirekte *Folgen* (*consequences*). Die direkten Folgen sind oft offensichtlich und entstehen durch Wertminderung des Objekts etc. Die indirekten Folgen werden durch Abhängigkeiten weiterer Objekte und Prozesse vom beschädigten Objekt hervorgerufen.

Formell setzt sich ein Risiko zusammen aus *Gefahr*, *Bedrohung*, *Schwachstelle*, *Gefährdung*, *Wahrscheinlichkeit* und *Schaden*.

> Def.: *Der Begriff* Gefahr *(danger) bezeichnet die Möglichkeit, dass ein Schaden eintritt.*

Eine Gefahr richtet sich nicht gegen ein bestimmtes Objekt, höchstens gegen eines aus einer Gruppe von Objekten. Beispiele: Die Hacker[14] im Internet stellen eine Gefahr dar für alle, die sich ans Internet anschliessen. Ein Mann mit einer Schusswaffe ist eine Gefahr für die Bevölkerung.

> *Def.: Eine* Bedrohung *(threat) ist eine Gefahr, welche sich gegen ein konkretes Objekt richtet.*

Beispiel: Ein Hacker greift unser System an. Der Mann bedroht eine Frau mit der Schusswaffe.

> *Def.: Eine* Schwachstelle *(weakness, vulnerability) ist ein Bereich eines Objektes, welcher einer Gefahr weniger Widerstand entgegenzusetzen hat als ein vergleichbarer anderer Bereich desselben Objektes.*

---

13 Dies entspricht dem oben erwähnten *sicherheitssenkenden Einfluss*.

14 Der Begriff *Hacker* wird heute allgemein für Personen verwendet, welche sich ungerechtfertigt Zugang zu einem technischen Informationssystem verschaffen. In der ursprünglichen Bedeutung bezeichnete *Hacker* einen Programmierer, der grösstmögliche Effizienz bei Entwurf, Eingabe und Ausführung eines Programms anstrebte und zu diesem Zweck viel und schnell auf der Tastatur des Gerätes „herumhackte". In diesem Zusammenhang werden Einbrecher in fremde Systeme als *Cracker* bezeichnet. Ein *Cracker* ist aber auch jemand, der den Kopierschutz eines Softwareproduktes umgeht.

Hier wird in der Folge der Begriff *Hacker* für einen böswilligen Angreifer verwendet, weil sich dies in der Praxis so etabliert hat. [vgl. Raymond91, S. 110, 191]

Wenn ein Objekt bedroht wird und Schwachstellen aufweist, so wird eine intelligenter Angreifer die Schwachstelle als Startpunkt für den Angriff wählen. Beispiel: Die Attributierung der Datei `passwords` als `world readable` stellt eine Schwachstelle in einem *UNIX*-System dar. Die Schusswaffe kann die Frau verletzen.

> *Def.: Eine* Gefährdung *(hazard, endangerment) ist diejenige Beeinträchtigung des Objekts, welche aus einer Bedrohung entsteht.*

Beispiel: Der Angriff gefährdet die Verfügbarkeit des Servers und die Vertraulichkeit der darauf gespeicherten Daten. Die Bedrohung mit der Waffe gefährdet die Gesundheit der Frau.

> Def.: Wahrscheinlichkeit *(*probability*) bezeichnet das angenommene Mass für die anteilmässige Anzahl von gleichartigen Fällen, in welchen eine Bedrohung zum Schaden wird.*

Es kann immer nur von einem *angenommenen Mass* ausgegangen werden, weil gerade in Situationen, in welchen von Risiko gesprochen wird, keine wirklich gleichartigen Fälle verglichen werden können, weshalb die quantitative Angabe einer Wahrscheinlichkeit sehr schwierig ist. Sind vergleichbare Fälle vorhanden, spricht man von der statistischen Wahrscheinlichkeit; diese ist jedoch nur in Modellen bestimmbar. Umgangssprachlich werden verschiedene Wahrscheinlichkeitsgrade durch die Ausdrücke *unwahrscheinlich, vielleicht, kann sein, möglich, wahrscheinlich, sicher, zu erwarten*, und weitere Phrasen und Begriffe qualifiziert, deren eindeutige Zuordnung zu Anteilswerten, oder auch nur schon deren eindeutige Ordnung untereinander, nicht möglich ist. Beispiel: Die Wahrscheinlichkeit eines Angriffes auf unser System ist gering. Der Mann wird vielleicht schiessen.

> Def.: Risiko *(risk) bezeichnet die quantitative oder qualitative Grösse für die Gefährdung einer Eigenschaft eines Objektes durch eine Bedrohung. Bei statistischer Betrachtungsweise bezeichnet Risiko den Erwartungswert des eintretenden Schadens als Produkt aus Wahrscheinlichkeit und Schadenshöhe.*

Beispiel: Das Risiko eines Vertraulichkeitsverlusts der auf dem Server gespeicherten Daten durch Hackerangriffe ist gering. Die Verletzungsgefahr durch die Bedrohung mit der Schusswaffe ist gegeben.

Oft wird das Risiko auch ohne Bezug auf ein bestimmtes Objekt oder die konkrete Bedrohung angegeben, jedoch fälschlicherweise auch, wenn diese Objekte nicht

implizit gegeben sind (z.B. „Angriffe über das Internet sind bei uns unwahrscheinlich“).

Ein *Schaden* (*damage*) entsteht, wenn eine Bedrohung sich konkret manifestiert. Schäden lassen sich in direkte und indirekte Schäden unterteilen. *Indirekte Schäden* werden auch als *Folgeschäden* bezeichnet. Diese lassen sich wieder in direkte und indirekte Folgeschäden unterteilen. Direkte Schäden werden als Schäden ersten Grades bezeichnet, direkte Folgeschäden als Schäden zweiten Grades und indirekte Folgeschäden als Schäden dritten Grades.

> Def.: *Ein* Schaden ersten Grades *(G1-Schaden, first degree / level damage) ist die Manifestation einer Bedrohung bzw. die Höhe des Aufwandes, welcher notwendig ist, um den durch diese Manifestation veränderten Zustand des direkt betroffenen Objekts zum gewünschten Zustand zurück-zuführen.*

G1-Schäden sind oft sehr gut quantitativ bestimmbar, wenn der Wert des betroffenen Objektes bekannt ist und neu festgestellt werden kann; der Schaden kann dann als Differenz oder als wertmässiger Anteil angegeben werden (Bsp.: Aufwand zur Wiederherstellung der Daten nach einem Datenverlust).

> Def.: Schäden zweiten Grades *(G2-Schaden, second degree / level damage) entstehen durch Wertminderungen von Objekten oder Prozessen, welche mit dem geschädigten Objekt in einem nachvollziehbaren und beurteilbaren Zusammenhang stehen und entstehen nur, wenn ein Schaden ersten Grades eintritt.*

G2-Schäden sind manchmal quantitativ bestimmbar, ihre genaue Abgrenzung von parallel eintretenden Veränderungen des Gesamtsystems beeinträchtigen jedoch diese Bestimmbarkeit (Bsp: Betriebsunterbruch aufgrund temporärer Nicht-Verfügbarkeit von Daten).

> Def.: Schäden dritten Grades *(G3-Schaden, third degree / level damage) umfassen diejenigen Schäden, welche sich nicht logisch argumentativ, sondern nur durch Annahmen mit dem ursprünglichen Schaden in Verbindung bringen lassen.*

Sie entstehen nur, wenn ein Schaden ersten Grades eintritt. G3-Schäden sind in der Regel quantitativ nicht bestimmbar. (Bsp.: Auftragsverluste durch Bekanntwerden von Datenverarbeitungsproblemen und Lieferunfähigkeit der Unternehmung).

Die Begriffe sind in Abbildung 2-2 dargestellt.

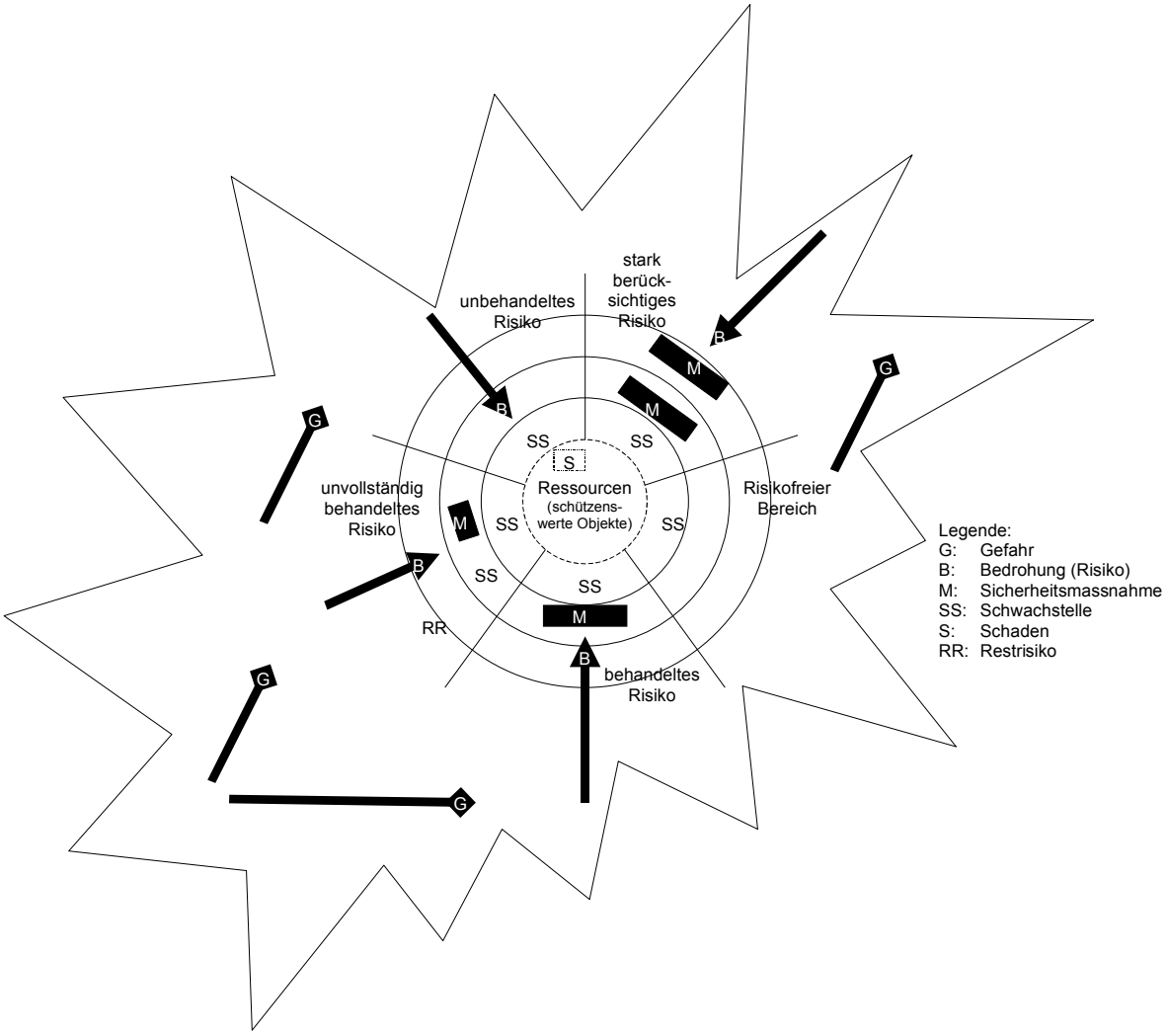


Abbildung 2-2: Darstellung der Risikobegriffe [in Anlehnung an ISO13335-1, S. 15]

Schutzziel und Sicherheitsniveau

Zur Erreichung des Ziels Informationssicherheit sind Vorgehensweisen und Verfahren notwendig (vgl. Kapitel 6), die generisch beschrieben werden können. Diese umfassen unter anderem die Festlegung des gewünschten *Sicherheitsniveaus* (*desired security degree / level*), auch *Schutzziel* (*protection goal*) oder *Sicherheitsziel (security goal)* genannt, und erzeugen Massnahmen zur Beeinflussung der einzelnen Risiken. Diese Massnahmen werden gesamthaft als *Sicherheitsdispositiv* (*security arrangement / security disposition*) bezeichnet.

Das aktuelle und das angestrebte Sicherheitsniveau können für jedes beliebige schützenswerte Objekt (auch für die Unternehmung als Ganzes) idealisiert als Wert auf einer kontinuierlichen Skala von 0 bis 100% angesehen werden. Dabei ist das Schutzziel in der Regel höher als der aktuelle Sicherheitszustand, wodurch Massnahmen gerechtfertigt werden. Die *Senkung* des Sicherheitsniveaus ist

ebenfalls möglich, indem sicherheitserhöhende Massnahmen entfernt oder zusätzliche Risiken eingegangen werden. Abbildung 2-3 stellt diesen Zusammenhang dar. Es handelt sich dabei jedoch um eine rein theoretische Betrachtung, da in einem konkreten Fall die in der Abbildung verwendeten Zeiger nicht genau positioniert werden können.

Das angestrebte Sicherheitsziel sollte so festgelegt werden, dass sich der Aufwand für die notwendigen Massnahmen und der Nutzen (die Werterhöhung durch zusätzliche Sicherheit) die Waage halten (vgl. auch gekennzeichneter Punkt in Abbildung 2-1, Seite 28).

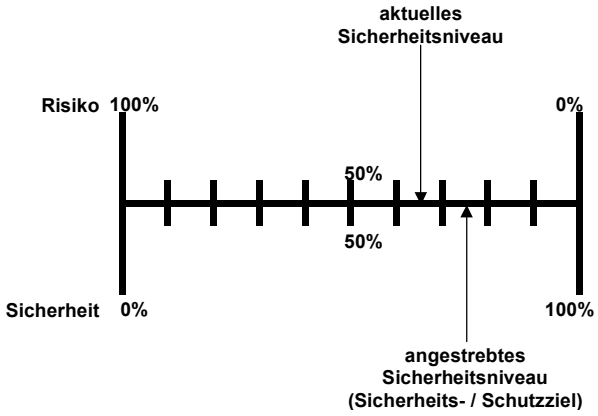


Abbildung 2-3: Sicherheits- / Schutzziel [in Anlehnung an Winterthur90, S. 3]

Inkonsistente Verwendung von Sicherheitsbegriffen in der Praxis

In der Praxis haben sich im deutschen Sprachraum verschiedene Begriffe im Zusammenhang mit Sicherheit, Sicherung und Schutz etabliert, welche inkonsistent sind, in der Folge aber in der allgemein üblichen Form verwendet werden müssen.

Werkschutz beispielsweise impliziert, dass ein „Werk" „geschützt" wird, ist aber doppeldeutig: Einerseits wird damit der urheberrechtliche Schutz eines intellektuellen kreativen Werkes bezeichnet (*copyright*), welche vom Gesetzgeber durch das Urhebergesetz geschützt werden, wobei dieser Schutz reaktiv angewendet wird. Andererseits bedeutet es weitgehend dasselbe wie *Arbeitssicherheit (works security services)*, umfasst jedoch auch Aspekte des Feuer- und Wasserschutzes (*fire and water prevention / protection)*, welche in der Praxis auch als *Objektschutz* (*protection of property*) bezeichnet werden und gesamthaft präventiv geschehen.

Arbeitssicherheit sichert jedoch nicht Arbeit – dafür wird der Begriff *Sicherheit des Arbeitsplatzes* oder *Jobsicherheit* (*job security, safeguarding of jobs*) verwendet – sondern umfasst alle Massnahmen zum *Schutz* der *Arbeiter* (*workplace or workspace security*). Ziel der Arbeitssicherheit ist also die Sicherheit der Arbeiter, müsste dementsprechend *Arbeitersicherheit* genannt werden. Es werden dabei die Arbeiter als physische Teile der Unternehmung geschützt, nicht jedoch die

Arbeitsabläufe, welche sie ausführen; letzteres wäre *Arbeitsablaufsicherung*, und müsste im Rahmen der *Qualitätssicherung* betrachtet werden.

Eine näherliegende unangemessene Begriffsverwendung ist die von *Datenschutz* (*data protection*). Datenschutz schützt die Persönlichkeitsrechte und Privatsphäre (*privacy*) derjenigen Individuen, welche durch die Daten beschrieben werden, indem es die Weitergabe solcher Daten rechtlich regelt und die rechtliche Grundlage für die Ahndung von Missbräuchen schafft (Rechtsschutz). Es müsste also als *Personendatenverwendungssicherheit* o.ä. bezeichnet werden. Im Englischen heissen die entsprechenden gesetzlichen Regelungen *privacy laws*. Der Schutz von Daten (jeglichen Inhalts) wird i.d.R. unter dem Begriff *Datensicherheit* zusammengefasst.

Es ist nicht das Ziel dieses Textes, diese Begriffe neu zu definieren. Dies wäre unangebracht; insbesondere wäre auch eine Neudefinition der fremdsprachigen Begriffe notwendig, was nicht erreichbar scheint. Es soll hier lediglich aufgezeigt werden, dass viele Begriffe nicht die offensichtliche Bedeutung haben, welche sich aus ihren sprachlichen Komponenten herleitet, sondern historisch gewachsen sind und durch die Verknüpfung verschiedener Bereiche (insbes. in Recht und Informatik) ihren Sinn erhalten haben. Davon sind die hier grundlegenden Begriffe *Sicherheit, Schutz, Sicherung,* und ihre englischen Pendants *safety & security, protection, prevention* betroffen.

Security and Safety

Im Englischen wird weiterhin zwischen *security* und *safety* unterschieden. *Security* bezeichnet dabei die Sicherheit eines Objekts gegen von aussen einwirkende Bedrohungen, während *safety* eher Sicherheitsprobleme beim Einsatz des Objekts selbst bezeichnet. Ein *secure system* ist deshalb ein System, welches gegen Unwägbarkeiten der Umwelt geschützt ist, während ein *safe system* eines ist, dessen Gebrauch keine Sicherheitsprobleme erzeugt. Ein *security system* schützt gegen aussen (z.B. Zutrittsschutz mit Personenschleusen, Firewall-Rechner im EDV-System), ein *safety system* gegen innen (Bsp.: Schleudersitz im Flugzeug, redundante Datenhaltung innerhalb eines EDV-Systems). Die Verwendung hängt jedoch auch vom betrachteten Fachgebiet bzw. der Branche ab. So wird in der Luft- und Raumfahrt vermehrt von *safety* gesprochen, während in der Informatik *security* häufiger verwendet wird. Ausserdem wird eher von *Safety* gesprochen, wenn die Gesundheit oder das Leben von Menschen bedroht ist, während materielle Sicherheit eher mit *Security* bezeichnet wird.

Fazit

Sicherheit ist ein Zustand eines Objekts, in welchem es die Anforderungen eines Betrachters erfüllt. Sicherheit ist subjektiv (vom Betrachter abhängig) und wird durch Einflüsse aus der Umwelt (security-Aspekt), durch Unvollkommenheit des Objekts (safety-Aspekt) und durch die Zeit verändert, weil sich Individuum,

beurteiltes Objekt oder Anforderungen ändern. Zur Beurteilung der Erfüllung der Anforderungen müssen möglichst Beurteilungskriterien verwendet werden, welche unabhängig voneinander sind.

Schutz ist die Tätigkeit, um Sicherheit zu erreichen. Die einzelnen Tätigkeiten werden als Massnahmen bezeichnet und haben eine bessere Erfüllung der Anforderungen zum Ziel.

Risiko ist als Eigenschaft einerseits mit nicht vorhandener Sicherheit gleichzusetzen (*das* Risikopotential eines Objekts). Das Adjektiv "riskant" bezieht sich auf Tätigkeiten, deren Resultat nicht absehbar ist. Andererseits umschreibt *ein* Risiko ein sicherheitsminderndes Ereignis und setzt sich aus verschiedenen Komponenten (Gefahr, Bedrohung, Gefährdung, Wahrscheinlichkeit etc.) zusammen. Risiken sind quantitativ oder qualitativ beurteilbar.

2.3 Grundanforderungen und Grundbedrohungen

Der subjektiv wahrgenommene Zustand "sicher" einer Information muss vom Betrachter definiert werden, um überprüfbar zu sein. Sicherheit wird dabei als Sammlung von *Anforderungen* betrachtet, welche die Information erfüllen muss. Üblich sind die Anforderungen an *Vertraulichkeit*, *Integrität* und *Verfügbarkeit* von Daten, welche im englischem Sprachgebrauch mit *CIA* abgekürzt werden (*confidentiality, integrity, availability*).

In neuerer Zeit wird Integrität genauer betrachtet, ausserdem werden auch Anforderungen an die sinngemässe bzw. beabsichtigte Verwendung erhoben. Gemäss [Holbein96, S. 50ff] lassen sich auf technischem Niveau die Kriterien *Vertraulichkeit (confidentiality), Verfügbarkeit (availability)* und *Interne Integrität (Konsistenz, integrity)* unterscheiden, auf sozialer Ebene *Verbindlichkeit (obligation),* und auf ökonomischer Stufe *Externe Integrität (Kongruenz, content authenticity)* und *Beabsichtigte Verwendung (intended usage).*

Weitere Anforderungen wurden von der ISACF im ihrem COBIT-Framework [COBIT96.3, S.13] als *information criteria* definiert. Neben *confidentiality, integrity* und *availability* werden angegeben: *Effektivität* (*effectiveness*), *Effizienz* (*efficiency*), *Ordnungsmässigkeit* (*compliance*) und *Verlässlichkeit* (*reliability*).

Pordesch und Schneider identifizieren in [Pordesch97, S. 69ff] die Anforderungen *Vertraulichkeit, Unbeobachtbarkeit, Unverkettbarkeit, Anonymität, Pseudonymität, Integrität* und *Unbestreitbarkeit.*

Rannenberg, Müller und Pfitzmann beispielsweise sprechen in [Müller97b] von mehrseitiger Sicherheit und unterteilen diese in *Vertraulichkeit von Nachrichteninhalten, Anonymität, Unbeobachtbarkeit, Vertraulichkeit des Orts der Kommunikationsteilnehmer, Erkennbarkeit von Fälschungen des Nachrichteninhalts, Verfügbarkeit jeder gewünschten Kommunikationsbeziehung,*

Nachweisbarkeit des Sendens, Beweisbarkeit des Absendens und *Nachweisbarkeit von Entgeltansprüchen.*

Es fällt bei dieser Zusammenstellung einerseits auf, dass die Anforderungen sich überschneiden und nicht voneinander unabhängig sind (Verlässlichkeit und externe Integrität sind ähnlich), andererseits, dass die beiden letztgenannten Anforderungen nicht die Information an sich betreffen, sondern explizit die Informationsverarbeitung. Weder Holbein noch die ISACF haben ihre Definition jedoch präzise im Hinblick auf das hier betrachtete Management der Informationssicherheit getroffen, welche hier sehr breit verstanden wird. Es liegt deshalb nahe, beide Sätze zu kombinieren und hier die nachfolgend beschriebenen Grundanforderungen zu unterscheiden.

Bei dieser Zusammenstellung wurde Unabhängigkeit der einzelnen Kriterien untereinander angestrebt. Ein Beweis für diese Unabhängigkeit kann hier jedoch nicht erbracht werden. Da jedoch auf den von Holbein und der ISACF ebenfalls mit dem Ziel der relativen Unabhängigkeit definierten Kriterien aufgebaut wird, soll die hier wiedergegebene Zusammenstellung die Basis für die weiteren Betrachtungen bilden.

Technische Ebene

- *Vertraulichkeit (confidentiality) "concerns the protection of sensitive information from unauthorised disclosure"* [COBIT96.3, S.13] *"... within an [IT] system and during transmission between different [IT] systems"* [Holbein96, S. 51]
- *Interne Integrität (integrity) "relates to the accuracy and completeness of information [...]"* [COBIT96.3, S.13] and *"is concerned with the internal state of data which must be syntactically correct and cannot be modified in an unintended way [...] and the accuracy or validity of the data, i.e. the relationship between data and its representation"* [Holbein96, S. 51]
- *Verfügbarkeit (availability) "relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities"* [COBIT96.3, S. 13] "and *"requires a state of existence or readiness of [the IT system] for being used"* [Holbein96, S.52].

Ökonomische Ebene:

- *Effektivität (effectiveness) "deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner"* [COBIT96.3, S.13]
- *Effizienz (efficiency) "concerns the provision of information through the optimal (most productive and economical) use of resources"* [COBIT96.3, S.13]

- *Zuverlässigkeit (reliability)* of information is *"related to the provision of appropriate information for management to operate the entity and for management to exercise its financial and compliance reporting capabilities"* [COBIT96.3, S.13]
- *Beabsichtigte Verwendung* (intended usage) *"concerns the pragmatic relevance of information arising from human interaction. It refers to the enabling character of information concerning goal-oriented human behaviour and requires ensuring that the use of information is bound to the intention of its sender. [...] confidentiality ensures nondisclosure by unauthorised parties and, therefore, is a precondition to ensure intended usage which refers to authorised parties. i.e. the communication partners themselves."* [Holbein96, S. 53]

Soziale Ebene

- *Ordnungsmässigkeit* (compliance) *"deals with complying with those laws, regulations and contractual arrangements to which the business process is subject, i.e. externally imposed business criteria"* [COBIT96.3, S.13)]
- *Verbindlichkeit (obligation) "concerns interpersonal relationships which emerge from information exchange. It requires the communication partners to accept these relationships, i.e. they must be willing to fulfil their obligations. [...] It covers two [other] security aspects: authenticity of communication partners and authenticity of origin".* [Holbein96, S.52]
- *Externe Integrität (content authenticity) "concerns the correspondence between a data representation and reality. It requires an accurate and valid mapping of external reality onto physical data, i.e. the content of data must correspond to some objective reality. [...] Content authenticity is often considered as the 'external aspect' of integrity. [...] Integrity ensures that the internal state of a representation is syntactically correct and therefore, is a precondition for content authenticity but not vice versa."* [Holbein96, S. 52] *"Content authenticity [...] relates to the validity of information in accordance with business values and expectations"* [COBIT96.3, S.13]

Da Information im Mittelpunkt der Betrachtungen steht, sollen diese Anforderungen explizit als Anforderungen an die unternehmerische Information verstanden werden. In einigen Fällen (Effizienz, Effektivität) überträgt sich diese Anforderung jedoch direkt auf die Informationssysteme, mit welchen die Informationen verarbeitet werden.

Diese Anforderungen werden als *Grundanforderungen (base requirements)* bezeichnet. Die Bedrohung, dass eine dieser Anforderungen nicht mehr eingehalten werden kann, wird *Grundbedrohung* (*basic threat*) genannt.

Keine der Anforderungen kann letztlich vollständig erfüllt werden (vollständige Sicherheit ist nicht möglich). Um eine Anforderung erfüllen zu können, sind jedoch Voraussetzungen notwendig. So bedingt beispielsweise die Anforderung nach Vertraulichkeit, dass bekannt ist, *wem* die Informationen weitergegeben werden dürfen.

Da Sicherheit subjektiv ist, können für eine Information verschiedene konfliktierende Ansprüche entstehen. Wenn beispielsweise der Urheber einer Information entscheidet, dass diese nur einigen wenigen Personen zur Verfügung stehen soll (Vertraulichkeitsanforderung), so ist dies nicht vereinbar mit dem Verfügbarkeitsanspruch anderer Personen, welche diesem engen Kreis nicht angehören. Es ist deshalb wichtig, dass festgelegt wird, welches Individuum die Anforderungen massgeblich festlegt. Dies wird als *Eigentümerprinzip (information ownership principle)* bezeichnet und verlangt die Zuordnung jeder Information zu genau einer dafür verantwortlichen Person.

Fazit

Sicherheit muss genau spezifiziert werden, um überprüfbar zu sein. Dies bedeutet, dass ein sicheres Objekt eine oder mehrere Anforderungen erfüllt, welche der Betrachter mit dem Begriff Sicherheit verbindet. Üblicherweise werden Vertraulichkeit, Integrität und Verfügbarkeit genannt. Es bestehen aber weitere Möglichkeiten, Grundanforderungen zu definieren. Für diese Dissertation werden *Vertraulichkeit, Interne Integrität, Verfügbarkeit, Effektivität, Effizienz, Zuverlässigkeit, Beabsichtigte Verwendung, Ordnungsmässigkeit, Verbindlichkeit* und *Externe Integrität* als vollständiger Satz untereinander unabhängiger Grundanforderungen betrachtet. Die Nichterfüllung einer Grundanforderung wird als Grundbedrohung bezeichnet.

Damit festgelegt ist, wessen Anforderungen massgeblich für die Beurteilung der Sicherheit eines Objekts sind, muss jedes Objekt genau einem Individuum zugeordnet werden. Dies wird als Eigentümerprinzip bezeichnet.

2.4 Typisierung von Bedrohungen und Risiken

Die Grundbedrohungen sind theoretische Konstrukte, welche wahrgenommene Veränderungen von betrachteten Informationsobjekten beschreiben. Diese Veränderungen entstehen immer aus realen Veränderungen bzw. Einflüssen im Umfeld der Informationsverarbeitung. Dabei gibt es bei jeder Bedrohung ein betroffenes Objekt („was“), eine Aktivität („wie“), einen Urheber der Bedrohung („wer“) und eine Motivation („warum“). Wird darüber hinaus das Risiko betrachtet,

sind auch Klassifizierungen der Häufigkeit („wie oft“) und des entstehenden Schadens („wieviel“) möglich[15].

Somit sind mehrere Typisierungen von Bedrohungen möglich, die nachfolgend beschrieben werden. Diese Typisierungen erlauben zwar nicht immer eine scharfe Abgrenzung, können jedoch als Basis für Bedrohungsanalysen verwendet werden.

Typisierung nach Ursache bzw. Urheber („wer“):

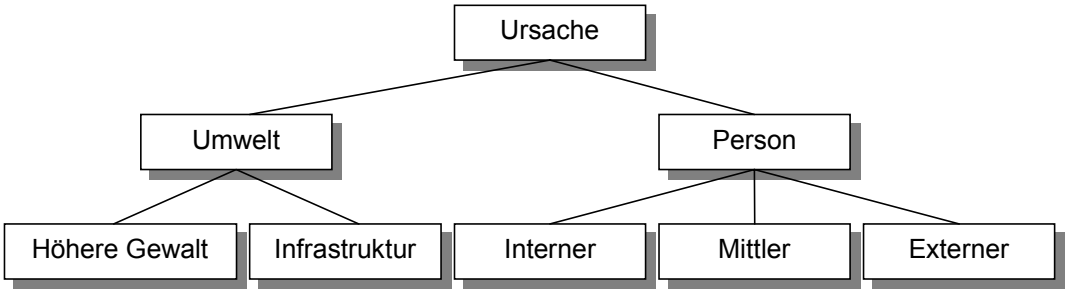


Abbildung 2-4: Typisierung nach Ursache / Urheber

Die Ursache für eine Bedrohung (vgl. Abbildung 2-4) kann in der Umwelt liegen, d.h. nicht direkt auf Personen zurückführbar sein. Naturereignisse wie Erdbeben oder Vulkanausbrüche sind beispielsweise Bedrohungen, bei denen kein menschlicher Einfluss nachgewiesen werden kann. Sie werden unter dem Begriff „*Höhere Gewalt*“ zusammengefasst.

Doch auch Ereignisse wie Überschwemmungen, Stromausfälle etc. werden der Umwelt zugerechnet, wenngleich sie aus einer mangelhaften Beherrschung der Umwelt durch Menschen entstehen und letztlich auf Probleme der *Infrastruktur* zurückzuführen sind. (Bei beiden Typen kann betrachtet werden, welche zugrundeliegenden Annahmen (z.B. „kein erdbebengefährdetes Gebiet“, „Stromversorgung mit 99.999% Verfügbarkeit“) angepasst werden müssen, um Schäden zu verhindern.)

Bei personengebundenen Ereignissen kann unterschieden werden, ob die Person, von welcher die Bedrohung ausgeht, ein Mitarbeiter der Unternehmung ist, ein Mittler (Berater, In- / Outsourcer, Geschäftspartner etc.) oder eine externe, der Unternehmung nicht verbundene Person. Die Trennung kann jedoch nicht immer eindeutig vorgenommen werden, da die möglichen Beziehungen vielfältig sind (Bsp.: Als was gilt ein Angreifer, der früher in der Unternehmung angestellt war?)

---

15 Implizit wird vorausgesetzt, dass ein Individuum diese Bedrohung und das Risiko beobachten kann und beurteilt. Risiken, die nicht beobachtet werden können, entziehen sich einer Betrachtung und damit einer Berücksichtigung bis zu dem Zeitpunkt, in dem daraus ein Schaden entsteht. Dann können die hier identifizierten Aspekte nachträglich betrachtet werden.

Typisierung nach Motivation, Intention, Absicht („warum“)

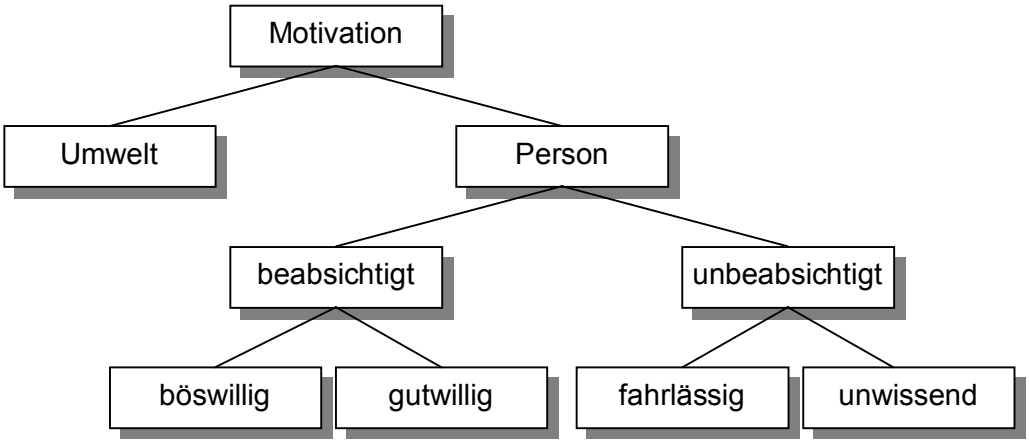


Abbildung 2-5: Typisierung nach Motivation

Falls eine Bedrohung von der Umwelt ausgeht, ist die Motivation (vgl. Abbildung 2-5) i.d.R. nicht festzustellen. Motivationen von Personen können grundsätzlich in beabsichtigte und unbeabsichtigte Bedrohungen unterschieden werden. Unbeabsichtigte Bedrohungen können durch Unwissenheit entstehen, wenn beispielsweise eine Person nicht weiss, welche Auswirkungen ihre Aktivitäten haben. Bsp.: Die Verwendung von privaten Disketten am Arbeitsplatz kann zur Verbreitung von Viren führen.

Wenn der Person die Gefährdung bekannt ist, sie allerdings das Risiko falsch einschätzt, handelt sie fahrlässig (z.B. bei Missachtung des Verbots, private Disketten einzusetzen und unter der Annahme „dass schon nichts geschieht“).

Beabsichtigte Motivationen können gutwillig sein, wenn ein Mitarbeiter durch eine vermeintlich sicherheitserhöhende Aktion die Sicherheit senkt, z.B. durch Löschung vireninfizierter Dokumente, welche anderweitig nicht vorhandene Daten enthalten. Er kann auch böswillig handeln, wenn er die ihm zur Verfügung gestellten Ressourcen zu seinem eigenen Vorteil in einer Weise benutzt, die von seinem Arbeitgeber nicht vorgesehen ist und nicht in dessen Interesse liegt.

Bei allen personenbezogenen Motivationen kann weiterhin die strafrechtliche Relevanz in *strafbar (Offizialdelikt etc.)*, *einklagbar* (evtl. *privatrechtlich strafbar)* und *nicht strafbar* unterteilt werden.

Typisierung nach Tätigkeit („wie“)

Bei böswilligen Aktionen ist weiterhin interessant, wie vorgegangen wurde, um einen Schaden auszulösen.

Wie in Abschnitt 2.2 erwähnt wurde, wirkt eine Bedrohung auf eine Schwachstelle des Systems. Diese Schwachstelle entsteht bei der *Herstellung* des Produkts (beabsichtigt oder unbeabsichtigt), beim *Transport* (Verfälschung des Produkts) oder beim *Einsatz* beim Betreiber. Die Schwachstelle bleibt entweder *unentdeckt* oder

wird *entdeckt* durch Hersteller, Benutzer, Betreiber oder Dritte. Schwachstellen des Produkts können bei jedem Einsatz auftreten, während aus der Verwendung entstehende Schwachstellen Einzelfälle, aber auch typisch für ein Produkt sein können.[16]

Wird die Schwachstelle beim Hersteller entdeckt, wird er sie einerseits entfernen, andererseits seine Kunden (sofern er sie kennt) über Existenz der Schwachstelle und Möglichkeiten der Entfernung informieren (sog. *Upgrade*, *Patch* bei Software, oder allg. *Workaround*, *Nachtrag*, *Fehlerbehebung*, *Nachbesserung*). Kennt er seine eigenen Kunden nicht, wird er sich an öffentliche Zertifizierungsstellen oder andere Institutionen wenden (bei Software sind dies v.a. die Computer Emergency Response Teams (CERT), allg. Interessenverbände, Vereine und die staatliche Exekutive), welche die Schwachstelle allgemein beschreiben und die Betreiber öffentlich zur Entfernung gemäss Anleitung des Herstellers auffordern.

Wird die Schwachstelle durch einen Betreiber entdeckt, wird er sich mit dem Hersteller und / oder anderen Betreibern in Verbindung setzen, um herauszufinden, ob die Schwachstelle durch seinen spezifischen Einsatz entstand (Einzelfall), typisch für den Einsatz des Produkts ist oder im Produkt selbst begründet liegt. Akzeptiert der Hersteller die Existenz der Schwachstelle, wird er das bereits beschriebene Vorgehen auslösen.

Wird die Schwachstelle durch einen Benutzer entdeckt, wird er die Schwachstelle entweder ignorieren, die Behebung der Schwachstelle forcieren oder sie für einen Angriff (eine böswillig motivierte Bedrohung) nutzen. Zur Behebung setzt er sich mit dem Betreiber und / oder anderen Benutzern in Verbindung und dann das bereits beschriebene Vorgehen auslösen. Möchte er die Schwachstelle für einen Angriff nutzen, wird er die Entdeckung geheim halten.

Wird die Schwachstelle durch einen Dritten entdeckt, kann er sich prinzipiell wie ein Benutzer verhalten. Er wird jedoch in der Regel nicht zufällig auf die Schwachstelle stossen, sondern (in Abhängigkeit seiner Informationsquellen) mehr oder weniger gezielt danach gesucht haben. Er kann die Existenz und Nutzung der Schwachstelle geheim halten, sie selbst nutzen (das System angreifen und so z.B. zum „Hacker“ werden) oder sie mit anderen Gleichgesinnten austauschen und auf diese Weise zur Verbreitung der Information (z.B. „in Hackerkreisen“) beitragen. Auf diese Weise können viele Angriffe stattfinden, bevor die Schwachstelle dem Betreiber oder Hersteller bekannt wird. Nach einiger Zeit wird die Information über die Schwachstelle den Hersteller erreichen, z.B. indem Verbindungen zwischen den „Hackerkreisen“ und dem Hersteller bestehen (z.B. könnte ein Mitarbeiter des

---

16 Im Vordergrund dieser Betrachtung stehen Softwareprodukte für den Einsatz auf vernetzten IT-Systemen. Die Argumentation gilt aber analog für jedes komplexe System: Auch eine Personenschleuse für die Zutrittskontrolle, ein Auffangbecken für Löschwasser bei Chemieunfällen etc. können als (Sicherheits-)Systeme bezeichnet werden und Schwachstellen aufweisen.

Herstellers auf einer Mailing-List der Hacker eingeschrieben sein), oder indem Angriffe entdeckt und die Schwachstelle identifiziert wird, auf der sie beruhen.

Als Typisierungskriterien für Schwachstellen ergeben sich demnach

- *Art* der Schwachstelle: produktbezogen, produkteinsatzbezogen („produkttypisch"), einsatzbezogen (Einzelfall),
- *Entdeckung* der Schwachstelle: durch Benutzer, durch Hersteller, durch Betreiber, durch Dritte,
- *Verbreitung* der Information über die Schwachstelle (mehrere möglich): in Fachkreisen und Interessengruppen (z.B.„Hackerkreisen"), durch den Hersteller, durch Benutzer, durch Betreiber, durch öffentliche Stellen.

Quantitativ kann (idealerweise) angegeben werden, wieviel Zeit zwischen Entdeckung und Bereitstellung eines Patches verstrich, wieviel Zeit zwischen Bereitstellung des Patches und Entfernen der Schwachstelle verstrich und wie oft die Schwachstelle für Angriffe genutzt wurde. Die praktische Feststellung der quantitativen Werte ist jedoch fast unmöglich, und auch der Nachvollzug der Entdeckung und Benutzung ist nur in Einzelfällen möglich.

Wird ein Schaden ausgelöst, so beschränkt er sich oft nicht nur auf das System[17] mit der Schwachstelle (sei es aufgrund eines Angriffes oder durch eine andere Ursache). Folgeschäden entstehen, weil einerseits Systeme voneinander abhängig sind und andererseits, weil die nachfolgenden Systeme gegenüber den betroffenen Systemen oft nicht so gut abgesichert sind, wie die Systeme an der „Aussengrenze" der Unternehmung. Die Bestimmung von möglichen Folgeschäden ist nur durch Analyse der gegenseitigen Systemabhängigkeiten möglich; sie können teilweise durch Simulation entdeckt werden. Die Senkung der Penetrationsgeschwindigkeit (die Fortpflanzungsgeschwindigkeit der Folgeschäden) kann durch die Verwendung von Sicherheitszonen erreicht werden.

Typisierung nach Wahrscheinlichkeit und Häufigkeit („wie oft")

Es bestehen verschiedene Ansätze, die Häufigkeit zu bestimmen, mit welcher sich eine Bedrohung manifestiert.

Beispielsweise können Phasen identifiziert werden, in welchen die Bedrohungen eher existieren als in anderen (vgl. auch Typisierung der Häufigkeit), z.B. „Regenzeit", „Hurricane Season" etc. Generell können Bedrohungen kontinuierlich, stossweise (*burst*) oder punktuell auftreten.

Eine oft verwendete Methode ist die statistische Fortschreibung historischer Werte mit dem logischen Schluss von der Vergangenheit auf die Zukunft. Diese Methode

---

17 Der Begriff System bezieht sich hier nicht nur auf technische Informationssysteme, sondern auf jedes Instrument, welches die Informationsverarbeitung in der Unternehmung unterstützt.

kann nur angewendet werden, wenn verlässliche Informationen über vergangene Vorkommnisse bestehen. Dies ist gerade in der Informationssicherheit selten der Fall. Ausserdem impliziert sie Kontinuität.

Wenn schon Annahmen über Häufigkeiten bestehen, können diese durch Berücksichtigung aktueller Umgebungsfaktoren modifiziert werden. Beispiele sind Zustand und Tendenzen von Wirtschaft und Börse, Stimmungen der Bevölkerung etc. aber auch chaotische Faktoren wie z.B. die aktuelle Wetterlage.

Häufigkeiten von Bedrohungen hängen vom Verhalten der Urheber ab. Wenn beispielsweise Hacker bevorzugt nachts aktiv sind, ist zu dieser Zeit die Wahrscheinlichkeit von Angriffen höher. Während der Arbeitszeit kommt es häufiger zu Problemen der Benutzer als ausserhalb dieser Zeiten, wenn nicht mit den Geräten gearbeitet wird.

Typisierung nach bedrohtem Objekt („was“)

Jede Bedrohung bezieht sich auf die Sicherheit eines Objekts, welches als Teil eines Informationssystems identifizierbar ist. Die Typisierung der Bedrohungen kann entsprechend auf einer Typisierung des Bezugsobjektes geschehen (dieses wird in Kapitel 3 erläutert). So lassen sich Bedrohungen der Information von solchen der Informatik-Infrastruktur oder solchen des sicheren Verhaltens von Personen unterscheiden.

Typisierung nach Schadenhöhe ("wieviel")

Der durch die Bedrohung potentiell entstehende Schaden kann quantitativ oder qualitativ bestimmt werden (vgl. Grad des Schadens). Für die quantitative Bestimmung eines G1-Schadens können die betriebswirtschaftlichen Bewertungsgrundsätze verwendet werden, welche beispielsweise im Management Accounting Anwendung finden (Neuwert, Zeitwert, Wiederbeschaffungswert etc.). Die quantitative Bestimmung von G2- und G3-Schäden ist in den seltensten Fällen möglich. Gerade die Höhe von G2- und G3-Schäden hängt in hohem Masse vom betroffenen Objekt und der Bedrohung ab, welche zum Schaden führte.

Typisierung nach Grundbedrohung

Eine Typisierung nach Grundbedrohung (vgl. Liste der Grundbedrohungen in Abschnitt 2.3) ist ebenfalls möglich. Dabei wird betrachtet, ob eine konkrete Bedrohung zu einem Verlust von Vertraulichkeit, Verfügbarkeit, Verbindlichkeit oder einer anderen Anforderung an das betroffene Objekt führt.

Szenarien

Die oben genannten Typisierungen der Bedrohungen können einerseits verwendet werden, um eine manifestierte Bedrohung (also einen Schaden und seine Entstehung) nachträglich zu analysieren.

Ebenfalls möglich ist die Verwendung zur vorgängigen Analyse. Dieser Vorgang, *Bedrohungsanalyse* (*threat analysis*) genannt, dient der Zusammenstellung mehrerer Bedrohungen zu einem *Szenario*. Dieses Szenario drückt eine bestimmte Bedrohungssituation aus, in welcher sich eine Unternehmung befinden kann. Mehrere solche Szenarien können erarbeitet und als Basis einer *Risikoanalyse* (vgl. Kapitel 6) verwendet werden. Sie dienen ebenfalls als Grundlage für das Krisenmanagement.

Fazit

Die Typisierung von Bedrohungen dient der nachträglichen Analyse von entstandenen Schäden oder der vorgängigen Zusammenstellung von Szenarien, welche als Basis für eine Risikoanalyse verwendet werden können. Typisierungen nach Urheber, Motivation, Tätigkeit, Häufigkeit, betroffenem Objekt, Schadenhöhe und Grundbedrohung wurden erläutert, weitere sind denkbar. Insbesondere bei der Betrachtung von Tätigkeit und Häufigkeit können vertiefte Angaben über das bedrohte System notwendig sein, um die Typisierung korrekt vornehmen zu können.

2.5 Informationssicherheit

Der Begriff Informationssicherheit lässt sich rein sprachlich auf die *Sicherheit* von *Information* zurückführen.

Information (im weiteren Sinne) ist ein Oberbegriff für die Begriffe Wissen, Daten, Nachrichten und Information (im engeren Sinne). Der Informationsbegriff ist überladen und kann sich auch auf Medien beziehen (beispielsweise enthalten eine Fernsehnachrichtensendung oder eine Zeitung Information). *Sicherheit* ist ein Zustand, in welchem ein Objekt sich genau so verhält, wie ein Betrachter es erwartet. Die Sicherheit eines Objekts wird über die Erfüllung von Anforderungen beurteilt.

> Def.: Informationssicherheit *ist derjenige Zustand von Information, in welchem sie alle Anforderungen erfüllt, welche eine beurteilende Person an sie stellt.*

Informationssicherheit wird oft mit *Sicherheit der Informationstechnik (IT-Sicherheit)* gleichgesetzt. Dies kann einerseits darauf zurückgeführt werden, dass durch den verbreiteten Einsatz von Informationstechnologie neue Risiken

geschaffen wurden, die es zu betrachten gilt. Andererseits bietet sich das *deterministische Verhalten* von informationstechnologischen Systemen an, um nachvollziehbare sicherheitserhöhende Verfahren und Massnahmen vorzuschlagen. Im Gegensatz zu personen- oder organisationsbasierten Systemen, welche sich nicht deterministisch verhalten, ist bei technischen Systemen also eine direktere Kontrolle der Einflussnahme möglich. Dabei gerät allerdings in den Hintergrund, dass Sicherheit nicht durch die Technik definiert wird, sondern als Anforderung von den Benutzern des Informationssystems gestellt wird und im unternehmerischen Umfeld betriebswirtschaftlichen Charakter hat. Informationssicherheit und IT-Sicherheit beziehen sich also auf unterschiedliche Objekte.

Informationssicherheit wird üblicherweise in einem gesellschaftlichen oder wirtschaftlichen Kontext betrachtet. Hier wird für die Informationssicherheit die Unternehmung als informationsverarbeitende Organisation betrachtet. In diesem Umfeld ist Informationssicherheit ein wünschbarer Zustand der Information, der nicht vollständig erreicht werden kann. Das Fachgebiet oder die Aufgabe der Informationssicherheit umfasst deshalb alle Grundlagen, Ziele, Massnahmen und Mittel zur Sicherung der unternehmerischen Ressource Information, d.h. zur Erreichung dieses Zustands. Informationssicherheit wird damit zum Prozess. *Informationsschutz* umfasst alle konkreten Tätigkeiten (also die Umsetzung von Massnahmen) zur Erreichung von Informationssicherheit.

Es können drei Aspekte des Begriffs Informationssicherheit unterschieden werden:

- Informationssicherheit als sicherer *Zustand* eines Informationsobjekts (erster Aspekt) entspricht der obigen Definition und stellt das *Ziel* dar, welches die Unternehmung anstrebt,
- Informationssicherheit als *Prozess* zur Erreichung dieses Zustands (zweiter Aspekt), und die Durchführung dieses Prozesses bezogen auf ein konkretes Objekt werden *Management der Informationssicherheit* genannt, und
- Informationssicherheit als Aufgabe (dritter Aspekt) umfasst die gesamten *Inhalte* der Informationssicherheit: Motivation, Fachgebiete und Beeinflussung des Bezugsobjekts.

Eine entsprechende Erweiterung der oben angegebenen Definition von Informationssicherheit ist möglich, wird hier jedoch ausgelassen, um Missverständnissen vorzubeugen.

Wirtschaftsinformatik und Informationsmanagement

Wirtschaftsinformatik befasst sich mit der Anwendung der Informatik im Unternehmen, insbesondere mit den Problemen der betrieblichen Informationsverarbeitung. *Informationsmanagement* beschäftigt sich mit den Führungsaspekten im Zusammenhang mit dem Einsatz von Informations-

technologie in Wirtschaft und Verwaltung und ist Teil der Wirtschaftsinformatik. Informationsmanagement ist eine der Aufgaben der Unternehmensführung und umfasst alle Aktivitäten, um Information als Ressource der Unternehmung zu planen, zu organisieren zu steuern [vgl. Earl89, S.24] und zu mehren.

Die Beziehungen zwischen den drei Elementen Mensch, Technik und Aufgabe des Informationssystems stellen, zusammen mit den Methoden und Werkzeugen zur (Re-) Konstruktion von Mensch-Technik-Aufgabe-Systemen, die vier Gegenstände der Wirtschaftsinformatik dar [vgl. Heinrich93, S. 14]. '*Folglich sind für die Wirtschaftsinformatik Informationssysteme primär im Sinn* dynamischer Systeme *von Interesse; das Hauptaugenmerk richtet sich auf das, was im Beziehungszusammenhang zwischen den Komponenten dieser Systeme geschieht [...].*' [Heinrich93, S. 14]. Sekundär müssen natürlich auch die drei Komponenten selbst betrachtet werden[18]. Heinrich äussert sich nicht gesamthaft über die Inhalte der Beziehungen. Auf Basis seiner Grundlegung [Heinrich93] kann jedoch gesagt werden:

- Die Beziehungen zwischen Mensch und Aufgabe in Heinrichs Informationssystem umfassen die An- und Verwendung der Methoden und Werkzeuge auf die Aufgabenlösung der Menschen im Feld der sich stellenden Probleme.
- Die Beziehungen zwischen Aufgabe und Technik umfassen die An- und Verwendung der Methoden und Werkzeuge beim Einsatz von Informations- und Kommunikationstechnologie zur Lösung der bestehenden Aufgaben sowie die Kombination derartiger Technologien zur Informations- und Kommunikationsinfrastruktur (IuK-Infrastruktur) der Unternehmung.
- Die Mensch-Technik-Beziehungen umfassen den Umgang der Personen mit der IuK-Infrastruktur und umfassen die gesamte technikgestützte Kommunikation zwischen Personen in der Unternehmung und über ihre Grenzen.

Informationssicherheit und Informationsmanagement

Informationssicherheit ist ein Teilgebiet der Wirtschaftsinformatik [vgl. Heinrich93, S. 201]. Sie wird von Heinrich im Rahmen seines Zielsystems für Informationssysteme betrachtet. Neben Zielen der Prozessqualität definiert er auch Ziele der Produktqualität, von denen Sicherheit eines ist. Es *„beschreibt die Eigenschaft eines Informationssystems, die Entstehung von Gefährdungszuständen vermeiden zu können. Primäre Einflussgrössen der Sicherheit sind Wirksamkeit, Verfügbarkeit und Vertraulichkeit.“* [Heinrich95, S. 201].

---

[18] '*Diese Komponenten allein sind aber nicht Gegenstand der Wirtschaftsinformatik.*' [Heinrich93, S. 14].

Das *Management der Informationssicherheit* umfasst alle Tätigkeiten, welche zur Erreichung dieses Ziels notwendig sind. Es ist also Teil der Informationssicherheit und ein Teil des Informationsmanagements.

Das Management der Informationssicherheit liegt im Interesse der Unternehmung: Wenn Teile des Informationssystems – also Informationen, die Informationsverarbeitung oder die informationsverarbeitenden Personen – durch eine Störung beeinträchtigt werden, hat das in *erster* Linie negative Auswirkungen auf die Zielerreichung der Unternehmung, beispielsweise auf die Effizienz. Wenn die Effizienz allerdings sinkt, gefährdet dies die Erreichung anderer betrieblicher Ziele, etwa der Gewinnmaximierung. In *zweiter* Linie erzeugt eine einzelne Störung in der Regel Folgestörungen. Als Folge der Effizienzmaximierung verfügen betriebliche Informationssysteme in der Regel nicht über redundante Elemente, so dass der Ausfall eines einzelnen Elementes des Informationssystems weitere Elemente beeinträchtigen kann. In *dritter* Linie können die Wirkungen von Ausfällen des betrieblichen Informationssystems über die Unternehmensgrenzen hinaus spürbar sein, so dass die Unternehmung gegen aussen weniger zuverlässig wirkt (Beeinflussung des Goodwill). Dies entspricht der schon zuvor beschriebenen Einleitung in Schäden ersten, zweiten und dritten Grades (vgl. Abschnitt 2.2, Seite 25)

Bezugsobjekt der Informationssicherheit

Heinrich definiert Informationssicherheit als *"Sicherheit der Informationsinfrastruktur"* [Heinrich95, S. 246]. Als Informationsinfrastruktur bezeichnet er *"die Einrichtungen, Mittel und Massnahmen zur Produktion, Verbreitung und Nutzung von Information im Unternehmen (z.B. die technische Infrastruktur)."* [Heinrich95, S.19]. Dies entspricht dem in Kapitel 3 abgegrenzten Bezugsobjekt *Informationssystem* (vgl. Abschnitte 3.2 und 3.3).

Obwohl sich Informationssicherheit rein sprachlich nur auf Information bezieht, so entzieht sich Information direkter Einflussnahme aufgrund ihrer Eigenschaften der Immaterialität, der leichten Kopierbarkeit und Flüchtigkeit etc. Informationssicherheit kann deshalb nur indirekt über die Verarbeitung und die Speicherung von Information erreicht werden. Die Beeinflussung der Informationssicherheit muss also über die Prozesse der Informationsverarbeitung und über die Beziehungen zwischen den Komponenten des Informationssystems stattfinden. Informationssicherheit bezieht sich also direkt auf Informationen und indirekt auf die Personen und Werkzeuge, welche die Informationsverarbeitung durchführen und auf die dabei durchlaufenen Prozesse.

Fazit

Informationssicherheit ist ein Teil des Informationsmanagement. Es umfasst einerseits die konkreten *Zielsetzungen*, welche als *Anforderungen* an das

Informationssystem der Unternehmung gestellt werden müssen und gemeinsam die Forderung nach *sicherer* Informationsverarbeitung darstellen. Andererseits umfasst Informationssicherheit die Vorgehensweisen und Tätigkeiten, welche zur Erreichung dieses Ziels führen: das *Management der Informationssicherheit*.

Informationssicherheit umfasst zunächst *alle* Sicherheitsaspekte des Informationsmanagements. Da jedoch völlig unterschiedliche Anforderungen an das Informationsmanagement und die Informationsverarbeitung gestellt werden können, und da sehr viele unterschiedliche Tätigkeiten der unternehmerischen Informationsverarbeitung bestehen, entstehen sehr vielfältige und breit gestreute Aufgaben der Informationssicherheit.

Es ist eine Frage der konkreten Ausgestaltung der Informationssicherheit in einer Unternehmung, wieviele dieser einzelnen Aufgaben unter dem Begriff Informationssicherheit verstanden werden sollen. Einige Aufgaben werden in Unternehmungen von dedizierten Stellen wahrgenommen, z.B. die Sicherstellung der gewünschten Wirkung der von der Unternehmung an die Öffentlichkeit abgegebenen Informationen (Öffentlichkeitsarbeit) oder die Sicherheit der Informationsanteile an den Produkten (Produktsicherheit). Das Management der Informationssicherheit muss deshalb einerseits eine Zusammenarbeit mit diesen Stellen anstreben und andererseits ihren Aufgabenbereich in der Praxis von den Tätigkeiten dieser einzelnen Teilfunktionen der Unternehmung abgrenzen.

Unternehmerisches Sicherheitsmanagement ist ebenfalls eine der Aufgaben der Unternehmensführung und umfasst den Schutz aller Ressourcen der Unternehmung gegen Störungen aller Art. Es bezieht sich auf die Unternehmung als Ganzes sowie auf die Infrastruktur und das Produktionssystems (gemäss Unterteilung in Kapitel 3). Da jedoch auch das Informationssystem Teil der Unternehmung ist, ist das Management der Informationssicherheit deshalb auch Teil des Sicherheitsmanagements.

2.6 Unternehmerische Führung

Die unternehmerische Führung wird hier näher erläutert, um die Basis und Referenz für den Aufbau des ISi-Management-Prozesses zu definieren.

2.6.1 Führungskonzeption

Jede Unternehmung verfolgt Ziele, welche vom obersten Management im Interesse der Eigentümer der Unternehmung festgelegt werden. Die Steuerung der Zielerreichung wird von Rühli *Führung* oder *Management* genannt. Rühli hat im

Zürcher Ansatz[19] die Führung strukturiert und erfasst mit seinem Führungsmodell „das ganze Führungsgeschehen unter den Stichworten gemäss [Abbildung 2-6]“ [Rühli91a, S. 15]. Er spricht dabei von einer *Führungskonzeption*, also einem *generischen Konzept* der Führung, welches eine formelle und eine inhaltliche (materielle) Seite umfasst und sich noch nicht konkret auf die Zielerreichung einer Unternehmung bezieht.

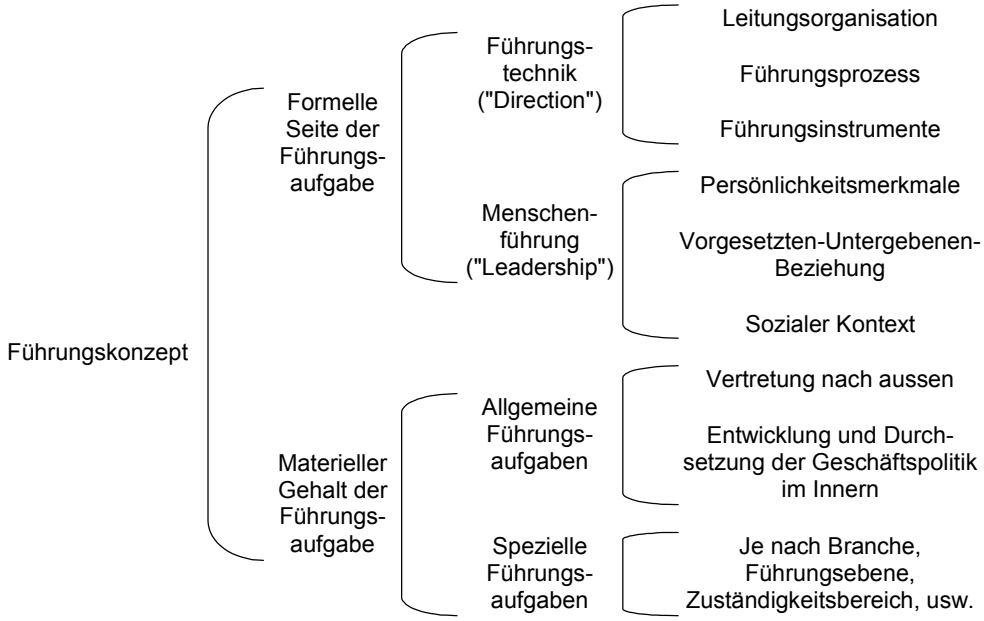


Abbildung 2-6: Dimensionen einer Führungskonzeption [Rühli91a, S. 16, Abb. 1]

Die formelle Seite der Führung umfasst einerseits die Führungstechnik, d.h. die Institutionen (Leitungsorganisation), die Vorgehensweisen und Verfahren (Führungsprozesse) und die Mittel und Massnahmen (Führungsinstrumente). Die Führungsprozesse werden zusätzlich als *Elemente der Führung* und Ablauf von Willensbildung (Planung und Entscheidung) und Willensdurchsetzung (Umsetzung und Kontrolle), beschrieben und mit dem Akronym PEAK bezeichnet. Dabei können jeder PEAK-Phase die *Aspekte der Führung: Institutionen, Funktionen, Instrumente (IFI)* zugeordnet werden, was zu einer Matrix mit zwölf Elementen führt (Planungsinstitutionen[20] bis Kontrollinstrumente) (vgl. Tabelle 2-1).

---

19 Der *Zürcher Ansatz* wurde unter anderem in den Publikationen [Rühli85], [Rühli88], [Rühli91], [Sauter92a], [Rühli93a], [Rühli95] sowie einigen Bänden von [Rühli71] dokumentiert und weiterentwickelt. Er wird hier auch als *Zürcher Managementansatz* oder *Zürcher Führungsansatz* bezeichnet.

20 Die Begriffe *Institution* und *Instanz* werden synonym verwendet.

Aspekte	Elemente der Führung			
	Willensbildung		Willensdurchsetzung	
	Planung	Entscheidung	Anordnung	Kontrolle
Institutionell	Planungs-instanzen	Entscheidungs-instanzen	Anordnungs-instanzen	Kontroll-instanzen
Funktionell	Planungs-prozesse	Entscheidungs-prozesse	Anordnungs-prozesse	Kontroll-prozesse
Instrumental	Planungs-instrumente	Entscheidungs-instrumente	Anordnungs-instrumente	Kontroll-instrumente

Tabelle 2-1: Elemente und Aspekte der Führung [Rühli85, S. 28]

Andererseits beschreibt Rühli die *Menschenführung*, wobei er zwischen Persönlichkeitsmerkmalen (individualistischer Aspekt), Vorgesetzten-Untergebenen-Verhältnis (dualistischer Aspekt) und sozialem Kontext unterscheidet. Gesamthaft wird dies auch als Steuerung der unternehmerischen Kultur bezeichnet.

Auf der materiellen (inhaltlichen) Seite der Führung spricht Rühli von allgemeinen Führungsaufgaben, welche die Vertretung nach aussen und die Entwicklung und Durchsetzung der Geschäftspolitik im Innern umfassen, und von speziellen, branchen- und ebenenabhängigen Führungsaufgaben.

2.6.2 Strategisches Führungskonzept

Rühli wendet diese allgemeine Führungskonzeption auf das spezielle Feld der strategischen Unternehmungsführung an. Dies bedeutet die Einführung einer Unterscheidung von strategischer, taktischer und operativer Ebene. Die strategische Ebene zeichnet sich durch langfristig orientierte, umfassende und hochaggregierte Inhalte aus. Dies weicht einer weniger hohen Aggregierung, höheren Detailtreue und kürzerfristigen Orientierung auf taktischer und v.a. operativer Ebene.

Die Begriffe Unternehmungsstrategie und Unternehmungspolitik umfassen die *„Massnahmenbündel zur Erreichung der Unternehmensziele“* [Rühli91, S. 19] und weisen dabei die konstitutiven Elemente *Grundlagen, Ziele*, *Massnahmen* und *Mittel (Ressourcen)* [Rühli85, S. 35] auf.

Gesamthaft stellt sich das daraus abgeleitete strategische Führungskonzept gemäss Abbildung 2-7 dar.

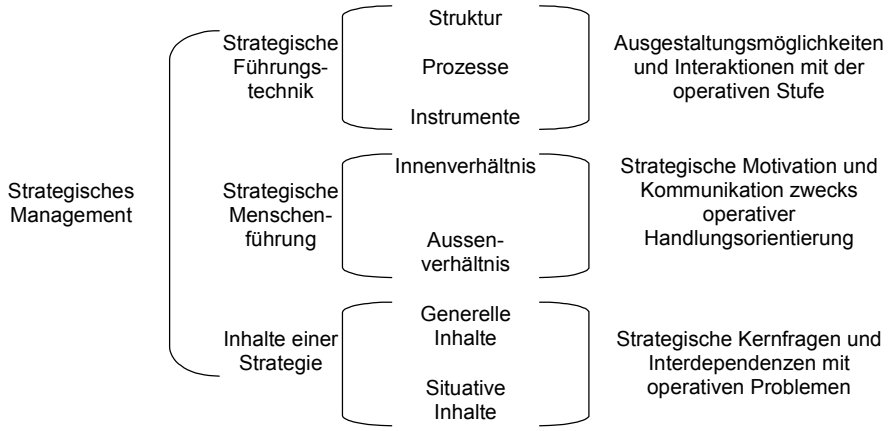


Abbildung 2-7: Dimensionen eines strategischen Führungskonzeptes [Rühli91a, S. 24]

2.6.3 Phasen der strategischen Führung

Varianten und Aufbau

Rühli identifiziert vier Varianten der strategischen Führung [Rühli91a, S. 26f]:

- Enge Koppelung von strategischem und operativem Management
- Punktuelle strategische Führung
- Verzicht auf formalisierte strategische Führungsprozesse
- Institutionalisierung eines besonderen strategischen Führungsprozesses.

Für eine generische und formalisierte Betrachtung, wie sie hier angestrebt wird, eignet sich nur der letzte Fall. Dabei werden folgende Phasen durchlaufen:

1. Strategische Planung	• Strategische Bewusstseinsbildung • Erfassung der strategischen Lage • Strategische Lagebeurteilung • Erarbeitung strategischer Optionen
2. Strategischer Entscheid	• Wahl der gültigen Strategie
3. Strategiedurchsetzung	• Umsetzung der Strategie in operatives und taktisches Handeln • Überprüfung der Markt- bzw. Umweltkonformität
4. Strategisches Controlling	• Realisierungskontrolle

Tabelle 2-2: Phasen der strategischen Führung [Rühli91a, S. 27]

Diese vier Phasen können auch als Führungskreislauf mit den vier Phasen *Planung*, *Entscheidung*, *Anordnung* und *Kontrolle* bezeichnet werden [Rühli85, S. 27]. Eine ähnliche Darstellung findet sich auch bei Ulrich (*Entscheiden, In Gang setzen, Kontrollieren* [Ulrich90, S. 15, Abb. 3]) oder bei Venables (*Defining objectives, planning the activities necessary to achieve the objectives, organising resources and*

directing performance, monitoring results, regulating by reviewing and adjusting plans or directives [Venables91, S. 11]).

Ablauf

Ausgangspunkt jedes strategischen Führungsprozesses sind die *Ziele*, welche als Teil der *Unternehmungspolitik* vorgegeben wurden. Zur Umsetzung dieser Ziele müssen die vorhandenen *Mittel* (*Ressourcen*) möglichst effizient im Rahmen von *Massnahmen (measures, controls)* eingesetzt werden. Dazu stehen in der Regel verschiedene Möglichkeiten zur Verfügung, welche in einer *Planungsphase* einander gegenübergestellt werden, und aus denen das Management eine durch *Entscheidung* auswählt.

Die *Umsetzung* dieser Entscheidung wird sodann *angeordnet*, und löst ihrerseits Entscheidungs- und Umsetzungsprozesse auf den untergeordneten Ebenen des Managements aus. Diese Anordnungsphase umfasst hauptsächlich die Mitteilung der Entscheidung über die Mittelverwendung an die davon Betroffenen. Sie ist v.a. von den vielfältigen Faktoren menschlicher Motivation geprägt und führt letztendlich dazu, dass die Betroffenen denjenigen Teil der Unternehmung, der ihrem Einfluss unterliegt, im Sinne der Entscheidung steuern (und dabei kontrollieren), um diese Entscheidung umzusetzen. In diesen untergeordneten Prozessen werden die Anordnungen dazu konkretisiert und so aus strategischen zunehmend taktische und operative Prozesse geformt. Gesamthaft dienen die auf allen Ebenen angewendeten Massnahmen der Zielerreichung und können als *Umsetzung* oder *Durchführung* bezeichnet werden. Die Durchführung als Teilphase des Führungsprozesses ist also einfach eine Wiederholung des Führungsprozesses auf untergeordneter Stufe mit (üblicherweise) geringerer Betrachtungsbreite und höherer Betrachtungstiefe.

Schliesslich dient die *Kontrollphase* dazu, die Zielerreichung zu überprüfen und Rückmeldungen über den Erfolg der ersten drei Phasen zu erlangen. Es wird also *geprüft*, ob das angestrebte Ziel erreicht wurde, und welche Korrekturen allenfalls vorzunehmen sind.

Gesamthaft identifiziert Rühli die Gliederungsmöglichkeiten der Führung gemäss Abbildung 2-8. Dazu sei bemerkt, dass hier ein Obermenge der von Rühli im Laufe seiner Arbeiten entwickelten Strukturierungsmerkmale gebildet wird, welche die Entwicklung von Rühlis Arbeit nicht berücksichtigt. Es ist selbstverständlich nicht adäquat, die komplexe Struktur des Zürcher Führungsansatzes nur als einfache hierarchische Liste zu begreifen. Für diesen Text besteht jedoch lediglich Interesse an den Strukturierungsmöglichkeiten der Führung, deshalb ist diese Reduktion hier angemessen.

Gliederung der Führungskonzeption

- **Inhaltliche Aspekte**:
  Führungsinhalte und materieller Gehalt der Führungsaufgabe (formuliert in der Unternehmungspolitik oder als Unternehmungsstrategie)
  - **konstitutive Elemente**
    - Grundlagen
    - Ziele
    - Massnahmen
    - Mittel
  - **Aufgabenorientierte Betrachtung**
    - Allgemeine Aufgaben / Generelle Inhalte
      - Vertretung nach aussen, Beziehungen zu externen Stakeholdern
      - Entwicklung und Durchsetzung der Geschäftspolitik nach innen
    - Spezielle Aufgaben / Situative Inhalte
      - Abhängig von der Branche, Führungsebene, Zuständigkeitsbereich, etc.
- **Formelle Aspekte:**
  - **Führungstechnik** („Direction“)
    - Elemente der Führung (PEAK): **Führungsprozess** mit
      - Willensbildung (Planung, Entscheidung) und
      - Willensdurchsetzung (Anordnung, Durchführung, Kontrolle)
    - **Aspekte der Führung** (IFI):
      - Institutionen (Instanzen, Strukturen, Aufbauorganisation)
      - Funktionen (formell definierte Abläufe, Aufgaben, Tätigkeiten, Vorgehensweisen)
      - Instrumente (Mittel, Werkzeuge, Technologien)
  - **Menschenführung** („Leadership“), Strategische Motivation und Kommunikation
    - Personen- und gruppenbezogene Betrachtung
      - Individualistischer Aspekt, Persönlichkeitsmerkmale
      - Dualistischer Aspekt, Beziehung zwischen Vorgesetzten und Untergebenen
      - Sozialer Aspekt, Beziehungen von Personen in Gruppen
    - Innen- / Aussenbetrachtung
      - Innenverhältnis der Unternehmung
      - Aussenverhältnis der Unternehmung
- **Perspektiven** / Betrachtungslinsen:
  - Strategie: Übergeordnetes Vorgehen zur Zielerreichung
  - Struktur: Aufbau der Organisation und Ablauf der unternehmerischen Prozesse
  - Kultur: Werte, Normen, Wissensbestände und Verhalten der Mitarbeiter und Stakeholder
- **Betrachtungsebenen**:
  - Strategische Ebene
  - Taktische Ebene
  - Operative Ebene

Abbildung 2-8: Gliederung der Führungskonzeption

2.6.4 Aspekte der Führung

Führung bezieht sich in ihrer Anwendung auf eine Unternehmung, in welcher die oben genannten Elemente der Führung identifiziert werden können. Im folgenden soll kurz die Struktur einer typischen Unternehmung (Aktiengesellschaft nach

schweizerischem Obligationenrecht) skizziert werden[21], um das Bezugsobjekt für diesen Text festzulegen:

Institutionen

Eine Unternehmung ist als Ganzes Eigentum einer Personengruppe (Aktionäre), welche Kapital zur Verfügung stellt und die Ziele der unternehmerischen Tätigkeit definiert. Diese Personengruppe stellt gesamthaft das oberste Organ der Unternehmung dar, die *Generalversammlung (D: Hauptversammlung, E[22]: General Meeting (of Shareholders))*.

Die Generalversammlung (GV) bestellt ein Gremium (einen Ausschuss), welches die oberste Überwachung der Unternehmung wahrnimmt und *Verwaltungsrat (D: Aufsichtsrat, E: Board)* genannt wird. Dieses wählt einen *Vorsitzenden (D: Aufsichtsratsvorsitzender, E: Chief of the Board)*.

Die GV bestellt ausserdem (aufgrund gesetzlicher Anforderungen) eine *externe Revisionsstelle* (*D: Externe Prüfstelle, E: External Auditor*), welche die Ordnungsmässigkeit der Geschäftsführung zyklisch überprüft und der GV darüber Bericht erstattet.

Der Verwaltungsrat führt die Unternehmung selbst oder delegiert diese (v.a. bei grossen Unternehmungen) an eine *Geschäftsleitung (D: Vorstand, E: Board of Directors),* welche ihrerseits einen Vorsitzenden wählt (*Vorsitzender der Geschäftsleitung, D: Vorstandsvorsitzender, E: Chief Executive Officer (CEO),* diesem untergeordnet der *Chief Operational Officer (COO)).* Dieses „Top Management" steuert die Unternehmung, um die von den Eigentümern vorgegebenen Ziele zu erreichen.

Zur laufenden Überprüfung der effizienten und effektiven Ressourcenverwendung durch die Geschäftsleitung bestellt der Verwaltungsrat eine *interne Revisionsstelle (D auch: interne Rechnungsprüfungsstelle, E: internal Auditor)*, welche an den Verwaltungsrat Bericht erstattet.

---

21 Die Betrachtung der Struktur einer Aktiengesellschaft nach schweizerischem Obligationenrecht ist hier stellvertretend für alle Unternehmungsformen und wird hier gewählt, weil ihre Kontrollstrukturen sich in der Praxis einheitlich etabliert haben, teilweise gesetzlich festgelegt sind (vgl. auch [Rühli85, S.60ff, S.87ff]) und auch im internationalen Kontext ähnlich bestehen. Die Argumentation lässt sich jedoch auch auf andere Rechtsformen übertragen.

22 Es werden jeweils zusätzlich die Termini für Unternehmungen nach deutschem Recht (D:) sowie die englischsprachigen Termini (E:) angegeben. Die englischsprachigen Termini entsprechen den deutschsprachigen nicht immer genau, da die zugrundeliegenden Rechtsnormen und die darausfolgende Aufteilung der Kompetenzen und Verantwortungen sich je nach Land unterscheidet. "*NOTE: the board of an American company may be made up of a large number of non-executive directors and only one or two executive officers; a British board has more executive directors.*" [PonsWirtsch90, S. 32f]

Das untergeordnete Linienmanagement wird, nach Funktionen getrennt, hierarchisch aufgebaut. Oft steht je ein Mitglied der Geschäftsleitung an der Spitze jeder der übergeordneten unternehmerischen Funktionen. Die Vorgesetzten der einzelnen Bereiche haben jeweils Weisungsbefugnis (Kompetenz) bzw. Verantwortung für ihren Bereich.

Beratende Funktionen werden in *Stäben* organisiert, welche jeweils einzelnen Linienstellen (auch dem Top Management) unterstehen, in sich wieder hierarchisch aufgebaut werden können und ihre Dienstleistung allen der Linienstelle unterstehenden Linien- und Stabsstellen anbieten, jedoch i.d.R. keine Weisungsbefugnis haben.

Funktionen

Unternehmerische Funktionen sind beispielsweise *Einkauf, Verkauf, Marketing, Produktion, Logistik, Personal, Finanzen, Organisation, Informatik, Forschung und Entwicklung*[23]. Die Aufteilung variiert stark. Verschiedene Zuordnungen der Funktionen zu Institutionen sind möglich; üblich sind funktionelle Gliederung der Organisation (d.h. für jede Funktion wird eine eigene Abteilung geschaffen) oder regionale oder produktspezifische Aufteilung. Bei funktioneller Gliederung wird der Leiter des jeweiligen Bereichs mit *Leiter*, *Chef*, *Manager*, *Direktor* bezeichnet, z.B. *Verkaufsleiter*, *Marketingmanager*, im englischen mit *Chief*, *Officer*, *Manager*, *Director*, z.B. *Chief Production Officer*, *Chief Financial Officer*, *Marketing Director*. Auch diese Bezeichnungen variieren stark.

Einzelne Funktionen werden nicht unbedingt dem Linienmanagement zugeteilt, sondern können Stäben zugeteilt werden. Stabsstellen haben in der Regel keine Weisungsbefugnis und beraten die Linienmanager ihres Bereichs auf Anfrage oder bereiten grundsätzliche Entscheidungen vor. Dies betrifft z.B. unternehmerische Sicherheit (mit dem *Chief Safety and Security Officer*, CSO oder CSSO), Risikomanagement, Qualität, Forschung und Entwicklung etc. Eigene Institutionen für diese Funktionen sind meist nur in grossen Unternehmungen zu finden, in kleineren werden diese Funktionen in bestehende integriert.

Instrumente

Der Begriff *Instrument* bezeichnet ein Werkzeug, um Inhalte zu verarbeiten. Die Art der Instrumente unterscheidet sich stark je nach Institution und Funktion. Informationstechnologie ist eines der Werkzeuge der Unternehmung und umfasst verschiedene Teilwerkzeuge, die in den verschiedenen Funktionen durch die Institutionen verwendet werden. Das IT-System als ein wichtiges Instrument der Unternehmung wurde in Kapitel 3 beschrieben.

---

[23] Z.B. gemäss [Ulrich90, S. 111]: *Absatz, Produktion, Forschung und Entwicklung, Personalwesen, Anlagenwirtschaft, Materialwirtschaft, Finanzwesen, Informationswesen.*

2.6.5 Verwendung in dieser Dissertation

Rühli hat im Zürcher Managementansatz viele verschiedene Aspekte der Führung betrachtet und erfasst auf diese Weise unterschiedlichste Einflüsse auf die Führung von Unternehmungen. Die Gliederung der Führung gemäss Abbildung 2-8 (Seite 53) ist eine wichtige Basis für diese Dissertation, denn die Strukturierung folgt der von Rühli vorgegebenen inhaltlichen und formellen Betrachtung. Die hier verwendete, bereits in Abschnitt 1.2 definierte Terminologie beruht in weiten Teilen auf Rühlis Definitionen und auch die in den Abschnitten 1.3 und 3.1 dargestellte Gliederung wurde davon massgeblich beeinflusst. Dennoch ist das Management der Informationssicherheit keine so komplexe Aufgabe wie die Führung einer Gesamtunternehmung, weshalb in dieser Dissertation nicht auf alle Einzelaspekte der Führung eingegangen wird.

Fazit

In diesem Kapitel wurden die der Informationssicherheit zugrundeliegenden Begriffe hergeleitet und definiert. *Information* wurde als Oberbegriff für die vier voneinander abgrenzbaren Aspekte *Wissen, Daten, Nachrichten* und *Verwendung von Information* erklärt und wird im weiteren Text in dieser übergeordneten Bedeutung verwendet. Information ist medienneutral; Informationsverarbeitung ist demnach nicht an informationstechnische Systeme gebunden. Umgangssprachlich ist der Informationsbegriff überladen.

Darauf aufbauend wurden die Begriffe *Dokument* und *Datensatz* als Bezeichnungen für die kleinsten unstrukturierten bzw. strukturierten Informationseinheiten eingeführt, welche im unternehmerischen Umfeld gebräuchlich sind. *Informationssammlungen* sind inhaltliche Kollektionen von Dokumenten und / oder Datensätzen zu demselben Thema. *Datenbanken* sind besondere Informationssammlungen, auf welche mit einem Datenbanksystem mit Selektions- und Sortierungsmöglichkeiten zugegriffen werden kann. Es wurde darauf hingewiesen, dass diese und weitere übliche Begriffe oft Struktur, Inhalt, Übertragungs- oder Speichermedium einer Information bezeichnen und nicht die Information selbst (Bsp.: Auftrag, Fax).

Weiterhin wurde *Sicherheit* als subjektiv wahrgenommener Zustand (Qualität) eines Objekts definiert und in umgekehrte Abhängigkeit zum Begriff Risiko gesetzt: Risiko ist nicht vorhandene Sicherheit. Sicherheit kann ferner in einen Security-Aspekt (Sicherheit des Objekts gegen äussere Einflüsse) und einen Safety-Aspekt (Sicherheit des Objekts gegen Fehler aus dem Objekt selbst) unterteilt werden. Um Sicherheit zu erreichen, müssen Schutz- oder Sicherheitsmassnahmen angewendet werden; Schutz ist die Tätigkeit zur Erreichung von Sicherheit.

Ein Risiko bezeichnet ferner ein möglicherweise eintretendes sicherheitsminderndes Ereignis und kann idealerweise quantitativ oder qualitativ angegeben werden. Die vorhandenen Risiken bilden zusammen das (Gesamt-)Risiko. Ein Risiko besteht aus

den Komponenten *Gefahr, Bedrohung, Schwachstelle, Gefährdung, Wahrscheinlichkeit* und *Schaden (ersten, zweiten, dritten Grades),* welche aufeinander aufbauen. Risiken können nach betroffenem Objekt, nach Aktivität, Urheber, Motivation, Häufigkeit und Höhe des entstehenden Schadens typisiert werden.

Umgangssprachlich ist auch der Sicherheitsbegriff überladen. Es bestehen viele zusammengesetzte Wörter mit "Sicherheit", welche nicht die direkt ableitbare Bedeutung haben (z.B. Arbeitssicherheit).

Die Sicherheit (bzw. das Risiko) eines Objektes bestimmt sich über die Erfüllung von Anforderungen, welche das Individuum an das Objekt stellt. Diese Anforderungen sind idealerweise unabhängig voneinander definiert. Wenn alle von einem Individuum gestellten Anforderungen vollständig erfüllt werden, ist vollständige Sicherheit aus Sicht dieses Individuums gegeben. Als *Grundanforderungen* beschrieben wurden *interne* und *externe Integrität*, *Vertraulichkeit, Verbindlichkeit, Verfügbarkeit, beabsichtigte Verwendung*, *Effektivität, Effizienz, Ordnungsmässigkeit* und *Verlässlichkeit*.

Bedrohungen und Risiken lassen sich typisieren, um eingetretene Schäden zu analysieren oder präventiv Szenarien aufzustellen und so eine Bedrohungsanalyse durchzuführen, welche Basis einer Risikoanalyse sein kann.

Informationssicherheit lässt sich darauf aufbauend als *derjenige Zustand von Information definieren, in welchem sie alle Anforderungen erfüllt, welche eine beurteilende Person an sie stellt*. Informationssicherheit kann als angestrebter Zustand verstanden werden und repräsentiert dann ein Ziel, sie kann als Prozess verstanden werden, welcher alle Tätigkeiten zur Erreichung des Ziels umfasst oder als Aufgabe, womit die Motivation, die Fachgebiete und die Beeinflussung des Bezugsobjektes gemeint sind.

Informationssicherheit ist Teil des Informationsmanagements und bezieht sich auf das unternehmerische Informationssystem. Die allgemeinen Managementgrundlagen zur Führung von Unternehmungen nach dem von Rühli entwickelten Zürcher Managementansatz wurden daran anschliessend kurz vorgestellt. Für diese Dissertation relevant sind die von Rühli vorgenommene Aufteilung in inhaltliche und formelle Betrachtung, die Identifikation von Institutionen, Instrumenten und Funktionen sowie der von ihm beschriebene Führungsprozess in vier Phasen. Diese Elemente sind für die Gliederung des Rahmenwerks der Informationssicherheit in dieser Dissertation grundlegend (vgl. Abschnitte 1.3 sowie 3.1).

USERS. THE VERY WORD IS GUARANTEED TO SEND A CHILL OF ANIMOSITY THROUGH MANY DATA PROCESSING MANAGERS AND ANALYSTS AND A SHIVER OF APATHY DOWN THE SPINES OF MOST DESIGNERS AND PROGRAMMERS. YET, IT IS THE USERS – OR, RATHER, THE BUSINESS OF THE USERS' CORPORATION – THAT KEEP THE DP DEPARTMENT IN BUSINESS. WHY ARE THE RELATIONS BETWEEN USER DEPARTMENTS AND DP DEPARTMENTS SO FRAGILE?

– MEILIR PAGE-JONES,
PRESIDENT, WAYLAND SYSTEMS DEVELOPMENT
IN: PRACTICAL PROJECT MANAGEMENT, S. 1

Teil II: Rahmenwerk der Informationssicherheit

In diesem Teil der Dissertation wird das Rahmenwerk der Informationssicherheit definiert und zu Beginn von Kapitel 3 gesamthaft beschrieben. In einer formellen Betrachtung in Kapitel 3 wird sodann festgelegt, auf welches Objekt sich Informationssicherheit bezieht. Dabei wird zwischen Elementen und Tätigkeiten des Bezugsobjekts unterschieden. In einer inhaltlichen Betrachtung werden dann in Kapitel 4 zunächst die inhaltlichen Elemente der Informationssicherheit beschrieben, um dann in Kapitel 5 die inhaltlichen Tätigkeiten beschreiben zu können. Schliesslich wird in Kapitel 6 der Prozess der Informationssicherheit aus den in den Kapiteln 3 bis 5 betrachteten Elementen und Tätigkeiten integriert und generisch definiert. Eine spezifische Form des Informationssicherheitsprozesses wird dann in Teil III behandelt. Abbildung 1-5 (Seite 17) bietet einen Überblick über diese Aufteilung.

3 Bezugsobjekt

Worauf bezieht sich Informationssicherheit? In welchem Zusammenhang steht sie zur IT-Sicherheit, zur Kommunikationssicherheit, zur Computer- und Netzwerksicherheit, zur unternehmerischen Sicherheit und zu weiteren Sicherheitsfachgebieten?

Die eindeutige Beantwortung dieser Fragen bedingt ein übergreifendes Modell der Informationssicherheit, welches in diesem und den drei folgenden Kapiteln definiert werden soll.

3.1 Rahmenwerk der Informationssicherheit

Das Rahmenwerk der Informationssicherheit, dessen einzelne Elemente in den Kapiteln 3 bis 6 definiert werden, wird in diesem Abschnitt gesamthaft beschrieben. **Dabei wird von der Darstellung in Abbildung 1-5 (Seite 17) ausgegangen**.

Zunächst erfolgt eine statische formelle Betrachtung der Unternehmung, um darauf aufbauend die Informationssicherheit ebenfalls statisch formell zu analysieren. Eine inhaltliche Betrachtung – noch immer mit Ausrichtung auf die statischen Elemente – folgt daran anschliessend. Der Prozess der Informationssicherheit wird abschliessend als dynamisches Element betrachtet.

Statisch-formelle Betrachtung der Unternehmung

Aufbauend auf den Grundlagen der Informationssicherheit gemäss Kapitel 2 wird das unternehmerische Informationssystem als *Bezugsobjekt der Informationssicherheit* festgelegt und zunächst *statisch formell* genauer untersucht (**Kapitel 3**). Es wird hierarchisch in die *Elemente Institutionen, Informationen* und *Instrumente* aufgegliedert. Jedes dieser Elemente wird weiter unterteilt.

Diese Unterteilung ist einerseits die Voraussetzung dafür, dass eindeutige Teil-Bezugsobjekte für die spätere Betrachtung der Informationssicherheit gewählt werden können. Andererseits dient sie der Identifikation der *Management-Tätigkeiten*, welche in diesen Teilelementen des Bezugsobjektes ablaufen, bzw. derjenigen Tätigkeiten, in welchen diese Elemente verwendet werden. (vgl. Abbildung 3-1).

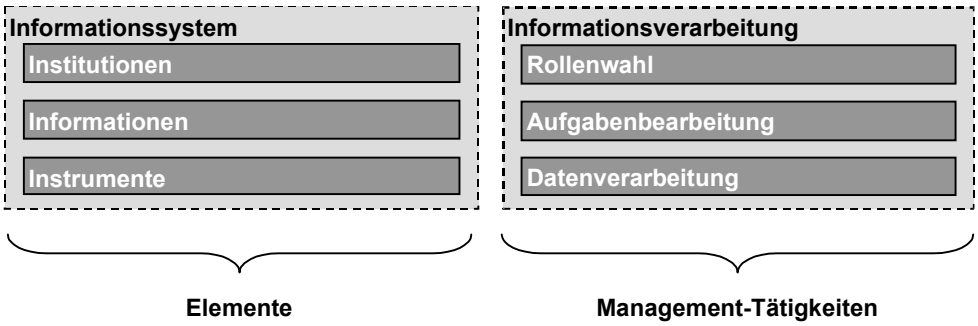


Abbildung 3-1: Formelle Betrachtung der Elemente und Management-Tätigkeiten des Bezugsobjekts

Das Bezugsobjekt der Informationssicherheit umfasst diejenigen Objekte der Unternehmung, deren Sicherheit durch die Informationssicherheit beeinflusst wird. Es wird hier festgelegt, dass Informationssicherheit sich auf das

Informationssystem der Unternehmung bezieht. Dieses Informationssystem wird als derjenige Teil der Unternehmung angenommen, in welchem sämtliche informationsverarbeitenden Prozesse ablaufen und wird anhand der in Kapitel 2 dargelegten Strukturierung in *Institutionen*, *Informationen* und *Instrumente* unterteilt.

Es wird hier streng hierarchisch aus verschiedenen Teilelementen aufgebaut. Beispielsweise lassen sich *IT-System (digitale Instrumente)* und *nicht-digitale Instrumente* unterscheiden. Das IT-System umfasst u.a. *IT-Ressourcen,* welche sich in *IT-Plattformen*, *Anwendungs-* und *Kommunikationssysteme* unterteilen lassen etc.

Die jeweiligen Management-Tätigkeiten, die in diesen Elementen ablaufen, lassen sich ebenso identifizieren. Beispielsweise wird das *IT-System* zur *elektronischen Datenverarbeitung (EDV)* verwendet, die *IT-Ressourcen* werden im *IT-Betrieb* verwendet etc.

Statisch-formelle Betrachtung der Informationssicherheit

Gesamthaft wird die in Abschnitt 2.6 beschriebene formelle Strukturierung der Unternehmung verwendet, um die einzelnen Elemente der *Informationssicherheit* und ihres *Managements* genauer zu betrachten (vgl. Abbildung 3-2). Dazu wird zunächst für jedes Element der Unternehmung derjenige *inhaltliche Fachbereich* definiert, der sich mit der Sicherheit dieses Elementes befasst. Diese inhaltlichen Bereiche bilden die eigentlichen Tätigkeits- und Einflussbereiche der Informationssicherheit, da die darin ablaufenden Aktivitäten das Bezugsobjekt direkt beeinflussen. Beispielsweise bezieht sich *IT-Sicherheit* auf das *IT-System* und die damit durchgeführte *EDV, IT-Betriebssicherheit* auf die *IT-Ressourcen* und den *IT-Betrieb*. So lässt sich Informationssicherheit hierarchisch in ebensolche Elemente unterteilen wie die Unternehmung. Deshalb kann so auch eine eindeutige Unter- / Überordnung der Begriffe der Informationssicherheit erreicht werden.

Die Fachbereiche umfassen die Inhalte, welche im Rahmen des ISi-Managements betrachtet werden sollen. Dabei lässt sich das Management wieder in die drei Elemente Institutionen, Informationen und Instrumente gliedern. Bei den *Institutionen* werden diejenigen Stellen inner- und ausserhalb der Unternehmung identifiziert, welche ein Interesse an der Sicherheit der Informationen haben und die Erreichung dieser Sicherheit vorantreiben. Welcher Natur die dabei verfolgten Ziele sind, wird unter dem Stichwort *Information* betrachtet. Und schliesslich betrachtet der Bereich *Instrumente* die allgemeinen Massnahmengruppen, deren einzelne Bezugsobjekte zuvor bei der Vorstellung der Fachbereiche identifiziert wurden.

Im Gegensatz zur Unternehmung, wo sich durchaus einzelne Management-Tätigkeiten benennen lassen, die sich auf die Elemente der Unternehmung beziehen (z.B. *Geschäftstätigkeit* auf *Unternehmung*), ist dies bei der Informationssicherheit

selbst nicht möglich. Dies zum ersten deshalb, weil Informationssicherheit eine Querschnittsfunktion innerhalb der Unternehmung innehat, Informationssicherheit kein Selbstzweck ist und die Beeinflussung der Unternehmung deshalb im Zentrum steht. Zum Zweiten ist das Management der Informationssicherheit keine so umfassende Aufgabe wie die Führung einer Unternehmung und drittens beruht Informationssicherheitsmanagement darauf, dass seine einzelnen Elemente in die Elemente der Unternehmung integriert sind. In dieser Hinsicht lassen sich die *Fachbereiche* der Sicherheit als die eigentlichen Management-Tätigkeiten der Informationssicherheit auffassen. Ihre Verknüpfung wird deshalb gesamthaft im Rahmen des in Kapitel 6 betrachteten Informationssicherheitsprozesses geschildert.

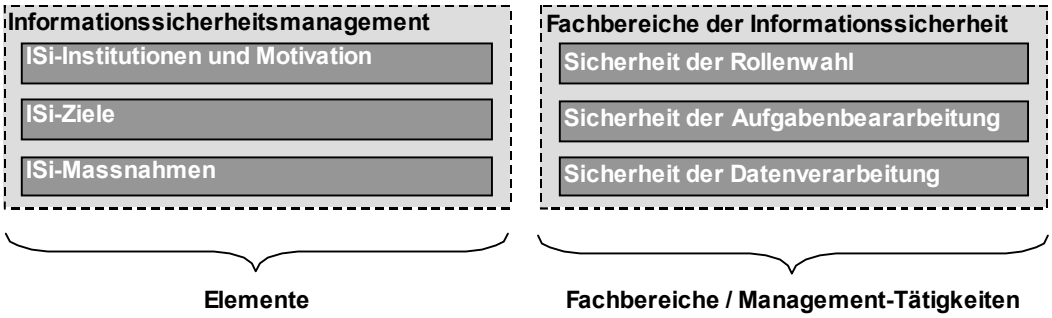


Abbildung 3-2: Formelle Betrachtung der Elemente und Management-Tätigkeiten der Informationssicherheit

Kapitel 3 umfasst also die gesamte formelle Betrachtung der Informationssicherheit und identifiziert dabei insbesondere die in den nachfolgenden Kapiteln zu betrachtenden Inhalte.

Statisch-inhaltliche Betrachtung der Elemente der Informationssicherheit

Kapitel 4 beinhaltet die statische Betrachtung der inhaltlichen Elemente. Auch hier wird wieder zwischen Institutionen, Informationen und Instrumenten unterschieden.

Die *Institutionen* der Informationssicherheit umfassen diejenigen Strukturen (Aufbauorganisation) mit Stellen und Gremien, *deren Aufgabenbereiche Informationssicherheit enthalten*. Dabei stehen die unternehmerischen Kontrollinstitutionen im Vordergrund. Insbesondere werden Controlling und Revision genauer behandelt. Darauf aufbauend werden Gestaltungsvorschläge für die konkrete Ausgestaltung der Informationssicherheitsstrukturen innerhalb der Unternehmung abgegeben. Diese umfassen zum Ersten die Schaffung der dedizierten Stellen für *Informationssicherheitsbeauftragten (ISiBe)* und / oder *Informationssicherheitsverantwortlichen (ISiVA)*. Zum Zweiten werden auch die Aufgaben derjenigen Personen beschrieben, welche sich nur sekundär mit Informationssicherheit beschäftigen, bei deren Tätigkeit Informationssicherheit also nur eine von mehreren Aufgaben darstellt. Zum Dritten wird die Schaffung von Gremien für die Behandlung übergreifender Informationssicherheitsfragen

vorgeschlagen. Zum Vierten wird die Verantwortung der Linienstellen aller Fachbereiche betont und herausgehoben sowie die Verantwortung des Managements beschrieben. Die Institutionen bilden gemeinsam die Organisation der Informationssicherheit.

Die *Informationen* der Informationssicherheit enthalten Ziele und Motivationen der Informationssicherheit. Zunächst werden die *generischen inhaltlichen Ziele* mit Bezug auf die einzelnen Interessengruppen in der Unternehmung betrachtet. Unter dem Aspekt der *Motivation* wird untersucht, welche Gründe eine Unternehmung dazu bewegen, Informationssicherheit zu betrachten und als Ziel zu wählen. Dabei wird von Entwicklungen in Märkten und Gesellschaft und von den allgemeinen unternehmerischen Zielen auf die Ziele der Informationssicherheit geschlossen. Damit wird die Basis für die später zu betrachtende Auslösung des ISi-Prozesses gelegt.

Die *Instrumente* der Informationssicherheit umfassen die Festlegung, welche Elemente des Bezugsobjektes betrachtet werden sollen (Kategorisierung der schützenswerten Objekte) und die Identifikation von Massnahmenbereichen und einzelnen spezifischen Massnahmen. Die Hilfsmittel bei der Durchführung des Informationssicherheitsprozesses werden als *interne Instrumente* der Informationssicherheit beschrieben. Massnahmenbereiche und Massnahmen, welche die *Beeinflussung des Bezugsobjektes* bewirken, werden als *externe Instrumente* der Informationssicherheit definiert.

Statisch-inhaltliche Betrachtung der Tätigkeiten der Informations-sicherheit

Kapitel 5 beinhaltet die statische Betrachtung der inhaltlichen Tätigkeiten (Fachgebiete). Beispielsweise werden hier Idee, Probleme und Lösungen von Qualitätsmanagement, Beratung, Wirtschaftsspionage und -sabotage, Kongruenz, inhaltlicher Daten- und Kommunikationssicherheit, Verschlüsselung, Informatik-Sicherheit, Informatik-Recht, Anwendungssicherheit, Internet-Sicherheit und weiteren Fachgebieten genauer ausgeführt und in den Zusammenhang der Informationssicherheit eingeordnet.

Dynamische Betrachtung

Nach der statischen Betrachtung der Elemente und des Managements erfolgt in **Kapitel 6** eine dynamische Analyse der Prozesse. Dabei werden die *unternehmerischen* Prozesse zunächst generisch dargestellt und, aufbauend auf den in Abschnitt 2.6 beschriebenen Erkenntnissen, in die Phasen Planung, Entscheidung, Anordnung, Umsetzung und Kontrolle unterteilt. Darauf aufbauend wird der Prozess der *Informationssicherheit* allgemein definiert. Der gesamte Führungsprozess der Informationssicherheit wird hier als *Informations-sicherheitsprozess* bezeichnet.

Beim Informationssicherheitsprozess (ISi-Prozess) können drei Problembereiche unterschieden werden:

- die *Organisation* des ISi-Prozesses, also die Anordnung der *Institutionen* innerhalb dieses Prozesses, die Ziele (Informationen) und die zur Verfügung stehenden Werkzeuge (Instrumente),
- die *inhaltlichen Themenbereiche (Fachgebiete)* der Informationssicherheit, welche beim Durchlaufen des ISi-Prozesses behandelt werden müssen und die Beeinflussung des Bezugsobjektes bewirken,
- der *Ablauf* des ISi-Prozesses, welcher die einzelnen Aktivitäten und Phasen in einem Führungskreislauf umfasst und die Untersuchung und Beeinflussung des Betrachtungsobjekts steuert.
    - Besonderes Augenmerk wird dabei auf die *Auslösung* gelegt, also auf diejenigen Ereignisse und Tätigkeiten, welche zur Schaffung und Initiierung des ISi-Prozesses notwendig sind.

Die Auslösung verdient eine spezielle Heraushebung, da vor Beginn des ISi-Prozesses noch keine Institutionen bestehen, welche den Prozess durchlaufen könnten. Der Aspekt *Auslösung* behandelt also die Initialisierungsprobleme des Ablaufs und die Erstellung der Organisation.

Innerhalb dieses *Ablaufs* des Prozesses können verschiedene Ansätze unterschieden werden, wobei die bestehenden Ansätze aus der Literatur beschrieben und zu einem einheitlichen generischen Ablauf zusammengefasst. Dieser besteht aus fünf Phasen:

- In der *Inventur* werden die schützenswerten Informationen inventarisiert. Dabei werden oft auch die Informationssysteme erhoben, welche die Informationen speichern und / oder verarbeiten. Die Erhebung weiterer Objektkategorien ist möglich. Gesamthaft wird von *schützenswerten Informationsobjekten* gesprochen.
- Bei der *Analyse* werden *Werte* der Informationsobjekte festgelegt oder die *Bedrohungen* und *Risiken analysiert*, welche die Sicherheit der Informationsobjekte gewährleisten. Ein *angestrebtes Sicherheitsniveau* oder *Schutzziel* wird festgelegt.
- Danach werden *Massnahmen* ausgewählt und beschlossen, welche die Werte erhalten oder die Risiken senken. Die Massnahmen werden als *Sicherheitsdispositiv* bezeichnet.
- Anschliessend werden diese Massnahmen *umgesetzt*, d.h. die durch die Massnahmen bestimmten Veränderungen der Institutionen, Informationen, Instrumente und Prozesse der Unternehmung werden veranlasst und durchgeführt.
- Abschliessend wird die Umsetzung der Massnahmen *kontrolliert*. Dabei können beispielsweise Wirksamkeit, Angemessenheit und Wirtschaftlichkeit geprüft werden.

Diese fünf Phasen können direkt mit den generischen Führungsphasen Planung, Entscheidung, Anordnung, Umsetzung und Kontrolle in Beziehung gesetzt werden (vgl. Abbildung 3-3).

Verschiedene Ansätze lassen eine Variation v.a. der zweiten und dritten Phase zu:

- Im *Grundschutzansatz* werden für alle inventarisierten Objekte dieselben Massnahmen angewendet.
- Der *Werteansatz* erlaubt die Zuteilung von Werten zu den einzelnen Objekten, aus denen Prioritäten für den Schutz abgeleitet werden können.
- Der *Bedrohungs- und Risikoansatz* betrachtet die bestehenden Bedrohungen und Risiken im Detail und erzeugt sehr spezifische, gut angepasste, aber schnell veraltende Sicherheitsdispositive.
- Der *kombinierte Ansatz* integriert den Grundschutz- mit dem Bedrohungs- und Risikoansatz.
- Der Vollständigkeit halber werden auch *Ad-Hoc-* und *Do-Nothing-Ansatz* beschrieben.

Diese genauere Betrachtung liefert die Basis für die Erstellung eines Beurteilungsschemas, welches in Teil III verwendet werden soll.

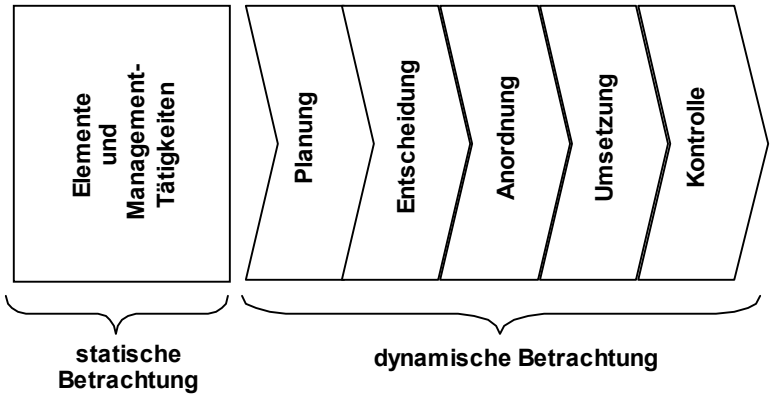


Abbildung 3-3: Statische und dynamische Betrachtung mit generischer Unterteilung der Managementprozesse

Rahmenwerk

Das *Rahmenwerk des Managements der Informationssicherheit* (vgl. Abbildung 3-4) setzt sich aus folgenden Teilen zusammen:

- Elemente und Tätigkeiten (vgl. Abbildung 3-3, linker Teil)
- Informationssicherheitsprozess (vgl. Abbildung 3-3, rechter Teil).

Das *Rahmenwerk der Informationssicherheit* (vgl. Abbildung 3-4) besteht aus

- Grundlagen (vgl. Abbildung 1-4, Seite 16) und

- Rahmenwerk des Managements der Informationssicherheit.

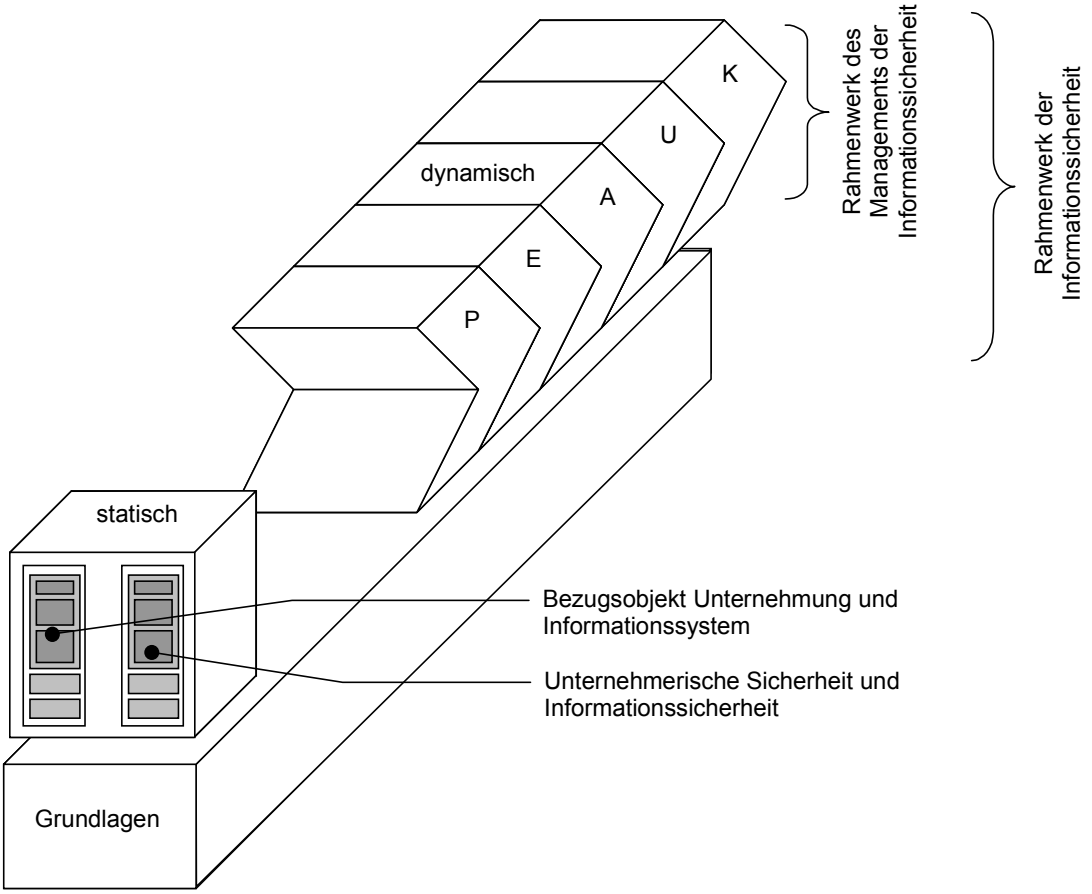


Abbildung 3-4: Rahmenwerk der Informationssicherheit

3.2 Bezugsobjekt der Informationssicherheit

Um klären zu können, in welchem Zusammenhang *Informationssicherheit*, *Kommunikationssicherheit*, *Computer-* und *Netzwerksicherheit*, *unternehmerische Sicherheit* und weitere Begriffe zueinander stehen, genügt eine einfache Betrachtung der wörtlichen Bedeutung nicht, denn es wird nicht sofort klar, in welchem Zusammenhang *Information*, *Kommunikation*, *Computer*, *Netzwerk* und *Unternehmung* stehen. Benötigt wird also ein *Modell des unternehmerischen Informationssystems*, in welches sich diese Elemente einordnen lassen, und welches durch diese Einordnung der Elemente auch die Beziehung der verschiedenen Sicherheitsfachgebiete erkennen lässt. Wenn in diesem Modell also beispielsweise festgelegt wird, dass ein Netzwerk Teil des Informationssystems, und dieses Teil der Unternehmung ist, so ist die Annahme gerechtfertigt, dass Netzwerksicherheit ein Teilgebiet der Informationssicherheit und Informationssicherheit ein Teilgebiet der unternehmerischen Sicherheit ist.

Ziel dieses Kapitels ist es, dieses Modell *top-down* zu entwickeln und dabei die statischen Elemente und Tätigkeiten formell zu identifizieren (vgl. Abschnitt 1.3). Da schon früher festgelegt wurde, dass Informationssicherheit im unternehmerischen Umfeld betrachtet werden soll, wird hier die Unternehmung als übergeordnetes Element festgelegt und versucht, möglichst klar voneinander abgrenzbare Teilelemente zu identifizieren und zu beschreiben. Dieses Vorgehen wird rekursiv fortgesetzt, bis eine genügende Tiefe erreicht wird (die identifizierten Elemente genügend klein sind), um die bestehenden Sicherheitsfachgebiete alle einzuordnen.

Eine rein *elementenorientierte* Betrachtung greift jedoch zu kurz. Deshalb werden im Folgenden immer *zwei Aspekte* betrachtet:

- die *Elemente* der Unternehmung (z.B. *Informationssystem*) und deren Teilelemente,
- die *Tätigkeiten*, welche in diesen (Teil-)Elementen ablaufen oder in welchen diese Elemente verwendet werden (z.B. *Informationsverarbeitung*)[24].

Darauf aufbauend werden die *Fachgebiete der Sicherheit* diesen Elementen und Tätigkeiten jeweils zugeordnet (z.B. *Informationssicherheit*). Die Fachgebiete stellen die Tätigkeiten der Informationssicherheit dar. In Kapitel 3 werden sie lediglich zugeordnet; eine ausführlichere Betrachtung geschieht in Kapitel 5. Die Elemente der Informationssicherheit werden im Kapitel 4 behandelt.

In Abschnitt 2.5 wurde definiert, dass das Bezugsobjekt der Informationssicherheit in erster Linie die *Information* ist. Innerhalb der Unternehmung wird diese im *Informationssystem verarbeitet*. Informationssicherheit bezieht sich also *indirekt* auf das *unternehmerische Informationssystem* und die darin ablaufende *unternehmerische Informationsverarbeitung*.

Gesamthaft stellt das entwickelte Modell *nur eine Möglichkeit* zur Unterteilung einer Unternehmung in verschiedene Elemente dar. Es wird hier kein absoluter Anspruch auf Vollständigkeit oder Erreichung einer idealen Abbildung gestellt.

Zum besseren Verständnis sei noch erwähnt, dass jeder der nachfolgenden Abschnitte den jeweils vorausgehenden *detailliert*. Die Abschnitte beschreiben also, obwohl sie auf gleicher hierarchischer Stufe nummeriert sind, Elemente, welche Teile des jeweils zuvor identifizierten Elements sind. Beispielsweise beschreibt Abschnitt 3.3 die Elemente der Unternehmung, während Abschnitt 3.4 dann auf das Informationssystem als eines dieser Elemente der Unternehmung eingeht und

---

[24] Die Begriffe *Tätigkeiten* und *Prozesse* werden hier *nicht* synonym verwendet. Eine *Tätigkeit* beschreibt lediglich, was zu tun ist und bezieht sich auf ein Element der Unternehmung. Ein *Prozess* hingegen umfasst eine gesamthafte Vorgehensweise, welche die einzelnen Tätigkeiten in eine Sequenz zueinander stellt, Institutionen definiert, welche diese Sequenz durchlaufen und aus einer Eingabe eine Ausgabe produziert.

Abschnitt 3.5 Institutionen als Elemente des Informationssystems beschreibt. Das gesamte Modell ist in Abbildung 3-12 (Seite 95) dargestellt.

3.3 Unternehmung

Elemente

Als übergeordnetes Element in dieser Betrachtung wird die Unternehmung gewählt.

Verständnis der Unternehmung

Eine Unternehmung steht als eigenständige Organisation im Rahmen einer Marktwirtschaft und ist der Leistungserbringung durch Be- und Verarbeitung[25] von materiellen und immateriellen Objekten zu Produkten verpflichtet. Ihre primären Ziele sind Existenzerhaltung und Gewinnoptimierung. Zur Erreichung dieser Ziele werden Aufgaben definiert, einzelnen Personen innerhalb der Unternehmung zugeordnet und von ihnen durchgeführt[26]. Es soll hier vorausgesetzt werden, dass sich das Unternehmen in einem marktwirtschaftlichen Umfeld befindet, und dass die Verrechnung aller Arten von Dienstleistungserbringung über monetäre Zahlungsmittel erfolgt, welche als knappe und begehrte Ressourcen innerhalb der Unternehmung zur Verfügung stehen.

Unternehmungen sind dynamische, zielgerichtete und zielsuchende produktive, soziale Systeme [vgl. Rühli85, S. 15]. Als solche bestehen sie aus *Personen*, welche diese Ziele wählen und durch gezielte Beeinflussung weiterer Personen zu lösen anstreben. Dieses Verhalten wird Führung genannt und beinhaltet gemäss Rühli '*die Einflussnahmen (Steuerung) bei der multipersonalen Problemlösung.*' [vgl. Rühli85, S. 21] Die Steuerung geschieht direkt oder indirekt über Aufbau- und Ablauforganisation in der Unternehmung, und beruht auf interpersonellen Kommunikationsvorgängen[27]. Die Stellen und Gremien, in welchen die Personen im Rahmen der Aufbauorganisation angeordnet sind, werden hier als *Institutionen* bezeichnet.

---

25 Unter *Verarbeitung* eines Objekts im engeren Sinne soll dessen Verwendung ohne beabsichtigte Veränderung verstanden werden, unter *Bearbeitung* dessen Verwendung zur Veränderung des Objekts. *Verarbeitung* ist im weiteren Sinne jedoch Oberbegriff für beide Arten von Tätigkeiten.

26 Mit Unternehmung ist hier deshalb jede Art von Organisation zur Erreichung gemeinsamer Ziele gemeint; in diesem Sinne also auch öffentliche Verwaltungen, Stiftungen etc.

27 Es sei hier erwähnt, dass der Führungsbegriff mit den Inhalten von Heinrichs Mensch-Aufgabe-Beziehung identisch zu sein scheint, und dass Führung nur aus Steuerungsinformationen besteht.

Aus der Herleitung des Informationsbegriffs (vgl. Abschnitt 2.1) kann geschlossen werden, dass die gesamte Organisation und ihre Steuerung nur über *Wissen* bei den involvierten Individuen geschieht, z.B. Wissen über die jeweils eigene Position einer Person innerhalb der Organisation und die erlernten und anzuwendenden Verhaltensweisen. Auch die beispielsweise in Marketing und Verkauf verwendeten immateriellen Objekte – seien es Beschreibungen von Produkten, Preise, Lieferfristen oder Konditionen – erfüllen allesamt die in Abschnitt 2.1 hergeleiteten Eigenschaften von Information und Wissen. Ebenso ist es im Finanz- und Personalbereich: es wird nur mit Informationen über Objekte, Personen, finanzielle Mittel etc. gearbeitet, und diese Informationen beschreiben Menschen, Teile des Produktionsprozesses[28] oder die Aufgabe, welche diese Personen zu lösen haben[29]. Es liegt also nahe, diese gesamten Inhalte mit dem schon definierten Begriff (unternehmerische) *Information* zusammenzufassen.

Bei diesen Steuerungstätigkeiten werden die Personen bei der Informationsverarbeitung von unterschiedlichen *Werkzeugen* unterstützt, wobei einfache Systeme (Büroeinrichtung, Beleuchtung etc.) darin ebenso enthalten sind wie komplexe (Computer und IT-Systeme). Sie werden gesamthaft als *Instrumente* bezeichnet. Die komplexeren Systeme, welche direkt zur Steuerung beitragen, werden als *Informationssystem* bezeichnet, während diejenigen Systeme, welche lediglich als Voraussetzung für die Funktionsfähigkeit einer Unternehmung bestehen müssen, als *Infrastruktur* bezeichnet werden.

Ein Hauptelement innerhalb der Unternehmung ist also dieses steuernde System, welches *Steuerungsinformationen* (handlungsrelevantes Wissen), die steuernden Personen (Institutionen) sowie dabei verwendeten Werkzeuge und Hilfsmittel (Instrumente) umfasst und in welchem die gesamte Informationsverarbeitung (Prozess) abläuft.

Produkte der Unternehmung

Die Unternehmung verwendet zu ihrer Problemlösung auch materielle Objekte, welche entweder in der Produktion der Güter eine Rolle spielen[30] (Hilfs- und Betriebsstoffe, Produktionsinfrastruktur) oder selbst das Produkt bilden. Bei den Produkten einer Unternehmung kann grob zwischen rein immateriellen Produkten, immateriellen Produkten mit physischen Elementen[31] und materiellen Produkten

---

28 Finanzielle Mittel werden hier der Einfachheit halber als Hilfsmittel zur Produktion gesehen, bestehen aber im Geschäftsablauf selten als physisch vorhandene Münzen und Noten, sondern normalerweise nur als in Zahlen repräsentiertem Wissen über verfügbare Geldmengen.

29 Für alle weiteren Bereiche einer Unternehmung lässt sich diese Argumentation sinngemäss fortführen.

30 Mit Produktion ist hier der gesamte Weg eines Produktes von der Produkt-Idee bis zum Einsatz und Wartung beim Kunden gemeint.

31 z.B. ein Datenträger, auf welchem ein Softwareprodukt ausgeliefert wird.

unterschieden werden [vgl. auch Peters96, S. 64ff]. Letztere enthalten immer einen minimalen, oftmals sogar einen hohen Anteil an Wissen, welches als Design, Qualität, Funktionsweise[32], Innovation, Markenname, Inhalte der Bedienungsanleitung etc. an die Kunden übermittelt wird, und welches einen grossen Teil der Herstellungskosten ausmachen kann.

Es sollen hier zwei Klassen von Produkten unterschieden werden:

- materielle Produkte (Objekte mit materiellen und immateriellen Elementen) und
- rein immaterielle Produkte (Objekte ohne materielle Elemente).

Dementsprechend sollen zwei Klassen von Organisationen unterschieden werden: Produktionsbetriebe und reine Dienstleistungsorganisationen.

- In *Produktionsbetrieben* werden materielle Objekte be- und verarbeitet (Rohstoffe, Geräte etc.). Dies geschieht in einem *Produktionssystem für materielle Produkte*. Die Steuerung des dazu notwendigen Produktionsprozesses geschieht über Informationen, d.h. alle bearbeiteten Elemente werden in einem *steuernden Informationssystem* beschrieben und verwaltet[33]. Das entstehende Objekt ist materiell, hat jedoch immer immaterielle Elemente (z.B. Design, Anordnung der physischen Elemente, Funktion), welche in einem *Produktionssystem für immaterielle Produkte* produziert werden.
- *Reine Dienstleistungsorganisationen* produzieren ausschliesslich immaterielle Objekte (Informationen). Zur Erstellung des Produkts werden materielle Elemente ver- und bearbeitet, und ihre Überlassung zur Verwendung kann Teil des Produktes sein (z.B. bei der Vermietung eines Autos), muss es aber nicht (z.B. bei der Weiterleitung von Börsenkursen). Die materiellen Objekte gehen höchstens in den Besitz, jedoch nicht ins Eigentum des Kunden über (z.B. ein Flugzeugsitz während des Fluges). Die Produktion der Produkte geschieht hier in einem *Produktionssystem für immaterielle Produkte*. Auch hier geschieht die *Steuerung* über ein *Informationssystem*.

Beide Klassen benötigen darüber hinaus auch *Infrastruktur*, um die jeweilige Produktion durchführen zu können.

Daraus lässt sich ableiten, dass neben den schon identifizierten *Steuerungsinformationen Information* auch *als Produktelement* existiert, welche das

---

[32] Dass die Funktionsweise ein nicht materieller Teil eines Produktes ist, wird durch die Erfolge der japanischen Industrie der sechziger und siebziger Jahre belegt. Sie hatte sich teilweise darauf spezialisiert, Funktionsweisen von europäischen und amerikanischen Produkten zu kopieren und eigene Produkte mit ähnlicher Funktionalität zu vermarkten – ohne materielle Elemente des Originals zu verwenden. Der immaterielle Anteil der materiellen Objekte wurde also kopiert, verändert und neu verwendet.

[33] Das Informationssystem muss nicht computergestützt sein; auch eine karteikartenbasierte Komponentenverwaltung ist möglich und war in der Praxis früher üblich.

Resultat der Steuerung ist und deren Verarbeitung durch die Steuerung gelenkt wird, und welche als Eigenschaft (Funktionsweise, Anordnung etc.) des Produktes wiedergefunden werden kann.

Zusammenfassung

Bisher wurden somit folgende Elemente der Unternehmung identifiziert:

a) Information als steuerndes Element der Unternehmung (Ziele, Aufgaben, Wissen, Organisation etc.),

b) Information als immaterielles Element eines Produktes der Unternehmung,

c) Institutionen, welche die Steuerung durchführen,

d) Produktionssystem für die materiellen Elemente der Produkte mitsamt der dabei benötigten Roh- und Hilfsstoffe,

e) Produktionssystem für die immateriellen Elemente der Produkte, mitsamt der dabei benötigten Eingangs- und Zwischeninformation,

f) Informationssystem als steuerndes System der Produktion,

g) Instrumente (Hilfsmittel und Werkzeuge) bei der Steuerung,

h) Produkte der Unternehmung als Resultat der Leistungserbringung.

i) Infrastruktur als Voraussetzung für die Steuerung und Produktion.

Strukturierung

Diese Elemente sollen zur Betrachtung der *Informationssicherheit* wie folgt geordnet werden:

- In einer erste Gruppe werden alle Elemente zusammengefasst, welche mit Information und Informationsverarbeitung in Zusammenhang stehen (Elemente a, b, c, e, f, g, h). Diese werden gesamthaft als *Informationssystem* (*information system)* bezeichnet.
- In einer zweiten Gruppe werden die Elemente zusammengefasst, welche direkt der Produktion von materiellen Gütern dienen und noch nicht in einer anderen Gruppe enthalten sind (nur Element d). Sie werden *Produktionssystem* (*production system)* genannt. Dieses Produktionssystem kann auch Personen umfassen, welche jedoch keine steuernden Tätigkeiten wahrnehmen (und als solches Informationen verarbeiten würden). Es handelt sich also um rein ausführende Arbeiten, welche auch keine Kommunikationsprozesse umfassen[34].

---

[34] Diese vollständige Absenz von Information ist in der Praxis wohl kaum anzutreffen. Die Abgrenzung dient hier nur dem Denkmodell.

- In einer dritten Gruppe werden die restlichen Elemente zusammengefasst (nur Element i). Dies betrifft nur die *unterstützende Infrastruktur* (*infrastructure, supporting systems*), welche als Voraussetzung für jede Art von unternehmerischer Tätigkeit vorhanden sein muss. Diese unterstützende Infrastruktur umfasst ebenfalls keine Informationsverarbeitung[35]. Auch hier können Personen mitbetrachtet werden, welche jedoch keine steuernden Tätigkeiten wahrnehmen, sondern nur für die korrekte Funktionsweise der Infrastruktur besorgt sind (z.B. Hauswart)[36].

Eine Unternehmung besteht für die weiteren Betrachtungen deshalb aus den drei Elementen *Informationssystem*, *Produktionssystem* und unterstützende *Infrastruktur* (vgl. Abbildung 3-5, Seite 74, linker Teil).

Teilelemente

Alle drei Elemente umfassen jeweils *Personen* (*people, persons*), *Werkzeuge* (*tools*) und *Objekte* (*objects*), wobei die Personen die Werkzeuge einsetzen, um die Objekte zu be- und verarbeiten. Die Steuerung der Bearbeitung geschieht ausschliesslich im Informationssystem. Die Steuerungsinformationen werden den Objekten innerhalb des Informationssystems zugerechnet. Das führt zur Darstellung gemäss Tabelle 3-1.

---

35 Die Infrastruktur steht nicht in Zusammenhang mit der Informations- und Kommunikationsinfrastruktur im Sinne von Heinrich [Heinrich93, S. 14f], denn letztere wird hier als Teil des Informationssystems betrachtet.

36 Gemäss Duden umfasst die Infrastruktur '*die Gesamtheit der (für etwas, z.B. für die Wirtschaft) notwendigen Anlagen, Einrichtungen, welche die Grundlage, den Unterbau für die Arbeit, Tätigkeit bildet, auf der weitere Planung usw. aufgebaut werden kann.*' [Duden85, S.353] Zur Infrastruktur einer Unternehmung zählen demnach u.a. alle physisch vorhandenen Gegenstände, welche die Unternehmung zu ihrer Leistungserbringung benötigt, z.B. Gebäude mit Büroräumen, Möblierung, Energie-, Klima- und Wasserversorgungsysteme, Beleuchtung und den entsprechenden Sicherheitsvorkehrungen (Zutrittskontrolle, Notstromversorgung etc.). Auch Produktionseinrichtungen zur Herstellung der physischen Produkte (und der physischen Elemente immaterieller Produkte) wie z.B. Maschinen, Lagereinrichtungen, würden dazugehören, werden hier jedoch separat betrachtet. Auch alle der Informations- und Kommunikationstechnologie zuzurechnenden Anlagen und Einrichtungen sind Teil der Infrastruktur, werden hier jedoch als Teil des Informationssystems betrachtet. Üblicherweise nicht der Infrastruktur zugerechnet werden finanzielle Mittel, rechtliche und gesellschaftliche Rahmenbedingungen etc., obwohl auch für sie die obige Duden-Definition von Infrastruktur zutrifft. Dabei handelt es sich jedoch um Informationen, die hier im Rahmen des Informationssystems betrachtet werden.

	Personen (Institutionen)	Werkzeuge (Instrumente)	Objekte
Informationssystem	Informationsarbeiter	IT-System und nicht-digitale Werkzeuge	Informationsprodukte und Steuerinformationen
Produktionssystem	Produktionsarbeiter	Produktionstechnisches System und Werkzeuge	Materielle Produkte
Infrastruktur	unterstützende Personen	Technisches Unterstützungssystem	(keine)

Tabelle 3-1: Elemente der Unternehmung

Besonders herauszuheben ist hier der Begriff des *Informationsarbeiters* (*information worker*), welcher alle Personen beschreibt, die Elemente des Informationssystems sind und als solche Informationen verarbeiten[37].

Tätigkeiten

Die Tätigkeit, welche in der Unternehmung als Ganzes abläuft, soll hier als *Geschäftstätigkeit* (*business activity*) bezeichnet werden (vgl. Abbildung 3-5, Mitte). Sie umfasst

- die *Informationsverarbeitung* (*information processing*), welche vollständig im Informationssystem abläuft,
- die *Materialverarbeitung* (*material processing*), welche im Produktionssystem geschieht. Die Bezeichnung *Produktion* wäre irreführend, da sie auch steuernde Tätigkeiten impliziert,
- die *Unterstützung (support)*, welche die unterstützende Infrastruktur bereitstellt.

Fachgebiete der Sicherheit

Wenn Sicherheit für die gesamte Unternehmung betrachtet wird, wird dies i.d.R. mit *unternehmerischer Sicherheit* (*business security, corporate security*) bezeichnet (vgl. Abbildung 3-5, rechter Teil). Weitere Begriffe sind *unternehmerisches Sicherheits-* oder *Risikomanagement* (*risk management*). Darin sind jeweils eingeschlossen

- die *Informationssicherheit* (ISi, *information security, infosec*) welche sich als Sicherheit der Information primär auf ein Element des Informationssystems bezieht, aber als *Sicherheit der Informationsverarbeitung* sekundär auch die Tätigkeiten der Informationsverarbeitung und die dabei involvierten anderen

37 Kuhlen spricht in diesem Zusammenhang von *Informationsarbeit* [Kuhlen89, S. 21] und betrachtet theoretisch die einzelnen damit verbundenen Tätigkeiten.

Elemente des Informationssystems betrachten muss und als Ziel im Rahmen eines *Informationssicherheitsmanagements* durchlaufen wird,

- die *Produktionssicherheit* (*production security*), welche die Sicherheit der Materialverarbeitung sicherstellt. Teilgebiete sind z.B. die Arbeitssicherheit, der Werkschutz und die Betriebssicherheit des Produktionssystems,
- die *Infrastruktursicherheit* (*infrastructure security*), welche sicherstellt, dass die Unterstützungsdienste der Infrastruktur wunschgemäss funktionieren. Teilgebiete sind z.B. Feuerschutz (= Brandschutz), Wasserschutz, Umgebungssicherheit, Objektschutz, allgemeiner Zutrittsschutz.

Fazit

Eine Unternehmung kann als eine eigenständige Organisation in einer Marktwirtschaft verstanden werden, welche Eingabe- zu Ausgabeprodukten verarbeitet. Grob kann sie in Informationssystem, Produktionssystem und Infrastruktur unterteilt werden (vgl. Abbildung 3-5), wobei jedes Element Personen, Werkzeuge und Objekte umfasst.

Alle Informationsverarbeitung findet im Informationssystem statt. Dieses umfasst alle Informationen sowie die gesamte Informationsverarbeitung der Unternehmung, also auch die Steuerung des Produktionsprozesses, die Erstellung immaterieller Produkte sowie die Verarbeitung der immateriellen Elemente materieller Produkte (z.B. Design). Das Produktionssystem dient nur der Verarbeitung des materiellen Anteils der Produkte. Die Infrastruktur unterstützt die Informationsverarbeitung und den Produktionsprozess.

Informationssicherheit ist ein Teilgebiet der unternehmerischen Sicherheit, welches sich auf das Informationssystem der Unternehmung bezieht. Da die Informationsverarbeitung das Produktionssystem steuert und ihrerseits Teil der Infrastruktur ist, aber auch darauf aufbaut, müssen die Tätigkeiten der Informationssicherheit mit denjenigen der unternehmerischen Sicherheit (als übergeordnetes Element) sowie der Infrastruktur- und Produktionssicherheit koordiniert werden.

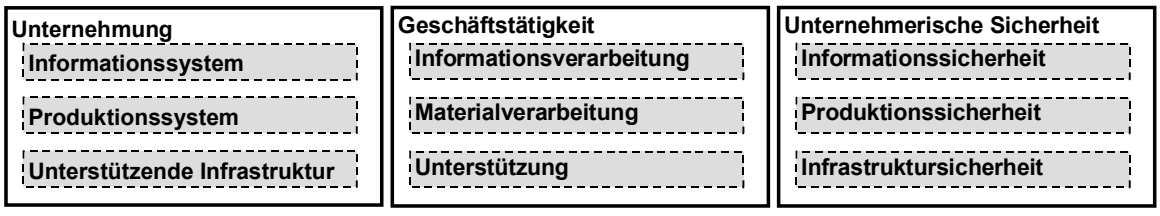


Abbildung 3-5: Elemente, Tätigkeiten und Sicherheitsfachgebiete der Unternehmung

Produktionssystem und Infrastruktur werden nicht weiter detailliert. Die Teilelemente des Informationssystems werden im nächsten und den darauf folgenden Abschnitten beschrieben.

3.4 Informationssystem

Elemente

Das Informationssystem umfasst alle Elemente im Zusammenhang mit der Informationsverarbeitung.

Das Informationssystem setzt sich nach Heinrich aus *Mensch*, *Technik*, *Aufgabe* und den *Beziehungen* zwischen diesen drei Elementen zusammen[38],[39]. Dabei machen Mensch, Technik und Aufgabe statische Elemente aus. Die Beziehungen Mensch-Aufgabe, Mensch-Technik und Aufgabe-Technik werden als dynamische Elemente bezeichnet [Heinrich93, S. 14]. Auch [Lockemann88, S.203] und [Zahn91, S.226] unterteilen die Elemente eines Informationssystem in *verarbeitete Informationen*, *Personen*, welche diese Informationen verarbeiten, *Werkzeuge*, mit deren Hilfe die Personen die Informationen verarbeiten und (Informationsverarbeitungs-) Tätigkeiten, welche diese drei Elemente kombinieren.[40]

Die Informationsinfrastruktur nach Heinrich umfasst *„die Einrichtungen, Mittel und Massnahmen, welche die Voraussetzung für die Produktion von Information und Kommunikation in einem Unternehmen schaffen (z.B. Hardware, Software, Personal)“* [Heinrich93, S. 330]. Diese sehr weite Definition umfasst bei grober Betrachtung alle Tätigkeiten der Unternehmung, welche in irgendeiner Weise mit Information zu tun haben, und damit die gesamte Führung der Unternehmung. Tatsächlich stellt auch Heinrich die Frage, in welchem Verhältnis die Informationsinfrastruktur *„zur Struktur- und Ablauforganisation und letztlich zu den strategischen Zielen der Unternehmung“* steht [Heinrich93, S. 15], ohne sie jedoch eindeutig zu beantworten. Seine Abgrenzung eines Informationssystems als Mensch-Technik-Aufgabe-System betrifft nahezu jede Unternehmung als Ganzes. Seine Ausführungen [Heinrich93, S. 171ff] lassen jedoch darauf schliessen, dass es sich bei seiner Auffassung eines Informationssystems bei dessen *technischer*

---

38 Heinrich bezeichnet es vollständig mit „Informations- und Kommunikationssystem (IuK-System)“

39 Die Elemente des Informationssystems werden in diesem Abschnitt vorerst mit den in Heinrichs Grundlegung verwendeten Begriffen bezeichnet. Dennoch gilt auch hier die Terminologiedefinition aus Abschnitt 1.2. Im besonderen gilt: *Person* wird synonym zu *Institution* verwendet, *Informationen und Aufgaben* zu *Information*, *Instrumente* zu *Werkzeuge*.

40 Diese Definition erlaubt auch, die von Buckland als Grenzfälle genannten *Museum*, *Bibliothek* und *Archiv* als Informationssysteme zu bezeichnen [Buckland91, S. 8]. Gleichwohl kann nicht davon ausgegangen werden, dass eine vollständige Aufteilung jeder denkbaren Unternehmung oder jedes Informationssystems in die genannten Elemente möglich ist.

Komponente primär um ein digitales System handelt, welches komplexe Abbildungen realer Sachverhalte verarbeitet[41].

"Informationssysteme sind in der Regel offene Systeme; sie interagieren mit ihrer Umwelt, insbesondere auch mit anderen Informationssystemen. Informationssysteme sind in der Regel komplex oder sogar äusserst komplex, weil die Anzahl ihrer Elemente und ihr Beziehungsreichtum gross sind. Informationssysteme sind in der Regel dynamische Systeme; beispielsweise entstehen in ihnen Veränderungen durch Lernprozesse der Benutzer im Umgang mit ihnen, etwa bezüglich solcher Systemeigenschaften wie Akzeptanz oder Produktivität. Informationssysteme sind zweck- und zielorientiert, weil sie bewusst von Menschen zur Informationsproduktion geschaffen werden und ganz bestimmte Qualitätseigenschaften haben sollen." [Heinrich93, S. 173].

Informationssysteme sind als Ganzes Werkzeuge zur Verarbeitung und Verteilung von Informationen, welche zur Steuerung von realen Objekten dienen. Beim hier näher zu betrachtenden unternehmerischen Einsatz wird das Informationssystem zur Erreichung von betrieblichen Zielen verwendet. Informationssysteme werden eingesetzt, um die Effizienz der unternehmerischen Abläufe zu erhöhen (Erreichung von Zielen mit möglichst geringem Mitteleinsatz). Eine Unternehmung betreibt ihr Informationssystem also, um die während der Geschäftstätigkeit anfallenden Tätigkeiten der Informationsverarbeitung durchführen zu können. Das Informationssystem ist deshalb derart angelegt, dass diese anfallenden Verarbeitungsvorgänge gemäss den Zielen der Unternehmung durchgeführt werden können.

Bearbeitete Informationen und Aufgaben

Die Zuordnung von Heinrichs Begriff *Mensch* zur Spalte *Personen* von Tabelle 3-1 ist einfach und eindeutig, dieses Element wird hier konsequenterweise als *Institutionen* bezeichnet. Ebenso kann *Technik* einfach der Spalte *Werkzeuge* zugeordnet werden und wird im Folgenden *Instrumente* genannt. Die Zuordnung der Begriffe *Aufgabe*, *verarbeitete Informationen*, *Beziehungen* und *Prozesse* ist etwas schwieriger.

Beziehungen und *Prozesse* umfassen die dynamischen Komponenten des Informationssystems und werden in Kapitel 6 betrachtet.

---

41 Ein Telefon fiele demnach nicht unter seinen Technikbegriff, da es nur die Form des Gesprächs simpel abbildet und kein Modell des Gesprächsinhaltes umfasst, aufbaut oder füllt. Andererseits sind die komplexen Datenstrukturen von Programmen Anordnungen zur inhaltlichen Abbildung des gespeicherten Wissens. Mit der zunehmenden Durchdringung der Unternehmungen mit digitalen Technologien und der zunehmenden Integration der verschiedenen Technologien zu einer (allenfalls wenigen miteinander verbundenen) Multimediatechnologien wird eine eindeutige Trennung zunehmend schwieriger.

Aufgaben im Sinne von Heinrich sind *"Einzelprobleme oder Problembereiche der verschiedenen sozial- und wirtschaftswissenschaftlichen Disziplinen, z.B. Administrations-, Dispositions- und Planungsaufgaben [...]"* [Heinrich93, S. 13]. Aufgaben steuern in diesem Sinne die unternehmerische Informationsverarbeitung und lassen sich deshalb direkt dem Begriff steuernde Informationen in der rechten oberen Zelle von Tabelle 3-1 zuordnen. Der Begriff *Verarbeitete Information* umfasst diese Steuerinformationen ebenfalls, schliesst jedoch auch die Ergebnisse einer Informationsverarbeitung mit ein. Daraus lässt sich folgern, dass es zwei verschiedene Objekte der Be- / Verarbeitung des Informationssystems gibt: *Informationsprodukte* und *Steuerinformationen*. Die Steuerinformationen beeinflussen den Prozess der Informationsverarbeitung, die Informationsprodukte sind ihr Ergebnis.

Personen und Kommunikation

Informationsverarbeitung findet gesamthaft im Kontext eines Informationssystems statt[42]. Die Personen, welche diese Verarbeitungen durchführen, werden als *Informationsarbeiter* (*information workers*) bezeichnet. Sie benutzen für Ihre Tätigkeit *Informationsobjekte*: Inhalte (Informationen) und Werkzeuge (Informationstechnologie).

In diesen Beziehungen zwischen den einzelnen Elementen des Informationssystems sind Information, Wissen, Daten und Nachrichten als Elemente enthalten. Sie lassen sich jedoch in einer statischen Betrachtung nicht eindeutig isolieren und gesondert betrachten; auch in Heinrichs Sichtweise ist dies nicht vorgesehen. Aufgrund der Herleitung des Informationsbegriffes wird aber davon ausgegangen, dass die dynamischen Elemente der Information – die Weitergabe als Nachricht in einem Informationsprozess – notwendiger Bestandteil eines Informationssystems ist und in den genannten Beziehungen enthalten ist. Informations- und Kommunikationssystem sind dementsprechend zwei Bezeichnungen desselben Gebildes [vgl. Heinrich93, S. 108][43]. Information in ihren Ausprägungen kann deshalb als Element eines dynamischen Informationssystems gesehen werden (vgl. Abschnitt 3.6).

Grenzen von Informationssystemen

Die Grenze zwischen zwei Informationssystemen wird im Folgenden durch die Eigentümerrechte gezogen. Es wird davon ausgegangen, dass das

---

42 '*Informationssysteme umfassen alle Funktionen, mit denen Informationen manipuliert werden, nämlich Erfassen, Bearbeiten, Verarbeiten, Speichern, Transportieren und Ausgeben.*' [Heinrich93, S. 173]

43 Allenfalls könnte das Kommunikationssystem als Teil des Informationssystems bezeichnet werden (z.B. gemäss [Rüttler91, S. 33]. Dies soll jedoch nicht weiter verfolgt werden.

Informationssystem als Teil der Unternehmung einem oder mehreren Eigentümern innerhalb der Unternehmung gehört, welche massgeblichen Einfluss auf seine Entwicklung und seine Verwendung haben, da sie unter anderem die Ziele der Unternehmung festlegen. Die Begriffe *zwischenbetriebliches Informationssystem* oder *überbetriebliches Informationssystem* sollen deshalb nur andeuten, dass ein Informationsaustausch zwischen verschiedenen Unternehmungen stattfindet. Es soll jedoch hier festgelegt werden, dass die entsprechenden Informationsflüsse über Schnittstellen laufen, welche die jeweiligen Informationssysteme mit ihrer Umwelt haben. Dies entspricht der Realität am ehesten, in welcher eine Kommunikation zwischen zwei Firmen beispielsweise über Modem-Leitungen und eindeutig definierte Protokolle erfolgt, welche einer dritten Firma (dem Betreiber des Kommunikationsnetzes) gehören.

Es darf allerdings nicht vernachlässigt werden, dass aus der informationellen Kooperation zweier Unternehmungen ein Mehrwert entstehen kann (Synergie). Bei den Sicherheitsbetrachtungen wird dies noch zur Sprache kommen (Abgrenzungs- und Verantwortlichkeitsproblematik).

Outsourcing stellt ebenfalls einen Spezialfall dar. Dabei werden Teile des technischen Informationssystems aus der Firma ausgelagert und ihr Betrieb, ihre Wartung oder sogar ihr Eigentum an eine andere Unternehmung übertragen. Doch auch eine Unternehmung mit maximalem Outsourcing behält ihr eigenes Informationssystem im hier definierten Sinne, lediglich das IT-System (vgl. Abschnitt 3.8) wird ausgelagert. Die Steuerung der übergeordneten Informationsflüsse und die Informationsverarbeitung selbst (also die Verarbeitung der Inhalte) geschieht nach wie vor im Informationssystem, lediglich die Datenflüsse und Datenverarbeitung (also die Verarbeitung der Abbildungen auf Medien) werden vom Insourcer[44] bestimmt.

Das Informationssystem kann also – gemäss der in Abschnitt 1.2 hergeleiteten Terminologie und dem hier hergestellten Bezug zu Heinrichs Definition des Informationssystems – in Institutionen, Informationen und Instrumente unterteilt werden (vgl. Abbildung 3-6, Seite 81, linker Teil).

Tätigkeiten

Das Informationssystem dient der *Informationsverarbeitung* (*information processing*). Diese umfasst alle Vorgänge der Erstellung, Speicherung, Weitergabe, Sammlung, Löschung (etc.) von Informationen.[45] Informationsverarbeitung bezieht

---

44 *Insourcer* ist derjenige, welcher die vom *Outsourcer* ausgelagerten Prozesse und Elemente übernimmt.

45 Alle in den vorhergehenden Abschnitten im Zusammenhang mit Information, Wissen, Daten oder Nachrichten erwähnten Vorgänge werden oft unter dem Oberbegriff der

sich dabei auf Information im weiteren Sinne und umfasst auch die Verarbeitung von Wissen, Daten, Nachrichten und Information im engeren Sinne (vgl. Abschnitt 2.1). Der Begriff *Wissensverarbeitung* (*knowledge processing*) ist dafür nicht gebräuchlich, *Datenverarbeitung* (*data processing*) und *Nachrichtenverarbeitung* (*message processing*) bzw. synonym *Kommunikation* (*communications*) werden jedoch als Prozesse innerhalb des Informationssystems bezeichnet.

In bezug auf die drei Elemente Institutionen, Informationen und Instrumente ist es schwierig, die jeweiligen Teilaspekte der Tätigkeiten zu bezeichnen, da die Informationsverarbeitungsabläufe sich gerade dadurch auszeichnen, dass sie diese drei Elemente verbinden. Der spezifisch institutionsbezogene Teilaspekt ist jedoch, dass sich jede Person bei der Informationsverarbeitung eine *Rolle wählt*, welche die Randbedingungen und Regeln festlegt, in welchen die konkreten Verarbeitungsprozesse ablaufen. Die Informationen stellen dabei die *Inhalte und Aufgaben* (als Element) dar, welchen die Informationsverarbeitung unterliegt, und diese *inhaltliche Informationsverarbeitung* wird hier als *Aufgabenbearbeitung* bezeichnet. Dies umfasst sowohl die Steuerung als auch die Bearbeitung der immateriellen Produktelemente. Die Werkzeuge dienen schliesslich zur *Datenverarbeitung*, wobei das Werkzeugelement gegenüber dem Inhalt betont werden soll (vgl. Abbildung 3-6, Seite 81, Mitte).

Der Lebenszyklus der Informationen beginnt mit dem Eintritt der Informationen in das Informationssystem (Erzeugung oder Aufnahme) und endet mit ihrem Austritt (Löschung oder Verfall). Informationen (i.w.S., vgl. Abschnitt 2.1) sind mediengebunden; Medien können anorganische (z.B. Disketten) oder organische Datenträger sein (z.B. menschliches Gehirn).

Fachgebiete der Sicherheit

Die Bezeichnung der Sicherheitsaspekte der einzelnen unternehmerischen Elemente und Tätigkeiten führt erneut zu Begriffsproblemen. Vergleichsweise einfach ist die Bezeichnung desjenigen Teilgebiets, welches sich mit dem personellen Element der Informationssicherheit beschäftigt, als *Sicherheit der Rollenwahl*. Dabei wird betrachtet, ob die von einer Person gewählte Rolle mit allen damit verbundenen Zielsetzungen der Aufgabenerfüllung gerecht wird.

Die Sicherheit der inhaltlichen Verarbeitung könnte als Informationssicherheit bezeichnet werden. Angebrachter ist jedoch der Begriff *Sicherheit der Aufgabenbearbeitung* oder *inhaltliche Informationssicherheit*.

Informationsverarbeitung subsumiert. Es bestehen sehr viele verschiedene Begriffe, welche alle in der einen oder anderen Art den Umgang mit Informationen beschreiben, z.B. *Erstellen, Ablegen Sortieren, Löschen, Senden, Formatieren, Bewerten, Ausgeben*. Eine abschliessende Aufzählung aller Verarbeitungsmöglichkeiten ist nicht möglich und soll hier deshalb auch nicht angestrebt werden.

Darüber hinaus umfasst Informationssicherheit das *Management der Informationssicherheit* (ISiM). Dies ist ein Prozess der Informationssicherheit selbst, wird damit der Aufgabenbearbeitung (vgl. oben) untergeordnet und wird hier deshalb nicht speziell erwähnt.

Die *Sicherheit der Datenverarbeitung* schliesslich bezieht sich auf die Werkzeuge (vgl. Abbildung 3-6, rechter Teil).

Fazit

Das Informationssystem einer Unternehmung setzt sich aus Institutionen, Informationen und Instrumenten zusammen. Jede Informationsverarbeitung der Unternehmung findet im Informationssystem statt. Dies umfasst die Datenverarbeitung, Nachrichtenverarbeitung (Kommunikation) und Wissensverarbeitung.

Die Sicherheit des Informationssystems, der darin ablaufenden Informationsverarbeitungsvorgänge und der enthaltenen Information wird mit Informationssicherheit bezeichnet. Die Personen innerhalb des Informationssystems nehmen Rollen ein, welche die Randbedingungen und Regeln festlegen, in welchen sie Informationen verarbeiten können.

Da Informationsverarbeitung an Personen gebunden ist (vgl. Herleitung des Informationsbegriffs in Abschnitt 2.1), geschieht in den Werkzeugen lediglich Datenverarbeitung. Sicherheit der Datenverarbeitung bezieht sich also nur auf die Werkzeuge.

Die Objekte des Informationssystems bestehen gesamthaft nur aus Informationen, wobei zwischen steuernden Informationen und Informationsobjekten unterschieden werden kann. Steuernde Informationen beeinflussen den Ablauf der unternehmerischen Prozesse und sind als solches den "Aufgaben" im Sinne von Heinrich gleichzusetzen; Informationsobjekte sind Ein- und Ausgabeprodukte der unternehmerischen Prozesse und stellen eigenständige Informationsprodukte oder Teile von materiellen Produkten dar.

Die Grenzen zwischen Informationssystemen werden durch die Eigentumsrechte daran gezogen. Zwischen- und überbetriebliche Informationssysteme sind demnach miteinander kommunizierende Informationssysteme verschiedener Unternehmungen. Informationssysteme können nicht gesamthaft ausgelagert werden (Outsourcing), da die inhaltliche Verarbeitung immer innerhalb der Unternehmung selbst erfolgt, sondern lediglich der Datenverarbeitungsteil inkl. technischem Kommunikationssystem wird im Extremfall ausgelagert.

Abbildung 3-6: Elemente, Tätigkeiten und Sicherheitsfachgebiete des Informationssystems

3.5 Institutionen

Elemente

Als Elemente des Informationssystems sollen die Institutionen nicht detaillierter betrachtet werden. Eine Unterscheidung anhand hierarchischer Einordnung, Intensität der durch sie durchgeführten Informationsverarbeitung, Ausbildung etc. wäre zwar möglich, ist aber aufgrund unscharfer Kriterien schwierig und erzeugt keinen Erkenntnisgewinn.

Tätigkeiten

Personen nehmen im Rahmen der unternehmerischen Informationsverarbeitung Rollen ein, welche in starkem Zusammenhang mit der Stellung stehen, welche die Institutionen in der Unternehmung innehaben. Grundsätzlich kann zwischen *aktiven* und *passiven Rollen* unterschieden werden (vgl. Abbildung 3-7, Mitte).

In aktiven Rollen wird die Fähigkeit von Personen betrachtet, Informationen zu verarbeiten; Personen werden als *handelnde Individuen (aktive Subjekte)* betrachtet. Welche konkrete aktive Rolle eine Person wahrnimmt, ergibt sich aufgrund der Inhalte der zu verarbeitenden Information. Die Person kann ihre Rolle – d.h. die Rahmenbedingungen, die Zielsetzungen und die Auswahl der zu berücksichtigenden zusätzlichen Informationen – in einigen Fällen selbst auswählen, in einigen Fällen ist die Rolle auch aufgrund der äusseren Umstände oder durch Beschluss einer vorgesetzten Stelle in der Unternehmung vorgegeben.

Passive Rollen beschreiben Personen als Objekte, welche in die Informationsverarbeitungsprozesse eingebunden sind und deren Existenz und Mitarbeit für die Unternehmung einen Wert darstellt. Personen können also *als schützenswerte Objekte* betrachtet werden.

Fachgebiete der Sicherheit

Als passives Subjekt der Informationsverarbeitung muss eine Person geschützt werden. Dies wird als *Personensicherheit* oder *Personenschutz* bezeichnet. Darunter fällt die rein physische Sicherheit der Person, aber auch die Sicherung des erwarteten Verhaltens der Person (eine ungeplante Absenz beispielsweise kann

zum Verlust der Handlungsfähigkeit einer Unternehmung oder eines Teils davon führen).

Ausserdem unterliegt die Beschreibung einer Person durch Dritte Sicherheitsanforderungen: Über eine Person als Mitarbeiter, Kunde oder sonstiger Stakeholder einer Unternehmung bestehen Datensammlungen, welche im Sinne dieser Person verarbeitet werden müssen. Dies wird als *Persönlichkeitsschutz*, als *Datenschutz* und der *Schutz der Privatsphäre* der Person bezeichnet. Dies gilt auch für juristische Personen.

Als aktives Subjekt muss die Person zum sicheren Verhalten angeregt werden. Dazu gehört einerseits die Wahl der korrekten Rolle und die Vermeidung von Rollenkonflikten, andererseits die Förderung eines generell sicherheitsbewussten Verhaltens, um durch die Handlungen der Personen sicherheitsrelevante Vorfälle zu verhindern. Das sichere Verhalten von aktiven Personen wird gesamthaft als *Sicherheitskultur* bezeichnet und durch *Sicherheitsmotivation* erreicht (vgl. Abbildung 3-7, rechter Teil).

Fazit

Personen (Institutionen) können innerhalb des Informationssystems einer Unternehmung als handelnde Individuen oder als schützenswerte Objekte betrachtet werden. Als handelnde Individuen sind Personen Teil einer Rolle und müssen zum sicheren Verhalten motiviert werden; gesamthaft muss eine Sicherheitskultur aufgebaut werden. Als schützenswerte Objekte sind Personen notwendige Teile von betrieblichen Abläufen und müssen durch Personenschutz geschützt werden. Ihre Persönlichkeit und Privatsphäre muss ebenfalls geschützt werden.

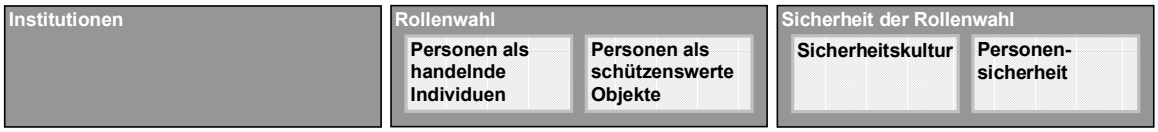


Abbildung 3-7: Elemente, Prozesse und Sicherheitsfachgebiete von Institutionen

3.6 Informationen

Elemente

Die Subelemente der Informationen sollen nicht näher unterteilt werden. Zwar sind die verschiedenen Aspekte von Information relevant, diese werden aber erst bei der Verwendung der Information durch Personen wirksam, und deshalb nur im nächsten Abschnitt beschrieben.

Tätigkeiten

Bei der Verarbeitung von Informationen im Rahmen der Aufgabenbearbeitung können die vier verschieden Aspekte von Information unterschieden werden. Dabei handelt es sich (in Anlehnung an die Ausführungen in Abschnitt 2.1, vgl. Abbildung 3-8, Mitte) um

- die *Verwendung von Information zur Aufgabenlösung*, wobei das verfügbare gesammelte Wissen durch eine Person eingesetzt wird, um eine konkret sich stellende Aufgabe zu lösen,
- die *Interpretation von Daten zu Wissen* und umgekehrt, wobei die Einordnungs- und Abbildungsvorgänge im Zentrum der Betrachtung stehen,
- die *Speicherung von Wissen als Daten* und umgekehrt die Wiederherstellung von Wissen aus Daten durch Interpretation und Sinngebung,
- die *Übertragung* von Daten *als Nachricht*, wobei das inhaltliche Element dieser Datenübertragung im Vordergrund steht.

Fachgebiete der Sicherheit

Die vier Aspekte der Aufgabenbearbeitung können direkt mit Teilbereichen der Sicherheit in Verbindung gebracht werden (vgl. Abbildung 3-8, rechte Seite):

- Bei der Verwendung von Wissen zur Aufgabenlösung muss sichergestellt werden, dass das richtige Wissen verwendet wird (Auswahl und Qualität), was hier als *sichere Informationsverwendung* bezeichnet werden soll und alle Sicherheitsaspekte der Verwendung von Information zur Lösung von Aufgaben im unternehmerischen Kontext umfasst, z.B. die Sicherung der Grundanforderungen nach beabsichtigter Verwendung und Verbindlichkeit (vgl. Abschnitt 2.3),
- Bei der Interpretation von Daten zu Wissen und zurück ist die Sicherheit der dabei durchlaufenen Abbildungsprozesse zu beachten. Es muss erreicht werden, dass das durch das Wissen aufgespannte Modell der Umwelt möglichst genau mit der tatsächlichen Umwelt übereinstimmt. Dies wird als *Kongruenz* oder *externe Integrität* betrachtet und ist auch eine Grund-anforderung der Informationssicherheit (vgl. Abschnitt 2.3)[46].
- Bei der Speicherung von Wissen als Daten müssen inhaltliche Anforderungen an die Abbildungsprozesse gestellt werden, welche ein einfaches Wiederauffinden und Sinngebung erlauben. Dies wird hier als *inhaltliche Datensicherheit* bezeichnet und umfasst z.B. die Sicherung der Grund-

---

[46] Kongruenz wird in der Mengenlehre verwendet und bedeutet „Deckungsgleichheit". Hier wird es im Sinne der Lockemannschen Datenbanktheorie (vgl. [Lockemann88]) verwendet und bedeutet Übereinstimmung zwischen der Realität und ihrer Abbildung in Daten.

anforderungen nach Verfügbarkeit, interner Integrität, Vertraulichkeit (Zugriffsschutz) (vgl. Abschnitt 2.3).

- Bei der Übertragung von Nachrichten zwischen zwei an der inhaltlichen Informationsverarbeitung beteiligten Institutionen muss sichergestellt werden, dass die Nachricht so ankommt, wie sie gesendet wurde. Dies wird hier als *inhaltliche Kommunikationssicherheit* bezeichnet.

In diesen Teilbereich der Sicherheit fallen alle Tätigkeiten des Informationsschutzes, welche den Inhalt von Informationen schützen, also z.B. auch der *Schutz von geistigem Eigentum* durch *Urheberrecht* und *Patentwesen*.

Fazit

Bei der Information können also die vier schon in Abschnitt 2.1 beschriebenen Aspekte (Informationsverwendung, Wissen, Daten, Nachrichten) wiedergefunden werden. Es können je einzelne Sicherheitsbereiche bestimmt werden, welche teilweise direkt der Erfüllung der Grundanforderungen gemäss Abschnitt 2.3 dienen (vgl. Abbildung 3-8).

Abbildung 3-8: Elemente, Tätigkeiten und Sicherheitsfachgebiete der Information

3.7 Instrumente

Elemente

Bei der Informationsverarbeitung im Informationssystem werden Instrumente (Werkzeuge und Hilfsmittel) eingesetzt. Heinrich beschränkt sich in seinen Betrachtungen des Informationssystems auf die mit Informations- und Kommunikationstechnik unterstützten Elemente. Der hier zu wählende Fokus ist etwas weiter: Da das Informationssystem nur sekundär betrachtet wird und primär auf die in der Unternehmung vorhandene *Information* fokussiert wird, muss auch derjenige Teil der Informationsverarbeitung betrachtet werden, der nicht mit Informations- und Kommunikationstechnik unterstützt wird. Da die Informations- und Kommunikationstechnik grösstenteils auf Basis digitaler Darstellungen funktioniert, soll hier also zwischen *digitalen* und *nicht-digitalen Instrumenten* unterschieden werden. Dies geschieht auch in der Annahme, dass für

Beeinträchtigungen der Informationssicherheit nicht unbedingt digitale Instrumente verwendet werden müssen.[47]

Die Informations- und Kommunikationsinfrastruktur einer Unternehmung umfasst gemäss Heinrich *"alle Einrichtungen, Mittel und Massnahmen, welche die Voraussetzung für Information und Kommunikation in einem Unternehmen schaffen."* [Heinrich93, S. 14f]. Dazu gehören bei Heinrich neben Hardware und Systemsoftware unter anderem auch organisatorische Regelungen, Menschen als Aufgabenträger sowie Räume. [Heinrich93, S. 15][48]. Infrastruktur und personelle Elemente wurden hier schon behandelt. Die Informations- und Kommunikations-infrastruktur soll hier nachfolgend nur die Elemente umfassen, welche direkt der Informationsverarbeitung dienen, also die Gesamtheit der verwendeten Informationstechnologien und -techniken umfassen. Die Begriffe *Technik* und *Methode* sollen dabei gleichgesetzt werden und eine Vorgehensweise zur Lösung eines Problems beschreiben, während *Technologie* eine konkrete benutzbare Ressource beschreibt. [Buckland91, S. 69] Ein informationstechnisches System ist demzufolge ein informationstechnologisches System, welches Techniken der Informationsverarbeitung unterstützt.

Unter Informationstechnologie müssen in der weiten Auslegung auch simple Systeme wie z.B. Papier und Bleistift verstanden werden. Buckland nennt das entstehende Gesamtsystem ein *information-supplying system* [Buckland91, S. 80]. Die IuK-Infrastruktur ist also in diesem Sinne mit dem informationstechnischen System identisch. Ein informationstechnisches System wird in der Regel mit *IT-System* abgekürzt.

Diese Auffassung steht jedoch im Widerspruch zur üblichen Verwendung von IT-System zur Beschreibung eines computergestützten Systems: IT-System wird im Sprachgebrauch für den Spezialfall eines *computerunterstützten* IuK-Systems verwendet (IT-System im engeren Sinne). Die Grenze zwischen diesem und dem Rest der IuK-Infrastruktur ist fliessend und kann kaum scharf gezogen werden. Gesamthaft werden die Instrumente in *digitale* und *nicht-digitale* Elemente unterteilt. Diese Abgrenzung ist zwar insofern problematisch, als jede Schnittstelle eines digitalen Systems zu den Personen, welche das System bedienen, analog sein muss, da Personen nicht über digitale Schnittstellen verfügen. Diese Einschränkung wird jedoch toleriert, so dass beispielsweise eine analoge Spracheingabe und Sprachausgabe beim Telefonieren über ein digitales Netzwerk nur den ersten und letzten Übertragungsschritt darstellt, das System aber prinzipiell digital ist. Auch

---

47 Beispielsweise verletzt das unberechtigte Abhören eines persönlichen Gesprächs die Vertraulichkeit der dabei kommunizierten Information ebenso wie der Diebstahl eines Papiers mit der Niederschrift des Gesprächs oder das unberechtigte Anfertigen einer Dateikopie, in welcher die Niederschrift oder eine Sprachaufzeichnung gespeichert ist.

48 Hier finden sich die im Zürcher Management-Ansatz erwähnten inhaltlich definierten Instrumente wieder, welche unter den inhaltlichen Aspekten in Kapitel 5 genauer betrachtet werden.

eine Tastatur zur Dateneingabe ist eine analoge Schnittstelle (das Drücken mehrerer Tasten gleichzeitig ist möglich, auch die Verwendung unterschiedlicher Eindrucktiefen, Anschlagsgeschwindigkeiten etc.), welche nur durch Filterung der möglichen Zustände eine digitale Eingabe erlaubt.

Stift und Papier sind konkrete Beispiele für nicht-digitale Instrumente zur Informationsverarbeitung. Auch Folien für Vorträge, Texte auf Papier, Ablagestrukturen wie Ordner und Dossiers, eine auf Papier geführte Agenda, eine mündliche Besprechung etc. sind nicht-digitale Instrumente zur Informationsverarbeitung.[49] [50] Diese Werkzeuge eignen sich v.a. für die Bearbeitung nicht-digital verfügbarer Informationen. Doch auch die Kenntnis von Über- und Unterordnungen in einer Hierarchie, der Ablauf von Prozessen etc. sind steuernde Informationen der unternehmerischen Tätigkeit. Es soll also in der Folge davon ausgegangen werden, dass der technische Teil des Informationssystems aus digitalen und nicht-digitalen Instrumenten besteht. Nur der digitale Teil wird als *IT-System* (oder für den deutschen Sprachgebrauch als EDV-System[51]) bezeichnet.

Für alle Instrumente wird ferner davon ausgegangen, dass sie in ihrer Funktion zur Informationsverarbeitung verwendet werden. Bei einer zweckentfremdeten Verwendung wird das Instrument nicht im Rahmen des Informationssystems, sondern als Teil des Produktionssystems oder der Infrastruktur betrachtet.

Die Struktur des Informationssystems wird bestimmt durch die Anforderungen, welche in der unternehmerischen Tätigkeit entstehen. Die Herstellung, Wartung und Ergänzung des Informationssystems erfordert Aufwand und wird zur Erfüllung der Effizienzanforderungen minimal gehalten.

Die Instrumente des Informationssystems können also in digitale (IT-System) und nicht-digitale Instrumente unterteilt werden (vgl. Abbildung 3-9, linker Teil).

Tätigkeiten

Die Tätigkeiten, welche innerhalb der Instrumente ablaufen, wurden schon früher gesamthaft als *Datenverarbeitung* bezeichnet. Dabei bezieht sich diese Verarbeitung auf die *Form* der Daten, nicht auf die Inhalte. In Analogie zur Teilung der Elemente besteht (vgl. Abbildung 3-9, Mitte)

---

49 '*Commonly* information technology *is used in a narrow sense to denote computers and associated technology, but, in a more general sense, pen, paper, photography, photocopying, and other devices are also information technology.*' [Buckland91, S. 5]

50 Datenverarbeitung ausserhalb des IT-Systems: Erstellung oder Vernichtung von Papierdokumenten, z.B. feines Zerschneiden einer Papier-Tabelle mit Finanzdaten der Unternehmung.

51 Die Begriffe EDV, Informatik und IT werden in Anhang A in Beziehung zueinander gesetzt.

- eine *digitale Datenverarbeitung*, welche in der Praxis oft auch einfach als *elektronische Datenverarbeitung (EDV)* bezeichnet wird, und
- eine nicht-digitale Datenverarbeitung, die auch als manuelle Datenverarbeitung bezeichnet werden kann.

Fachgebiete der Sicherheit

Die Sicherheit der Datenverarbeitung (DV-Sicherheit, *data processing security*, *DPSec*) kann unterteilt werden in (vgl. Abbildung 3-9, rechter Teil):

- Die Sicherheit der digitalen oder elektronischen Datenverarbeitung. Sie wird als *EDV-Sicherheit* oder *Sicherheit der elektronischen Datenverarbeitung* bezeichnet.
- Die Sicherheit der nicht-digitalen Datenverarbeitung.

Fazit

Die Instrumente des Informationssystems können in digitale und nicht-digitale Instrumente unterteilt werden. Digitale Instrumente umfassen alle Elemente des Informationssystems, welche der technischen Verarbeitung digital gespeicherter Informationen dienen, deren Schnittstellen untereinander digital sind, und deren Kommunikation mit den bedienenden Personen soweit wie möglich digital verläuft.

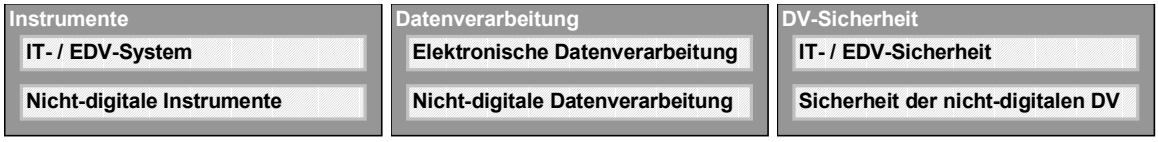


Abbildung 3-9: Elemente, Tätigkeiten und Sicherheitsfachgebiete des Informationssystems

3.8 IT- / EDV-System

Elemente

Da das IT-System von Personen verwendet wird, entstehen durch diese Verwendung einerseits digitale Prozesse[52]. Diese werden in der Betrachtung der Tätigkeiten im nächsten Abschnitt genauer erläutert. Andererseits benötigen diese digitalen Prozesse Abbildungen der Benutzer im System, bestehend aus

---

52 Der Begriff *Prozess* ist doppelt belegt. Im allgemeinen wird in diesem Text darunter ein Ablauf innerhalb des Informationssystems verstanden. Im konkreten Fall hier umschreibt *Prozess* die technische Durchführung einer programmgesteuerten Aktivität, welche durch den Benutzer ausgelöst wird.

Verbindungs- und Kontrolldaten (-strukturen) zur Steuerung des Prozessablaufs und der Berechtigungen, welche dem Benutzer eingeräumt werden. Diese Strukturen werden gesamthaft als *Principals* bezeichnet.

Alle digitalen Prozesse (deren Verwaltung durch die Principals geschieht) greifen auf *Ressourcen* des IT-Systems zu, welche wieder dreigeteilt werden können (vgl. Abschnitt 3.9). Die Elemente des IT-Systems sind Abbildung 3-10, linker Teil, dargestellt.

Tätigkeiten

Das IT- / EDV-System erlaubt die elektronische Datenverarbeitung (EDV). Diese kann unterteilt werden in (vgl. Abbildung 3-10, Mitte)

- die Ausführung der *digitalen Prozesse* einerseits und
- den Betrieb der Ressourcen andererseits (*IT- / EDV-Betrieb*)

Digitale Prozesse sind dabei die aktiven Elemente, welche vorgängig festgelegte Befehle abarbeiten und dazu auf die IT- / EDV-Ressourcen zugreifen. Digitale Prozesse werden von Personen initiiert und kontrolliert, wobei völlig divergierende Frequenzen und Quantitäten der Beeinflussung möglich sind (Extrembeispiele: kurzer interaktiver Echtzeitprozess vs. ständig laufender Hintergrundprozess zur g*arbage collection*).

Fachgebiete der Sicherheit

Die *IT- / EDV-Sicherheit* als Sicherheit des IT- / EDV-Systems (auch: IT-Sicherheit, Informatik-Sicherheit, *information technology security*, *IT Security*, *IT-Sec*, *electronic data processing security*, *EDP Security*) umfasst (vgl. Abbildung 3-10, rechter Teil)

- die *digitale Prozesssicherheit*, welche die Unabhängigkeit und Funktionsfähigkeit der ablaufenden digitalen Prozesse sicherstellt und
- die *IT- / EDV-Betriebssicherheit*, in welcher der Betrieb des IT-Systems und die Sicherheit der Ressourcen betrachtet wird.

Fazit

Die Tätigkeiten, welche von den Benutzern mit Hilfe des IT- / EDV-Systems durchgeführt werden, sind dort als digitale Prozesse abgebildet. Diese bestehen einerseits aus aktiven Elementen (den digitalen Prozessen selbst), andererseits aus den Kontrollstrukturen, welche zu ihrer Ausführung notwendig sind und als Principals bezeichnet werden sollen. Die Sicherheit der digitalen Prozesse umfasst ihre Unabhängigkeit, ihre Termination und weitere Anforderungen und wird mit dem Begriff *digitale Prozesssicherheit* bezeichnet.

Die digitalen Prozesse greifen auf Ressourcen des IT-Systems zu: Ein- und Ausgabegeräte, Speichermedien, Kommunikationsinfrastruktur etc. Die Funktionsfähigkeit dieser Ressourcen muss durch einen IT-Betrieb und IT-Betriebssicherheit gewährleistet werden (vgl. Abbildung 3-10).

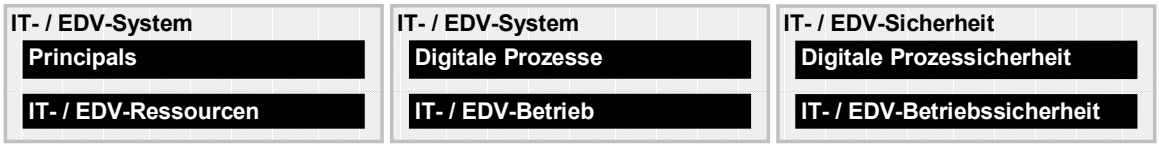


Abbildung 3-10: Elemente, Prozesse und Sicherheitsfachgebiete des IT- / EDV-Systems

3.9 IT- / EDV-Ressourcen

Elemente

Die IT- / EDV-Ressourcen können in *IT-Plattformen*, *Anwendungssysteme* und *Kommunikationssysteme* unterteilt werden (vgl. Abbildung 3-11, linker Teil). Middleware stellt einen Sonderfall dar.

IT-Plattformen

Als *IT-Plattform* sollen Geräte eines bestimmten Herstellers oder einer Gruppe von Herstellern gelten, welche über dasselbe, gerätespezifisch konfigurierte Betriebssystem verfügen und zueinander binärkompatibel sind. Dies bedingt in der Regel das Vorhandensein eines Hauptprozessors eines bestimmten Herstellers oder die softwareseitige Emulation desselben. Die IT-Plattform bietet die vorhandene Hardware des Geräts in einheitlicher Weise den darüberliegenden Programmen an. Eine IT-Plattform zeichnet sich deshalb durch eine einheitliche Programmschnittstelle aus (Application Program Interface, API). Beispiele für IT-Plattformen sind *WINDOWS*, *MACINTOSH*, *UNIX*, *VMS* etc., wobei jeweils Untervarianten existieren, welche durch verschiedene Versionen entstehen oder durch verschiedene Hersteller herausgegeben werden.

Anwendungssysteme

Unter *Anwendungssystemen* werden all diejenigen Software-Lösungen verstanden, welche konkret zur Lösung einer unternehmerischen Aufgabe beschafft oder hergestellt wurden. Beispiele sind Textverarbeitungen, Lagerverwaltungen, finanzielle Buchführungssysteme etc.

Middleware

Zwischen IT-Plattform und Anwendungssystemen besteht ein fliessender Übergang. In den heute bestehenden komplexen IT-Systemen bieten die Plattformen viele Funktionen an, welche früher der Anwendung zuzurechnen waren, z.B. die Identifikation und Authentisierung der Benutzer. Andererseits beziehen sich viele dieser Funktionen nicht direkt auf Hardwarekomponenten (z.B. das Anlegen von Sicherheitskopien), so dass sie andererseits nicht dem Betriebssystem zuzurechnen sind. Es besteht also eine Grauzone zwischen den beiden Elementen eines IT-Systems.

Darüber hinaus können viele Anwendungen auch als Plattformen für weitere Anwendungen gesehen werden. Die Makro- und Interpretersprachen gängiger Tabellenkalkulationen, Textverarbeitungen und Datenbankmanagementsysteme (DBMS) lassen die Entwicklung völlig unterschiedlicher Anwendungssysteme zu.

Ausserdem ist ein genereller Trend der Funktionsverschiebung von der Anwendung zum Betriebssystem festzustellen. So war beispielsweise ein WWW-Client (Browser) während mehrerer Jahre ein Anwendungssystem, musste er doch separat und passend zum Betriebssystem beschafft und installiert werden. In neuester Zeit wird er mit einigen Betriebssystemen direkt ausgeliefert und auf einigen auch direkt installiert. Bei einigen Systemen ist die Verknüpfung zwischen Betriebssystem und Browser sogar so eng, dass eine Trennung nicht mehr möglich ist; der Browser ist also Teil der Plattform. Derartige Verschiebungen gab es schon früher (z.B. Benutzerverwaltung, Kommunikation zwischen getrennten Computern), gibt es noch heute (z.B. die Software für die Ansteuerung spezieller Hardware, welche mit der Hardware ausgeliefert wird) und ist auch in Zukunft abzusehen (z.B. Integration von Spracherkennungsfunktionen oder Integration der „IT-Plattform“ *JAVA* zuerst in Browser, dann ins Betriebssystem und schliesslich in Hardware).

Für derartige Funktionalitäten hat sich der Begriff *Middleware* etabliert. Eine Middleware setzt auf den Funktionen auf, welche das API der IT-Plattform zur Verfügung stellt, ist selbst jedoch keine Anwendung, sondern stellt ihrerseits Anwendungen ein API zur Verfügung, mit dessen Hilfe sie spezielle vermittelnde Funktionen nutzen können. Beispiele für APIs sind Konversions-, Format- und Protokollanpassungsmodule, Inventarisierungs- und Personenverzeichnisdienste, Identifikations- und Authentisierungsfunktionen sowie alle Programme, welche eine von einer spezifischen IT-Plattform abstrahierte Plattform zur Verfügung stellen (z.B. *JAVA*). Auch ein Emulator eines Betriebssystems auf einem anderen kann als Middleware bezeichnet werden.

In der hier gewählten Darstellung wird Middleware nicht explizit erwähnt, weil dies für die Sicherheitsbetrachtungen nicht zentral ist. Anforderungen, welche an die Sicherheit von Middleware zu stellen sind, lassen sich auch als Anforderungen an IT-Plattformen und Anwendungssysteme formulieren und die Einführung der zusätzlichen Mittelschicht „Middleware“ führt nur ein weiteres Abgrenzungsproblem ein: Es müssen dann auch Kriterien angeben werden, wann

und warum ein Software-Modul der Plattform, der Middleware oder der Anwendung zuzurechnen ist.

Benutzer bearbeiten Daten (Informationen) inhaltlich, während IT-Plattformen nur „Formen und Strukturen“ zur Verfügung stellen. Anwendungssysteme erlauben die Verwendung der Formen und Strukturen zur Bearbeitung der Inhalte. Middleware unterstützt die Anwendungen dabei, indem sie häufig verwendete oder standardisierbare Grundfunktionen bietet. Middleware ist der Teil der Applikationen, welche tendenziell und langfristig in ein Betriebssystem integriert wird (Bsp.: WWW-Browser und Server, Authentisierungsverfahren und Verfahren zur sicheren Kommunikation, Systemapplikationen wie Benutzerverwaltung und Backup).

Kommunikationssysteme

Unter *Kommunikationssystem* werden hier all diejenigen Elemente eines IT-Systems subsumiert, welche der Verbindung und Datenübermittlung zwischen zwei getrennten Computern dienen. Auch hier ist die Abgrenzung schwierig. Eine genauere Aufteilung in Clients und Server, Terminals und Hosts etc. trägt nur wenig zur Abgrenzung zwischen IT-Plattform und Kommunikationssystem bei. Auch die Formulierung spezifischer Anforderungen an Prozessor, Haupt- und Sekundärspeicher etc. hilft nicht: viele Geräte sind heute so komplex, dass sie für verschiedenste Funktionen eingesetzt werden können: ein Personal Computer beispielsweise als Arbeitsplatzgerät, Datenserver, Applikationsserver, Router, Gateway, Firewall, Datensicherungsstation etc., und das sogar teilweise gleichzeitig. Es soll hier nicht noch eine Klassifizierung von Computersystemen abgegeben werden.

Unter Kommunikationssystemen sollen deshalb diejenigen Elemente der IT-Ressourcen zusammengefasst werden, welche der Datenkommunikation über Distanzen von mehr als einem Meter dienen (Kabel und Stecker, Repeater, Router, Bridges, Gateways der unteren 4 Kommunikationsschichten gemäss ISO/OSI-Modell und ihre Zusammenfassungen zu LANs, WANs, MANs, GANs etc. oder zum Internet). Nicht dazu gehören die Dienste, für welche diese Systeme verwendet werden: diese werden den Anwendungssystemen zugerechnet (vgl. obige Diskussion des Terms Middleware).

Tätigkeiten

Der IT / EDV-Betrieb ist unterteilbar in den *Systembetrieb* der IT-Plattformen, die *Anwendung* der Anwendungssysteme und die *Datenübertragung* (oder *technische Nachrichtenverarbeitung*) der Kommunikationssysteme (vgl. Abbildung 3-11, Mitte).

Fachgebiete der Sicherheit

Die Sicherheit der IT- / EDV-Ressourcen kann unterteilt werden in (vgl. Abbildung 3-11, rechter Teil)

- die Sicherheit der IT-Plattformen (*Systemsicherheit*). Dazu gehören *Computersicherheit* (*computer security, CompSec*), welche sich auf einzelne Computer oder Geräte bezieht und auch als *Rechnersicherheit* bezeichnet wird, sowie *technische Datensicherheit* (*data security, DataSec*), welche sich auf alle technischen Datenverarbeitungsvorgänge auf einer IT-Plattform bezieht,
- die Anwendungssicherheit oder Applikationssicherheit (application security, AppSec) und
- die technische Kommunikationssicherheit (communications security, CommSec) der Datenübertragung über Kommunikationssysteme inkl. Netzwerksicherheit (network security, NetSec).

Fazit

Die Ressourcen des IT-Systems lassen sich in IT-Plattformen, Anwendungen und Kommunikationssysteme unterteilen. Die Abgrenzung ist aufgrund der vielfältigen Durchmischung von Funktionalität teilweise schwierig. Middleware als zusätzliches Element wird hier als Teil von IT-Plattform und / oder Anwendungssystem betrachtet.

Die Sicherheit muss für jedes der Elemente gewährleistet werden: Systemsicherheit umfasst die Sicherheit der Plattform, Anwendungssicherheit diejenige der Anwendung und technische Kommunikationssicherheit gewährleistet Sicherheit im technischen Kommunikationssystem und der darin stattfindenden Nachrichtenverarbeitung.

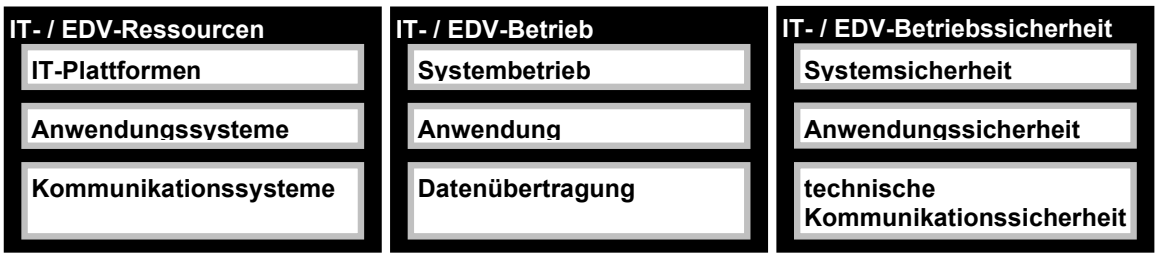


Abbildung 3-11: Elemente, Prozesse und Sicherheitsfachgebiete der IT- / EDV-Ressourcen

3.10 Integration des Bezugsobjekts

In den vorhergehenden Abschnitten wurde die Unternehmung und ihr Informationssystem hierarchisch in möglichst gut voneinander abgrenzbare Elemente unterteilt, um auf diese Art Bezugsobjekte von Sicherheitsfachgebieten zu

identifizieren. Auch wenn die hier gewählte Aufteilung nur eine von mehreren möglichen ist, erfüllte sie diesen Zweck. Die hierarchische Gliederung ist gesamthaft nochmals in Abbildung 3-12 dargestellt und hier nochmals im Text beschrieben.

Elemente

Eine Unternehmung kann in die Elemente *Produktionssystem*, *unterstützende Infrastruktur* und *Informationssystem* der Unternehmung unterschieden werden (vgl. Abbildung 3-12, linker Teil). Das Informationssystem umfasst alle Elemente der unternehmerischen Informationsverarbeitung und besteht aus allen *Institutionen*, welche in der Unternehmung Informationen verarbeiten, aus den (bearbeiteten und steuernden) *Informationen* und den *Instrumenten*.

Die Instrumente können wieder unterschieden werden in *nicht-digitale Instrumente* und digitale Instrumente, letztere werden gesamthaft als *IT-System* bezeichnet. Das IT-System besteht aus *Principals* (Abbildungen von Benutzern im System) und *Ressourcen*. Die Ressourcen sind weiter unterteilbar in *IT-Plattformen*, *Anwendungssysteme* und *Kommunikationssysteme*, wobei zusätzlich noch der Term Middleware alle Softwareelemente bezeichnet, welche nicht direkt dem Zugriff auf Hardware dienen, welche andererseits aber nicht zur Funktionalität von Anwendungssystemen gehören.

Tätigkeiten

Die Tätigkeiten einer Unternehmung lassen sich gesamthaft als *Geschäftstätigkeit* bezeichnen und unterteilen in *Materialverarbeitung*, *Unterstützung* und *Informationsverarbeitung* (vgl. Abbildung 3-12, Mitte). Informationsverarbeitung lässt sich analog zur Unterteilung des Informationssystem trennen in die *Wahl der Rollen* der Personen, welche als handelnde Individuen oder schützenswerte Objekte die Institutionen besetzen, in die *Bearbeitung der Aufgaben* durch Verwendung von Information zur *Aufgabenlösung*, der *Interpretation* von Information *zu Wissen* und umgekehrt, der *Speicherung* von Information *als Daten* und die *Übertragung* von Information *als Nachricht*, sowie in die technischen Aspekte der *nicht-digitalen* und der *elektronischen Datenverarbeitung*. Letztere besteht aus *digitalen Prozessen* und dem *IT- / EDV-Betrieb*, welcher wiederum in *Systembetrieb*, *Anwendung* und technische *Datenübertragung* gegliedert werden kann.

Fachgebiete der Sicherheit

Zu jedem der Elemente und Prozesse der Unternehmung können Sicherheitsbereiche bestimmt werden (vgl. Abbildung 3-12, rechter Teil)[53]. Das

[53] Die Sicherheitsfachgebiete werden in Kapitel 5 detailliert.

Gebiet, welches die Unternehmung als ganzes schützt, wird *unternehmerische Sicherheit* genannt. Es lässt sich unterteilen in *Produktionssicherheit* (als Sicherheit des Produktionssystems und der Materialverarbeitung), *Infrastruktursicherheit* (als Sicherheit der unterstützenden Infrastruktur und der damit durchgeführten Unterstützungstätigkeiten) und *Informationssicherheit* (als Sicherheit des Informationssystems und der Informationsverarbeitung).

Informationssicherheit lässt sich weiter unterteilen in die *Sicherheit der Rollenwahl* mit *Sicherheitskultur* und *Personensicherheit* (als Sicherheit des Personals und seiner Rollen als handelnde Individuen und schützenswerte Objekte), *Sicherheit der Aufgabenbearbeitung* (als Sicherheit der inhaltlichen Informationen und Aufgaben und der Aufgabenbearbeitung) und *Sicherheit der Datenverarbeitung* und der Werkzeuge, welche dazu notwendig sind.

Die Sicherheit der Aufgabenbearbeitung ist wiederum unterteilbar in *Sichere Informationsverwendung*, *Kongruenz, inhaltliche Datensicherheit* und *inhaltliche Kommunikationssicherheit*. Die Sicherheit der Datenverarbeitung ist weiter unterteilbar in die *Sicherheit der nicht-digitalen Datenverarbeitung* und der dazugehörigen Werkzeuge und die *IT-Sicherheit* als Sicherheit der elektronischen Datenverarbeitung. Diese ist weiter unterteilbar in *digitale Prozesssicherheit* und *IT-Betriebssicherheit* mit den Teilen *Systemsicherheit, Anwendungssicherheit* und *technische Kommunikationssicherheit*.

Alle weiteren Fachgebiet der unternehmerischen Sicherheit, welche sich auf Elemente der Unternehmung oder des unternehmerischen Informationssystems beziehen, beispielsweise die Netzwerksicherheit, lassen sich in eines der hier genannten Gebiete einordnen.

Abbildung 3-12: Zusammenfassende Darstellung der Elemente, Tätigkeiten und Sicherheitsfachgebiete des Bezugsobjekts der Informationssicherheit

3.11 Klassifikation der schützenswerten Objekte

Das in den vorhergehenden Abschnitten beschriebene Modell umfasst alle Elemente der Unternehmung, welche im Rahmen des Informationssicherheitsmanagements als schützenswerte Objekte bezeichnet werden können. Es bietet sich daher an, aus der hierarchischen Gliederung eine Klassifikation[54] zu entwickeln.

Dazu bestehen verschiedene Vorschläge in der Literatur. Beispielsweise unterteilt das Grundschutz-Verfahren des schweizerischen Bundesamtes für Informatik (vgl. Abschnitt 7.2.2) die schützenswerten Objekte in *Anwendungen*, *Daten* und *Systeme*. Damit werden zwar bei weitem nicht alle der in den vorhergehenden Abschnitten identifizierten Elemente abgedeckt, jedoch der für die elektronische Datenverarbeitung relevante Teil.

Deutlich weiter geht die Klassifizierung des deutschen Bundesamtes für Sicherheit in der Informationstechnik, welches im IT-Sicherheitshandbuch definiert wurde (vgl. Abschnitt 7.2.1). Es unterschiedet die acht Objektkategorien gemäss Tabelle 3-2.

Materielle Objekte	Infrastruktur
	Hardware
	Datenträger
	Paperware
Logische Objekte	Software
	Anwendungsdaten
	Kommunikation
Personelle Objekte	Personen

Tabelle 3-2: Kategorisierung der schützenswerten Objekte in Gruppen gemäss [BSI-IT-SHB92, S.43]

Diese Kategorisierung dient ebenfalls dem Zweck, die Objekte eindeutig einander unterordnen zu können; aus der obigen Einteilung könnte also geschlossen werden, dass es sich hierbei um die vom BSI vorgeschlagene Gliederung der Unternehmung handelt. Wie jedoch in Kapitel 7 noch weiter ausgeführt wird, bezieht sich das IT-Sicherheitshandbuch zentral auf das IT-System. Es müsste also eine Konkretisierung dieser Klassifikation aufbauend *auf der in diesem Kapitel* geschehenen Einteilung der Unternehmung vorgenommen werden. Tabelle 3-3 zeigt die schon identifizierten Elemente einer solchen Kategorisierung.

---

54 Die Begriffe *Kategorie* und *Klasse* werden synonym verwendet, entsprechend auch die Begriffe *Kategorisierung* und *Klassifikation*, da das Duden-Fremdwörterbuch den Begriff *Kategorie* mit dem deutschen Begriff *Klasse* erklärt [Duden90, S. 395].

Kategorie	Elemente	Prozesse	Sicherheits-fachgebiete
0	Unternehmung	Geschäftstätigkeit	Unternehmerische Sicherheit
1	Informationssystem	Informations-verarbeitung	Informationssicherheit
1.1	Institutionen	Rollenwahl	Sicherheit der Rollenwahl
1.1.1		Personen als handelnde Individuen	Sicherheitskultur
1.1.2		Personen als schützenswerte Objekte	Personensicherheit
1.2	Informationen	Aufgabenbearbeitung	Sicherheit der Aufgabenbearbeitung
1.2.1		Verwendung zur Aufgabenlösung	Sichere Informations-verwendung
1.2.2		Interpretation zu Wissen	Kongruenz
1.2.3		Speicherung als Daten	Inhaltliche Sicherheit
1.2.4		Übertragung als Nachricht	Inhaltliche Kommunikations-sicherheit
1.3	Instrumente	Datenverarbeitung (DV)	DV-Sicherheit
1.3.1	IT- / EDV-System	Elektronische Datenverarbeitung (EDV)	IT- / EDV-Sicherheit
1.3.1.1	Principals	Digitale Prozesse	Prozesssicherheit
1.3.1.2	IT- / EDV-Ressourcen	IT- / EDV-Betrieb	IT- / EDV-Betriebssicherheit
1.3.1.2.1	IT-Plattformen	Systembetrieb	Systemsicherheit
1.3.1.2.2	Anwendungssysteme	Anwendung	Anwendungssicherheit
1.3.1.2.3	Kommunikations-systeme	Datenübertragung	technische Kommunikations-sicherheit
1.3.2	Nicht-digitale Instrumente	Nicht-digitale Datenverarbeitung	Sicherheit der nicht-digitalen Datenverarbeitung
2	Produktionssystem	Materialverarbeitung	Produktionssicherheit
3	Unterstützende Infrastruktur	Unterstützung	Infrastruktursicherheit

Tabelle 3-3: Klassifikation nach hier vorgeschlagener Gliederung des Bezugsobjekts

Dabei zeigen sich sofort drei Effekte:

- Erstens ist es trivial, die Klassifikation aufgrund der streng hierarchischen Unterteilung des Bezugsobjekts vorzunehmen.

- Zweitens ist die Klassifikation sehr stark geschachtelt, was zu langen Klassenbezeichnungen führt, welche dennoch nicht durchgängig und nicht ausgewogen erscheinen. So bestehen für Klasse 1 gesamthaft 16 Unterklassen, für Klassen 2 und 3 keine. Dies ist nur konsequent und richtet den Fokus auf die unternehmerische Informationsverarbeitung.
- Drittens sind diese Klassen noch immer nicht detailliert genug, um verschiedene Systemtypen, Anwendungsumgebungen, Informationsarten etc. zu beschreiben. Es drängt sich also eine weitere Detaillierung des Bezugsobjektes auf, um im konkreten Fall die Klassifizierung vornehmen zu können.

Für die praktische Anwendung der in diesem Kapitel definierten Aufteilung des Bezugsobjekts wäre eine detailliertere Klassifikation notwendig, welche einzelne Objektkategorien und Technologien identifiziert. Sie könnte dazu dienen, schon im Voraus die Breite eines Informationssicherheitsprojektes zu bestimmen, indem bestimmt wird, welche Elemente zu berücksichtigen sind.

Fazit

Durch die Entwicklung eines Modells des unternehmerischen Informationssystems und der darin ablaufenden Informationsverarbeitung konnte ein Bezugsrahmen für die verschiedenen Sicherheitsgebiete geschaffen werden. Darauf aufbauend können nun die Vorgehensweisen betrachtet werden, mit welchen die Sicherheit dieser einzelnen Elemente erreicht werden soll. Bei dieser Vorgehensweise kann immer wieder Bezug auf diese Elemente genommen werden, um die Breite und Tiefe eines konkreten Projekts zu bestimmen oder um festzustellen, welche benachbarten Bereiche im Rahmen eines Projekts der Informationssicherheit berücksichtigt werden müssen. Die Breite der Betrachtung kann insbesondere auch durch die vorgängige Definition und Auswahl von Kategorien schützenswerter Objekte abgegrenzt werden. Zusammenfassend kann dieses Modell des Bezugsobjekts also verwendet werden, um das Management der Informationssicherheit zu strukturieren.

4 Elemente

Dieses Kapitel umfasst die Identifikation und Beschreibung der Elemente der Informationssicherheit und der wichtigsten darin ablaufenden Tätigkeiten. Dabei handelt es sich um die *inhaltliche* Betrachtung gemäss Rahmenwerk (vgl. Abschnitte 1.3 und 3.1).

Zunächst werden in Abschnitt 4.1 die wichtigsten *Institutionen* beschrieben, d.h. die Strukturen der Aufbauorganisation der Unternehmung mit denjenigen Fachbereichen der Unternehmung, welche für die Informationssicherheit relevant sind. Da im Kapitel 8 ein Führungsprozess der Informationssicherheit spezifiziert werden soll, wird in diesem Kapitel auf diejenigen Institutionen der Unternehmung eingegangen, welche in der Umsetzungs- und Kontrollphase des Führungsprozesses aktiv werden. Hier zu betrachten sind insbesondere die *Informatik-Sicherheit*, welche die Sicherheit der informationstechnischen Datenverarbeitung beeinflusst und die *Revision*, welche sicherstellt, dass die Anforderungen von externen und internen Stakeholdern durch die unternehmerischen Prozesse und Produkte erfüllt werden. Weiterhin dient auch das *Controlling* der Informationssicherheit der Unternehmung, denn es beschäftigt sich zumindest teilweise oder indirekt mit dem sicheren Zustand unternehmerischer Information.

Aufbauend auf der Beschreibung der bestehenden Institutionen wird in Abschnitt 4.2 ein Vorschlag für die Gestaltung spezifischer Institutionen der Informationssicherheit abgegeben. Dieser wird durch ein Rollenmodell ergänzt, welches total 9 Rollen definiert.

Der zweite Schwerpunkt liegt bei den *Informationen.* Zunächst werden in Abschnitt 4.3 die externen Einflüsse auf die Unternehmung identifiziert, welche Auswirkungen auf die Informationssicherheit haben. Anschliessend wird Informationssicherheit in Abschnitt 4.4 als unternehmerisches Ziel festgelegt.

Schliesslich werden die *Instrumente* der Informationssicherheit in Abschnitt 4.5 betrachtet und in *interne* und *externe* Instrumente unterteilt.

4.1 Umsetzung und Kontrolle

Führung umfasst einerseits die Steuerung der Zielerreichung selbst, andererseits auch die Überprüfung, ob diese Steuerung erfolgreich war (vgl. auch [Rühli93a, S. 191ff]). Es handelt sich bei Führung also um die Herleitung (Planung) und Festlegung (Entscheidung) eines *Solls* sowie um Massnahmen zur Erreichung dieses *Solls* (Anordnung, Durchführung). Schliesslich muss geprüft werden, ob das Ziel erreicht wurde (*Soll-Ist-Vergleich*), und welche Korrekturen allenfalls vorzunehmen sind. Kontrolle muss also als nachgelagerte Tätigkeit verstanden werden; allerdings muss auch während der Umsetzung eine Kontrolle stattfinden.

In den folgenden Abschnitten sollen die verschiedenen Aspekte der Kontrolle genauer herausgearbeitet werden. Üblicherweise werden in diesem Zusammenhang die Begriffe *Controlling, Überprüfung, internes Kontrollsystem* und *Revision / Audit* genannt. Insbesondere interessiert hier die Organisation der Kontroll*strukturen* (d.h. die Kontrollinstitutionen) und ihrer Kompetenzen und Verantwortungen, da diese später als Vorlage für die Definition der Kontrollstrukturen der Informationssicherheit verwendet werden sollen.

Die verschiedenen Institutionen innerhalb und ausserhalb der Unternehmung, welche Informationssicherheit fordern und fördern, verwenden ein unterschiedliches Verständnis der Informationssicherheit. Die interne Revision einer Unternehmung versteht darunter die Wirtschaftlichkeit, Ordnungsmässigkeit und Wirksamkeit des Einsatzes von Informationssystemen. Die externe Revision ist an Ordnungsmässigkeit im Sinne der Gesetzmässigkeit interessiert. Die Unternehmungsführung selbst versteht unter sicherer Informationsverarbeitung das Ausbleiben ungewollter Einflüsse (Sicherheitsvorfälle) bei gleichzeitig maximierter Effizienz der Abläufe. Im Qualitätsmanagement geht darum, die an die Produkte zu stellenden qualitativen Anforderungen festzulegen, daraus Anforderungen an die Produktionsprozesse herzuleiten und Verfahren und Institutionen zu implementieren, um diese Anforderungen zu erreichen. Die Aufgaben und Inhalte dieser Fachbereiche und ihrer IT-spezifischen Teilbereiche (IT-Revision, IT-Qualitätssicherung etc.) sind in der Literatur gut dokumentiert. In diesem Kapitel wird die bestehende Basis an organisatorischem Wissen aus der Literatur aufgenommen und integriert, denn nur durch eine Berücksichtigung und Integration der bestehenden Strukturen kann eine optimale Durchführung des neuen Verfahrens *ISIWAY* in der Unternehmung erreicht werden.

4.1.1 Controlling

Controlling

- *„als Routineüberwachung auf allen Stufen der Unternehmung wird als Ausführungs- oder Verfahrenskontrolle bezeichnet und bezieht sich auf technische und kaufmännische Arbeitsvorgänge“* [Korber93, S. 26].
- als Führungsinstrument besteht aus *„der ständigen Überwachung der Unternehmensziele, der Planung und Organisation, der Durchführung von Ergebniskontrolle und den damit zusammenhängenden Aufgaben wie Abweichungsfeststellung und Abweichungsanalyse.“* [Korber93, S. 27]

Ziele des Controlling der Unternehmung sind (nach [Korber93, S.28]) die Sicherung des Vermögens, die Gewährleistung der Richtigkeit der Abrechnungsdaten, die Förderung der Wirtschaftlichkeit der Abläufe und die Unterstützung der Einhaltung der Geschäftspolitik.

Ist die Anordnungsphase zu stark von der Planung und Entscheidung getrennt, z.B. bei starker Arbeitsteilung oder mehreren Hierarchiestufen einer grösseren Unternehmung, ist die Berufung einer eigenen Steuerungsinstitution – eines Controllers – sinnvoll. Dieser wird in Planung und Entscheidung stärker mit einbezogen als die u. U. vielen untergeordneten Stellen und überwacht und beeinflusst im Auftrag der ihm übergeordneten Institution die Steuerung in seinem Bereich ganzheitlich, um so Ineffizienzen zu vermeiden. Er ist damit das Bindeglied zwischen über- und untergeordnetem Management.

4.1.2 Überprüfung

Die *Überprüfung* als Teil der Kontrolle innerhalb des Führungsprozesses überwacht, ob

- die Umsetzung der Anordnung im Sinne der getroffenen Entscheidung stattgefunden hat,
- ob durch diese Umsetzung das ursprüngliche Ziel erreicht wird.

Die Kontrollfunktion umfasst eine Rückmeldung (*feedback*), wie die Anordnungsphase abgelaufen ist und welche Ergebnisse dabei entstanden sind. Falls Abweichungen vom angestrebten Ziel festgestellt werden, sind Korrekturen in der Umsetzung vorzunehmen. Wenn dies nicht genügt, muss möglicherweise die Entscheidung revidiert werden, indem ein anderer Weg der Zielerreichung gewählt wird, z.B. durch Auswahl einer bei der ursprünglichen Entscheidung verworfenen Alternative oder durch Prüfung neuer, bisher nicht betrachteter Auswahlmöglichkeiten. Allenfalls muss das ursprüngliche Ziel neu festgelegt oder veränderten Umweltbedingungen angepasst werden. Dies ist dann zugleich die Voraussetzung für ein erneutes Durchlaufen des Führungsprozesses, der damit zum Führungszyklus wird. Die Kontrollfunktion ist also integraler Bestandteil des Führungsprozesses.

Diese Rückmeldung muss durch Usanz oder Festlegung veranlasst oder im Einzelfall eingeholt werden. Es wird zwischen in die Prozesse integrierten und ausserhalb der Prozesse stehenden Kontrollfunktionen unterschieden.

4.1.3 Internes Kontrollsystem (IKS)

Die in die Geschäftstätigkeiten integrierten Kontrolltätigkeiten werden gesamthaft als das interne Kontrollsystem (IKS) einer Unternehmung bezeichnet. Dieses Kontrollsystem ist inhaltlicher Teil der Aufbau- und Ablauforganisation und manifestiert sich durch Regelungen der internen Berichterstattung oder durch die Verabschiedung von internen Richtlinien und Vorschriften – also letztlich durch die

Definition von Teilprozessen mit Tätigkeiten, Zeitpunkten und Schwellenwerten[55], zu welchen diese ausgeführt werden müssen.

Das interne Kontrollsystem (IKS) umfasst (nach [Korber93, S. 29f]):

1. Überwachung durch Gestaltung der Aufbau- und Ablauforganisation, z.B. Organigramme, Stellenpläne, Richtlinien und Regelungen,
2. Überwachung durch spezifische Kontrollprinzipien, z.B. vertikale (Funktionstrennung) und horizontale Aufgabengliederung (Vier-Augen-Prinzip),
3. Überwachung durch institutionalisierte Ergebniskontrollen, z.B. spezifische Kontrollrechnungssysteme, Kennzahlensysteme, Budgetkontrollsysteme,
4. Überwachung durch eingebaute Prozesskontrollen, z.B. direkten Kontrollen von Wareneingang, Qualität oder Rechnungen, Vergleichskontrollen und Plausibilitätskontrollen.

Das interne Kontrollsystem umfasst alle Tätigkeiten, welche innerhalb der Unternehmung die Erreichung der Ziele unterstützen. Einrichtung, Überwachung und Dokumentation des IKS ist Aufgabe der Geschäftsleitung der Unternehmung. [Korber93, S. 80] Die interne Revision sollte keine derartigen Richtlinien entwickeln oder einführen [Korber93, S. 101].

Die Vorschriften werden in Zusammenarbeit zwischen den Stäben der Unternehmung und der obersten Führung, möglicherweise auch unter Einbezug des Linienmanagements erarbeitet und verabschiedet. Sie müssen vom Linienmanagement eingehalten werden. Der Controller muss auf die Einhaltung des IKS achten, ist jedoch in erster Linie an der Erfüllung der Aufgaben seiner direkt übergeordneten Stelle interessiert. Kontrolle geschieht über die interne Berichterstattung und folgt i.d.R. der hierarchischen Anordnung der Institutionen der Unternehmung. Die ausserhalb der Prozesse stehenden Kontrollen werden durch die Revision wahrgenommen.

4.1.4 Revision / Audit

„Auditing is a systematic process of objectively obtaining and evaluating evidence regarding assertions about economic actions and events to ascertain the degree of correspondence between the assertations and established criteria and communicating the results to interested users.“ [Robertson93, S. 8]. Revision umfasst dabei die erneute Betrachtung von vergangenen Geschäftsfällen und Sachverhalten der Unternehmung. Dabei werden diese Sachverhalte dokumentiert, es werden

---

55 Die Budgetkompetenz einer Stelle ist beispielsweise durch einen derartigen Schwellwert begrenzt. Ihre Überschreitung löst eine Tätigkeit (Einholen einer Bewilligung bei der übergeordneten Institution) aus.

mögliche Fehler gesucht und Fehlerspuren zur Klärung des Sachverhaltes verfolgt. *„Ziel der Revision ist ein Urteil über die Ordnungsmässigkeit, Richtigkeit oder Wirtschaftlichkeit des Prüfungsobjektes, auf das alle hievon zu Unterrichtenden vertrauen können und das als Grundlage für Entscheidungen dienen kann.“* [Korber93, S.33] Es wird also von der Revision angestrebt, dass die Information, welche eine Unternehmung über sich selbst verbreitet, möglichst klar ihre Lage wiedergibt. Die Revision beeinflusst diese Lage (und die von der Unternehmung getragenen Risiken) jedoch nicht [Robertson93, S. 11f].

Revision kann unterteilt werden (nach Wysocki, zitiert aus [Korber93, S. 34f])

- nach Rechtsnatur in gesetzlich vorgeschriebene, gesetzlich vorgesehene, vertraglich ausbedungene und freie Prüfungen,
- nach Prüfungsträgern in interne und externe Prüfungen,
- nach Häufigkeit in periodische, einmalige und sporadische Prüfungen,
- nach Art der Urteilsbildung in Ordnungsmässigkeits-, Wirtschaftlichkeits-, Geschäftsführungs-, Aufdeckungs- und Unterschlagungsprüfungen,
- nach Prüfungsobjekt.

4.1.5 Interne Revision

Aufgabe und Ziel

Aufgabe der internen Revision (auch: Innenrevision, Innere Revision, interne Rechnungsprüfung oder *internal audit* genannt) ist die Überwachung der Anwendung des internen Kontrollsystems (IKS) der Unternehmung. Die interne Revision wird durch Personen durchgeführt,, welche derselben Unternehmung angehören [Robertson93, S. 13]. Diese Überwachung ist notwendig, da das IKS unvollständig sein kann, Fehler aufweisen kann, durch Umwelteinflüsse ungenügend werden kann und ausserdem den Fehlern der Mitarbeiter unterworfen ist. Die Wahrnehmung dieser Aufgabe muss durch eine Institution erfolgen, welche zwar in den Gesamtprozess integriert ist, jedoch genügend exponiert, unabhängig und qualifiziert ist, um die Kontrollfunktion des IKS wahrzunehmen (vgl. auch [Robertson93, S. 14]). Ziel der internen Revision ist die Information der übergeordneten Institution über die Wirtschaftlichkeit, Wirksamkeit und Angemessenheit des internen Kontrollsystems [Robertson93, S.13].

Interne Revision bezeichnet gleichermassen diese Aufgabe und die Institution innerhalb der Unternehmung[56], welche diese Aufgabe wahrnimmt. Die interne

---

[56] Prinzipiell kann die interne Revision ausgegliedert werden, dies geschieht in der Praxis jedoch selten. [Korber93, S. 103]

Revision kann ebenfalls als Teil des erweiterten IKS gesehen werden (nach [Korber93, S. 31]).

Delegation und organisatorische Einordnung

Die Leitung der Unternehmung kann ihre Kontrollfunktion ganz oder teilweise an eine Interne Revisionsstelle delegieren, z.B. wegen steigender Unternehmensgrösse oder Diversifikation [Korber93, S. 91] [Venables91, S. 1]. Die Delegation betrifft dabei nur die Aufgabe der Kontrolle, entbindet die oberste Führung allerdings nicht von der Verantwortung für die Wahrnehmung der Überwachungsfunktion gemäss OR 716a Abs.5. Daraus folgt, dass die oberste Führung die Interne Revisionsstelle kontrollieren muss, an welche sie die Kontrolle der Unternehmung delegiert hat.

Die interne Revision ist in der Regel als Stabstelle der obersten Führung der Unternehmung eingegliedert. Organisatorisch wird sie direkt dem Präsidenten / Vorsitzenden, oder einem einzelnen Mitglied oder dem Gesamtvorstand untergeordnet [Korber93, S. 105] [Robertson93, S. 14] und handelt in dessen / deren Auftrag. Alternativ ist auch eine Unterstellung unter ein *Audit Committee* (ein Managementausschuss zur Koordination der Revisionstätigkeiten) möglich [Korber93, S. 102], oder direkt unterhalb des Verwaltungsrates. Für die letztgenannte Anordnung spricht, dass der Verwaltungsrat so seine Überwachungsfunktion besser wahrnehmen kann, dagegen spricht, dass auch die Unternehmungsleitung die Informationen benötigt. Beide Institutionen sollten also über die Informationen der internen Revision verfügen. [Korber93, S. 102f] In grossen Konzernen kann die Interne Revision hierarchisch zwischen Konzernleitung, Regionen und Einzelgesellschaften aufgeteilt werden.

Aufgaben

Die interne Revision prüft in den drei Bereichen [Robertson93, S.13] [Korber93, S.119ff]

- *financial auditing* das Finanz- und Rechnungswesen,
- *operational auditing* v.a. den (geplanten) Ablauf von Prozessen, z.B. im EDV-Bereich
- *management auditing* die unternehmerischen Entscheidungen (inhaltlich und formell).

Die letzten beiden Bereiche gefährden die Unabhängigkeit der Revision, da sie dort gestalterisch mitwirkt. Dies geschieht allerdings, damit sie bei der später erfolgenden nachträglichen Prüfung von dieser vorgängigen Beeinflussung der Prozesse profitieren kann. Bei der Prüfung wird selbst v.a. auf Ordnungsmässigkeit und Wirtschaftlichkeit geachtet.

Rechte

Um die Arbeit der internen Revision erst zu ermöglichen, muss sie über ein aktives und passives Informationsrecht verfügen, d.h. sie muss sowohl benötigte Informationen auf Verlangen erhalten als auch ohne Nachfrage über die wichtigen Ereignisse innerhalb der Unternehmung informiert werden. [Korber93, S. 129]

4.1.6 Externe Revision

„Bei der externen Revision wird die von der Unternehmensleitung delegierte oder gesetzlich geregelte Überwachungsfunktion durch prozessunabhängige unternehmensfremde Personen wahrgenommen.“ [Korber93, S. 63, S. 91] Gründe dafür sind die von aussen nicht sofort ersichtliche Komplexität der Unternehmung, die Distanz zwischen buchhalterischen Vorgängen und den publizierten Resultaten der Unternehmung und die Notwendigkeit einer klaren und wahren Berichterstattung über die vorhandenen Risiken der Unternehmung [Robertson93, S. 4]. Als externe Revisionsstellen gelten Wirtschaftstreuhänder, Revisionsverbände, Abgabenbehörden, Banken (für Kreditprüfungen) und weitere externe Prüfungsträger, z.B. Rechnungshof oder staatliche oder private Organe im staatlichen Auftrag. Im Folgenden werden nur Wirtschaftstreuhänder als externe Revisionsstellen näher betrachtet.

Anforderungen und Auftragsvergabe

Wirtschaftstreuhänder als externe Revisionsstellen sind privatrechtliche Organisationen, welche die gesetzlich geforderten [OR92 Art. 727] und, wo gegeben, die von Wirtschaftsverbänden spezifisch festgelegten Kriterien erfüllen. Die externe Revisionsstelle wird von der Generalversammlung der Gesellschaft bestimmt. Die wichtigsten Anforderungen an Wirtschaftstreuhänder als externe Revisionsstellen sind Gewissenhaftigkeit (Sorgfalt), Verschwiegenheit, Eigenverantwortlichkeit und Unabhängigkeit ([Korber93, S. 75], vgl. auch [OR92 Art 727-731]).

Aufgrund der Forderung nach Unabhängigkeit kann die externe Revisionsstelle auch nur prozessunabhängige Prüfungen durchführen und darf insbesondere keine prozessabhängige Kontrolle [Korber93, S. 66] oder Beratung anbieten [Korber93, S. 68].

Aufgabe

Aufgabe der externen Revisionsstelle ist die Prüfung der Klarheit und Wahrheit der Buchführung der Unternehmung und die Verfassung und Abgabe eines Revisionsberichts im (üblicherweise) jährlichen Rhythmus [Korber93, S. 77], [Eggmann97, S. 10ff]. Die Abschlussprüfung ist eine Gesetzmässigkeitsprüfung und erstreckt sich nur auf den Jahresabschluss [vgl. OR92 Art. 728-731]. *„Die Prüfung hat sich nicht darauf zu erstrecken, ob andere gesetzliche Vorschriften (z.B.*

Abgabenrecht, Preisrecht, Wettbewerbsbeschränkungen, Devisenrecht) beachtet wurden. Die Abschlussprüfung ist auch nicht auf die Aufdeckung strafbarer Tatbestände (z.B. Veruntreuungen) ausgerichtet.“. Im Prüfungsbericht muss jedoch auf die möglichen Auswirkungen solcher Tatbestände auf die Gesetzmässigkeit des Abschlusses hingewiesen werden. Gesamthaft muss der Revisionsbericht einen möglichst sicheren Einblick in die Lage des geprüften Unternehmens gewähren. [Korber93, S. 74] Um dies feststellen zu können, muss auch die Wirksamkeit des internen Kontrollsystems der Unternehmung geprüft werden, denn dieses ist eine notwendige Voraussetzung für eine klare und wahre Rechnungslegung [Korber93, S. 77]. Unabhängig von der Abschlussprüfung sind auch Prüfungen im Auftrag möglich.

Die Prüfung beschäftigt sich insbesondere mit jenen Teilen des IKS, welche für die Rechnungslegung ausschlaggebend sind.

4.1.7 Zusammenarbeit zwischen interner und externer Revision

Interne und externe Revision arbeiten in Teilbereichen zusammen [Robertson93, S. 266].

- Erstens müssen die externen Revisoren die Funktionsweise der internen Revision verstehen, um das interne Kontrollsystem der Unternehmung verstehen zu können.
- Zweitens können die internen den externen Revisoren Unterlagen und Informationen bereitstellen, und so deren Arbeit erleichtern. Die externe Revision kann so effizienter ablaufen. In diesem Fall muss die externe Revision jedoch auch die Objektivität (Unabhängigkeit) und Kompetenz der internen Revision prüfen.

Gesamthaft bezieht sich die externe Revision wie die interne auf das interne Kontrollsystem der Unternehmung, wobei die externe Revision v.a. die finanzielle Berichterstattung zuhanden der Generalversammlung prüft, während die interne Revision v.a. die Anwendung des IKS bei der internen finanziellen Berichterstattung prüft sowie ihre eigenen Berichte nur intern abgibt.

4.1.8 IT- / Informatik-Revision

Informationstechnologie wird in nahezu jeder geprüften Unternehmung eingesetzt. Entsprechend müssen die Revisoren befähigt sein, mit diesen Technologien umzugehen und ihre Potentiale und Risiken einschätzen können. Die Informatik-Revision hat sich daher aus der (unternehmerischen) Revision herausgebildet und während langer Zeit vor allem die aus ihrer Mutterdisziplin übernommenen Anforderungen an den formal korrekten unternehmerischen Einsatz der Informatik überprüft. Eines der ersten Einsatzgebiete der Informatik war die Buchführung. Die

Informatik-Revision hat sich von Beginn an darauf spezialisiert, die Ordnungsmässigkeit und Nachvollziehbarkeit der Rechnungslegung auch bei Rechnerunterstützung überprüfen zu können. Die *interne IT-Revision* macht dabei vor allem die Vorgaben der Geschäftsführung operationalisierbar, indem sie Vorschriften verfasst und ihre Umsetzung motiviert, kontrolliert und den Erfolg bzw. die Einhaltung der Vorschriften an die Geschäftsführung zurückgibt (Kontrollfunktion). Die *externe IT-Revision* betrachtet mehr die Einhaltung der rechtlichen Normen des umgebenden Wirtschaftssystems und muss als solche auch Einblick in die elektronische Informationsverarbeitung erhalten. Die IT-Revision beschäftigt sich gesamthaft jedoch nur mit der Form, nicht mit dem Inhalt der unternehmerischen Informationsverarbeitung.

Die Art des Systems, welches in der geprüften Unternehmung eingesetzt wird, ist für Planung und Durchführung der Prüfung wichtig, da die Kompatibilität der verwendeten Werkzeuge und das Verständnis des Prüfers für das konkrete System Voraussetzung für die Prüfung sind. [Robertson93, S. 53] Die Definition, Zielsetzung, Massnahmen, Aufgabe und Berichterstattung der Revision bleiben jedoch von der verwendeten Technologie unabhängig. [Robertson93, S. 53 und S. 716]. Es ist die besondere Aufgabe der IT-Revision, die speziellen Risiken des verwendeten Systems und die Wirksamkeit des internen Kontrollsystems auf das IT-System (das „control risk“) zu erheben und zu beurteilen. [Robertson93, S. 717] Dabei wird besonders darauf hingewiesen, dass es durch die Konzentration verschiedener Tätigkeiten auf dem Computer möglich ist, dass Betreuungs- und Überwachungspersonal des Computersystems oder verwandter Bereiche Zugriff auf die Daten von Bereichen und Funktionen haben, die voneinander unabhängig sein sollen (z.B. wenn die Buchhaltungsabteilung Zugriff auf Revisionsberichte hat). und so Interessenkonflikte entstehen können. Dies muss durch spezielle Massnahmen verhindert werden. Ausserdem können durch die komplexe automatisierte Verarbeitung (unmotiviert oder vorsätzlich entstandene) potentielle oder manifestierte Unregelmässigkeiten länger unentdeckt bleiben, solange sie keine offensichtlichen Fehlverhalten des Systems nach sich ziehen.

Unterstützend für die IT-Revision sind Transaktionslogs und Aufzeichnungen, welche während beschränkter Zeit für die Revision zur Verfügung stehen und die Rückverfolgung der Verbuchungsvorgänge erlauben.

Prüfziele

Die interne IT-Revision prüft insbesondere auf Wirtschaftlichkeit (Maximierung der Ausnutzung der Ressourcen), Wirksamkeit, Effizienz (Maximierung des Gesamtnutzens der Unternehmung), Sicherheit, Schutz des IT-Systems, Notfallvorsorge und Versicherung von Risiken [Venables91, S. 155].

4.1.9 IT- / Informatik-Controlling

„Informatik-Controlling dient als Sammelbegriff für Controlling-Aktivitäten im Bereich des betrieblichen Informationsmanagements. Die Hauptzielsetzung des Informatik-Controllings besteht darin, Effektivität und Effizienz der betrieblichen Informationsverarbeitung sicherzustellen." [Suter95, S. 1][57]. Im Gegensatz zur Leitungs- und Steuerungsfunktion, welche das Informationsmanagement umfasst, nimmt das Informatik-Controlling *„die Aufbereitung und Analyse ergebnisorientierter Informationen zur Führungsunterstützung"* vor [Suter95, S. 5]. Essentiell umfasst das Controlling die Prüfung der unternehmerischen Abläufe durch in den Prozess integrierte weisungsbefugte Fachleute, wobei die fünf voneinander abhängigen Bereiche *Control Environment*, *Risk Assessment*, *Control Activities*, *Information and Communication* und *Monitoring* definiert werden können[58]. Fehlt der Controller als eigene Institution, fällt seine Aufgabe dem zuständigen Manager zu. Im amerikanischen Raum umfasst Controlling auch die interne Revision, also die prozessexterne Prüfung (vgl. oben), was hier jedoch nicht weiter verfolgt wird.

Informatik-Controlling als eigene Funktion und Institution ist notwendig, weil Informatik ein noch immer stark sich veränderndes unternehmerisches Hilfsmittel darstellt, welches nur mit konkretem Fachwissen für die unternehmerischen Zwecke einsetzbar gestaltet und beherrscht werden kann. Der Controller dient in diesem Prozess als integrierte Fachperson mit meist breitem Wissen und bevorzugt betriebswirtschaftlicher Erfahrung. Informatik-Controlling umfasst jedoch keine Revisionsaspekte [Suter95, S. 24].

4.1.10 Fazit

Kontrolle ist ein integraler Bestandteil jedes Führungsprozesses. Sie gewährleistet, dass das in Planung und Entscheidung festgelegte *Soll*, welches durch Anordnung und Durchführung erreicht werden soll, mit dem dabei entstehenden neuen *Ist*-Zustand verglichen wird.

Die Überprüfung und Kontrolle kann in einen begleitenden, als Teil des Prozesses zu betrachtenden Teil – oft *Controlling* genannt – und einen prozessunabhängigen Teil – oft *Revision* genannt – unterteilt werden. Beide Begriffe sind jedoch mehrfach belegt, so dass eine Unterteilung in einen *weiteren* und einen *engeren Sinn* angebracht erscheint. Es ergibt sich eine Unterteilung und Zusammenhang der Begriffe gemäss Abbildung 4-1.

---

57 Informatik bezeichnet dabei „die *Gesamtheit der mit der elektronischen Informationsverarbeitung und Kommunikation zusammenhängenden Aspekte".* [Suter95], S. 3

58 zitiert nach [Suter95, S. 22f], ähnlich auch in [Robertson93, S. 478]

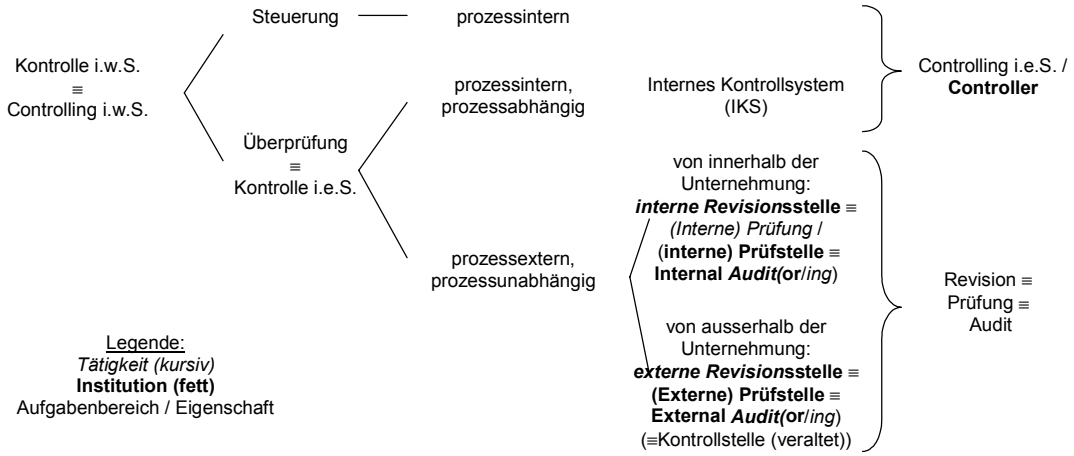


Abbildung 4-1: Kontrollbegriffe, -stellen / -institutionen und -tätigkeiten (basierend auf [Rühli93, Korber93])

Die Begriffe Controlling und Kontrolle sind sich ähnlich. In einem engeren Sinne unterscheiden sie sich deutlich; in einem weiteren Sinne können sie gleichgesetzt werden.

> *Def.: Controlling i.w.S. ist identisch mit Kontrolle i.w.S. und umfasst **alle** Kontrollfunktionen des Führungsprozesses. Es lässt sich unterteilen in eine direkte, in die jeweiligen Prozesse integrierte Steuerung (die eigentliche Aufgabe des Managements mit Planung, Entscheidung, Anordnung, Durchführung) und in die Überprüfung, welche einen Soll-Ist-Vergleich umfasst (Kontrolle i.e.S.).*

Die Überprüfung (Kontrolle i.e.S.) kann in eine in den Prozess integrierte und eine prozessunabhängige Kontrolle unterteilt werden. Die in den Prozess integrierte Kontrolle wird durch das Linienmanagement oder einen damit beauftragten Controller vorgenommen, wobei vorgegebene Richtlinien und Vorschriften einzuhalten sind, welche gemeinsam das interne Kontrollsystem (IKS) bilden. Prozessexterne Kontrolle wird als Revision bezeichnet.

> *Def.: Revision ist die i.d.R. nachträgliche Betrachtung von Geschäftsvorfällen und die Berichterstattung an die übergeordnete Institution.*

Bei grösseren Unternehmungen beruft der Verwaltungsrat (der gesetzlich die Kontrollfunktion der Unternehmung wahrnehmen muss) eine interne Revisionsstelle als Institution. Diese berichtet ihm über die Einhaltung des internen Kontrollsystems und somit über die Gewährleistung seiner Anforderungen. Bei gesetzlicher Vorschrift (z.B. Aktiengesellschaften nach Schweizer Recht) müssen die Eigentümer der Unternehmung zusätzlich eine externe Revisionsstelle berufen, welche die Konformität der unternehmerischen Tätigkeit mit den gesetzlichen Rahmenbedingungen prüft. Schwerpunkt der Revision ist traditionell die Berichterstattung über die finanzielle Abwicklung der Geschäftsfälle. Durch den

Einsatz von Informationstechnologie für die Verwaltung der Finanzen hat sich IT-Revision als Teilgebiet der Revision etabliert. Durch die entstehende Abhängigkeit von der Informationstechnik rückt auch in der IT-Revision die Erhaltung der Leistungsfähigkeit der Unternehmung immer mehr in den Vordergrund.

> *Def.: Controlling i.e.S. umfasst den* „Soll-Ist-Vergleich durch prozessabhängige Personen oder durch maschinell bzw. mechanisch wirkende Verfahren“*, wobei zwischen* „(laufender) Ausführungskontrolle auf allen Stufen“ *und* „Kontrolle als Führungsinstrument auf Führungsebene“ *[Korber93, S. 21] unterschieden wird.*

Da diese Kontrolle also direkte Auswirkungen auf den aktuell ablaufenden Prozess hat, wird im deutschen Sprachgebrauch oft auch von (korrektiver und kontrollierender) „Steuerung“ [Korber93, S.28] gesprochen.

> *Def.: Revision (Audit) ist ein* „Soll-Ist-Vergleich durch prozessunabhängige Personen“*, wobei die Überwachungsträger interne, unternehmensangehörige Personen oder externe, unternehmensfremde Personen sein können [Korber93, S. 21]. Revision wird auch Prüfung genannt.*

Die Kontrollfunktion gliedert sich also in ein Controlling, welches die Steuerung eines Prozesses durch Beeinflussung, Überwachung und Korrektur aus dem Prozess heraus umfasst, und eine Revision, welche die Prozesse und ihre Ergebnisse nachträglich betrachtet.

Die Kontrollstrukturen einer Unternehmung sind in Abbildung 4-2 schematisch dargestellt.

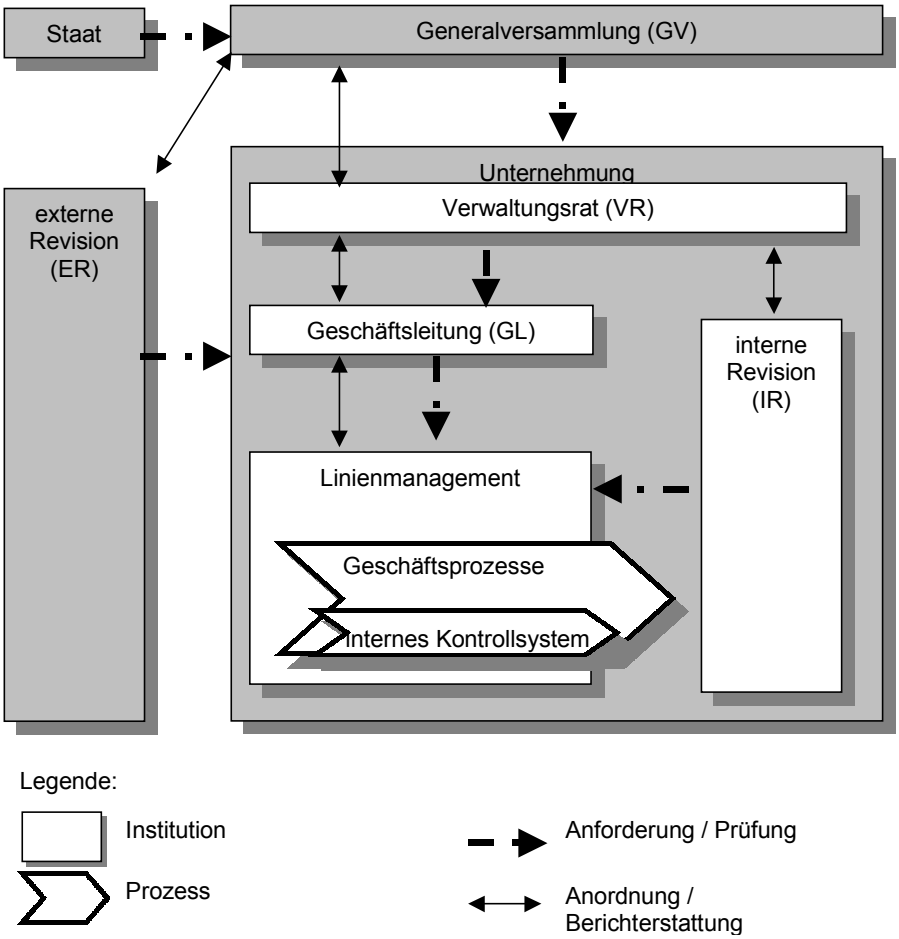


Abbildung 4-2: Kontrollstrukturen der Unternehmung

4.2 Strukturen der Informationssicherheit

In welcher Beziehung stehen nun der Aufbau strategischer Führung, der generische Führungsprozess und diese Kontrollstrukturen der Unternehmung mit der Informationssicherheit?

Informationssicherheit wurde schon in Kapitel 2 als Ziel innerhalb einer Unternehmung definiert. Zur Erreichung dieses Ziels sind Führungsprozesse notwendig, deren Erfolg kontrolliert werden muss. Diese Kontrolle kann durch die gerade identifizierten Kontrollinstitutionen innerhalb der Unternehmung erfolgen.

Informationssicherheit muss also in die bestehenden unternehmerischen Kontrollstrukturen integriert werden, um Teil der unternehmerischen Problemlösung zu werden. Dies geschieht durch Schaffung spezieller Institutionen für die Betrachtung einzelner Teilgebiete der Informationssicherheit und durch Aufnahme von Informationssicherheitselementen in das Interne Kontrollsystem der Unternehmung, also beispielsweise durch die Erstellung von Informations-sicherheitsvorschriften.

Die von der internen Revision überprüften Anforderungen beziehen sich auf die Steuerung und Führung der Unternehmung. Da im vorherigen Kapitel diese Steuerung als Element des unternehmerischen Informationssystems identifiziert wurde, handelt es sich bei allen identifizierten Institutionen um Institutionen der Informationssicherheit.

4.2.1 Gestaltungsvorschlag Controlling

Voraussetzung für die prozessintegrierte Berücksichtigung der Informationssicherheit ist es, dass Informationssicherheit von der Unternehmungsführung als *Ziel* formuliert wird. Das kann informell, aber auch formell im Rahmen einer *Vorschrift* oder *Weisung* geschehen. Sie muss für alle Mitarbeiter der Unternehmung so verbindlich festgelegt werden, dass die Mitarbeiter die *Verantwortung* für ihre Einhaltung tragen. Diese Weisung kann von einem Berater der Geschäftsleitung vorbereitet werden, welcher i.d.R. als *Informationssicherheitsbeauftragter* eine Stabsfunktion innehat. Dieser nimmt ausserdem übergeordnete Koordinationsaufgaben wahr und erstattet der Geschäftsleitung Bericht über den Zustand der Sicherheit innerhalb der Unternehmung.

Für spezielle Bereiche innerhalb der Unternehmung können weitere beratende und koordinierende Stellen geschaffen werden, z.B. gemäss Identifikation der Fachbereiche in Kapitel 3. Besonders zu erwähnen sind Institutionen für *IT-Sicherheit* und *IT-Recht*, weil bei diesen Fachgebieten besonderes umfangreiches Fachwissen notwendig ist. Bei IT-Sicherheit handelt es sich jedoch um werkzeugorientierte und nicht um inhaltlich orientierte Spezialisierung.

Darüber hinaus ist auch der Beizug externer Berater eine Möglichkeit, nicht-weisungsbefugte Institutionen einzubinden.

Als weitere weisungsbefugte Institutionen können Stellen für *Verantwortliche für Informationssicherheit* geschaffen werden. Dies ist in Organisationen mit hohen Anforderungen an die Informationssicherheit angebracht. Diese Stellen entheben die anderen Linienstellen nicht von ihrer Verantwortung, haben jedoch aufgrund ihrer dedizierten Tätigkeit grösseren Einfluss. Sie können auch als Controller-Stellen ausgeführt sein und die Informationssicherheit in ihrem Bereich durch ihre Weisungsbefugnis koordinieren bzw. die Umsetzung der Sicherheitsvorschriften forcieren.

Falls keine derartigen Stellen bestehen, sind die leitenden Institutionen *besonders* angehalten, die Vorschriften im eigenen Bereich umzusetzen. Dabei können Interessenkonflikte zwischen eigenen Zielen, Zielen des direkten Vorgesetzten und den in der Weisung festgehaltenen Zielen der obersten Geschäftsleitung entstehen.

Auch weisungsbefugte Stellen können für spezielle Bereiche geschaffen werden. Insbesondere sind hier IT-Sicherheitsverantwortlicher innerhalb der IT-Abteilung

zu nennen, welche die Sicherheitsverantwortung für einzelne Teilsysteme tragen. Die Schaffung dedizierter informationssicherheitsverantwortlicher Stellen für andere Bereiche ist kaum möglich, da sich die inhaltliche Verantwortung einer Stelle logisch mit der Verantwortung für die Informationssicherheit dieser Stelle deckt. Um so mehr ist das *Eigentümerprinzip* als klare Zuweisung von Informationen zu einzelnen Institutionen (personenbezogen) geeignet, um diese inhaltliche Verantwortung zu unterstreichen.

Die Einbindung externer weisungsbefugter Institutionen ist sinnvoll, wenn Informationssicherheitsprojekte in einem gut abgrenzbaren Bereich durchgeführt werden sollen (vgl. auch *Beratung* in Abschnitt 5.4).

Für übergeordnete interdisziplinäre Koordinationsaufgaben empfiehlt sich die Einrichtung eines Gremiums, welches z.B. ISi-Forum genannt werden kann (vgl. [ISO13335-2, S.6]) und Koordinationsaufgaben, die Zuweisung von Zuständigkeiten, fachliche ISi-Beratung, Förderung der Zusammenarbeit zwischen verschiedenen Unternehmungen und unabhängige Revision bieten kann.

Ein Vorschlag für die Gestaltung des Controlling-Prozesses (des Informationssicherheitsprozesses) wird in Kapitel 8 abgegeben.

4.2.2 Gestaltungsvorschlag Revision

Die interne Revisionsstelle ist aufgrund des hier breit verstandenen Informationssicherheitsbegiffs, welcher alle Aspekte der Führung umfasst, implizit die Revisionsstelle für Informationssicherheit. Auch hier ist die Schaffung dedizierter, fachspezifischer Institutionen möglich, wobei (aus den schon genannten Gründen) auch hier die IT-Revision und die Rechtsrevision im Vordergrund stehen. Die Rechtsrevision befasst sich mit der rechtlichen Relevanz einzelner Vorfälle innerhalb der Unternehmung, beispielsweise mit dem Nachweis von Betrug oder Fälschung und soll den Eigentümern Beweismittel zur Verfügung stellen, um fehlbare Mitarbeiter zur Rechenschaft zu ziehen. Weitere Spezialbereiche sind möglich und von der Zielsetzung der Eigentümer der Unternehmung und dem unternehmerischen Umfeld abhängig.

Für die Prüfung der allgemeinen rechtlichen Konformität (der Ordnungsmässigkeit) ist die externe Revisionsstelle zuständig. Da sie im Auftrag der GV aktiv wird und selbst rechtlichen Normen unterliegt, kann sie die Bestätigung der Ordnungsmässigkeit von der genaueren Betrachtung einzelner Vorfälle und inhaltlicher Teilbereiche abhängig machen und dazu spezialisierte Mitarbeiter als weitere "Institutionen" in die Unternehmung entsenden. In jedem Fall geschieht die Informationsweitergabe über die Leitung der Revision, also über die externe Stelle.

Ausserdem muss ein übergeordneter Informationssicherheitsbeauftragter aufgrund seiner Distanz zu den von ihm koordinierten Bereichen Revisionen durchführen. Er agiert damit als Revisor der Geschäftsleitung.

4.2.3 Rollenkonzept

Die Schaffung der oben genannten Institutionen gestaltet sich für jede Unternehmung aufgrund ihrer Grösse, Informationsintensität und weiterer Faktoren unterschiedlich. Es ist deshalb angebracht, generische Rollen der Informationssicherheit vorzuschlagen, welche die einzelnen Institutionen im Rahmen ihre Tätigkeit ausfüllen sollen. Jede Rolle wird dabei durch Aufgabe, Kompetenz und Verantwortung festgelegt sowie durch die allgemeine Beschreibung von hierarchischer Unter- / Überordnung.

Folgende Rollen werden hier vorgeschlagen (vgl. auch Abbildung 8-3, S.228):

- Geschäftsleitung (GL)
- Beauftragter für Informationssicherheit (ISiBe)
- Übergeordneter Manager (ÜM)
- Koordinator für Informationssicherheit (ISiKo)
- Ansprechpartner für Informationssammlungen (InfoOwner)
- Ansprechpartner für IT-Systeme (Verwalter)
- Benutzer
- Sponsoren
- Berater

Geschäftsleitung

Mit Geschäftsleitung (GL) wird das oberste, die Unternehmung operativ führende Gremium bezeichnet, oft bestehend aus Verantwortlichen für die verschiedenen Divisionen, Produktbereiche, Sparten oder Regionen unter Führung eines Vorsitzenden, Präsidenten etc. Die Geschäftsleitung ist an der störungsarmen Leistungserbringung interessiert und initiiert und unterstützt zu diesem Zweck Projekte der Sicherheit, insbesondere der Informationssicherheit.

Die Geschäftsleitung nimmt in der Regel nicht an diesen Projekten teil, sondern bestimmt einen Beauftragten, diese Projekte vorzubereiten und die Durchführung zu koordinieren. Die Geschäftsleitung ist also Initiant, Auftraggeber und übergeordneter Anspruchsteller der Informationssicherheit.

Beauftragter für Informationssicherheit

Der Beauftragte für Informationssicherheit (ISiBe) hat die oberste Verantwortung für die Festlegung und die allgemeine und langfristige Erreichung der Ziele der Informationssicherheit. Er kann mit weitreichenden Kompetenzen ausgestattet sein (dann wird vom Verantwortlichen für Informationssicherheit (ISiVA) gesprochen), ist in der Regel aber nur der oberste Koordinator für die Informations-

sicherheitsanstrengungen der Unternehmung. In dieser Funktion fördert er die Zusammenarbeit der einzelnen Linienbereiche und unterstützt diese bei der Wahrnehmung der konkret auf die einzelnen Bereiche bezogenen Verantwortung für die Informationssicherheit. Zu diesem Zweck stellt er Verfahren, Referenzen, Kataloge, Produktinformationen und weitere allgemein gültige Informationen zur Verfügung und löst die Durchführung der Verfahren innerhalb der Unternehmung aus, beobachtet und unterstützt sie und erstattet Bericht über die unternehmerischen Tätigkeiten im Informationssicherheitsbereich. Er kann auch, falls er über entsprechende Kompetenzen verfügt, als übergeordneter Informationssicherheitscontroller bezeichnet werden.

Der Informationssicherheitsbeauftragte (Information Security Delegate oder Officer), veranlasst, koordiniert, steuert und kontrolliert die Untersuchung und Erreichung der Informationssicherheit in der gesamten Unternehmung im Auftrag der Geschäftsleitung. Er ist dafür verantwortlich, dass die einzelnen Bereiche zur Durchführung der Informationssicherheit befähigt werden und dass Informationssicherheitsmanagement geschieht. Er ist also dafür verantwortlich, dass ein Sicherheitsniveau definiert und langfristig erreicht wird, nicht jedoch für die einzelnen Resultate.

Die Besetzung dieser Stelle sollte mit einer Person geschehen, welche nicht nur weitreichende Informatik-Kenntnisse aufweist. Fast ebenso wichtig ist die Erfahrung im Umgang mit dem Management von Unternehmungen, was voraussetzt. dass die Person auch bisher eine relativ hohe Position innehatte. Ferner muss die Person Sachkenntnisse in den Bereichen Organisation, Informations-, Prozess- und Projektmanagement mitbringen. Von Vorteil ist Fachwissen im juristischen Bereich und in konkreten Sicherheitstechnologien. Gerade der Aufbau von Know-How im letztgenannten Bereich gehört zur Aufgabe dieser Person. Darüber hinaus ist Fachwissen in den verschiedenen inhaltlichen Fachbereichen (vgl. Kapitel 5) von Vorteil, ebenso Erfahrung im Sicherheitsmanagement und Kenntnisse über die Unternehmung, in welcher er eingesetzt wird.

Übergeordneter Manager

Der Begriff *übergeordneter Manager* (ÜM) wird verwendet, um den jeweils *über* einer Stelle angeordneten Manager zu bezeichnen. Der übergeordnete Manager ist jeweils für einen Teilbereich der Unternehmung (z.B. eine Abteilung, einen Bereich, eine Arbeitsgruppe) zuständig und verantwortlich. Ein übergeordneter Manager existiert auf jeder Stufe der unternehmerischen Organisation (mit Ausnahme der oben beschriebenen Geschäftsleitung). Dies soll die Identifikation dieser Rolle auf jeder unternehmerischen Stufe ermöglichen. Die übergeordneten Manager bilden gemeinsam das Linienmanagement der Unternehmung.

Der übergeordnete Manager ist für die Sicherheit der in seinem Verantwortungsbereich stattfindenden Informationsverarbeitung verantwortlich.

Es obliegt also diesem Manager, Informationssicherheit in seinem Bereich zu fördern und dazu Informationssicherheitsmanagement einzusetzen. Er kann dies selbst tun, kann diese Aufgabe auch einem Mitarbeiter delegieren. Der übergeordnete Manager ist gegenüber der Geschäftsleitung bzw. dem ihm übergeordneten Manager für die Erreichung der Informationssicherheit in seinem Bereich verantwortlich. Er steuert also die Informationsverarbeitung so, dass Informationssicherheit gefördert wird.

Koordinator für Informationssicherheit (ISiKo)

Der Koordinator für Informationssicherheit ist derjenige, der innerhalb eines Teilbereichs der Unternehmung das Informationssicherheitsmanagement durchführt. Dies kann der Leiter dieses Teilbereichs (also der übergeordnete Manager) selbst sein. In der Regel ist der ISiKo ein direkter oder indirekter Mitarbeiter des übergeordneten Managers und fungiert als Controller. Er führt also im Auftrag und mit Unterstützung des übergeordneten Managers das Informationssicherheitsmanagement durch und ist verantwortlich für die Festlegung und Erreichung des Sicherheitsniveaus. Er berichtet dem übergeordneten Manager und erhält von ihm die notwendigen Kompetenzen.

Als Qualifikationsmerkmale muss er eine möglichst genaue Kenntnis der Informationsabläufe und der verwendeten Technologien in seinem Bereich mitbringen. Dazu gehört Prozess- und Produktwissen, aber auch Erfahrung in der Motivation von Kollegen (soziale Integration) sowie Fähigkeiten und Fertigkeiten im Projektmanagement. Technisches und juristisches Wissen ist von Vorteil, um einzelne Fragestellungen direkt behandeln zu können, aber nicht notwendig, da bei Bedarf der übergeordneten Informationssicherheitsbeauftragten beigezogen werden kann.

Ansprechpartner für Informationssammlungen ("Info Owner")

Die Geschäftsprozesse, in welchen die unternehmerische Leistung erbracht wird, und die letztendlich das Überleben der Unternehmung ermöglichen, laufen in den einzelnen Teilbereichen der Unternehmung ab. Dazu werden Informationen aufgenommen, verarbeitet und ausgegeben; Geschäftsprozesse stellen also den Rahmen für die inhaltliche Informationsverarbeitung dar.

Die dabei verarbeiteten Informationen lassen sich im Idealfall genau einer Person zuordnen, welche für diese Informationen verantwortlich ist. In diesem Fall handelt es sich um den "Information Owner", der in vielen Fällen auch der Verantwortliche für den Geschäftsprozess ist, in welchem diese Information verarbeitet wird ("Process Owner").

Oft ist die Verantwortlichkeit für eine Information jedoch auf verschiedene Stellen aufgeteilt, beispielsweise wenn dieselbe Information von verschiedenen Parteien verwendet wird (Benutzer, vgl. unten), oder von verschiedenen Stellen in

unterschiedlicher Form erstellt und verteilt wird. In diesen Fällen können die betroffenen Stellen einen gemeinsamen Ansprechpartner für die Information bestimmen.

Da die Betrachtung einzelner Informationen aus Aufwandsgründen nicht sinnvoll ist, werden sie zu Sammlungen zusammengefasst, deren einzelne Elemente jeweils ein inhaltliches Thema gemeinsam haben.

In der Praxis finden sich oft Mischlösungen. So ist ein Personalinformationssystem denkbar, welches von einer Stelle zentral betrieben wird, und für dessen Inhalt der Personalverantwortliche der Unternehmung gesamthaft verantwortlich ist. In der ganzen Unternehmung können aber Personalverantwortliche verteilt sein, welche auf die Daten nicht nur passiv zugreifen dürfen, sondern auch Mutationen (Adressänderungen etc.) und Ergänzungen (Einträge von Qualifikationsgesprächen etc.) eingeben dürfen. Die Informationssammlung "Personalinformationen" muss in diesem Fall so aufgeteilt werden, dass der übergeordnete Personalverantwortliche (z.B. der "Director Human Resources") die Gesamtverantwortung, die einzelnen Personalverantwortlichen der Unternehmungsbereiche jedoch die Verantwortung für die Wahrung der Anforderungen in ihren Teilbereichen zu tragen haben.

Da der Info Owner oft ein Sachbearbeiter innerhalb der Unternehmung ist, kann nicht erwartet werden, dass er über besondere Qualifikationen im Bereich Informationssicherheit verfügt. Es muss deshalb dafür gesorgt werden (z.B. durch ISiBe oder ISiKo), dass der Info Owner ausreichend für die Problematiken der Informationssicherheit sensibilisiert wird und im Bereich, in welchem er tätig ist, eine Sicherheitskultur aufgebaut wird. Darüber hinaus sind Fachkenntnisse über die von ihm bearbeitete Information die einzige Voraussetzung – die er ohnehin aufweisen muss, denn ansonsten könnte er die Stelle nicht füllen, in welcher er beschäftigt ist.

Ansprechpartner für IT-Systeme ("Verwalter")

In vielen Unternehmungen besteht eine Abteilung, deren Aufgabe der Betrieb und Unterhalt der computergestützten Werkzeuge ist ("Informatik-Abteilung"). Diese Abteilung leistet normalerweise keinen grossen inhaltlichen Beitrag bei der Informationsverarbeitung. Sie sorgt lediglich dafür, dass andere Personen innerhalb der Unternehmung effizienter arbeiten können und verwaltet die von diesen Personen bearbeiteten Informationen. Diese Abteilung hat deshalb eine treuhänderische Verwaltungsfunktion.

Im Vordergrund der Verwaltung stehen die Informatiksysteme, aber es sind alle informationsspeichernden und -verarbeitenden Medien zu betrachten, also auch Telefon, Fax, Briefpost, Ablagesysteme, Papierarchive, Schreibmaschinen, Diktiergeräte etc., letztendlich aber auch Bleistift und Papier. Die Prioritäten dieser Betrachtungen werden von den Fachbereichen festgelegt. Alle diese Medien und

Werkzeuge sollen hier gesamthaft als Instrumente bezeichnet werden und umfassen das IT-System (vgl. auch Definition von Instrumenten in Kapitel 3).

Die Ansprechpartner der Fachbereiche müssen grossen organisatorisches und technisches Wissen für ihren Bereich und die von ihm zur Verfügung gestellten Systeme aufweisen. Kenntnisse in Sicherheitsmanagement und -technologien sind von Vorteil und sollten gefördert werden, werden aber im Zuge der Massnahmenerarbeitung und -umsetzung ohnehin aufgebaut werden müssen. Auch hier ist der Aufbau von sicherem individuellem und sozialem Verhalten notwendig, damit Bedrohungen schon früh erkannt werden können. Denkbar ist die Einrichtung einer dedizierten Sicherheitsstelle mit einer Person, doch ist die Breite Streuung von Sicherheitswissen der konzentrierten Anordnung vorzuziehen.

Benutzer

Benutzer verwenden die Information der Unternehmung, um die ihnen gestellten Aufgaben zu erledigen. Passive Benutzer der Informationen greifen nur lesend auf die Informationen zu. Die Information ist für sie also nur ein Hilfsmittel, das sie z.B. als Referenz oder Verzeichnis benutzen, von ihnen aber nichts selbst verändert werden darf. Aktive Benutzer sammeln, erfassen und verändern die Information. Benutzer sind i.d.R. zugleich aktiv und passiv. Ihnen ist gemein, dass sie zwar die Verantwortung für die von ihnen verarbeiteten Informationen tragen, dass diese Verantwortung aber i.d.R. nicht die Kompetenz umfasst, sicherheitsfördernde Massnahmen zu veranlassen oder umzusetzen. Dies geschieht durch den übergeordneten Manager oder den von ihm beauftragten Informations-sicherheitskoordinator auf Anregung der Information Owner.

Besondere Qualifikation im Bereich Informationssicherheit müssen Benutzer zunächst nicht aufweisen. Es gilt aber das beim *Info Owner* Gesagte.

Sponsoren

Die Sponsoren sind an der Zielerreichung des Projekts interessierte Personen und unterstützen das Projekt deshalb, ohne direkt involviert zu sein.

Berater

Die Unabhängigen Berater stehen für übergreifende Fragestellungen zur Verfügung und können ihrerseits koordinierende Funktionen auf übergeordneter Ebene wahrnehmen. Sie müssen hohe Qualifikationen in den Bereichen aufweisen, in welchen sie jeweils tätig sind. Kenntnis der Unternehmung, ihrer Organisation und ihrer Produkte sind von Vorteil.

Zuordnung

Diese neun Rollen bilden die Grundlage für die Aufteilung des Informationssicherheitsmanagements innerhalb der Unternehmung. Ihre Kommunikation, Koordination und Kooperation untereinander wird im Rahmen des Verfahrens *ISIWAY* (Kapitel 8) noch genauer betrachtet.

4.3 Externe Einflüsse

Warum beschäftigen sich Unternehmungen mit Informationssicherheit? Die Antwort auf diese grundlegende Frage stellt die Basis für die *Motivation* des Informationssicherheitsmanagements dar und soll in diesem Abschnitt genauer betrachtet werden. Aufbauend auf der Motivation können die Inhalte der Informationssicherheit in *Fachgebiete* mit Aufgabenbereichen gegliedert werden. Schliesslich muss beleuchtet werden, mit welchen Massnahmenbereichen und Massnahmen diese Inhalte konkret umgesetzt werden können. Dies wird davon beeinflusst, welche Teilelemente des Bezugsobjektes im Rahmen des Informationssicherheitsmanagements betrachtet werden.

Warum müssen sich Unternehmungen mit Informationssicherheit beschäftigen? Jede Unternehmung unterliegt marktwirtschaftlichen und sozialen Einflussfaktoren, an welche sie sich ständig anpassen muss. Dies geschieht über die Definition unternehmerischer Ziele und Strategien.

Äussere und innere Einflussfaktoren sind dabei immer weniger deutlich unterscheidbar, da Unternehmungen sich immer stärker untereinander vernetzen und zunehmend öffnen.

Hier sollen zunächst die aus den sozialen und marktwirtschaftlichen Entwicklungen hervorgehenden Ansprüche an die Unternehmung identifiziert werden, um daraus Anforderungen an das Informationssicherheitsmanagement der Unternehmung herzuleiten. Dazu werden einige aktuelle Entwicklungen kurz beschrieben. Anschliessend werden die Fachgebiete der Informationssicherheit anhand der in Tabelle 3-3 (Seite 98) wiedergegebenen Kategorien detailliert erklärt.

4.3.1 Veränderungen des unternehmerischen Umfelds

Informationssicherheit steht inhaltlich im Kontext der Unternehmung und des unternehmerischen Zielsystems. Die unternehmerischen Zielsetzungen sind das Produkt des unternehmerischen Umfelds und der Entwicklungen des wirtschaftlich-sozialen Kontextes, denn Unternehmungen sind Teil der Gesellschaft. Sie funktionieren innerhalb von Rahmenbedingungen, welche durch das rechtliche System vorgegeben sind und haben ihrerseits grossen Einfluss auf das Verhalten ihrer Mitarbeiter, Kunden, Lieferanten und der weiteren Stakeholder (Stakeholder-Prinzip, vgl. [Sauter92a, S. 64]). Wenn sich dieses Umfeld verändert, muss die

Unternehmung darauf reagieren und sich daran anpassen, um langfristig überleben zu können.

Es gibt zahlreiche Studien und Prognosen, welche für sich beanspruchen, die wichtigen Entwicklungen zu antizipieren. Oft werden die Entwicklungen gesamthaft unter den Begriffen *Informationsgesellschaft, Globalisierung*, *virtuelles Dorf* o.ä. (vgl. [Peters96], S. 18, S. 24ff, [Lutz95], S. 84ff) zusammengefasst. Dabei handelt es sich um Schlagworte, welche eine Vielzahl oft nicht genau voneinander zu unterscheidender, miteinander verquickter Einzelentwicklungen umfassen.

Für diese Argumentation wurden die in [Davidson97, Kelly97, Peters96, Popcorn96, Lutz95 und Negroponte95] beschriebenen Entwicklungen auf ihr Potential hin untersucht, welches sie für die Entwicklung der Informationssicherheit darstellen. Diese Entwicklungen und die darauf aufbauenden Schlussfolgerungen für die Informationssicherheit werden hier in der Folge vorgestellt, indem Anforderungen an die unternehmerische Informationssicherheit formuliert werden.

Folgende Entwicklungen sollen kurz skizziert werden:

- Zunehmendes Informationsbewusstsein
- Intensivierte Anwendung von Informationstechnologie
- Tertiarisierung
- Informationsflut
- Anforderungen an die individuelle Kommunikation
- Verlagerung des Arbeitsorts
- Veränderung von Arbeitsverhältnis und Arbeitsablauf
- Mehrfache Rollen
- Erwartung von Verbindlichkeit
- Zunehmender Missbrauch
- Propagation von Anomalien
- Abnehmende Transparenz
- Erstarkung externer Interessengruppen
- Individualisierung
- Zunehmende private Abhängigkeit

Zunehmendes Informationsbewusstsein

Die unternehmerische Nutzung von Informations- und Kommunikations-technologien nimmt weiterhin zu. Die digitale Informationsverarbeitung breitet sich auf immer weitere Anwendungsbereiche (z.B. Videoverarbeitung, Text- und Spracherkennung) in den Unternehmungen aus. Durch den so stattfindenden

Medienwechsel sowie die schon heute intensive, aber noch immer zunehmende Durchdringung der Unternehmungen mit Informationstechnologie wächst das Informationsbewusstsein in den Unternehmungen (vgl. [Lutz95], S. 111ff): Information wird zunehmend als unternehmerische Ressource anerkannt, die es zu schützen gilt. Der *Information Highway* wird zum Allgemeingut und Notwendigkeit. Fest installierte Terminals für den Netzzugang in der Öffentlichkeit und im privaten Bereich werden allgegenwärtig. Lutz sprich von der *„Ablösung des Autos durch den Multiscreen als Schlüsseltechnologie"* [Lutz95, S. 303]. Multifunktionale mobile Geräte ergänzen die Produkt- und Zugangsvielfalt.

Unternehmerische Informationssicherheit wird deshalb an Priorität innerhalb der Unternehmung gewinnen. Sie muss *Vorgehensweisen, Verfahren und Methoden*[59] bereitstellen um die unternehmerische Ressource Information zu schützen. Sie muss dazu die Anforderungen an diese Informationen aufnehmen und ihre Einhaltung durchsetzen. Bei der Spezifikation dieser Anforderungen entstehen die ersten Probleme, weil diese oft nicht bekannt sind und weil Sicherheit oft *implizit* angenommen wird. Mit wachsendem Informationsbewusstsein gilt es also auch, durch Verbreitung einer möglichst homogenen Sicherheitskultur sicheres Verhalten zu fördern. Diese Anstrengungen müssen um so mehr intensiviert werden, als multikulturelle Einflüsse und Fluktuation zunehmen, denn Sicherheit ist in hohem Masse vom Verhalten der Mitarbeiter abhängig.

Intensivierte Anwendung von Informationstechnologie

Es werden ständig neue Technologien zur Optimierung der Informationsverarbeitung entwickelt. Diese umfassen immer komplexere Teilsysteme, deren Transparenz[60] abnimmt. Zugleich wächst die Komplexität der unternehmerischen Informationssysteme mit der zunehmenden Benutzung und der fortschreitenden Automatisierung. Beispielsweise werden die Unternehmungen durch die globale Optimierung der Geschäftsprozesse nach Produktions- und Zielmärkten und den dadurch zunehmenden Gütertransport immer mehr von komplexen und miteinander vernetzten Logistik- und Produktions-Informationssystemen abhängig.

---

59 Unter *Vorgehensweise* wird hier eine zuvor nicht im Detail spezifizierte Abfolge einzelner Aktivitäten verstanden, während *Verfahren* eine in seinen Einzelheiten zuvor bekannte Abfolge mit definierten Ein- und Ausgabewerten bezeichnen soll. Vorgehensweisen sind daher weniger formal aufgebaut als Verfahren und erlauben grössere Flexibilität bei der Anwendung, während Verfahren weniger Erfahrung voraussetzen. Eine *Methode* umfasst einzelne kurze Aktivitätenfolgen, welche innerhalb eines Verfahrens oder einer Vorgehensweise angewendet werden.

60 *Transparenz* bezeichnet hier die Nachvollziehbarkeit der inneren Abläufe der Systeme. Die Analyse von Software-Quellcodes könnte der Erhöhung der Transparenz dienen. Bei fremdhergestellten Produkten sind sie jedoch nur in seltenen Fällen verfügbar, weshalb Fremdprodukte im allgemeinen als weniger transparent gelten als sogenannte Open-Source-Systeme.

Darüber hinaus führen unternehmensübergreifende Vernetzungen von Informationssystemen dazu, dass die Grenzen zwischen internen und externen Netzen schwinden und neu definiert werden.

Die *Sicherheit* der verwendeten Technologien ist jedoch nur in Ausnahmefällen und unter Laborbedingungen beweisbar. Neue Technologien können deshalb nur so lange als sicher gelten, wie kein erfolgreicher Angriff auf diese Technologie bekannt wird. Es bestehen staatliche (z.B. BSI in Deutschland) und private Organisationen (z.B. CERT, TÜV), welche die Sicherheit von Technologien prüfen und Aussagen darüber abgeben; Aufgabe der unternehmerischen Informationssicherheit ist es, diese Diskussionen zu verfolgen und unsichere Technologien kontinuierlich durch sichere zu ersetzen.

Dabei ist zu berücksichtigen, dass es nach wie vor sehr viel einfacher ist, ein komplexes System zum Funktionieren zu bringen, als es sicher zu gestalten: Zum Funktionsnachweis genügt es, das Verhalten der einen konkreten Funktion zu überprüfen und so lange zu verändern, bis sie sich wunschgemäss verhält. Ein Nachweis der Sicherheit wäre nur zu erbringen, indem die Absenz aller nur denkbaren Sicherheitsmängel belegt würde. Dies ist alleine wegen des dabei entstehenden Aufwands nicht möglich. Intransparenz verunmöglicht diesen Sicherheitsnachweis prinzipiell. Externe Prüfungen (sog. Produktzertifizierungen) beschränken sich oft auf die Messung der Einhaltung vorgegebener Verhaltensweisen. Unternehmerische Informationssicherheit wird deshalb immer mehr zur *Managementfunktion* werden, welche Vorgehensweisen und Verfahren bereitzustellen hat, um die Gliederung von Sicherheitsuntersuchungen zu erlauben und Prioritäten zu setzen. Sicherheit bleibt also angestrebtes, aber unerreichbares Ziel.

Eine der sicherheitserhöhenden Entwicklungen ist die gegenseitige Abschottung von Systemen, welche zu weniger komplexen Systemen mit klarer definierten Schnittstellen führt, z.B. die Trennung von Netzen in einzelne abgeschottete Subnetze. Darüber hinaus werden technologische Innovationen auch für Sicherheitstechnologien und -produkte eingesetzt und erlauben die Nachrüstung unsicherer Technologie mit sicheren Komponenten.

Mit der zunehmenden Abdeckung neuer Anwendungsgebiete durch die Informationstechnik kann auch die Bedienung der Systeme zu Sicherheits-problemen führen. Informationssicherheit muss also auch die Schnittstellen zwischen Mensch und Maschine betrachten und gestalten, indem sie das menschliche Verhalten zu beeinflussen versucht und auf diese Weise die Einhaltung der von den Betroffenen gestellten Anforderungen gewährleistet.

Tertiarisierung

Lutz spricht von zwei Phasen des Informationszeitalters: *„Die erste Phase [...] nennen wir jene der Hyperindustrialisierung [,...] weil das Organisationsmodell der*

Industrialisierung mit den Mitteln des Informationszeitalters zur letzten Perfektion entwickelt wurde.“. Die zweite, die postindustrielle Phase des Informationszeitalters umfasst gemäss Lutz eine starke Individualisierung des Einzelnen als Teil von Wertschöpfungsprozessen (im Gegensatz zum Mensch-Maschine-System), den Wunsch nach der Erfüllung individueller Ansprüche der Produkte (im Gegensatz zur Massenware) und die Flexibilisierung der Produktion. [Lutz95, S.111ff]

Entsprechend muss sich auch die Informationssicherheit von der zentral organisierten Sicherung maschineller Systeme zur individuellen Sicherung der von Einzelnen verwendeten Informationen wandeln.

Die *Tertiarisierung*[61] der Wirtschaft, das *„Vordringen von Dienstleistungen in Produktion und Beschäftigung“* ([Klodt97] in [Golder98]) führt nicht unbedingt zu einem Rückgang der industriellen Produktion, in jedem Fall aber zu einem Anstieg des Informationsanteils in Produkten [Kuhlen95, S. 64ff]. Informationssicherheit muss deshalb auch die Sicherheit der in die Produkte integrierten Informationen betrachten und dazu die Produktesicherheit unterstützen.

Informationsflut

Durch die zunehmend leistungsfähigeren Systeme und ihre Verwendung entstehen grosse Datensammlungen über die in den Unternehmungen stattfindenden Transaktionen, aber auch durch deren redaktionelle Bearbeitung inner- und ausserhalb der Unternehmungen. Rosenthal betont, dass *„nicht mehr die Beschaffung von Daten, sondern ihre Aussortierung schwierig geworden ist.“* [Rosenthal98]. Die Sammlung von Datenmengen birgt also die Gefahr, aufgrund fehlender Kanalisierung und Filterung eine Datenflut oder Informationsüberflutung auszulösen. Informationssicherheit muss neue Technologien wie *Data Warehousing* und *Data Mining* unterstützen, um die gewinnbringende Nutzung dieser Daten zu erlauben. Dadurch wird die Komplexität der Systeme allerdings zusätzlich erhöht. Jeder Einzelne muss darüber hinaus selbst Strategien entwickeln, um die Informationen effizient zu ordnen und auszuwählen (vgl. auch [Postman90]).

Anforderungen an die individuelle Kommunikation

Jeder einzelne der Informationsflüsse muss die Anforderungen der jeweils kommunizierenden Parteien erfüllen. Implizit angenommene Anforderungen wie beispielsweise Vertraulichkeit persönlicher Kommunikation müssen zunehmend explizit geäussert werden.

Auch bedeutet beispielsweise die weltweite Verbreitung der US-amerikanischen Kultur und Sprache oder die Integration von Organisationen aus anderen

---

61 *Tertiarisierung* bezeichnet die Verlagerung der volkswirtschaftlichen Leistungserbringung in den tertiären Sektor (Dienstleistungssektor).

Kulturkreisen in die Unternehmung nicht gleichzeitig den Verlust regionaler Identitäten und Kulturen oder die Vereinheitlichung von Einkommens- oder Kostenstrukturen. Wegen des multinationalen und multikulturellen Aufbaus grosser Unternehmungen entstehen so auch im Inneren der Unternehmung unterschiedliche Subkulturen bzgl. Verbundenheit und Verhalten, aber auch Spannungen. Dies wird durch die zunehmende Fluktuation der Mitarbeiter und das veränderte Arbeitsverhältnis (vgl. unten) noch verstärkt. Daraus folgt, dass soziale Unterschiede zum Missbrauch der Informationssysteme und zur ungerechtfertigten Bereicherung motivieren können[62]. Es müssen also zusätzliche Grenzen und Kontrollen innerhalb der Informationssysteme eingeführt werden, um derartige Missbräuche entdecken und verfolgen zu können.

Verlagerung des Arbeitsorts

Durch die Internationalisierung und die zunehmende Vernetzung von Unternehmungen untereinander intensiviert sich die Reisetätigkeit der Mitarbeiter. Das führt zu schlechterer Erreichbarkeit der einzelnen Personen, vermehrter Absenz vom Arbeitsplatz, im Extremfall zur Aufhebung eines persönlichen Arbeitsplatzes. Die Arbeitstätigkeit wird auf mobile Informationssysteme verlagert, welche über Kommunikationsnetze auf zentrale Serversysteme zugreifen. Arbeitsplätze befinden sich zunehmend im Umfeld des Kunden, in öffentlichem (Flugplatz, Bahnhof etc.), halbprivatem (Sitz im Flugzeug, in der Bahn oder im Auto) oder privatem Umfeld (Heimarbeitsplatz). Mobile (*mobile*) und entfernte (*remote*) Informationsverarbeitung wird deshalb weiterhin zunehmen. Die bisher übliche Abschottung des Arbeitsumfeldes durch Zutrittskontrollen und Schliesssysteme (z.B. Bürotüren, Ablageschränke) muss zunehmend auf die informationstechnischen Systeme übertragen und davon abgelöst werden. Dabei sind die einzelnen Mitarbeiter vermehrt selbst für die Sicherheit verantwortlich, welche früher an andere unternehmensinterne oder -externe Stellen (Objektschutz, Portier etc.) übertragen werden konnten. Die Informationssicherheit muss also im Interesse der Unternehmung Konzepte zum Schutz der Informationen durch die Mitarbeiter selbst bereitstellen.

Veränderung von Arbeitsverhältnis und Arbeitsablauf

Durch die fortschreitende Digitalisierung und Individualisierung wird eine Arbeitstransformation initiiert ([Peters96], S. 20, S. 50ff, [Lutz95], S. 18ff, S. 139), welche die Neuaufteilung und Neuorganisation der Arbeit und der

---

62 Beispiel: Ein Mitarbeiter in der schweizerischen Niederlassung wird sich wahrscheinlich nicht mit einem Monatsgehalt bestechen lassen, vertrauliche Informationen herauszugeben. Dieselbe Geldmenge kann jedoch den indischen Mitarbeiter an demselben unternehmensweiten Intranet durchaus zur Konspiration bewegen, da diese Geldmenge einem Jahresgehalt oder mehr entsprechen kann.

Arbeitsverhältnisse zur Folge hat. Allgemein wird von einer höheren Flexibilisierung der Kooperation zwischen Arbeitgeber und Arbeitnehmer ausgegangen. Arbeitszeit wird zur frei und stückweise handelbaren Ressource – sofern es sich um telefähige Informationsarbeit handelt oder um Wissensdienstleistungen. Zeitlich begrenzter Einsatz externen Fachwissens (Berater) kann sogar gegenüber der festen Anstellung eigener Mitarbeiter bevorzugt werden.

Auch der Ablauf der Arbeit oder Führung selbst in den Schritten „Planen – Entscheiden – Anweisen – Kontrollieren" (PEAK) wird in Frage gestellt, weil die zunehmend komplexen Tätigkeiten sich nicht mehr so linear steuern lassen wie die Maschine des industriellen Zeitalters. Die starken Rückkopplungen, denen Führungsprozesse unterliegen, können dazu führen, dass sie stark verkürzt werden. Neben den *Aktionen*, die PEAK innewohnen, können die *Reaktionen auf die Rückkopplung* einen höheren, wenn nicht gleichwertigen Stellenwert erhalten. [Lutz95 S. 18 und S. 139].

Die *Anstellung* wird zunehmend durch den *Auftrag* ersetzt; die Bindung zwischen Arbeitgeber und Arbeitnehmer also lockerer. Die Informationssicherheit muss gewährleisten, dass trotz der daraus folgenden verminderten Weisungsbefugnis die Rahmenbedingungen für die Nutzung von Informationen und Ressourcen des Auftraggebers so gestaltet werden, dass eine Kontrolle des Auftragnehmers durch den Auftraggeber erfolgen kann.

Die *zentrale* Anordnung von Vorschriften der Informationssicherheit wie auch anderer Weisungen verliert dadurch an Bedeutung und wird durch eine föderalistisch organisierte Subsidiarität ersetzt, welche die notwendigen Entscheidungen so dezentral wie möglich, so zentral wie notwendig veranlasst. Die direkte Kontrolle der Vorgehensweise ist nicht mehr möglich; immer mehr muss durch Zielvereinbarungen und Kontrolle der Zielerreichung geführt werden [Lutz95, S. 101].

Daraus folgt eine Teilautonomie vieler Unternehmungen und Unternehmungsteile. Die Informationssicherheit muss sich so organisieren, dass sie diese Teilautonomie unterstützt und sie benutzt, um die Anforderungen der Informationssicherheit zu gewährleisten. Sie muss also ebenfalls die dezentrale Organisation mit Koordination und Kooperation erlauben und unterstützen. Ausserdem muss sie in kleinen integrierten Zyklen ablaufen, also einerseits als eigenständiger Prozess erkennbar sein, andererseits in das Controlling und das Interne Kontrollsystem der Unternehmung integriert werden.

Mehrfache Rollen

Die Verlagerung des Arbeitsortes kann zur Vermischung unternehmerischer und privater Inhalte und zu Rollenkonflikten führen. Während beispielsweise im privaten Bereich jeder immer für sich selbst spricht, ist jede Person als Mitarbeiter

den Interessen seiner Unternehmung verbunden. Jede gültige Meinungsäusserung eines Mitarbeiters wurde bisher durch die Verwendung von firmeneigenem Briefpapier gekennzeichnet. Dies ist bei der Verwendung digitaler Medien momentan noch nicht Usanz.

Informationssicherheit muss also Richtlinien bereitstellen, um diese Rollenkonflikte zu verhindern oder zu zumindest auszuweisen.

Erwartung von Verbindlichkeit

Durch die zunehmende Verwendung digitaler Kommunikationsmittel werden die Kommunikationsinhalte (also z.B. auch E-Mail) zunehmend als verbindlich aufgefasst. Informationssicherheit muss die notwendigen Verfahren zur Verfügung stellen, um diese Verbindlichkeit zu gewährleisten. Dazu werden schon heute *Zertifizierungsinfrastrukturen* aufgebaut, welche die eindeutige Authentifizierung des Gesprächspartners erlauben. Zusätzlich erhöhen die verwendeten Technologien die Vertraulichkeits- und Integritätswahrung während der Kommunikation (z.B. durch Verschlüsselungsverfahren) und die Entdeckung und Eliminierung von Angriffen auf die Kommunikation. Die Einführung des notwendigen Wissens zur Nutzung dieser Strukturen durch die Mitarbeiter obliegt der Informations-sicherheit.

Zunehmender Missbrauch

Der Missbrauch der unternehmerischen Ressource Information und des Informationssystems nimmt gemäss Aussage des zweiten Sicherheitsreports von Atag, Ernst & Young zu. "*Vor allem in der Schweiz werden die Gefahren, die von Mitarbeitern, Partnern und nicht autorisierten Personen ausgehen, markant höher eingeschätzt als im Vorjahr. So sehen heute 22.6 Prozent der Firmen die eigenen Mitarbeiter als eine ernsthafte Bedrohung für die IT-Sicherheit.*" [Cash98.39, S. 59].

Die Entdeckung von Missbräuchen ist eine Aufgabe der unternehmerischen Revision, sie ist jedoch auf Massnahmen angewiesen, welche durch das Controlling aufgebaut und eingehalten werden müssen. Informationssicherheit muss also mit der Revision zusammenarbeiten.

Propagation von Anomalien

Domino- und andere Propagations-Effekte durch Softwareanomalien sind schon mehrfach aufgetreten, z.B. 1988, als ein *Internet-Wurm* zum zeitweisen Ausfall weiter Teile des Internet geführt hat [Neumann95, S. 133f]. Aufgrund der noch viel geringeren Verbreitung des Internet waren vor allem akademische und staatliche Organisationen betroffen. Ein gleichartiger Ausfall hätte heute viel grössere Konsequenzen und muss deshalb so gut wie möglich verhindert werden. Trotz ständiger Verbesserung der zugrundeliegenden Basistechnologien entstehen

aufgrund der zunehmenden Komplexität der Systeme immer wieder Sicherheitslücken, welche nur durch ständige Beobachtung der technologischen Entwicklung beseitigt werden können. Die Informationssicherheit muss durch Abgrenzung der Systeme die Propagation solcher Anomalien auf die unternehmerischen Systeme verhindern.

Abnehmende Transparenz

Informationssicherheit muss dazu betragen, alle Informationsflüsse für die jeweils Beteiligten transparent zu gestalten. Das bedeutet, dass einerseits jeder Benutzer sich jederzeit auf einfache Weise darüber informieren kann, welche Systeme an einem Verarbeitungsvorgang beteiligt sind und wer die Verantwortung für die Sicherheit dieser Systeme trägt. Andererseits müssen diese Vorgänge so transparent ablaufen, dass keine ungewollte Beeinflussung der Informationsverarbeitung selbst geschieht.

Erstarkung externer Interessengruppen

Durch die zunehmende Konkurrenz auf Arbeits- und Produktmärkten sowie die zunehmend angespannte ökologische Situation entstehen neue Interessengruppen, welche die Informationstechnologie in fragwürdiger Weise als Mittel zur Durchsetzung ihrer Interessen verwenden können. Beispielsweise fordern Anwaltsgruppen des Ökosystems von der Unternehmung Umweltverträglichkeit, also die neutrale oder positive Beeinflussung der Umwelt durch die Unternehmung, wobei die Beurteilung durch die Anwaltsgruppen selbst vorgenommen wird. Diese Beurteilung beruht auf Informationen, welche die Unternehmung nur teilweise freiwillig publik macht. Es ist denkbar, dass Anwaltsgruppen die weiteren, "unter Verschluss gehaltenen" Dokumente unter Ausnutzung von Schwachstellen des unternehmerischen Informationssystems zu beschaffen versuchen. Informationssicherheit muss derartige Angriffe abwehren können. Dazu muss sie mit der unternehmerischen Sicherheit und denjenigen Stellen innerhalb der Unternehmung zusammenarbeiten, welche über derart vertrauliche Informationen verfügen.

Nicht nur die Anwaltsgruppen des Ökosystems können grossen Einfluss auf die *öffentliche Meinung* besitzen. Die *Medien* wirken dabei als Verstärker. Die öffentliche Meinung äussert sich in dem Goodwill, welcher der Unternehmung durch bisherige und neue Partner entgegengebracht wird. Da negativer Goodwill zu Sanktionen der Gesellschaft führen kann (von der Behinderung bis zum Boykott) ist jede Unternehmung an möglichst hohem Goodwill interessiert. Das Management fordert entsprechend *positive Image-Wirkung* von den bekannt gewordenen Handlungen der Unternehmung. Die Beurteilung der Wirkung geschieht anhand von oft nicht genau bestimmbaren *Ethik-* und *Moralvorstellungen* und *Werthaltungen der Gesellschaft*, was grundsätzlich zur Anforderung nach *ethischem*

und moralischem Handeln führt. Diese Vorstellungen und Werte sind kulturabhängig und deshalb national verschieden.

Im Extremfall können soziale Unruheherde entstehen, welche sich in Gewalt gegen Sachen (z.B. Informationsinfrastruktur der Unternehmung), aber auch gegen ideelle Werte von Unternehmungen (Marktpolitik, Produktionspolitik, Personalpolitik etc.) richten kann (z.B. Informationen der Unternehmung) sowie gegen die Informationsträger (leitende Mitarbeiter).

Informationssicherheit muss deshalb auch berücksichtigen, welche Anforderungen externe Stellen an die unternehmensinterne Information stellen können und in Zusammenarbeit mit den entsprechenden Institutionen der Unternehmung die Erfüllung dieser spezifisch festzulegenden Kriterien gewährleisten. Darüber hinaus muss sie gewaltsame Übergriffe vorbeugend verhindern und Personen, Informationen und technische Einrichtungen schützen.

Individualisierung

Die Sättigung vieler Märkte in den hochentwickelten Ländern führt zu vermehrtem Individualismus ([Peters96], S. 19, S. 42ff, [Lutz95], S. 67) und Post-Konsum-Verhalten ([Peters96], S. 21, S. 87ff, [Lutz95], S. 101, S.114). Die Unternehmungen richten ihre Kundenbetreuung und Produkteherstellung stärker auf den einzelnen Konsumenten aus und werden dabei von der Informationstechnologie und der Sammlung kundenspezifischer Daten unterstützt. *Custom-Build-to-Order* und *One-To-One-Marketing* sind zwei dieser Post-Konsum-Entwicklungen, die auf individueller Bindung von Unternehmung und Kunde beruhen.

Das immer stärker auf den Einzelnen abgestimmte Produkteangebot setzt die Sammlung umfangreicher Konsumentendaten voraus. Die Informationssicherheit innerhalb der Unternehmung muss sicherstellen, dass der Umgang mit diesen Daten den gesetzlichen Normen entspricht, und dass die Verwendung im Einverständnis der Kunden geschieht.

Zunehmende private Abhängigkeit

Die zunehmende Abhängigkeit jedes Einzelnen führt dazu, dass auch im privaten Bereich Sicherheitskonzepte der Informationsverarbeitung bedacht werden müssen. Beispielsweise stellt der Ausfall von Energie- oder Kommunikationssystemen für den Einzelnen immer eher ein Problem dar. Doch auch die Computertechnologie hält in Privathaushalten Einzug. So schreibt beispielsweise Borchers in der NZZ: "*Die Eroberung des Heims wird durch verschiedene Technologien unterstützt. [...] Konvergenz von Computertechnik und Unterhaltungselektronik [...] Tatsächlich entstehen in vielen Heimen die ersten «Home Networks», bei denen mehrere PCs, Drucker und Kommunikationsleitungen gekoppelt werden.*" Verschiedene Technologien unterstützen die Vernetzung des Heimes mit Internet über Telefon-, Strom- und Fernsehkabel. [NZZ98.09.29]. Die unternehmerische

Informationssicherheit muss auch hier Konzepte bereitstellen, wenn es sich um wichtige Stakeholder (z.B. zuhause arbeitende Mitarbeiter oder Kunden) handelt.

4.3.2 Fazit

In den vorhergehenden Abschnitten wurden verschiedene antizipierte Entwicklungen betrachtet und aus ihnen Anforderungen an die Informationssicherheit hergeleitet. Aufgrund der geschilderten Entwicklungen obliegt der Informationssicherheit in der Unternehmung eine breit gefächerte Aufgabe.

Vordringlich muss Informationssicherheit also

- die Entwicklungen im sozialwirtschaftlichen Umfeld berücksichtigen, welche oft unter dem Schlagwort *Globalisierung* zusammengefasst werden, und allgemeine Vorgehensweisen und Verfahren zur Wahrung der Informationssicherheit bereitstellen,
- die Sicherheit der verwendeten Technologien kontinuierlich untersuchen und bekannt gewordene Schwachstellen konsequent ausmerzen,
- die sichere Verwendung der Informationstechnologie fördern, indem sie über die Beeinflussung der Sicherheitskultur sicheres Verhalten fördert,
- in Zusammenarbeit mit der Produktesicherheit die informationellen Komponenten der Produkte sicher gestalten,
- die Bündelung und Filterung grosser Datenmengen unterstützen,
- die Wirkung von Information auf die Stakeholder der Unternehmung berücksichtigen,
- die stattfindende Übertragung der Arbeit auf digitale Systeme unterstützen und insbesondere die Verbindlichkeit der unternehmerischen Transaktionen gewährleisten,
- die Transformation von Arbeitsform, -verhältnis und -ort sicher zu gestalten helfen,
- mit der Revision zusammenarbeiten, um Missbräuche zu verhindern, zu entdecken und zu belegen,
- dazu die konsequente Abgrenzung von Systemen vornehmen,
- von der zentralen zur persönlichen und individualisierten Betrachtung übergehen und sich dazu föderalistisch organisieren,
- die Transparenz der technischen Informationssysteme fördern,
- Mitarbeiter, Informationen und technische Systeme gegen gewaltsame Übergriffe schützen.

4.4 Informationssicherheit als Ziel

Ziel dieses Abschnittes ist es, die innere Motivation der Unternehmung zur Betrachtung der Informationssicherheit zu argumentieren.

4.4.1 Zielsystem der Unternehmung

Informationssysteme werden zur Erreichung der Ziele von Unternehmungen eingesetzt. Beispiele für Ziele der Unternehmungsführung sind *Gewinnmaximierung, Sicherung der Existenz, Maximierung des Shareholder Value, Konformität mit gesetzlichen Rahmenbedingungen (Ordnungsmässigkeit), Umsatzmaximierung, Effizienzsteigerung, Wachstum, Stabilität und Planbarkeit, Zufriedenheit der Stakeholder* etc.[63] Diese Ziele sind teilweise voneinander abhängig (z.B. kann Gewinnmaximierung über Effizienzsteigerungen erreicht werden), diese Abhängigkeiten sind jedoch nicht eindeutig und bei jeder Unternehmung unterschiedlich. Informationssicherheit unterstützt jedoch langfristig die Erreichung jedes dieser Ziele.

- Informationssicherheit trägt zur Gewinnmaximierung und zur Maximierung des Shareholder Value bei, indem sie die Verlässlichkeit der Informationen erhöht, auf welchen unternehmerische Entscheidungen aufbauen und so den benötigten Mitteleinsatz reduziert.
- Informationssicherheit sichert die Existenz, indem Sie Klarheit über die bestehenden Risiken schafft, so die Möglichkeit präventiven Handelns schafft und verhindert, dass entstehende Schäden existenzbedrohend werden.
- Informationssicherheit erhöht die Konformität mit gesetzlichen Rahmenbedingungen, indem in ihrem Rahmen die unternehmerischen Tätigkeiten auf ihre Konformität geprüft und gegebenenfalls Änderungen veranlasst werden.
- Informationssicherheit trägt zur Umsatzmaximierung und zur Effizienzsteigerung bei, indem sie die Verfügbarkeit von Informationen sicherstellt und indem sie Informationen über die Informationsverarbeitung selbst bereitstellt, welche zur Optimierung der Geschäftsprozesse verwendet werden können.
- Informationssicherheit trägt zur Stabilität und Planbarkeit der unternehmerischen Abläufe bei, indem sie Randbedingungen dieser Abläufe untersucht und gegebenenfalls Massnahmen veranlasst, um Störungen der Abläufe zu vermeiden, zu verhindern oder zu versichern.

---

63 Die relative Priorität dieser Ziele wird massgeblich von den Zielen der Aufgabenträger in der Unternehmungsleitung bestimmt, welchen die Erreichung dieser unternehmerischen Ziele obliegt. Diese Betrachtung soll hier nicht vertieft werden.

- Informationssicherheit trägt zur Zufriedenheit der Stakeholder bei, indem sie die Wirkung der Unternehmung und der von ihr nach aussen abgegebenen Informationen betrachtet.

4.4.2 Einfluss der Informationssicherheit auf die unternehmerische Zielerreichung

Die Aufgabe der Informationssicherheit umfasst die Herleitung eines sicheren Zustandes des Informationssystems unter Berücksichtigung der übergeordneten unternehmerischen Ziele.

Kurz und mittelfristig kann die Informationssicherheit die Flexibilität und Effizienz des Informationssystems einschränken. Beispielsweise ist es möglich, dass aus Gründen der Informationssicherheit Vorgehensweisen und Massnahmen umgesetzt werden, welche das System im bestehenden Zustand fixieren. Eine solche Fixierung auf Kosten der Flexibilität erhöht die Vorhersagbarkeit des Systemverhaltens und somit die Verlässlichkeit des Systems. Allerdings führt sie auch dazu, dass eine Veränderung des Informationssystems in einen neuen funktionstüchtigen Zustand erschwert wird. Solche Veränderungen sind notwendig, wenn die Unternehmung sich konsequent dem Markt anpassen will, um konkurrenzfähig zu bleiben und so die langfristigen Ziele zu erreichen.

Auch die Effizienz der Informationsverarbeitung kann durch Informationssicherheit kurz- und mittelfristig eingeschränkt werden. Beispielsweise kann es notwendig sein, aufwendige Benutzeridentifikations- und Authentifikationsmassnahmen durchzuführen, bevor die Benutzung einzelner Teilsysteme erlaubt wird. Auch diese Einschränkung ist jedoch gerechtfertigt, wenn dadurch langfristig Missbrauch der Systeme verhindert und so die Existenzsicherung und die Konformität mit gesetzlichen Anforderungen gewährleistet werden kann.

Die Ziele der Informationssicherheit konfliktieren also mit den oben genannten langfristigen unternehmerischen Zielen. Dies hat einerseits zur Folge, dass die Anforderungen an die Informationssicherheit unterschiedlich festgelegt werden: ein strategischer Blickwinkel führt eher zur Förderung der Informationssicherheit (also zur Festlegung eines höheren Sicherheitsniveaus), während aus taktischem und operativem Blickwinkel eher ein niedrigeres Sicherheitsniveau anstrebt wird.

In der Praxis allerdings beginnt sich erst langsam das Informationsbewusstsein durchzusetzen, welches eine strategische Förderung der Informationssicherheit erst möglich macht. Zwar sind schon heute die Kontrollstrukturen der Unternehmungen so aufgebaut, dass sie Informationssicherheit in der Unternehmung fordern. So ist es Aufgabe der externen Revisionsstelle, die Ordnungsmässigkeit der unternehmerischen Tätigkeiten (also auch der Informationsverarbeitung) zu prüfen. Die interne Revisionsstelle wird vom Verwaltungsrat beauftragt, Effizienz, Effektivität und die Einhaltung weiterer Anforderungen zu prüfen. Dabei verfolgt sie die Ziele der Eigentümerschaft der Unternehmung. Diese beiden

Revisionsstellen decken jedoch nicht notwendigerweise alle Anforderungen ab, welche von der Unternehmungsführung an eine sichere Informationsverarbeitung zu stellen wären. Die strategische Förderung der Informationssicherheit durch die Unternehmungsleitung könnte also die Zielerreichung der Unternehmungsführung besser unterstützen als die reine Beschränkung auf die Erfüllung der Anforderungen der Revision oder die Delegation der Informationssicherheit auf taktische und operative Ebene der Unternehmung.

4.4.3 Bewertungskonflikte

In einem unternehmerischen Umfeld verfolgen mehrere Personen ein gemeinsames Ziel. Entsprechend wird auch das Sicherheitsniveau von mehreren Personen beeinflusst. Jede Person bestimmt jeweils das Sicherheitsniveau derjenigen Objekte, welche in ihrem jeweiligen Zuständigkeitsbereich liegen. Da jedoch auch in gut funktionierenden Firmen Zielkonflikte bestehen, wird das Sicherheitsniveau oft von verschiedenen Personen nicht identisch festgelegt, was zu unterschiedlichen Sicherheitsniveaus innerhalb der Unternehmung führt (Bsp.: Unterschiedliche Meinungen über die relative Priorität von Projekten der Unternehmung).

Neben unternehmensinternen Anspruchsgruppen (Mitarbeiter) bestehen auch unternehmensexterne (Stakeholder) wie Kunden, Lieferanten, Staat und Gesellschaft. Die verschiedenen wirkenden Interessen haben Einfluss auf die Anforderungen, welche an die Unternehmung und an ihre Informationsverarbeitung von aussen gestellt werden und welche sie daraufhin selbst stellt.

Dies hängt wiederum davon ab, wieviel Information über die Tätigkeiten einer Firma aus ihr heraus- oder in sie hineinfliesst. Der Informationsfluss über die Grenze zwischen Unternehmung und Umwelt hinweg beeinflusst die Sicherheit der Unternehmung.

Die Unternehmung ist als Organisation nicht Eigentümer aller darin vorhandenen Informationen. Insbesondere Personendaten (also Angaben über Eigenschaften von natürlichen oder juristischen Personen, welche beispielsweise in Anstellungs-, Auftrags-, Liefer- oder Klientenverhältnis mit ihr stehen) bleiben Eigentum der dadurch beschriebenen Personen und sind lediglich im Besitz der Unternehmung. Auch Informationen, welche Dritte zur Leistungserbringung (z.B. zur Führung der Buchhaltung) oder aus wirtschaftlichem Interesse (z.B. als Folge von Lizenzvereinbarungen) zur Verfügung stellen, gehören der Unternehmung nicht. Es liegt im Interesse der Unternehmung, mit den ihr auf diese Weise anvertrauten Daten im Sinne der Eigentümer und gemäss den Richtlinien des umgebenden Rechts- und Wirtschaftssystems umzugehen, um Sanktionen zu vermeiden. Diese Fähigkeit der Unternehmung ist eine Eigenschaft ihres Informationssystems und muss von der Informationssicherheit betrachtet werden.

Um einen möglichst einheitlichen Umgang mit den Informationen zu erreichen wird jede in der Unternehmung vorhandene Information ideal genau einer Person

zugeteilt. Diese Person ist für die Sicherheit der Information verantwortlich und bestimmt dessen Sicherheitsniveau. Sie wird in der Regel als *Verantwortlicher* für das Objekt oder *Objekteigentümer* bezeichnet. Es liegt im Interesse dieser Person, unter Annahme des Wertes des Objektes und unter Minimierung der Kosten, welche durch Sicherheitsmassnahmen entstehen oder durch verlorene Effizienz, das Sicherheitsniveau so zu bestimmen, dass keines der angenommenen Risiken den Wert des Objekts zu stark senkt. Es liegt im Interesse des *rechtlichen* Besitzers des Objektes, dass die bewertende Person diese Bewertung im Interesse der Gesamtunternehmung durchführt und nicht vor allem in ihrem eigenen Interesse.

4.4.4 Wirkung von Informationen

Die gezielte Verbreitung verschiedener Informationen an bestimmte externe Empfänger und die Betrachtung der geplanten und tatsächlichen *Wirkung* dieser Informationen kann im Rahmen der Informationssicherheit eine Rolle spielen, da Rückwirkungen auf interne Verarbeitungen möglich sind. Auch sind alle Informationen, welche die Unternehmung von ihrer Umwelt aufnimmt, auf ihre Auswirkungen auf die innere Informationssicherheit zu prüfen. Möglicherweise müssen Veränderungen in externen Systemen angestrebt werden, um die Informationssicherheit innerhalb der Unternehmung effizienter gewährleisten zu können.

Beispielsweise ist es Aufgabe einer unternehmerische Stelle für Öffentlichkeitsarbeit, die Wirkung der von der Unternehmung an die internen und externen Stakeholder abgegebenen Informationen zu kanalisieren und zu prüfen, ob diese Wirkung dieser Informationen den daran gestellten Anforderungen genügt.

Eine Unternehmung – und das Informationssystem als eine wichtige Komponente – befindet sich immer in einem sozialen, wirtschaftlichen und politischen Kontext. Es darf deshalb nicht vernachlässigt werden, welche Wirkung Information hat, wenn sie aus der Unternehmung in einen dieser Kontexte eintritt oder umgekehrt, bzw. welche Wirkung das Informationsmanagement einer Unternehmung auf ihre Umwelt hat. So hat beispielsweise die Entscheidung einer Unternehmung, bisher frei verfügbare Information nur noch gegen Entgelt verfügbar zu machen, mehrere Rückwirkungen auf die Unternehmung. Einerseits die direkte, erwünschte Mehreinnahmen durch diejenigen Informationsnachfragen zu erreichen, welche von abhängigen Nachfragern stammen. Andererseits kommt es aber zum Verlust des Goodwills der Kunden, welche nach Substitutionsprodukten Ausschau halten und möglicherweise auch andere Produkte fortan bei der Konkurrenz beziehen. Drittens kann die Entscheidung der Unternehmung auch gegen geltendes Recht verstossen und staatliche Sanktionen nach sich ziehen. All dies kann wieder Rückwirkungen auf das Informationsmanagement auslösen. Falls nicht diejenigen Auswirkungen erreicht wurden, welche von den Trägern des Informationsmanagements beabsichtigt waren, so entsprach das Informationsmanagement nicht den Anforderungen. Dies kann als Sicherheitsproblem aufgefasst werden. Wegen des

Bezugs des Informationsmanagements auf Information ist es ein Problem der Informationssicherheit.

Es kommt allerdings selten vor, dass willentliche Entscheidungen des Informationsmanagements zu Sicherheitsproblemen führen, zumal wenn Informationsmanagement als kollektive Tätigkeit innerhalb einer Unternehmung gesehen wird. Eher problematisch sind Entscheidungen und Tätigkeiten Einzelner, welche auf Basis der Vorgaben des Informationsmanagements gefällt werden, diesem jedoch nicht entsprechen.

4.4.5 Fazit

Informationssicherheit ist ein Teil des Informationsmanagements der Unternehmung und hat ihre theoretischen Grundlagen in der Wirtschafts-informatik. Informationssicherheit bezieht sich auf das Informationssystem der Unternehmung und somit primär auf alle Informationsverarbeitungsvorgänge innerhalb der Unternehmung.

Ziel der Informationssicherheit ist es, dass die Informationsverarbeitungsvorgänge die an sie gestellten Anforderungen erfüllen. Dieses Ziel wird anderen Zielen der Unternehmung untergeordnet und unterstützt die Erreichung dieser anderen Ziele. Insbesondere beeinflusst die Informationssicherheit dabei Effizienz und Flexibilität der Zielerreichung auf einer operativen und taktischen Ebene negativ, um strategisch zur langfristigen Erreichung der übergeordneten Ziele beitragen zu können. Einzelne Teilziele der Informationssicherheit werden von der internen und externen Revisionsstelle der Unternehmung getragen. Es steht der Unternehmungsführung frei, die Erreichung darüber hinaus gehender Ziele durch Förderung der Informationssicherheit zu forcieren.

In jeder Unternehmung bestehen Bewertungskonflikte, welche aus den unterschiedlichen Zielen der einzelnen Personen entstehen. Es ist deshalb sinnvoll, jede Information genau einer Person zuzuordnen, welche die an diese Information zu stellenden Sicherheitsanforderungen festlegt (Sicherheitsniveau) und für die Sicherheit des entsprechenden Informationsobjekts verantwortlich ist (Objekteigentum).

Auch wenn Informationssicherheit sich rein begrifflich auf alle Informationen und Informationsverarbeitungsprozesse der Unternehmung bezieht, ist eine Beschränkung der Betrachtung auf Bedingungsrisiken sinnvoll. Es werden also vor allem diejenigen Eigenschaften der zu schützenden Systeme betrachtet, welche unwillentlichen Einflüssen unterliegen. Das Management der Informations-sicherheit muss allerdings mit denjenigen Stellen innerhalb der Unternehmung zusammenarbeiten, welche die willentliche Informationsverarbeitung steuern.

4.5 Instrumente

Bei den Instrumenten des Informationssicherheitsmanagements lassen sich diejenigen zur Beeinflussung des Bezugsobjekts und diejenigen zur Steuerung und Unterstützung des ISi-Prozesses unterscheiden. Erstere sollen als *externe Instrumente* bezeichnet werden, da sie sich auf Objekte des Informationssicherheitsmanagements beziehen; letztere als *interne Instrumente*, weil die das Informationssicherheitsmanagement selbst unterstützen.

4.5.1 Externe Instrumente

Die Beeinflussung des Bezugsobjekts geschieht beim Management der Informationssicherheit über *Massnahmen*. Sie lassen sich in Gruppen oder Bereiche einteilen und umfassen dabei die in Kapitel 3 identifizierten, in Kapitel 5 detaillierten Fachgebiete.

Üblich ist eine Einteilung in organisatorische, personelle, technische und bauliche Massnahmen.

Organisatorische Massnahmen beziehen sich auf die *Informationen* und *Prozesse* innerhalb der Unternehmung. Personelle Massnahmen beziehen sich auf *Institutionen* (auf Gremien sowie Personen als Subjekte und Objekte in der Unternehmung) und betreffen besonders die personellen Aspekte der Informationsverarbeitung, d.h. die Beeinflussung sicheren Verhaltens durch motivierende, fakultative und obligatorische Regelungen. Dies entspricht dem Führungsaspekt der Menschenführung und umfasst die Etablierung einer *Sicherheitskultur*.

Technische Massnahmen beziehen sich auf die *Instrumente* und auf das *Produktionssystem* und betreffen alle technischen Informationsverarbeitungsvorgänge innerhalb der Unternehmung. Bauliche Massnahmen beziehen sich auf die zugrundeliegende *Infrastruktur* inkl. Energieversorgung und Zutrittskontrolle.

Aufgrund der starken gegenseitigen Durchdringung dieser Gruppen ist die Abgrenzung nicht scharf. Ebenfalls möglich ist eine Unterteilung nach unternehmerischer Handlungsebene bzw. Fristigkeit der Massnahmenwirkung in strategisch / langfristig, taktisch / mittelfristig und operativ / kurzfristig. Weitere Unterteilungen sind möglich.

Massnahmen können nur in einer konkreten Anwendungsumgebung genau spezifiziert werden. Jede Abstraktion – so wie sie der Zusammenstellung und Publikation von Massnahmenkatalogen geschieht – hat auch eine Verallgemeinerung der Massnahmenformulierung zur Folge. Nur im technischen Bereich, in welchem die Spezifikationen konkreter Produkte als Basis für sicherheitsfördernde Massnahmen verwendet werden, lassen sich auch Massnahmen konkret formulieren. Beispielsweise umfassen das IT-

Grundschutzhandbuch [BSI-IT-GSHB97] oder die Publikation "Hacker Proof" [Klander97] konkrete Massnahmen zum Schutz technischer Systeme.

Sobald jedoch keine einheitliche Spezifikation vorausgesetzt werden kann, also sowohl im organisatorischen, personellen und baulichen Bereich jeder Unternehmung, müssen die Massnahmen vor der Anwendung interpretiert und konkretisiert werden.

4.5.2 Interne Instrumente

Die internen Instrumente werden vom Informationssicherheitsmanagement verwendet, um sich selbst zu verwalten und die Informationen über das Bezugsobjekt zu strukturieren und zu gestalten. Konkret sind Formulare, Massnahmenkataloge und Bewertungskriterienkataloge als interne Werkzeuge zu bezeichnen. Die Verwaltung der Informationen über die erhobenen Objekte sowie die Herstellung von Zusammenhängen zwischen ihnen kann geschieht i.d.R. durch computerunterstützte Werkzeuge, welche den Verwaltungsaufwand reduzieren (sog. Computer-Aided Audit Tools CAAT oder Computer Aided Information Security CAIS). Ein Beispiel für ein solches Werkzeug wird in Kapitel 10 entwickelt.

Fazit

Informationssicherheit muss als Ziel festgelegt werden, innerhalb der Unternehmung umgesetzt werden und diese Umsetzung muss kontrolliert werden. Dazu sind *Institutionen* notwendig. Die bestehenden Institutionen und Funktionen der Kontrolle wurden hier identifiziert und beschrieben. Dabei wurde festgestellt, dass die Begriffe *Controlling*, *Kontrolle*, *Überprüfung* und *Revision* teilweise doppelt belegt sind. Der hier hergeleitete Zusammenhang zwischen diesen Begriffen ist in Abbildung 4-1 (Seite 111) dargestellt.

Darauf aufbauend wurden Gestaltungsvorschläge für das Controlling und die Revision der Informationssicherheit abgegeben. Diese umfassen insbesondere ein Rollenmodell mit 9 Rollen. Jeder Person in der Unternehmung können dabei eine oder mehrere Rollen zugeordnet werden, welche jeweils Aufgaben, Verantwortungen und Kompetenzen umfassen.

Die Ziele und inhaltlichen Motivationen zur Betrachtung von Informations-sicherheit wurden aus Entwicklungen des sozialökonomischen Umfelds hergeleitet. Jede der Entwicklungen *zunehmendes Informationsbewusstsein, Intensivierte Anwendung von Informationstechnologie, Tertiarisierung, Informationsflut, Anforderungen an die individuelle Kommunikation, Verlagerung des Arbeitsorts, Veränderungen von Arbeitsverhältnis und Arbeitsablauf, mehrfache Rollen, Erwartung von Verbindlichkeit, zunehmender Missbrauch, Propagation von Anomalien, abnehmende Transparenz, Erstarkung externer Interessengruppen,*

Individualisierung und *zunehmende private Abhängigkeit* wurde kurz beschrieben. Es wurden jeweils Folgerungen für die Inhalte der Informationssicherheit daraus hergeleitet.

In einem zweiten Schritt wurden die Ziele der Informationssicherheit inhaltlich hergeleitet und festgestellt, dass Informationssicherheit die Erreichung der unternehmerischen Ziele langfristig unterstützt, wenngleich kurzfristig mit Einbussen bei Effizienz und Flexibilität gerechnet werden muss.

Schliesslich wurden die Massnahmen als *externe Instrumente* der Informationssicherheit kurz beschrieben und eingeteilt sowie Computer-Aided Audit Tools als Beispiel für *interne Instrumente* des Informationssicherheits-managements bezeichnet.

5 Tätigkeiten

Sicherheit kann als Querschnittsfunktion jeder unternehmerischen Tätigkeit betrachtet werden: Die einzelnen Fachgebiete der Informationssicherheit, welche in Kapitel 3 identifiziert und kurz erläutert wurden, werden in diesem Kapitel deutlicher und umfassender gemäss Rahmenwerk in Abschnitt 1.3 bzw. Abschnitt 3.1 beschrieben. Die Strukturierung erfolgt gemäss rechtem Teil von Abbildung 3-12, Seite 95) (identisch in Abbildung 5-1 wiedergegeben).

Viele der Sicherheitsgebiete haben Berührungspunkte untereinander. So ist beispielsweise die technische Kommunikationssicherheit von der Sicherheit der Infrastruktur abhängig und die Sicherheit der Aufgabenbearbeitung von der Sicherheitskultur. Einige der Themenbereiche betreffen mehrere der hier vorgesehenen Kategorien. Sie werden hier beim jeweils übergeordneten Bezugsobjekt erläutert; dabei wird jeweils auf die untergeordneten Aspekte und ihre Beschreibung in anderen Abschnitten verwiesen.

Es soll hier keine vollständige Aufzählung der Fachgebiete entstehen – ein Beweis der Vollständigkeit wäre ohnehin nicht zu erbringen – sondern es soll verdeutlicht werden, dass sich wichtige Fachgebiete in das hier verwendete (in Kapitel 3 entworfene und beschriebene) Modell eingliedern lassen und auf diese Art eine auf die *Informationen* ausgerichtete Strukturierung der Informationssicherheit möglich ist. Dies steht im Gegensatz zu der üblicherweise auf Technologien ausgerichteten Strukturierung der IT-Sicherheit. Ausserdem dienen die hier identifizierten Fachbereiche als Inhalte von Detaillierungsgrad 4 des in Kapitel 8 vorgeschlagenen Informationssicherheitsprozesses *ISiWAY*.

An einigen Stellen wird auf den Code of Practice for Information Security [BSI-COP95] oder auf das COBIT-Framework [COBIT96.3] verwiesen. Ähnliche Zusammenstellungen (mit abweichender Struktur und unterschiedlichem Umfang und Vollständigkeitsgrad) finden sich in der weiterführenden Literatur gemäss Literaturliste. Der Beitrag der vorliegenden Arbeit liegt in der neuen Strukturierung und inhaltlichen Abgrenzung.

Abbildung 5-1: Sicherheitsfachgebiete des Bezugsobjekts der Informationssicherheit

5.1 Unternehmerische Sicherheit

Die unternehmerische Sicherheit umfasst alle Themen zur Sicherung der Unternehmung als Ganzem und der Geschäftstätigkeit. Sie betrachtet die wichtigsten Risiken, welchen die Unternehmung unterliegt. Darunter fallen verschiedene Bereiche wie Sicherheit der Infrastruktur, finanzielle Sicherheit, Marktrisikomanagement, Produktehaftpflicht, Versicherungen, Umweltsicherheit etc., wobei keine einheitliche Struktur existiert.

Gesamthaft wird dies als unternehmerisches Risikomanagement bezeichnet. Sein Ziel ist die Reduktion der entstehenden Risiken durch ein Risikodispositiv, welches Massnahmen zur Reduktion von Schadenshöhe oder Eintrittswahrscheinlichkeit,

zur Vermeidung von Risiken durch Umgehung von risikobehafteten Strategien, zur Überwälzung entstehender Schäden an Dritte (Versicherungen) oder das bewusste Tragen von Risiken umfasst. Diese generische Strategie des unternehmerischen Risikomanagements unterscheidet sich nicht wesentlich von derjenigen der Informationssicherheit, welche in Kapitel 6 detailliert wird.

Wagnis- und Bedingungsrisiken

Unternehmerisches Risikomanagement ist eine strategische Aufgabe. Die durch die unternehmerischen Tätigkeiten entstehenden Risiken können grundsätzlich in zwei Bereiche eingeteilt werden: *willentlich* und *unwillentlich* eingegangene Risiken. *Willentlich* eingegangene Risiken (auch als unternehmerische Risiken, Wagnisrisiken, Geschäftsrisiken etc. bezeichnet) umfassen all diejenigen Risiken, welche auf *willentlichen* Entscheidungen der Unternehmungsführung beruhen und entstehen durch Anordnungen des Management zur bewussten, *willentlichen* Beeinflussung des unternehmerischen Handlungsspielraumes. Sie umfassen Marktrisiken, Finanzrisiken etc. *Unwillentlich* eingegangene Risiken (auch als Bedingungsrisiken, Infrastrukturrisiken, Prozessrisiken, Durchführungs- oder Umsetzungsrisiken bezeichnet) werden hervorgerufen durch Schwachstellen der zur Beeinflussung notwendigen Prozesse, Technologien und Infrastrukturen oder durch unvorhersehbare Ereignisse der Umwelt. Eine Trennung dieser beiden Risikogruppen ist jedoch schwierig, sie überlappen sich teilweise[64].

Das Management der Wagnisrisiken geschieht durch die Unternehmungsführung selbst als Bestandteil der Führungstätigkeit. Das Management der Bedingungsrisiken kann einem Sicherheitsbeauftragten (Risk Manager (RM) oder Safety & Security (S&S) Officer) übertragen werden, der z.B. als Stabsstelle der obersten Unternehmungsleitung agiert und in dieser Position die Reduzierung der Bedingungsrisiken vorantreibt. Er kann auf Anfrage auch Stellungnahmen über die Risiken einzelner Wagnisse abgeben. Die Verantwortung für das Risikomanagement selbst bleibt in der Linienorganisation der Unternehmung. Diese Einschränkung betrifft auch die Informationssicherheit und alle ihr untergeordneten Gebiete. Unternehmerische Sicherheit sowie Informationssicherheit beschäftigen sich mit den unwillentlich eingegangenen Risiken.

Illustration zur Abgrenzung der Informationssicherheit

Es soll angenommen werden, dass aus einer kleinen Zweigstelle einer international tätigen Unternehmung bei einem Diebstahl mehrere Computer entwendet wurden. Die bestohlene Unternehmung gibt an, dass darauf Informationen über ein neues

---

64 Von Stockar unterscheidet "*Störprozesse, welche die Erfüllung von bewusst gesetzten Unternehmenszielen beeinträchtigen*" und "*Störprozesse, welche die Zielerfüllung durch die Verletzung von unbewusst vorausgesetzten Erwartungen gefährden.*" [VonStockar95, S. 39].

Herstellungsverfahren gespeichert waren, dessen Anwendung essentielle Marktvorteile bewirken kann, falls es der Konkurrenz nicht bekannt wird.

Der Diebstahl selbst ist ein Problem physischer Sicherheit von Informations- und Kommunikationsinfrastruktur und als solches Betrachtungsgegenstand der Informationssicherheit, da es sich um ein Bedingungsrisiko handelt. Die Folgen auf den der Unternehmung entgegengebrachten Goodwill können jedoch nicht einfach abgeschätzt werden. Sollte die Unternehmung im betroffenen Marktsegment Technologieführer sein, kann dies durchaus negative Folgen für sie haben, beispielsweise ausgedrückt in einer sinkenden Börsennotierung. Dabei handelt es sich jedoch um Wagnisrisiken.

Der Verlust im Goodwill-Bereich ist möglicherweise auch auf mangelhafte Public Relations zurückzuführen, also beispielsweise darauf, dass der Fall überhaupt bekannt wurde oder dass bekannt wurde, was auf den Geräten gespeichert war. Hauptaufgabe der unternehmerischen Öffentlichkeitsarbeit ist die gezielte Verbreitung von Informationen, welche der Unternehmung nützen, und weil auch hier Information im Zentrum steht, kann dieser Vorfall deshalb ebenfalls als Problem der Informationssicherheit betrachtet werden. Es ist dabei nicht eindeutig, ob es sich bei der Reaktionsfähigkeit und -fertigkeit der Public Relations-Abteilung um Wagnis- oder Bedingungsrisiken handelt.

Wäre es – in einer weiteren Annahme – jedoch so, dass der eingangs geschilderte Vorfall nicht tatsächlich geschehen ist, sondern der Bericht darüber von einer Konkurrenzunternehmung erfunden und absichtlich verbreitet wurde, würden strategische Fragen der Beurteilung und des Verhaltens im Konkurrenzkampf in den Vordergrund rücken. Wenn zu Falschmeldungen als Waffe gegriffen wird, ist Information ebenfalls im Zentrum und deshalb Betrachtungsgegenstand der Informationssicherheit. Die gezielte Beeinflussung von Information liegt jedoch im willentlichen Einflussbereich der Unternehmungsleitung und muss deshalb als Wagnisrisiko eingestuft werden.

Die Abgrenzung der Informationssicherheit von den allgemeinen Risikomanagementaufgaben der Unternehmungsführung und des Informationsmanagements entspricht also der Abgrenzungsproblematik zwischen Wagnis- und Bedingungsrisiken.

5.2 Informationssicherheit

Die Tätigkeiten der Informationssicherheit umfassen alle Sicherheitsaufgaben aller Teile des Informationssystems und der darin stattfindenden Informationsverarbeitung. Hier werden Problemstellungen und Aufgaben von *Informationssicherheitspolitik, unternehmensübergreifender Informationssicherheit, Qualitätsmanagement, Störungs- und Krisenmanagement, Versicherungen, Vergleich von Umsetzungsresultaten* und *Outsourcing* betrachtet.

Informationssicherheitspolitik

Die Informationssicherheitspolitik (ISiPol) ist ein Grundsatzdokument, welches die Ziele und Richtlinien für die Informationssicherheit in der Unternehmung beschreibt. Das Dokument kann als Vorschrift, Richtlinie, Weisung, Anordnung etc. innerhalb der Unternehmung verteilt werden; essentiell dabei ist, dass die oberste Unternehmungsführung den Inhalt für verbindlich erklärt. Es enthält deshalb grundlegende Informationen.

Pohl identifiziert folgende möglichen Inhalte für die übergeordnete Richtlinie: Abstrakte Schilderung real aufgetretener Sicherheitsprobleme, Definition von Sicherheitszielen, Verantwortung für Sicherheitsstrategie und ihre Umsetzung, Definition untergeordneter Richtlinien[65], Delegation, Verantwortung und Verfahren für Produktauswahlprozesse, Abwicklung des Informationssicherheits-managements, Revision und Reporting, Einbindung der Mitarbeitervertretung, regelmässige Überarbeitung (gemäss [Pohl95a, S. 114f, Abb. 2.3-5]). Weitere Angaben finden sich in [Abrams95a], [Ølnes94], [Wood95b].

Auf der Informationssicherheitspolitik wird eine Informationssicherheitsstrategie aufgebaut. Das dazu notwendige Vorgehen geht aus dem generischen Prozess in Kapitel 6 hervor bzw. aus dessen Konkretisierung in Kapitel 8.

Unternehmensübergreifende Informationssicherheit

Jede Unternehmung muss zur Optimierung der Geschäftsprozesse ständig neue technische und personelle Verbindungen mit Geschäftspartnern etablieren. Eines der Ziele auf der operativen Ebene ist es dabei, die Partner mit Informationen aus der eigenen Unternehmung zu versorgen und andererseits Informationen direkt zu beziehen. Damit in diesem Zusammenhang keine Störungen entstehen, müssen notwendige Verhaltensweisen der Mitarbeiter beider Partner präventiv vertraglich geregelt werden (oft im Rahmen von Vertraulichkeitsverpflichtungen oder bei z.B. technischer Vernetzung durch EDI-Rahmenverträge etc.). Die Einhaltung dieser Verträge muss durch Controlling und Revision kontrolliert werden. Möglicherweise können sich beide Partner auf einen einheitlichen Sicherheitsstandard einigen, z.B. auf die Anwendung des gleichen Grundschutzmassnahmenkatalogs oder die Anwendung des gleichen Verfahrens.

Qualitätsmanagement

Das Qualitätsmanagement beschäftigt sich mit den Anforderungen an den Produktionsprozess von Produkten, und, im Rahmen der Qualitätssicherung, mit

---

65 Hier nennt Pohl *bereichsspezifische Sicherheitskonzepte, Datenschutzrichtlinie, Richtlinie zum Zugriffskontrollsystem, Passwort-Richtlinie, Prüfrichtlinien, Revisionsrichtlinien, Notfall- und Katastrophenrichtlinie, Störungsrichtlinie, Aktensicherheit (Schränke, Tresore), Revisionsrichtlinie, Backup-Richtlinie* [ebd.].

den Verfahren zur Einhaltung dieser Anforderungen. *"Qualitätsmanagement zielt darauf ab, den Wert des Produkts für den Kunden und Benutzer zu steigern."* [Wallmüller95, S. 1] Qualität ist subjektiv, d.h. jede Person kann die Qualität desselben Produktes unterschiedlich beurteilen. Da deshalb sehr viele verschiedene Anforderungen an ein Produkt formuliert werden können, wird zu ihrer Ordnung oft ein sogenannter Qualitätsbaum erstellt, welcher die Priorität und Hierarchie der einzelnen Anforderungen an das Produkt festlegt. Diese Priorisierung wird durch den Hersteller des Produktes vorgenommen.

Die Ursachen für Qualitätsprobleme unterteilt Wallmüller in *"Management, Technologie und Mitarbeiter"* [Wallmüller95, S. 4]: Managementprobleme werden dabei auf allgemeine Führungsprobleme zurückgeführt. Die technisch bedingten Probleme sind auf schnellen technologischen Wandel, Verwendung unausgereifter Technologien und unzureichende Kommunikationsmittel innerhalb der Unternehmung zurückzuführen. Die durch Mitarbeiter verursachten Probleme beziehen sich auf mangelnde Qualifikation, Engagement, Werthaltungen und Fluktuation. Zur Lösung dieser Probleme schlägt Wallmüller eine Unterteilung in normative Ebene (Vision und Planung der Qualität), strategische (Festlegen der Rahmenbedingungen und Einflussgrössen) und operative Ebene (Prozessmanagement) vor.

Um die Qualitätsanforderungen an die Produkte erfüllen zu können, muss auch der Produktionsprozess selbst Anforderungen erfüllen, welche eine qualitativ hochstehende Produktion zulassen. Umgekehrt allerdings ist ein qualitativ hochwertiger Prozess nur eine notwendige, nicht aber eine allein hinreichende Voraussetzung für hochwertige Produkte. Werden Produkte hergestellt, welche selbst wieder Werkzeuge für einen weiteren Produktions- oder Produktverarbeitungsschritt sind (z.B. Software), sind noch höhere Anforderungen zu stellen, da die Werkzeugqualität Einfluss auf die Produktqualität hat.

Informatik-Qualitätssicherung beschäftigt sich mit der Formulierung und Erfüllung von Anforderungen an Software-Produkte. Sie ist ein integraler Bestandteil jedes Informatik-Produktentwicklungsprozesses. Da Sicherheit auch als Qualitätsanforderung gesehen werden kann, ist eine Integration von Sicherheit und Qualität bei der Produktherstellung möglich. Die Informatik-Qualitätssicherung befasst sich also u.a. mit der Sicherheit der bei der informatikgestützten Informationsverarbeitung eingesetzten Werkzeuge, nicht jedoch mit der Informationsverarbeitung selbst.

Informationssicherheit und Qualitätsmanagement haben also primär keine Berührungspunkte, da sich Informationssicherheit auf Bedingungsrisiken der unternehmerischen Informationsverarbeitung bezieht und Qualitätsmanagement auf den Produktionsprozess und die dabei entstehenden Produkte. Allerdings ist das Qualitätsmanagement auf ein funktionierendes unternehmerisches Informationssystem angewiesen. Es ist deshalb möglich, dass aus den Anforderungen an die Produkte und die Produktionsprozesse Anforderungen an die

unternehmerische Informationsverarbeitung hergeleitet werden. Ausserdem ist es möglich, dass die Leistungen einzelner Abteilungen als Produkte definiert werden, an welche von innerhalb derselben Unternehmung Qualitätsanforderungen gestellt werden. Informationssicherheit kann deshalb als Qualität des Informationssystems aufgefasst werden. Die in ihrem Zusammenhang aufgestellten Anforderungen können beispielsweise in Qualitätsbäume aufgenommen werden, und das Ziel der Informationssicherheit kann konsequent im Rahmen des Qualitätsmanagements verfolgt werden.

Störungs- und Krisenmanagement

Unter Krisenmanagement wird der Umgang mit Störfällen verstanden mit dem Ziel, die Beeinflussung der Unternehmung und ihrer Prozesse durch diesen Störfall möglichst gering zu halten. Als Störfall wird jede ungeplante Abweichung der Informationsverarbeitung bezeichnet. Störfälle beeinflussen deshalb die unternehmerischen Prozesse. Kleine Störfälle können sofort behoben werden; grössere können Krisen auslösen, welche die Unternehmung "lähmen", weil die Geschäftsprozesse nicht mehr durchgeführt werden können. Das Krisenmanagement führt in diesem Fall die Unternehmung schrittweise in einen Zustand zurück, in welchem ein Durchlaufen der Geschäftsprozesse wieder möglich wird.

Das Krisenmanagement kann selbst als Prozess betrachtet werden[66]. Wichtige Elemente sind die Meldung von Schwächen von Systemen und von Vorfällen, die angemessene Reaktion auf Vorfälle sowie die Etablierung von Sanktionen für Verursacher von Störfällen [BSI-COP95, S. 22, S. 40]. Damit die Geschäftstätigkeit auch bei schweren Störungen fortgesetzt werden kann, muss schon zuvor eine Geschäftskontinuitätsplanung [BSI-COP95, S. 46f] durchgeführt werden. Die Ergebnisse dieser Planung müssen getestet werden, um Handlungsengpässe und gegenseitige Abhängigkeiten zu entdecken. Die Pläne müssen regelmässig aktualisiert werden, um den jeweils aktuellen Zustand des Informationssystems zu berücksichtigen. Sie sollten verschiedene Szenarien berücksichtigen, welche auf unterschiedliche Teilbereiche der Unternehmung wirken und unterschiedliche Lösungen erzeugen. In den Plänen muss insbesondere geregelt werden, wie bei Entdeckung eines Störfalls vorzugehen ist, an wen Störfälle gemeldet werden müssen, welche Grundlagen zur Einschätzung des entstandenen Schadens und des Potentials verwendet werden, wer diese Einschätzung vornimmt, wer über Krisenzustand entscheidet und auf welche Ausweichmöglichkeiten zurückgegriffen werden kann.

Bei einer detaillierten Erfassung der unternehmerischen Objekte in einem Informationssicherheitswerkzeug, so wie es in *ISIWAY* (vgl. Kapitel 8) vorgeschlagen

---

66 Ein Vorschlag für die Ausgestaltung des Krisenmanagements als Prozess wird in Kapitel 8 abgegeben.

wird, kann eine computergestützte Simulation einzelner Störfälle durchgeführt werden. Dies kann Aussagen zur Verbesserung des Krisenmanagements erzeugen.

Versicherungen

Grosse Versicherungsunternehmungen bieten verschiedenartige Versicherungsprodukte an, um die durch das Eintreten von Störfällen entstehenden Kosten und Einkommensausfälle abzudecken. Von der Versicherung einzelner IT-Systemkomponenten bis zur Übergangsfinanzierung von Rechenzentren können die Versicherungen stark variiert und skaliert werden.

Vergleich von Umsetzungsresultaten

Durch einen Vergleich der Umsetzungsresultate der Informationssicherheit kann die relative Güte eines Informationssicherheitsmanagements bestimmt werden (sogenanntes *Benchmarking*). Diese Vergleichbarkeit setzt einheitliche Datenerfassung und -verwaltung voraus sowie die Freigabe der Daten zum Vergleich. Gerade weil die Resultate in vielen Unternehmungen vertraulich behandelt werden, ist ein Vergleich zwischen verschiedenen Unternehmungen nur selten möglich. Auch innerhalb der Unternehmung besteht oft nur wenig Motivation, die Ergebnisse des eigenen Teilbereichs anderen Teilbereichen zur Verfügung zu stellen. Falls jedoch innerhalb der Unternehmung eine derartige Offenheit besteht und die angewendeten Verfahren vergleichbare Resultate erzeugen, können aus einem Vergleich Schlussfolgerungen für die Anpassung und Ergänzung des jeweiligen Informationssicherheitsmanagements gezogen werden.

Outsourcing

Outsourcing ist die Auslagerung von Teilen des IT-Systems aus der Unternehmung in einen auf dieses Outsourcing spezialisierten Dienstleister (Insourcer), der Betrieb, Wartung oder sogar das Eigentum der IT-Systeme übernimmt. Die *inhaltliche* Informationsverarbeitung verbleibt zwar weiterhin in der Unternehmung, die Kontrolle über die *technische* Ausgestaltung der Dienstleistungserbringung geht für die outsourcende Unternehmung jedoch verloren. Dies erschwert insbesondere die Kontrolle der Informationssicherheit vor allem für diejenigen Störfälle, welche nicht zu offensichtlichen Fehlfunktionen führen. Besonders betroffen ist die *Vertraulichkeit* der dem Insourcer anvertrauten Daten. Vertraulichkeitsverluste sind nur in Einzelfällen festzustellen und müssen deshalb durch präventive und aktive Strategien zu verhindern versucht werden, z.B. durch detaillierte vertragliche Vertraulichkeitsregelungen, die Vereinbarung von Überprüfungsverfahren, sowie durch konkrete Suche nach Fehlermöglichkeiten (z.B. fehlendem Zugriffsschutz) und Motivationen (z.B. Interessenkonflikte).

5.3 Sicherheit der Rollenwahl

Die Sicherheit der Rollenwahl umfasst alle Sicherheitsfachgebiete, welche sich mit Personen als Teil des Informationssystems der Unternehmung beschäftigen und die Sicherheit der aktiven und passiven Rollen dieser Personen beeinflussen. In einer aktiven Rolle muss die Person ständig zum sicheren Verhalten motiviert werden, in einer passiven Rolle muss sie vor äusseren Einflüssen geschützt werden.

5.3.1 Sicherheitskultur

Dem sicheren Verhalten der Mitarbeiter kommt eine Schlüsselrolle beim Management der Informationssicherheit zu. Im sozialen Kontext wird von *Sicherheitskultur* gesprochen, wenn sicheres Verhalten bei der überwiegenden Mehrheit der Mitarbeiter zum akzeptierten und als Wert empfundenen Verhalten gehört. Dem geht eine Motivation mit Zielformulierung und Zielübertragung im dualistischen Chef-Mitarbeiter-Verhältnis voraus, welche durch Vorbildfunktionen geschieht, sowie eine grundsätzliche Offenheit und Akzeptanz sicheren Verhaltens (Einsicht) auf individueller Ebene. Formell wird dies u.a. in der COBIT-Control Objective PO6 gefordert [COBIT96.3, S.27]. Dort wird weiter unterschieden in *Positive Information Control Environment, Management's Responsibility for Policies, Communication of Organisation Policies, Policy Implementation Resources, Maintenance of Policies, Compliance with Polices, Procedures and Standards, Quality Commitment, Security and Internal Control Framework Policy* und *Issue Specific Policies.* Dabei werden aber nur die Formen identifiziert, mit welchen die Inhalte (*Commitment*) transportiert werden müssen. Zu diesem sicheren Verhalten gehört es beispielsweise, den Schreibtisch nach Arbeitsabschluss aufzuräumen (vgl. "Clean Desk", [BSI-COP95, S.19]) oder das manuelle Aktivieren von vorhandenen Sicherheitssystemen (z.B. passwortgeschützter Bildschirmschoner, Verschliessen der Bürotüre).

Brandao hat sich in [Brandao94] detailliert mit Aufgabenstellung und Vorgehen des Sicherheitskulturmanagement beschäftigt. Er beschreibt vier verschiedene Kultursituationen, die er mit *Chaos-Kultur, Monokultur, pluralistische Kultur* und *integrierte pluralistische Kultur* bezeichnet. Als Einflussbereiche des Managements nennt der *Definition von Verantwortlichkeit, Definition und Kontrolle von Sicherheitspraktiken, Qualifikation und Training, Belohnung und Sanktion, Auditverfahren* sowie*, Überprüfung und Vergleich* [Brandao94, S. 33f]. Auf individueller Ebene nennt er *kritische Haltung, sorgfältiges und vorsichtiges Handeln* und *Kommunikation.* Gesamthaft beschreibt er sehr weitreichend, was IT-Sicherheitskultur ist und wie sie erreicht werden kann.

Kabay betrachtet Informationssicherheit in [Kabay93] vom sozialpsychologischen Standpunkt aus. Er identifiziert Schemata, welche die Wahrnehmung beeinträchtigen und Personen zu unsicherem, aber schemenkonformem Verhalten

verleiten. Er unterscheidet Meinungen, Glauben und Überzeugungen und argumentiert, warum nur eine aufwendige Veränderung der Überzeugungen hin zur Kenntnis, Akzeptanz und Weitergabe von informationssicherheitsfördernden Verhaltensweisen langfristigen Erfolg verspricht. Weiterhin nennt er Faktoren, wie solche Veränderungen erreicht werden können. Schliesslich bezieht er es auch auf das Gruppenverhalten und beschreibt, warum Verhaltensweisen, welche den Gruppenüberzeugungen entsprechen oder widersprechen, nicht eliminiert werden können, aber zur gezielten Beeinflussung der Sicherheitskultur genutzt werden können (vgl. auch [Lippa94]).

Ebenfalls formell können die Anforderungen an eine Person betrachtet werden, welche Mitarbeiter der Unternehmung werden soll. COBIT unterscheidet bei Control Objective *PO7 Manage Human Resources* [COBIT96.3, S. 28] zwischen *Personnel Recruitment and Promotion, Personnel Qualifications, Personnel Training, Cross-Training or Staff Backup, Personnel Clearance Procedures, Employee Job Performance Evaluation* sowie *Job Change and Termination* und deckt damit alle Zyklen von der Auswahl über Einstellung, Einführung über das Vorgehen bei Absenzen bis zum Austritt von Mitarbeitern ab. Auch im Code of Practice werden diese Themen unter Abschnitt 4 [BSI-COP95, S.14ff] abgedeckt. Wichtige Elemente sind konkrete und anforderungsgerechte Stellenbeschreibungen sowie die Vertraulichkeitserklärung als Teil der Treuepflicht zum Arbeits- / Auftraggeber.

Darüber hinaus können unbeabsichtigte Störungen durch eine gute Ausbildung der Benutzer vermindert werden. Zu dieser Ausbildung gehört auch sicherheitsbewusstseinsfördernder Unterricht.

5.3.2 Personensicherheit

Die Personensicherheit beruht auf der Überzeugung, dass Mitarbeiter oder der Unternehmung auf andere Weise verbundene Personen einen Wert darstellen. Diese ergibt sich nicht nur aus dem Wert der Person selbst, der objektiv nicht fassbar ist, sondern v.a. aus dem Wert, den die Existenz der Person und das von ihr getragene Know-How für die Unternehmung darstellt. Die Absenz einer Person kann zu schwerwiegenden Störungen in der Durchführung der Geschäftsprozesse führen. Darüber hinaus kann die böswillig herbeigeführte Absenz (z.B. durch eine Entführung) zu Schäden im Goodwill führen und beispielsweise Zweifel an der Wertschätzung der Mitarbeiter durch die Unternehmung aufkommen lassen, oder an der Fähigkeit der Unternehmung, trotzdem vertraglich vereinbarte Verpflichtungen einhalten zu können. Die physische Sicherheit des Personals muss also im Rahmen des Sicherheitsmanagements unter dem Stichwort Personenschutz und Personensicherheit berücksichtigt werden. Dazu gehören auch gesundheitsfördernde Massnahmen wie z.B. Ergonomie und Hygiene des Arbeitsplatzes, aber auch weitere (vgl. auch [Ulich94]).

5.4 Sicherheit der Aufgabenbearbeitung

Die Sicherheit der Aufgabenbearbeitung umfasst alle Teilgebiete, welche sich mit der *inhaltlichen* Sicherheit der Informationsverarbeitung beschäftigen. Entsprechend entsteht auch hier eine Vierteilung in die vier Aspekte der Informationsverarbeitung *Informationsverwendung, Wissen, Daten* und *Nachrichten* (vgl. Abschnitt 3.6). Während böswillige und fahrlässige Verhaltensweisen der Personen schon zuvor im Rahmen der Sicherheitskultur betrachtet wurden, geht es hier darum, welche Moralvorstellungen durch die Personen bei der Informationsverarbeitung berücksichtigt wird und wie man Personen bei der sinnvollen inhaltlichen Informationsverarbeitung unterstützen kann.

Übergreifende Fachgebiete der inhaltlichen Informationsverarbeitung sind die *Beratung,* der *ethische und moralische Umgang mit Informationen* sowie allgemeine *informationsrechtliche Fragestellungen.*

Beratung (Unternehmungsberatung und Informationssicherheits-beratung)

Beratung als Dienstleistung kann sich auf alle Aspekte unternehmerischer Tätigkeit beziehen. Grundsätzlich zielt die Beratung auf einen Know-how-Transfer in die Unternehmung hinein ab, der im Rahmen der Fragestellung des Beratungsauftrags definiert wird, und kommt deshalb v.a. dann zum Einsatz, wenn es der beratenen Unternehmung an derartigem Know-How mangelt. Beratung folgt dabei keinen festgelegten Schemen, sondern zeichnet sich gerade durch grösstmögliche Flexibilität aus. Dementsprechend sind auch Umfang, Klarheit der Zielvereinbarung und Messbarkeit der Zielerreichung, Abgrenzung der Fragestellung und andere bestimmende Parameter sehr variabel. Der Berater agiert innerhalb der Unternehmung (sofern das Mandat dies umfasst) im Interesse seines direkten Auftraggebers. Er ist in der Regel nicht weisungsbefugt und nicht Teil der von ihm betrachteten Prozesse. Der englische Entsprechung „Consultant" des deutschen Begriffs wird jedoch zunehmend auch für temporäre Mitarbeiter verwendet, welche zeitlich befristet – z.B. für die Dauer eines Projekts des Klienten – in Prozesse voll integriert werden. Letzteres soll als „Beratung im weiteren Sinne" verstanden werden, stellt jedoch nichts anderes als ein weitgehendes Outsourcing der Personalfunktion dar, während Beratung im engeren Sinne eine konstruktive einvernehmliche Zusammenarbeit zwischen Auftraggeber und Berater umfasst und hier weiter betrachtet wird.[67]

---

67 Hill unterscheidet zwischen Beratungsunternehmungen mit einer qualitativen und solchem mit einer gewinnorientierten Grundhaltung. Erstere sollten „*vornehmlich bei komplexen und diffusen Projekten gerufen werden* [...] *und auch dort, wo offene oder verdeckte Konflikte einen wichtigen Teil des Beratungsproblems ausmachen. Gewinnorientierte Beratungsfirmen dürften demgegenüber vor allem auf effiziente Auftragsabwicklung ausgerichtet sein und folglich vor*

Beratung im engeren Sinne (Management Consultancy) hat eine gestalterische Aufgabe in der Unternehmung[68], indem sie Empfehlungen für die Anpassung bestehender Prozesse und der damit zusammenhängenden Organisation entwirft und dem Auftraggeber zur Begutachtung und allenfalls zur Umsetzung übergibt. Beratungstätigkeit umfasst demnach v.a. eine Planungsphase mit der Formulierung der Anforderungen an das Ergebnis, einer Erhebung der bestehenden Verhältnisse, einem Entwurf des neuen Zustands und einer Planung der konkreten Umsetzung zur Erreichung des neuen Zustands. Ebenfalls möglich ist die Situation, in welcher eine Unternehmung den Entwurf des neuen Zustands schon weit vorangetrieben hat, diesen jedoch noch fachlich prüfen lassen möchte oder die Umsetzung mangels personeller Ressourcen oder aufgrund interner Widerstände nicht alleine durchführen kann. Die Entscheidungsphase wird vom Auftraggeber durchlaufen und allenfalls vom Berater moderiert. In der Anordnungsphase kann der Berater wieder gestaltend mitwirken. An der Durchführung, d.h. der konkreten Einführung des neuen Zustands kann der Berater ebenfalls beteiligt sein, jedoch i. d. R. nicht in weisungsbefugter, sondern in empfehlender Position. Die Kontrolle wird von der auftraggebenden Unternehmung wieder selbst durchgeführt.

Informationssicherheit kann Gegenstand von Beratungsaufträgen sein. In der Praxis fehlt v.a. auf höheren Ebenen des Managements die Erfahrung und die Kenntnis der Chancen und Risiken des Informatik-Einsatzes, was oft auf die schnelle technologische Entwicklung zurückzuführen ist. Gleichwohl werden diese Personenkreise durch Pressemeldungen oder auch durch die interne Revisionsstelle über die Notwendigkeit des Handelns im Bereich der Informationssicherheit informiert. Informationssicherheit wird dabei immer weniger nur als notwendiges Übel betrachtet, welches nur dem Schutz der bestehenden Infrastruktur dient, sondern immer mehr auch als Notwendigkeit und Konkurrenzvorteil für die Teilnahme an elektronischen Märkten sowie als Schutz vor Angriffen der Konkurrenz (Spionage und Sabotage, vgl. unten).

Ethisches und moralisches soziales Verhalten

Ermann, Williams und Shauf haben in [Ermann97] die ethischen und sozialen Auswirkungen der Informatisierung betrachtet. Sie heben dabei insbesondere

---

allem bei relativ klar strukturierten Problemstellungen gute Kosten-Nutzen-Relationen ausweisen können.“ [HillW90, S. 179]

Block unterscheidet zwischen drei möglichen Beziehungsformen zwischen Berater und Auftraggeber: die des *Experten*, die des *Handlangers* und die *gute Zusammenarbeit*. Der *Experte* erledigt seine Aufgabe im Auftrag weitgehend selbst, was v.a. bei hoch spezialisierten Arbeiten der Fall ist. Weder Auftraggeber noch Berater arbeiten darauf hin, Know-How langfristig zu transferieren. Der *Handlanger* führt im Gegenteil nur aus, was der Auftraggeber selbst schon erkannt und konzipiert hat. Bei der *guten Zusammenarbeit* bereiten Auftraggeber und Berater gemeinsam die Entscheidungsgrundlagen vor. [Block97, S. 31ff]

68 Vgl. [HillW90], [Wohlgemuth86], [Block97], [Wohlgemuth97a], [Wohlgemuth97b]

heraus, dass die gegenwärtigen technischen Entwicklungen Anpassungen des individuellen Verhaltens erzeugen und dass diese Veränderungen sehr unterschiedlich sein können. Sie betonen, dass die verschiedenen ethischen Codes, welche heute bestehen, durch die Internationalisierung und weitere Einflüsse (vgl. auch Abschnitt 4.3) stark divergieren und dass die globale Einigung auf einen einheitlichen ethischen Codes unwahrscheinlich ist [Barger87, S. 339].

Die ACM hat einen ethischen Code [ACMCode92] entworfen, der für die Anwendung durch Mitglieder des ACM selbst vorgesehen ist, aber auch allgemein verwendet werden kann. Er besteht aus 24 Imperativen, z.B. der Aufforderung, niemandem Schaden zuzufügen, sich ehrlich und vertrauenswürdig zu verhalten und die Privatsphäre anderer zu respektieren. Führungspersonen werden besonders betrachtet, indem sie z.B. soziale Verantwortung fördern und die Bereitstellung von Systemen zur Erhöhung der Lebensqualität aller Betroffenen fördern sollen. Die Anwendung dieses Codes ist in [Anderson93] beschrieben.

Wenn das Management der Informationssicherheit in einer Unternehmung auf einen breit getragenen ethischen Code aufbauen kann, der für die Unternehmung spezifisch formuliert wurde, so sind konkrete Ver- und Gebote überflüssig, weil sie von den allgemeinen Regeln des Codes abgedeckt werden.

Informationsrecht und Informatik-Recht

Ebenfalls inhaltlich übergreifend und die gesamte Informationsverarbeitung betreffend sind die juristischen Rahmenbedingungen, welchen die Informationsverarbeitung unterliegt. Aus juristischer Perspektive stellen IT-Systeme lediglich eine andere Kategorie von Werkzeugen dar, welche zur Erreichung der unternehmerischen Ziele eingesetzt werden. Die bestehenden Rechtsnormen lassen sich sinngemäss anwenden und behalten ihre Gültigkeit. In den letzten zehn Jahren sind dennoch verschiedene Rechtsnormen entstanden, welche auf die Spezifika der elektronischen Informationsverarbeitung eingehen, insbesondere auf die Flüchtigkeit von Information (Beweiskraft elektronischer Dokumente und Aufbewahrungspflicht), die Verwendbarkeit von geistigen Erzeugnissen als Werkzeuge (Softwarerecht, rechtliche Anerkennung elektronischer Aufzeichnungen), die einfache Reproduzierbarkeit von Programmen und Daten (Urheberrecht) und die sozialen Auswirkungen vereinfachter Personen-datenverarbeitung (Datenschutz) im Zusammenhang mit den Skaleneffekten, welche durch die maschinelle Informationsverarbeitung entstehen. Darüber hinaus wird auch der Missbrauch von Informatik-Mitteln rechtlich erfasst. Informatik-Recht als Teildisziplin beschäftigt sich mit der Rechtmässigkeit von Verarbeitungsvorgängen und deren Ergebnis.

Die Erfüllung von Verpflichtungen, welche aus gesetzlichen Vorgaben und vertraglichen Vereinbarungen entstehen, muss im Rahmen der Informationssicherheit ebenfalls betrachtet werden. Der Code of Practice listet konkret die Kopierkontrolle anwendereigener Software, die Sicherung

organisationseigener Aufzeichnungen, Datenschutz und Vorbeugung gegen Missbrauch als Themenbereiche auf [BSI-COP95, S. 48ff].

5.4.1 Sichere Informationsverwendung

Im Bereich der sicheren Informationsverwendung muss die Informationssicherheit v.a. die Grundanforderungen der ökonomischen Ebene (vgl. Abschnitt 2.3) sicherstellen: Effektivität, Effizienz, Zuverlässigkeit und beabsichtigte Verwendung.

Effektivität und Effizienz beziehen sich in erster Linie auf die Informationsverarbeitungsprozesse. Inhaltlich ist deren Optimierung v.a. eine Aufgabe unternehmerischer Organisation, welche dazu auf die Mittel der Informationstechnik zurückgreift. Informationssicherheit muss diese Optimierung dann beeinflussen, wenn durch diese Optimierungen Fehler in der Verarbeitung entstehen können. Beispielsweise darf die Umständlichkeit eines notwendigen Bewilligungsverfahrens nicht zu dessen Auslassung führen oder in einem konkreten Fall sollte die gemeinsame Benutzung von Informationen durch verschiedene Personen nicht dazu verleiten, dass alle Personen dieselbe Benutzerkennung und dasselbe Passwort verwenden.

Zuverlässigkeit (*reliability of information*) umfasst gemäss COBIT die Fähigkeit des Informationssystems, die für die Geschäftstätigkeit notwendigen Informationen auf Anfrage korrekt zur Verfügung zu stellen [COBIT96.3, S. 13][69].

Die beabsichtigte Verwendung fordert, dass Informationen nur für denjenigen Zweck verwendet werden, für den sie erfasst und verarbeitet wurden, also nicht zweckentfremdet werden. Dies umfasst bei personenbezogenen Daten den Schutz der dadurch beschriebenen Personen (Datenschutz), doch kann sich auch auf andere Informationen beziehen, z.B. zur Verhinderung von Insiderdelikten.

COBIT behandelt die Anforderungen der inhaltlichen Informationsverarbeitung teilweise in Control Objective PO 8.0. Im Code of Practice werden die Geschäftsanforderungen für den Informationszugriff ebenfalls betrachtet.

Wirtschaftsspionage, Sabotage und Wirtschaftskriminalität

Spionage bezeichnet die unberechtigte Weitergabe von Informationen, um daraus Vorteile zu ziehen. Der Begriff Spionage wird oft mit militärischen oder staatspolitischen Inhalten verbunden.

Bei der *Wirtschafts-* oder *Industriespionage* geht es darum, gezielt Informationen aus einer Unternehmung zu erhalten, um sich beispielsweise selbst Technologie-

---

69 Dierstein fasst unter dem Begriff Verlässlichkeit (im englischen ebenfalls *reliability*) lediglich die drei technischen Grundanforderungen Verfügbarkeit, Integrität und Vertraulichkeit zusammen [Dierstein97, S. 49] (vgl. auch Argumentation in Abschnitt 2.3).

oder Marktvorteile zu beschaffen. Wirtschaftsspionage wird deshalb in erster Linie von direkten Konkurrenten der Unternehmung betrieben. Diese Tätigkeiten werden auch als *Corporate Analysis* oder *Competitive Intelligence* bezeichnet (vgl. [Janal98, S. 191ff]). Doch es wird vermutet, dass auch die staatlichen Nachrichtendienste Wirtschaftsspionage betreiben [Heise98.01.13].

Sabotage bezeichnet die gezielte Behinderung der Geschäftstätigkeit einer Unternehmung durch die Auslösung von Störfällen. Auch Wirtschafts- und Industriesabotage können durch Konkurrenten verwendet werden, um eine Unternehmung bei ihrer Zielerreichung zu behindern und so deren Ausnutzung strategischer Marktvorteile zu verhindern.

Bei beiden Gebieten können legale Mittel eingesetzt werden. Oft laufen Spionage und Sabotage jedoch verdeckt ab, so dass auch die Verwendung illegaler oder vertraglich ausgeschlossener Praktiken möglich ist.

Unter Wirtschaftskriminalität wird jede Art von gesetzwidriger Verwendung unternehmerischer Ressourcen verstanden. Im englischen Sprachgebrauch wird auch von "White Collar Crime" gesprochen. Auch Spionage und Sabotage können teilweise darunter subsumiert werden.

5.4.2 Kongruenz

Kongruenz beschreibt die Übereinstimmung von Wissen mit den tatsächlichen Gegebenheiten, welche dieses Wissen beschreiben soll. Wissen wird aus Daten durch Interpretation gewonnen. Diese Interpretation hängt in hohem Masse vom Vorwissen des interpretierenden Individuums ab. Ziel der Kongruenz als Sicherheitsteilgebiet ist es, auch bei problematischer Interpretation ein möglichst wahrheitsgetreues Abbild der realen Situation zu gewinnen, indem Vorwissen in die Interpretation mit einbezogen wird. Beispielsweise ist die Gewinnung von Basisdaten für die unternehmerische Entscheidungsfindung oft nur aufgrund unvollständiger Information möglich (oder anders formuliert: es ist oft unmöglich, die Kongruenz zu gewährleisten).

Auch hier besteht eine grosse Überlappung zwischen rein unternehmerischen Anforderungen und Vorgehensweisen und denjenigen des Informations-managements und der Informationssicherheit. Informationssicherheit kann die Kongruenz beeinflussen, indem sie Interpretationsregeln für Unklarheiten aufstellt.

5.4.3 Inhaltliche Datensicherheit

Die inhaltliche Datensicherheit beschäftigt sich mit der korrekten Codierung des Wissens und der Rückgewinnung dieses Wissens aus der Betrachtung des gewählten Mediums. Im Unterschied zur inhaltlichen Kommunikationssicherheit, welche die Übermittlung von Informationen von einem Individuum zu einem

anderen betrachtet, bezieht sich die inhaltliche Datensicherheit auf die Überbrückung von Zeit und örtlicher Distanz. Darin eingeschlossen ist die *technische Datensicherheit*. Darüber hinaus wird die Auswahl des geeigneten Aufzeichnungsmediums und der Kodierungsform betrachtet.

Inhaltliche Datensicherheit muss sich beispielsweise mit der Wahl von Aufzeichnungsregeln, Sprache, Stil und Form schriftlicher Aufzeichnungen beschäftigen, um so grösstmögliche Effizienz und Eindeutigkeit bei der Neuinterpretation der Aufzeichnungen zu ermöglichen. Dazu gehören z.B. die Definition der unternehmerischen Identität (corporate identity), aber auch die Festlegung von unternehmensweiten Datenmodellen oder anderweitig mehrseitig verwendeten Aufzeichnungen, um Klassifikationsschemen (vgl. auch [BSI-COP95, S. 12f]) und Ablageregeln, und im besonderen um die Festlegung individueller Sicherheitsniveaus (vgl. [COBIT96, S.23ff]).

5.4.4 Inhaltliche Kommunikationssicherheit

Die inhaltliche Kommunikationssicherheit bezieht sich auf Sicherheit des Nachrichtenaspekts von Informationen. Dies umfasst grundsätzlich die Tatsache, dass eine Kommunikationsbeziehung aus einem Sender und einem Empfänger besteht und die Nachricht beim Empfänger so ankommen soll, wie der Sender sie abgeschickt hat. Der Sender verbindet mit der Nachricht eine Intention: Er will das Wissen des Empfängers erweitern. Inhaltliche Kommunikation ist also ein sozialer Vorgang, weshalb in diesem Zusammenhang mindestens zwei der Grundanforderungen der sozialen Ebene (gemäss Abschnitt 2.3) betrachtet werden müssen: Verbindlichkeit und externe Integrität. Die inhaltliche Kommunikationssicherheit umfasst deshalb Aspekte der Medienwahl, der Übertragung und der Rückgewinnung des Wissens aus der Beobachtung des Mediums. Rein technisch ist dementsprechend die *technische Kommunikations-sicherheit* als Teilgebiet enthalten. Darüber hinaus werden hier die personellen, zielgerichteten Komponenten betrachtet, d.h. beispielsweise die Wahl von Formulierung, um so im Idealfall beim Empfänger der Nachricht genau diejenige Reaktion auszulösen, welche beabsichtigt war. Dazu gehört die Bereitschaft, den Kommunikationspartner zu verstehen.

Konkret muss die Informationssicherheit sich mit Daten- und Softwareaustausch befassen, z.B. mit Vereinbarungen zwischen den kommunizierenden Individuen und Unternehmen (insbesondere bei EDI oder electronic banking), mit Sicherheit auf dem Transport und der Sicherheit der einzelnen Kommunikationsformen (z.B. E-Mail-Sicherheit). Darüber hinaus muss ist die Identifikation und Zertifizierung von Kommunikationspartnern relevant.

Zertifizierung von Kommunikationspartnern

Eine Zertifizierung ist eine (amtliche) Beglaubigung und Bescheinigung [sinngemäss nach Duden90, S. 827]. Der Begriff wird verwendet, um zu bestätigen, dass ein bestimmtes Objekt – z.B. eine elektrische Signatur – eindeutig zu einer Person gehört. Das ist Voraussetzung für die spätere gegenseitige Authentifizierung der Kommunikationspartner, z.B. bei der Teilnahme an elektronischen Transaktionen ohne direkte Kenntnis der Person.

Die Zertifizierung kann beispielsweise bestätigen, dass eine gegebene digitale Signatur zu einer Person gehört, dass diese Person mit dem entsprechenden digitalen Signatursystem umgehen kann und / oder dass die Person ein vertrauenswürdiger Handelspartner für Geschäftsbeziehungen ist. [vgl. auch Horster98 oder Camphausen98].

5.5 DV-Sicherheit

DV-Sicherheit umfasst alle technischen Sicherheitsaspekte, welche unabhängig von der digitalen oder analogen Natur der verwendeten Werkzeuge relevant sind. Dazu gehören u.a. die Klassifizierung und Überwachung der Anlagen und Bestände (vgl. auch [BSI-COP95, S. 12]), der Umgang mit Datenträgern ([BSI-COP95, S. 27ff]) mit der Verwaltung von entfernbaren Datenträgern, Verfahren zum Umgang mit vertraulichen Daten, Systemdokumentation sowie die Beseitigung von Datenträgern jeglicher Art.

5.5.1 IT- / EDV-Sicherheit

Die *Informatik*-Sicherheit beschäftigt sich mit der Sicherheit der einzelnen Komponenten des IT-Systems und den Risiken und Gefahren ihres Einsatzes. Ursprünglich – zu Zeiten des IT-Einsatzes in einer zentrierten automatisierten Administrationsunterstützung z.B. zur Rechnungsführung – ging es dabei um die Zuverlässigkeit technischer Systeme, um die Optimierung von Ausfallzeiten und deren Konsequenzen und um den effizienten Einsatz der technischen Ressourcen. Mit zunehmender Komplexität der Technologien haben sich Teilfelder der Informatik-Sicherheit entwickelt, welche den Teildisziplinen und Einsatzgebieten der Informatik entsprechen: Rechenzentrumssicherheit, Computersicherheit, Netzwerk- und Kommunikationssicherheit, Internet-Sicherheit etc..

Die Grenzen zwischen diesen einzelnen Gebieten sind fliessend, es gibt unterschiedlich grosse Teilgebiete und starke Einflüsse aus ingenieur-wissenschaftlichen Disziplinen. Die Sicherheit der physischen Komponenten wird durch immer neue (physikalisch-technische) Produktionsprozesse beeinflusst, die Mathematik, Physik und neuerdings die Biologie liefern wichtige Grundlagen für die Kommunikationssicherheit (Kryptologie, Identifikation und Authentifikation

z.B. durch Biometrie) und grosse Teile von Teilsystemen basieren auf Erkenntnissen diskreter Numerik (Prozessoptimierungen, Boolsche Algebra) und der Mengentheorie (Datenbanktechnologie). *Informatik*-Sicherheit ist gesamthaft *werkzeug*orientiert und ursprünglich unabhängig vom Einsatz der Technologie, über den sie nichts aussagt. *IT*-Sicherheit im engeren Sinne bezeichnet die technische Sicherheit der technischen Infrastruktur.

In einem weiteren Sinne beschäftigt sich IT-Sicherheit mit der Sicherheit der technischen Informationsverarbeitung in der Unternehmung und schliesst dabei die organisatorischen Komponenten mit ein.

IT- / EDV-Sicherheit umfasst die beiden zuvor genannten Komponenten. Neben der erwähnten, auf reine Technologien bezogenen Betrachtung gehört dazu auch das *Management* der IT- / EDV-Sicherheit. Es umfasst alle Tätigkeiten, welche zur Aufrechterhaltung eines sicheren IT- / EDV-Systems notwendig sind. Dazu gehört z.B. die Organisation von Sicherheitskopien, die Konzeption von Zugriffssicherungsverfahren und die Betrachtung der Sicherheit im Software-Entwicklungs-, -Beschaffungs- und -Einführungsverfahren.

Informatikmanagement und Informatik-Sicherheitsmanagement

Das Management der Informatik umfasst alle Tätigkeiten, um die in der Unternehmung stattfindende computergestützte Informationsverarbeitung zu organisieren und durchzuführen. Dabei werden in erster Linie die in das IT-System eingegebenen und von ihm ausgegebenen Datenströme kanalisiert. In zweiter Linie müssen die notwendigen Institutionen innerhalb derjenigen Abteilung festgelegt werden, welche diese Kanalisierung vornimmt und unterstützt. Die Informatik-Abteilung (auch: EDV-Abteilung, IT-Abteilung etc., vgl. Anhang A) folgt dabei den organisatorischen Strukturen der gesamten Unternehmung.

Ein bestehendes, funktionierendes Informatikmanagement ist eine essentielle Voraussetzung für den Erfolg von Informationssicherheitsmanagement bzw. im Konkreten der IT- / EDV-Sicherheit. Nur wenn festgelegt ist, wie etwas zu geschehen hat, kann kontrolliert werden, ob es auch so umgesetzt wird. Das Management der Informationssicherheit muss also auf die Ergebnisse der allgemeinen Informatikmanagement-Prozesse zurückgreifen. Es nimmt dabei v.a. die Kontrollfunktion im Führungsprozess wahr (vgl. Kapitel 4.1), kann aber auch gestaltend bei der Erstellung, Beschaffung und Einführung neuer Systeme mitwirken (Planungs- und Entscheidungsbeeinflussung).

COBIT verlangt vom Informatikmanagement die Definition eines strategischen IT-Plans mit Bezug zur kurz- und langfristigen Unternehmungs- und IT-Planung sowie Aussagen zur Organisation der Unterstützung der Systeme. Dazu muss eine

technische Informationsarchitektur erstellt werden[70], die technologische Richtung bestimmt werden mitsamt Berücksichtigung der technischen Entwicklung und Aufstellung von technologischen Einsatzstandards, sowie die Organisation des Informatikmanagement ausgebaut werden. Kosten und Budget müssen erstellt und beachtet werden und Veränderungen in Anforderungen und Technologien konsequent berücksichtigt werden, indem ständig Anpassungen des betriebenen Systems bis auf Benutzerebene vorgenommen werden. (vgl auch [COBIT96.3, S. 22ff]).

Im Verkehr zwischen rechtlich teilweise oder ganz voneinander unabhängigen Organisationen (z.B. Cost-/Profit Centers) müssen Dienstleistungen vereinbart (Service Level Agreements) und konsequent eingehalten werden; hier kann aus Unabhängigkeitsgründen insbesondere das Outsourcing Probleme im Bereich Informationssicherheit verursachen, da es oft keine Kontrolle durch den Auftraggeber erlaubt.

Darüber hinaus müssen Leistungsfähigkeit und Funktion der Systeme proaktiv überwacht werden, indem Prozesse zur Antizipation grosser Belastungen etabliert und flexibel auf anfallende Leistungsunterschiede reagiert wird.

Auch im Informatik- und Informatik-Sicherheitsmanagement müssen Budgets erstellt und Kosten kontrolliert werden.

Weitere Teilbereiche des Informatikmanagement, welche durch Informatik-Sicherheitsmanagement betrachtet werden müssen, sind die Organisation und Analyse von zentralen Anlaufstellen (Help Desk, Hotline).

Das Informatikmanagement muss gemeinsam mit dem Informatik-Sicherheitsmanagement eine ständige Überwachung der technischen Infrastruktur (Monitoring) durchführen, um entstehende Schwachstellen schon im Voraus zu erkennen. In besonderen Fällen kann auch eine aktive Störfallentdeckung vorgenommen werden (vgl. unten).

Informatik-Instrumentenherstellung und Informatik-Qualität

Unter der Informatik-Instrumentenherstellung wird die gesamte Systementwicklung (Software und Hardware) innerhalb der Unternehmung oder in ihrem direkten Auftrag verstanden. Dieses Feld ist für sich sehr weit und kann hier nur ansatzweise behandelt werden. COBIT gibt unter dem Titel "Acquisition and Implementation" eine Übersicht über den Prozess [COBIT96.3, S. 33ff]. Für die Informationssicherheit ist es v.a. wichtig, in jeder Phase des Entwicklungs- und Einführungsprozesses Sicherheitsüberlegungen einfliessen lassen zu können, also z.B. bei der Analyse und Spezifikation Sicherheitsanforderungen zu spezifizieren,

---

70 Unter dem Begriff Informationsarchitektur wird im COBIT v.a. ein Modell der Daten verstanden (z.B. ein unternehmensweites Datenmodell fiele etwa unter diesen Begriff).

bei der Implementation Einfluss auf die konkret verwendeten Technologien zu nehmen und bei der Einführung auch die Prüfung der Funktionsfähigkeit der Sicherheitskomponenten vorzunehmen. Diese Sicherheitsanforderungen müssen gemeinsam mit den anderen aus Analyse und Spezifikation hervorgehenden Anforderungen die Grundlagen für die Evaluation der Systemqualität bilden. Die Qualitätsanforderungen können auf verschiedene Weise gegliedert werden. Unter anderem gehören Robustheit und Erlernbarkeit zu den Anforderungen, welche auch der Informationssicherheit dienen.

Informatik-Instrumentenunterhalt und -wartung

Beim Unterhalt und Betrieb des technischen Informationssystems können wieder verschiedene Teilgebiete unterschieden werden, z.B. in Accounting Management, Performance Management, Fault Management, Configuration Management und Security Management [ISO7498-4]. Jeder Bereich umfasst informationssicherheits-relevante Inhalte; z.B. beeinflusst das Performance Management die Verfügbarkeit und das Fault Management muss mit dem Krisenmanagement koordiniert werden.

Im Konkreten müssen Benutzerzugriff, Softwarekontrolle, Virenschutz etc. auf dieser Ebene behandelt werden. Auch die Sicherheit von Anwendungsdaten vor Einflüssen von Testläufen oder der Schutz von Systemdateien vor unberechtigtem Zugriff durch Benutzer wird auf dieser Ebene gelöst.

Zertifizierung von Informationssystemen

Die Zertifizierung von Informationssystemen bestätigt, dass ein Informationssystem die Anforderungen eines Kataloges erfüllt und sich deshalb zur Verwendung in einer sicheren Umgebung eignet. Historisch sind v.a. das Orange Book [TCSEC85] des US-amerikanischen Verteidigungsministeriums und die IT-Sicherheitskriterien [BSI-IT-SK89] des deutschen BSI anerkannte und verbreitete Massnahmen-kataloge. Zum Zeitpunkt der Erstellung dieses Textes wurde in der ISO die Erstellung einheitlicher Kriterien unter dem Titel "Common Criteria" angestrebt; ein erster Entwurf (ca. 2000 Seiten) wurde 1997 zur weiteren Überarbeitung zurückgewiesen. Weitere Angaben finden sich u.a. in [Abrams95a].

Aktive Störfallentdeckung

Die Komplexität der IT-Systeme führt zu Intransparenzen, welche das Entstehen verdeckter Störfälle ermöglichen. Die aktive Störfallentdeckung sucht nach Störfällen im System, bevor diese ein offensichtliches Fehlverhalten erzeugen. Insbesondere wird sie eingesetzt, um unberechtigte Zugriffe auf das IT-System zu entdecken, bevor Vertrauensverlust eintritt. Dazu werden automatisierte Werkzeuge sowie manuelle Kontrollen eingesetzt. Speziell kann auch die aktive Penetration von Systemen zur Entdeckung von Schwachstellen verwendet werden.

5.5.2 Prozesssicherheit

Prozesssicherheit betrachtet als Spezialgebiet der IT- / EDV-Betriebssicherheit spezifisch die dynamischen Komponenten der technischen Informationsverarbeitung. Dazu gehören die Unabhängigkeit der Prozesse, die Terminierung und die Steuerung der kooperativen Ressourcennutzung im System, welche gesamthaft erst einen stabilen Systembetrieb ermöglichen. Beispielsweise gehört auch die Entdeckung und Entfernung verdeckter Kanäle zur Prozesssicherheit.

5.5.3 IT- / EDV-Betriebssicherheit

Virenschutz

Eine der wichtigen integritäts- und verfügbarkeitssichernden Massnahmen ist der aktive und passive Schutz gegen Viren und andere Softwareanomalien. Beim aktiven Schutz werden die bestehenden, ein- und ausgehenden Daten (und Programme) der geschützten Systeme auf Virenmuster geprüft, um so infizierte Bestände sofort deaktivieren bzw. invalidieren zu können und eine Ausbreitung der Anomalie zu verhindern. Der passive Virenschutz umfasst v.a. die Vermeidung virenträchtiger Daten und Programme, z.B. durch Downloads vom Internet oder die Weitergabe von Programmkopien.

Sicherheitskopien

Die Anfertigung von Kopien der unternehmerischen Informationssammlungen und der Softwaresysteme erlaubt den Rückgriff auf diese Kopien bei Ausfall der Originale. Wichtig beim Anfertigen der dabei entstehenden kontrollierten Redundanzen ist die Auslagerung an Orte, welche von den angenommenen Ausfällen nicht betroffen sind und der Schutz vor unbefugter Einsichtnahme oder Verfälschung der ausgelagerten Kopien.

Benutzer-, Rechner- und Netzwerkverwaltung

Die Benutzerverwaltung muss den Zugriff der Benutzer auf die vom System verwalteten Daten beschränken und dazu Identifikations- und Authentifikationsmechanismen zur Verfügung stellen (z.B. Passwörter, biometrische Geräte). Ein Ablage- und Ressourcenkonzept muss den Benutzern die für sie verfügbaren Ressourcen zuweisen und vom Systemmanagement gepflegt werden. Netzverwalter müssen besonderen Sicherheitsanforderungen unterworfen werden. Für die externe Verwaltung von Systemteilen müssen besondere Zugriffsverfahren mit Beschränkung auf die relevanten Systemteile eingesetzt werden.

Die Rechner- und Netzwerkverwaltung umfasst die Erstellung von Betriebsverfahren, Verantwortlichkeitsregelungen, Verfahren der

Vorfallverwaltung, die Berücksichtigung von Interessenkonflikten durch Pflichtentrennung sowie die Trennung von Entwicklung- und Betriebsanlagen. Bei Systemplanung und -betrieb müssen die Kapazitäten mit Reserven ausgestattet werden und die technischen Abläufe ständig überwacht werden, indem Aufzeichnungen über die Transaktionen angefertigt und ausgewertet werden. Die Möglichkeit, Fremdgeräten (mobile Computer, Modems etc.) an die Netze der Unternehmung anzuschliessen, muss geregelt werden.

Inbetriebnahme und Ausserbetriebsetzung von Teilsystemen jeglicher Art (insbesondere die Entsorgung) sowie der Betrieb von Systemen ausserhalb des Unternehmungsgeländes müssen betrachtet werden.

Gesamthaft muss die IT- / EDV-Betriebssicherheit die Grundanforderungen der technischen Ebene (Verfügbarkeit, Integrität, Vertraulichkeit, vgl. Abschnitt 2.3) sicherstellen.

5.5.4 Systemsicherheit

Die Systemsicherheit umfasst die *Computersicherheit*, welche die Systeme *eher von aussen* betrachtet und alle Aspekte des Hardwareaufbaus jener Geräte betrachtet, welche bei der Informationsverarbeitung eine zentrale Rolle spielen, also z.B. die Sicherheit von Arbeitsplatzrechnern, Servern, Grossrechnern oder mobilen Systemen. Computersicherheit umfasst auch den physischen Zutrittsschutz zu diesen Systemen, z.B. die Sicherung gegen Diebstahl der Geräte und der darauf gespeicherten Informationen oder die Einteilung der Räume der Unternehmung in verschiedene Sicherheitszonen. Letzteres jedoch nur, wenn dieser Diebstahl direkt am Gerät geschieht, anderes wird durch die technische Datensicherheit und die Netzwerksicherheit abgedeckt. Ausserdem befasst sich Computersicherheit mit der Sicherheit des Betriebssystems, also u.a. den Zugriffsschutz, welcher die lokale Identifikation und Authentifizierung des Benutzers durch das System vornimmt.

Die *technische Datensicherheit* betrachtet die Systeme *eher von innen* und umfasst die Sicherheit all der Datenverarbeitungsvorgänge innerhalb dieses Systems. Dazu gehören Wahrung von innerer Integrität bei jedem Datenverarbeitungsvorgang – insbesondere bei Speicherung, Abruf und Modifikation der Daten – sowie die grundlegende Verlässlichkeit des IT-Systems.

5.5.5 Anwendungssicherheit

Zur Anwendungssicherheit (synonym: Applikationssicherheit) gehören alle Betrachtungen der Sicherheit von Applikationen, also auf den IT-Plattformen ablaufenden Programmen zur Lösung benutzerspezifischer Probleme, z.B. die selektive Sichtbarkeit von Daten in Abhängigkeit vom Benutzer (*views*). Es ist zu betonen, dass die inhaltliche Festlegung der Sicherheitsanforderungen Teil der *inhaltlichen Datensicherheit* ist (vgl. unten). Die konkrete technische Umsetzung

mit Zugriffsverweigerung kann als Teil der Systemsicherheit implementiert werden (vgl. unten), oder durch die Applikation geregelt sein. Im letzteren Fall wären so geschützte Daten durch Umgehung der Anwendungssicherheit durch Nutzung von Betriebssystemwerkzeugen zugreifbar.

5.5.6 Technische Kommunikationssicherheit

Die technische Kommunikationssicherheit umfasst alle Inhalte welche sich mit der Sicherheit der Datenübertragung innerhalb technischer Datenkommunikationsnetze befassen. Dazu gehört die *Netzwerksicherheit*: Eine *Network Security Policy* legt die allgemeinen Sicherheitsregeln im Netzwerk fest, z.B. die Aufteilung in Teilnetze. Die Sicherheit der verwendeten Übertragungsprotokolle, also z.B. die Sicherheit der gängigen Internet-Protokolle (Bsp.: Secure MIME) oder die Sicherheit der im ISO / OSI- bzw. TCP/IP-Kommunikationsstapel vorgeschlagenen Beziehungen müssen betrachtet werden. Weiterhin ist die Sicherheit der technischen Infrastruktur, welche direkt der Datenübertragung dient, relevant, also beispielsweise die Sicherheit von Kabelkanälen, Netzwerk- und Telefonverteilanlagen. Es müssen also angemessene Sicherheitstechnologien eingesetzt werden, insbesondere die Anwendung von Verschlüsselung zur Kommunikation.

Internet-Sicherheit

Die Anbindung des eigenen unternehmerischen Netzwerkes an das Internet erfordert zusätzliche Schutzkonzepte des eigenen Informationssystems vor den Risiken, welche durch eine weltweite digitale Anbindung entstehen. Diese umfassen vor allem die Abgrenzung des eigenen Netzwerkes im Vordergrund durch die Definition von *Brandschutzmauern*, welche das äussere Netz gegen das oder die inneren Netze abschliessen und nur über dafür vorgesehene Durchgänge passiert werden können. Solche Durchgänge werden *Firewall-Pass-Through*-Rechner (oder kurz und ungenau *Firewalls)* genannt. Sie filtern gemäss zum Voraus festgelegter Regeln den Datenverkehr und können verschiedene Ebenen im ISO/OSI- bzw. TCP/IP-Schichtenmodell abdecken. Ihr Einsatz und ihre kontinuierliche Anpassung an neue Risiken und bekanntgewordene Schwachstellen der verwendeten Systeme muss im Rahmen der Informationssicherheit betrachtet werden.

Verschlüsselung

Verschlüsselung dient der Datensicherheit und wird zur Wahrung der Vertraulichkeit von Informationen eingesetzt. Verschlüsselung wandelt eine *Eingabe* mit einem *Verschlüsselungsalgorithmus* in eine *Ausgabe* um, wobei ein *Schlüssel* als Parameter verwendet wird. Bei idealer Verschlüsselung können von dieser Ausgabe keine Rückschlüsse auf den Inhalt der Eingabe gezogen werden. Ein

passender *Entschlüsselungsalgorithmus* kehrt diese Umwandlung um, wobei derselbe Schlüssel als Parameter benötigt wird (symmetrische Verschlüsselung) oder ein zu diesem „Zu"-Schlüssel passender „Auf"-Schlüssel (asymmetrische Verschlüsselung).

Es bestehen verschiedene Verschlüsselungsalgorithmen, die jeweils noch durch weitere Parameter individuellen Bedürfnissen angepasst werden können. Verschlüsselung eignet sich für

- die vertrauliche Übertragung von Daten,
- die Authentisierung des Nachrichtensenders und
- die vertrauliche Speicherung

Insbesondere die ersten beiden können gut kombiniert werden. Bei einer Übertragung einer verschlüsselten Ausgabe über öffentliche Netze muss also nicht befürchtet werden, dass der Inhalt der Nachricht bekannt wird, wenn er abgefangen werden konnte. Auch für die permanente Speicherung vertraulicher Daten kann Verschlüsselung verwendet werden. Hierbei ist jedoch die langfristige Verfügbarkeit der Schlüssel zu gewährleisten.

5.5.7 Sicherheit der nicht-digitalen Datenverarbeitung

Die Sicherheit der nicht-digitalen Datenverarbeitung betrachtet diejenigen Werkzeuge, welche nicht dem IT- / EDV-System angehören. Es handelt sich also einerseits um die Sicherheit jeder Art von analog codierter Information. Dies umfasst jede direkte Kommunikation zwischen Personen (z.B. ein persönliches Gespräch), und die Verwendung nicht-digitaler Werkzeuge zur Informationsspeicherung (z.B. Papier, Ordner) und Übermittlung (z.B. Folien für Hellraumprojektoren, Briefsendungen).

Als Teilgebiete der Sicherheit lassen sich z.B. Abhörsicherheit und -schutz nennen (Sicherheit von Telefonanlagen),aber auch Zutrittsschutz zu nicht-digitalen Datenspeichern (Archivsicherheit, Ablagesicherheit, Sicherheit der Büroräume).

5.6 Produktionssicherheit

Die Produktionssicherheit umfasst die Sicherheit aller Aspekte der physischen Verarbeitung von Gütern. Diese Inhalte werden unter den Begriffen Arbeitsschutz, Werkschutz, Produktesicherheit etc. zusammengefasst und hier nicht weiter detailliert.

5.7 Infrastruktursicherheit

Die informationssicherheitsrelevanten Inhalt der Infrastruktursicherheit umfassen die Energie- und Klimaversorgung mit Verkabelung sowie den allgemeinen physischen Zutrittsschutz, z.B. durch Abgrenzung des Geländes oder einzelner Sicherheitszonen der Räume der Unternehmung oder durch Begleitung von Dritten auf dem Firmengelände. Auch Umgebungseinflüsse (geographische Lage und natürliche Bedrohungen) müssen darin berücksichtigt werden. Darüber hinaus müssen alle zum Begriff Objektschutz gehörenden Inhalte in Zusammenarbeit mit den dafür zuständigen Sicherheitsbeauftragten und Fachleuten auf ihren Einfluss auf die Informationssicherheit hin überprüft werden.

Fazit

Die inhaltliche Struktur der Informationssicherheit kann anhand der Unterteilung des Bezugsobjekts aufgebaut werden. Dies erlaubt in vielen Fällen eine eindeutige Zuordnung des Inhaltes auf ein Teilsystem des Informationssystems und somit eine Unterteilung der Informationssicherheit in Fachgebiete. Viele der hier beschriebenen Fachgebiete werden auf Ebene des Informationssystems und der Informationsverarbeitung eingeordnet, da sie diese als Ganzes betreffen. Viele davon müssen auch mit anderen allgemeinen Aufgaben der Unternehmung koordiniert werden, z.B. Versicherungen, Informationsmanagement, Outsourcing, rechtliche Aspekte etc., so dass Informationssicherheit auf dieser Ebene als Querschnittsfunktion erscheint.

Auch auf den unteren Ebenen besteht eine starke Durchdringung der Fachgebiete. Jedes technische Gebiet umfasst auch managementorientierte Elemente, beispielsweise Zugriffsschutz oder die Anfertigung von Sicherheitskopien. Eine eindeutige Zuordnung ist also nicht immer möglich.

Die inhaltliche Ordnung zeigt jedoch, auf welchen Ebenen welche Inhalte hauptsächlich behandelt werden müssen und ist kann deshalb der Koordination der Informationssicherheit in der Unternehmung dienen. Ausserdem lassen sich so einzelne inhaltliche Gebiete abgrenzen, welche in Kapitel 8 im *ISIWAY*-Detaillierungsgrad 4 verwendet werden können.

6 Prozess

Um Informationssicherheit zu erreichen, muss ein Prozess durchlaufen werden (vgl. Abschnitte 2.6 und 4.1), welcher eine grundsätzliche Erkennung des Zustandes der Sicherheit, die Beurteilung des Zustandes, die Veranlassung und Umsetzung von Massnahmen zur Zustandsbeeinflussung und die Kontrolle der Wirksamkeit der Massnahmen umfasst. Dieser Prozess wurde in der Literatur mehrfach auf unterschiedliche Weise dokumentiert. Er soll hier generisch beschreiben werden, indem die zugrundeliegenden Konzepte einander gegenübergestellt werden. Im nachfolgenden Kapitel 7 werden einige publizierte Verfahren kurz beschrieben und bewertet, um im Kapitel 8 einen Vorschlag für ein neues Verfahren zu entwickeln, welches einen derartigen Führungsprozess umfasst.

6.1 Inhalt und Ablauf

Informationssicherheit ist eine Managementaufgabe. Das *Management der Informationssicherheit* stellt dabei die Spezialisierung von Risiko- und Sicherheitsmanagement (wie in Abschnitt 2.2 kurz beschrieben) für die Belange der Informationssicherheit dar. Insbesondere umfasst dieses Informationssicherheits-management die Schaffung der notwendigen inhaltlichen und organisatorischen Voraussetzungen und das Durchlaufen eines Prozesses.

Die vom Prozess zu behandelnden *inhaltlichen Fachgebiete* wurden in Kapitel 3 strukturiert und in Kapitel 5 beschrieben. Ihre Anwendung führt beim Durchlaufen des Prozesses zu einer Beeinflussung des Bezugsobjekts. Die Anordnung der *Institutionen* innerhalb dieses Prozesses, die Ziele (*Informationen*) und die zur Verfügung stehenden Werkzeuge (*Instrumente*) können gesamthaft unter dem Aspekt der *Organisation* zusammengefasst werden und wurden in Kapitel 4 beschrieben. Diese Elemente werden nun hier zu einem Prozess verbunden. Die *Auslösung* des Prozesses verdient eine spezielle Heraushebung, da vor Beginn des ISi-Prozesses noch keine Institutionen bestehen, welche den Prozess durchlaufen könnten. Der Aspekt *Auslösung* behandelt also die Initialisierungsprobleme des Ablaufs und die Erstellung der Organisation.

Diese Art von Vorgehen und seine Durchführung für ein konkretes Objekt wird gesamthaft als *Sicherheitsverfahren* bezeichnet, die dabei gelöste Aufgabe als *Sicherheitskonzeption*. Als Ergebnis der Sicherheitskonzeption entsteht ein *Sicherheitskonzept*. Die Sicherheitskonzeption ist der zentrale Ablauf innerhalb des *Informationssicherheitsmanagements*.

Der zu durchlaufende Prozess wird im allgemeinen in vier Schritte aufgeteilt, die zyklisch wiederholt werden und im Folgenden als *Phasen der Sicherheitskonzeption* bezeichnet werden sollen. Eine Unterteilung der Phasen in einzelne *Schritte* ist

möglich. In den Schritten können meist verschiedene *Aufgaben* und *Aktivitäten* identifiziert werden. Die hier nachfolgende Beschreibung beschränkt sich auf die Phasen. Der in Kapitel 8 definierte Prozess ist detaillierter gestaltet.

Informationssicherheitsmanagement umfasst neben der Durchführung der Sicherheitskonzeption noch die Organisation des Sicherheitsprozesses selbst: die Festlegung der Institutionen und Verantwortlichkeiten und der notwendigen Kommunikationsvorgänge zwischen ihnen. Das führt dazu, dass *vor* den vier erwähnten Phasen noch eine weitere ausgeführt werden muss, die hier mit der Nummer Null bezeichnet wird.

Die fünf Phasen können also wie folgt beschrieben werden:

0. Vorbereitung

Die notwendigen organisatorischen Voraussetzungen für die Durchführung des Informationssicherheitsmanagements werden geschaffen: klare *Willensäusserungen* der verantwortlichen Institutionen, Schaffung dedizierter *Institutionen*, deren Aufgabe diese Durchführung ist und Bereitstellung der notwendigen *Ressourcen*.

1. Inventur

Die schützenswerten Informationen werden *inventarisiert* (*inventory*). Dabei werden oft auch die Informationssysteme erhoben, welche die Informationen speichern und / oder verarbeiten. Die Erhebung weiterer Objektkategorien (gemäss Klassifikation in Abschnitt 3.11) ist möglich. Ergebnis ist ein Verzeichnis der *schützenswerten Informationsobjekte,* welches als *Planung*sgrundlage verwendet werden kann.

2. Analyse

Es werden *Werte* der Informationsobjekte festgelegt oder die *Bedrohungen* und *Risiken analysiert*, welche die Sicherheit der Informationsobjekte gewährleisten. Ein *angestrebtes Sicherheitsniveau* (*security level*) oder *Schutzziel* (*protection goal*) wird festgelegt. Auf diese Weise wird die *Entscheidungs*grundlage bereitgestellt.

3. Massnahmen

Es werden *Massnahmen* (*measures, controls*), welche die Werte erhalten oder die Risiken senken, *ausgewählt, beschlossen* und ihre Umsetzung *angeordnet,*. Diese Massnahmen werden gesamthaft als *Sicherheitsdispositiv* bezeichnet.

4. Umsetzung und Kontrolle

Die *Massnahmen* werden *umgesetzt* und ihre Wirksamkeit *kontrolliert*.

In der Folge werden alle Phasen detaillierter beschrieben. Die Phasen 1 bis 4 entsprechen den generischen Phasen des Führungsprozesse (Planung, Entscheidung, Anordnung, Umsetzung, Kontrolle), wobei Umsetzung und Kontrolle in Phase 4 zusammengefasst sind, weil diese Tätigkeiten integrativ stattfinden

müssen und in diesem Kapitel nicht genauer spezifiziert werden. In Kapitel 8 (eigener Vorschlag *ISIWAY*) werden Umsetzung und Kontrolle dann getrennt behandelt.

6.2 Vorbereitungen

Die Vorbereitungen stellen den strategischen Teil des Informationssicherheits-management dar: die Festlegung langfristig gültiger Strukturen und die z.T. abstrakte Formulierung von Inhalten.

Willensäusserung

Als Voraussetzung eines wirkungsvollen Managements der Informationssicherheit muss die Unternehmungsleitung zur Überzeugung gelangen, dass Information für die Unternehmung eine schützenswerte Ressource ist. Diese Motivation muss sodann mündlich und schriftlich wiederholt ausgedrückt werden; ein Hilfsmittel dazu ist die Verfassung einer *Informationssicherheitspolitik*, welche von der Unternehmungsleitung unterzeichnet und innerhalb der Unternehmung kommuniziert wird. Diese Informationssicherheitspolitik beschreibt die *Ziele*, welche im Bereich der Informationssicherheit erreicht werden sollen, und die *Institutionen*, welche für die Erreichung dieser Ziele verantwortlich sind. Sie kann als Anhaltspunkt für die Definition eines Sicherheitsniveaus dienen, muss aber immer bereichsspezifisch interpretiert und konkretisiert werden und so von strategischem auf taktisches und operatives Niveau überführt werden. Sie kann auch grundsätzliche Aussagen über die Verfügbarkeit von Informationen in der Unternehmung machen, indem sie eine *Need-to-Know*- oder eine *Need-to-Restrict*-Handhabung vorschreibt.

Bei *Need-to-Know* sind Informationen in der Unternehmung grundsätzlich nicht frei verfügbar, sondern Teilmengen werden einzelnen Mitarbeitern nur bei Bedarf anvertraut. Dies ist angebracht in Unternehmungen mit stark diversifizierten Bereichen oder mit hohen Sicherheitsanforderungen. Umgekehrt sind bei *Need-to-Restrict* alle Informationen innerhalb der Unternehmung frei verfügbar, ausser wenn ein Bedarf zur Einschränkung der Verteilung besteht, z.B. bei besonders schützenswerten Personendaten. Diese freie Verfügbarkeit der Information erlaubt mehr Flexibilität und Dynamik der Unternehmung, da keine bzw. nur wenige Sicherheitsmassnahmen eingehalten werden müssen.

Institutionen

Für die Bildung von Institutionen wurde in Abschnitt 4.2 ein Gestaltungsvorschlag abgegeben. Dieser muss in jedem Fall an konkrete Gegebenheiten angepasst werden.

Sind diese Institutionen geschaffen, müssen ihre Existenz und ihre Einflussmöglichkeit (Weisungsbefugnis, Verantwortung, Zuständigkeit) allen betroffenen Stellen mitgeteilt werden. Dies kann durch Erwähnung in der Informationssicherheitspolitik geschehen. Eine der ersten Aktivitäten der neu geschaffenen Institution sollte es jedoch sein, sich den betroffenen Stellen selbst vorzustellen. Falls gleichzeitig schon erste generische Lösungsvorschläge abgegeben werden können, z.B. Empfehlungen für Vorgehensweisen des Informationssicherheitsmanagements (sogenannte generische Sicherheitsverfahren), Massnahmenkataloge oder Produktbewertungen, kann dies von Vorteil sein, um die Akzeptanz der neuen Institution in der Unternehmung von Beginn an zu festigen.

Ressourcen

Informationssicherheitsmanagement kann nur durchgeführt werden, wenn auf allen betroffenen Ebenen die dazu notwendigen Ressourcen bereitgestellt werden. Die Informationssicherheitspolitik kann Hinweise zur Ressourcevergabe enthalten.

Prozess

Informationssicherheitsmanagement kann als dauerhafte, parallel zu anderen Geschäftstätigkeiten laufende Aufgabe betrachtet werden oder als Projekt mit definiertem Anfangs- und Endzeitpunkt organisiert werden. Ideal ist die Kombination: Informationssicherheit wird als dauerhaftes Projekt betrachtet. Dabei umfasst ein Projekt genau einen Zyklus der oben genannten Phasen 1 bis 4, schliesst mit der vierten Phase ab, wird aber nach Abschluss sofort neu begonnen.

Wichtig bei projektbezogener Arbeit ist die angemessene Festlegung von Untersuchungsbreite und -tiefe. Die Breite bestimmt, welche Objekte (Abteilungen, Personen etc.) in die Betrachtung aufgenommen werden sollen (Scope). Die Tiefe bestimmt, wie genau und wie intensiv diese Objekte betrachtet werden (Scale). Im Rahmen des Verfahrens *ISIWAY* in Kaptitel 8 wird auf die Festlegung dieser Rahmenbedingungen und auf die projektbezogene Arbeit noch genauer eingegangen.

6.3 Inventur

Bevor mit der Verfolgung der Ziele begonnen werden kann, muss geklärt werden, welche Objekte innerhalb der Unternehmung vorhanden sind, auf die sich die Informationssicherheitspolitik bezieht. Dies sind einerseits die Informationen und Informationssammlungen selbst, andererseits alle diejenigen Objekte, welche die Informationsverarbeitung innerhalb der Unternehmung ermöglichen.

Die Vorgehensweise, welche zur Erhebung der schützenswerten Objekte verwendet wird, bestimmt letztendlich die Grundlage für die spätere Beurteilung der

Sicherheit: Wenn systemzentrisch erhoben wird, kann nur *Systemsicherheit* entstehen; wird von Daten ausgegangen, entsteht letztlich *Datensicherheit*. Weitere Sicherheitsgebiete sind diesen dann nachgelagert. Die erhobenen Objekte werden wegen des hier angestrebten informationszentrischen Ansatzes *Informationsobjekte* genannt, auch wenn sie durchaus mehr als nur Informationen und Informationssammlungen umfassen können.

6.4 Analyse

Es bestehen im Wesentlichen drei verschiedene Ansätze, um Informationssicherheit zu erreichen: *Grundschutzansatz*, *Werteansatz* und *Bedrohungs-/ Risikoanalyse*.

2.a Grundschutzansatz (Baseline Security Approach)

Beim Grundschutzansatz werden die Eigenschaften und spezifischen Anforderungen an die erhobenen Informationsobjekte nicht näher betrachtet. Für alle erhobenen Informationsobjekte wird eine Menge von allgemeingültigen Massnahmen vorgeschlagen und später angewendet, ohne auf Wert oder Bedrohungssituation Rücksicht zu nehmen. Ziel dieses Vorgehens ist eine starke Senkung der Risiken bei geringem Aufwand („80-20-Regel“). Die zugrundeliegende Annahme des Grundschutzansatzes ist, dass die Risiken sich gleichmässig auf die Informationsobjekte verteilen und sie deshalb mit einer einheitlichen Anwendung eines Satzes von Massnahmen gleichmässig gesenkt werden können.

Dieses Vorgehen hat den Vorteil, dass die zweite Phase der Sicherheitskonzeption schnell durchgeführt werden kann, da praktisch kein Aufwand entsteht, um die erhobenen Objekte näher zu analysieren. Dem steht der Nachteil gegenüber, dass die Bedrohungen und Werte beim Grundschutzansatz grundsätzlich unbekannt bleiben. Der Grundschutzansatz eignet sich deshalb nur, wenn bisher wenig oder keine Sicherheitsvorkehrungen getroffen wurden – dies ist in der Praxis immer seltener der Fall. Generell ist die zugrundeliegende Annahme, dass die Risiken gleichmässig auf alle Objekte verteilt sind, nur bei distanzierter Betrachtung haltbar und muss bei näherer Untersuchung i.d.R. revidiert werden. Die Durchführung von Grundschutz wird deshalb oft nur in einem ersten Zyklus der Sicherheitskonzeption verwendet und wird in späteren Zyklen durch die anderen Ansätze ersetzt.

2.b Werteansatz (In-Out Approach)

Beim Werteansatz werden die *Werte* der erhobenen Informationsobjekte erhoben. Die Erhebung und Festlegung kann dann nach verschiedenen Methoden geschehen:

- *Direkte Wertezuteilung*

Die betriebswirtschaftlich ermittelbaren Werte der einzelnen erhobenen Objekte werden direkt als Werte der Objekte eingesetzt. Beispiele für Bewertungsmethoden: Zeitwert, Wiederbeschaffungswert, Neuwert, diskontierter Neuwert, Gebrauchswert, Investitionshöhe. Insbesondere in den Gebrauchswert fliesst nicht nur der Wert des Objekts selbst ein, sondern auch der Wert, den seine Integration in die bestehenden Arbeitsabläufe hat.

Vorteil dieser Methode ist es, dass die Kosten und Werte (idealerweise in monetären Einheiten) direkt die unternehmerische Realität abbilden und sofort von allen Beteiligten nachvollzogen werden können.

Problematisch ist allerdings die Wahl der richtigen Bewertungsmethode. Während der Wert von informationstechnischen Anlagen recht einfach anhand von Neuwert-, Zeitwert- oder Wiederbeschaffungswert-Berechnungen bestimmt werden kann, ist der Wert von Informationen nicht so direkt bestimmbar. So ist es bei einer Informationssammlung nicht eindeutig, ob der Wert sich am Zeitaufwand für Wiederbeschaffung und Erfassung bemessen soll oder wie die Verfügbarkeit einer Information zu einem bestimmten Zeitpunkt bewertet werden soll. Das führt dazu, dass die direkten Wertbestimmungen nur Anhaltspunkte für eine Bewertung darstellen können.

Nachteil der Methode ist also, dass die eigentlichen Werte in der Praxis nur selten zur Verfügung stehen oder ermittelt werden können und deshalb geschätzt werden müssen. Daraus entstehen Ungenauigkeiten, welche i.d.R. nicht explizit genannt werden. Deshalb ist diese Methode für praktische Bewertungen nur selten geeignet.

- *Grundanforderungen als Kriterien*

  Es können *Grundanforderungen* als Bewertungskriterien gewählt werden. Der Wert eines Informationsobjektes ist dann um so höher, je höher die Anforderung an das Objekt ist, dieser Grundanforderung zu genügen. Grundanforderungen wurden in Abschnitt 2.3 beschrieben.

  Beispiele: An Umsatz- und Gewinnzahlen einer Unternehmung werden vor der Veröffentlichung *hohe Anforderungen der Vertraulichkeit* gestellt. Die *Anforderung an die Verfügbarkeit* mehrere Jahre alter Korrespondenz ist *tief*, wenn sie nicht z.B. für die Beweisführung in einem Gerichtsverfahren benötigt werden.

  Der grösste Vorteil bei der Verwendung von Grundanforderungen als Bewertungskriterien ist die Unabhängigkeit der Anforderungen von unternehmensspezifischen Gegebenheiten und – bei richtiger Wahl – die Unabhängigkeit der Kriterien untereinander. Wenn die Entscheidung für die Verwendung von Grundanforderungen zu Beginn einer Untersuchung fällt, ist damit zugleich auch Einheitlichkeit über die gesamte Untersuchung hinweg gegeben. Dies erlaubt die Vergleichbarkeit der entstehenden Resultate.

Der Nachteil bei der Verwendung von Grundanforderungen ist die notwendige hohe Abstraktion und die vielfach bestehende Unmöglichkeit, konkrete Bedrohungen direkt einzelnen Grundbedrohungen zuzuordnen.

Die Methode ist für die Praxis gut geeignet.

- *Unternehmensspezifische gemeinsame Kriterien*

  Von der Unternehmungsleitung oder der Leitung des Informationssicherheitsmanagements können unternehmens- oder projektspezifische Bewertungskriterien ausgewählt werden, welche einzelne, spezifische anzustrebende Zustände identifizieren. Das Verfahren des schweizerischen Bundesamts für Informatik [BFIWS02.95.4] verwendet beispielsweise *Datenschutzrelevanz*, *Bundesarchivpflicht*, *Wiederherstellungsaufwand* und *Klassifikation* als Bewertungskriterien für Datensammlungen.

  Vorteil dieser Zusammenstellung ist ebenfalls Einheitlichkeit und somit Vergleichbarkeit, ausserdem die direkte Bezugnahme auf Anforderungen aus dem Alltag der unternehmensspezifischen Informationsverarbeitung. Nachteil ist die Unvollständigkeit, welche aus den fehlenden Bezugnahmen auf Grundanforderungen entsteht: es werden nicht alle Grundanforderungen abgedeckt.

- *Individuelle Kriterien*

  Als weitere Variante können von den Beurteilten individuell gewählte Kriterien verwendet werden. Dabei stellen diejenigen Personen, welche die Bewertung der Informationsobjekte durchführen, zuerst selbst ihre Anforderungen als Kriterien zusammen. Beispielsweise kann eine Person fordern, dass eine Informationssammlung innerhalb einer festgelegten *Reaktionszeit* die Veränderung einer Umgebungsvariablen aufzeigen muss. Individuelle Kriterien können völlig unterschiedliche Anforderungen beschreiben.

  Vorteil dieses Vorgehens ist die an die individuelle Informationsverarbeitung angepasste Bewertung der Anforderungen. Nachteil ist die fehlende Vergleichbarkeit und ebenfalls der fehlende Bezug auf die Grundanforderungen und die dadurch potentiell entstehende Unvollständigkeit.

  Für die Praxis ist diese Methode nur geeignet, wenn die Untersuchung sich auf ein gut abgrenzbares Teilobjekt bezieht und Vergleichbarkeit nicht notwendig ist. Vergleichbarkeit kann allerdings erreicht werden, indem diese individuellen Bewertungskriterien von Beginn der Untersuchung an für die gesamte Untersuchung berücksichtigt werden und diese Methode so mit den anderen kombiniert wird.

Stehen die Bewertungskriterien fest, müssen die Skalen zur Vergabe der Werte festgelegt werden. Sie können ebenfalls unterschiedlich aufgebaut sein:

- Es können *kontinuierliche numerische* Skalen verwendet werden. Dies bietet sich insbesondere dann an, wenn die Methode der *direkten Wertezuteilung* verwendet wird.
- Es können *diskrete anumerische Skalen* verwendet werden, indem z.B. die Werte mit *hoch*, *mittel*, *niedrig*, *kein* bezeichnet werden.
- Es können *diskrete numerische Skalen* verwendet werden. Beispielsweise kann eine *3* für eine hohe Bewertung der Anforderung, eine *2* für eine mittlere, *1* für eine tiefe und *0* für die Absenz der Anforderung stehen. Beispiel: Wenn die Verfügbarkeit der mehrjährigen Korrespondenz mit *0* bewertet wird, bedeutet dies, dass diese Informationen nicht mehr benötigt werden.

  Als Variation können dann Zwischenwerte erlaubt werden. Beispiel: Eine Bewertung der Verfügbarkeit mit *0.5* bedeutet, dass die Informationen noch benötigt werden, aber ihr Verlust keine gravierenden Folgen hat.

Generell gilt für diskrete Skalen, dass die verwendeten Werte in einer Ordnung untereinander stehen sollten (ein Wert muss grösser oder kleiner als sein Nachbar sein). Die *Anzahl* der Skalenwerte ist nicht beschränkt. Eine Unterteilung in drei bis fünf Hauptwerte ist oft geeignet, um die Handhabbarkeit der Methode nicht einzuschränken. Ausserdem sollte die Argumentation der Werte so konkret wie möglich beschrieben werden; es sollte für das obige Beispiel also festgehalten werden, was der Wert *0.5* genau bedeutet. Dies kann jedoch nur durch ständige Verfeinerung der Argumentation bei wiederholter Anwendung der Bewertungsskala erfolgen.

Die einzelnen Bewertungen stellen Punkte auf der Skala dar. Als Variation können die Werte als Intervalle (`x<Wert<y`) angegeben werden.

Wenn die Skalenwerte monetäre Einheiten oder Anteile am Gesamtwert der Unternehmung repräsentieren, ist eine logarithmische Skalierung sinnvoll. Der kleinste Wert sollte jeweils die Obergrenze einer *unternehmerisch unbedeutenden Grösse* darstellen (z.B. als "<100Fr."), der grösste die Untergrenze eines unter Idealbedingungen annehmbaren Maximalwertes aller bewerteten Objekte (z.B. ">20% der mittleren Bilanzsumme der Unternehmung").

Vorteile des Bewertungsansatzes sind, dass die weitere Bearbeitung der Informationssicherheit auf Basis der von den Durchführenden bzw. den Beurteilenden angenommenen Werten der Informationsobjekte beruht. Der unternehmensinterne Wert der Informationsobjekte wird also von den informationsverarbeitenden Institutionen bestimmt und nach aussen getragen, weshalb dieser Ansatz auch als *In-Out-Ansatz* bezeichnet werden soll. Nachteil dieses Ansatzes ist, dass die konkreten Bedrohungen und Risiken noch unbekannt bleiben.

2.c Bedrohungs- und Risikoansatz (Out-In Approach)

Bedrohungsanalyse

Beim Bedrohungsansatz werden für jedes Informationsobjekt (oder Gruppen davon) die Bedrohungen analysiert, welche die Sicherheit dieses Objekts beeinträchtigen. Diese Bedrohungen werden mit Wahrscheinlichkeiten des Eintritts und dem daraus entstehenden Schadens kombiniert sowie mit der Höhe dieses Schadens. Das Risiko errechnet sich als Produkt aus Eintrittswahrscheinlichkeit und Schadenshöhe und entspricht dem statistischen Erwartungswert. Für jedes Risiko werden dann später spezifische Massnahmen bestimmt und umgesetzt, welche dieses Risiko gezielt senken.

Die einzelnen Bedrohungen werden individuell durch die Beurteilenden hergeleitet, beispielsweise aufgrund von generischen Bedrohungslisten (z.B. [Winterthur97]) und durch Konkretisierung um neue Elemente ergänzt.

Eines der zentralen Probleme bei der Durchführung einer Bedrohungsanalyse besteht im Finden der angemessenen Abstraktion. Eine zu weit gefasst Abstraktion der Bedrohungsanalyse führt zu einer kleinen Zahl von Bedrohungen, welche jedoch so unspezifisch sind, dass ihr weder Wahrscheinlichkeiten zugeordnet (vgl. unten) noch konkrete Handlungsanweisungen daraus abgeleitet werden können. Ein zu tiefes Abstraktionsniveau führt zu einer grossen Zahl von Bedrohungen, aus denen sich zwar jeweils konkrete Handlungsanweisungen ableiten lassen und denen durch ihren konkreten Bezug auch Wahrscheinlichkeiten zugeordnet werden können, die jedoch in ihrer Gesamtheit unangemessen hohen Erhebungs- und Bearbeitungsaufwand erzeugen. Sinnvoll ist eine Abstraktion auf Gruppen von Informationsobjekten und Klassen von Bedrohungen.

Auch bei intensiver Herleitung der möglichen Bedrohungen kann nicht ausgeschlossen werden, dass einzelne Bedrohungen nicht bedacht werden. Es bleiben also immer unidentifizierte Bedrohungen bestehen.

Risikoanalyse

In einem zweiten Schritt werden die Risiken analysiert, welche aus den Bedrohungen entstehen. Dies umfasst die Beurteilung der Wahrscheinlichkeit der Manifestation der Bedrohung sowie die Beurteilung des Schadens, der dabei entsteht.

Die genaue Bestimmung der Wahrscheinlichkeit ist in den seltensten Fällen möglich. Oft lassen sich jedoch Wahrscheinlichkeitsklassen bilden, die beispielsweise mit den Häufigkeitsklassen *nie, selten, manchmal, häufig, immer* bezeichnet werden. In Analogie zu den Werten beim In-Out-Ansatz gilt, dass die Argumentation dieser Werte gesondert und möglichst ausführlich beschrieben werden muss. Auch eine Bezeichnung der Wahrscheinlichkeitsskala mit

quantitativen Frequenzwerten (`<1/Jahr`, `1/Jahr bis 1/Monat` *etc.*) oder anteilmässiger Dauer (`<1 Min./Jahr`, ... `>1 Min./Tag`) ist möglich.

Die genaue Bestimmung der Schadenshöhen ist ebenfalls in den seltensten Fällen möglich. Der Wert bestimmt sich aufgrund der Bewertung der von den Bedrohungen betroffenen Objekte. Dazu kann eine direkte Wertezuweisung (vgl. oben) verwendet werden. Auch die Unterteilung der Skalen kann entsprechend der beim Werteansatz beschriebenen Vorgehensweise erfolgen.

Die konkrete Bestimmung von Wahrscheinlichkeiten und Schadenshöhen geschieht in der Regel mit Hilfe einer Tabelle, welche die Nummerierung der Risiken erlaubt. Nachdem die Bestimmung abgeschlossen ist, können diese Risiken in eine Matrix gemäss Abbildung 6-1 eingetragen werden..

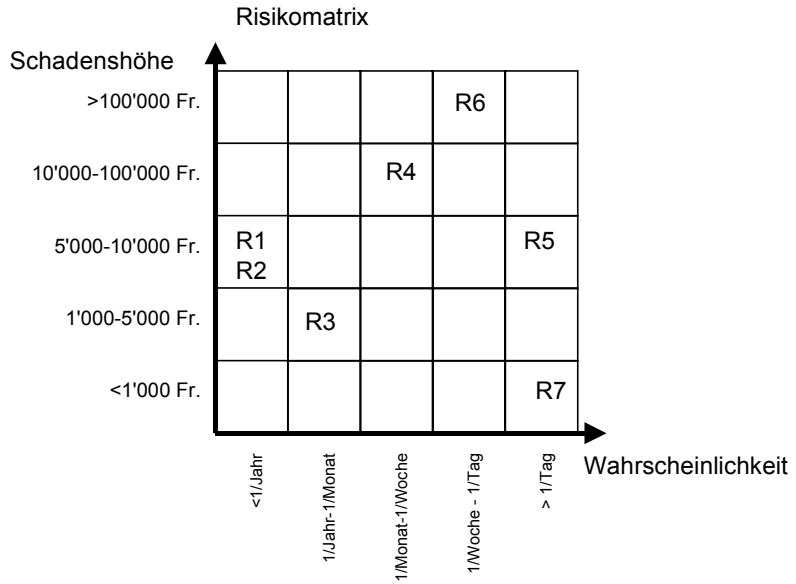


Abbildung 6-1: Risikomatrix mit Risiken

Die Bestimmung eines *Sicherheitsniveaus* durch die Beurteilenden legt nun fest, bis zu welcher Kombination von Schadenshöhe und Wahrscheinlichkeit die Risiken tolerierbar sind (es wird deshalb auch *Sicherheitsziel* oder *Risikoziel* genannt). Diese Bestimmung geschieht, indem für jedes Feld der Matrix bestimmt wird, ob Risiken in diesem Bereich für die Unternehmung tolerierbar sind (und entsprechend getragen werden sollen), oder ob Massnahmen ergriffen werden sollen, um diese Risiken zu senken. Bei dieser Festlegung entsteht eine Linie, welche prinzipiell der Bestimmung des Sicherheitsziels[71] gemäss Abbildung 2-1 (Seite 28) und Abbildung 2-3 (Seite 33) entspricht. Die in der Matrix oberhalb des Risikoziels liegenden Risiken (in Abbildung 6-2 grau hinterlegt) müssen mit Massnahmen gesenkt

71 Die Begriffe *Sicherheitsziel, Risikoziel* und *Schutzziel* werden synonym verwendet.

werden, bis sie unter dem Risikoziel zu liegen kommen (vgl. Abschnitt *Massnahmen* unten)[72].

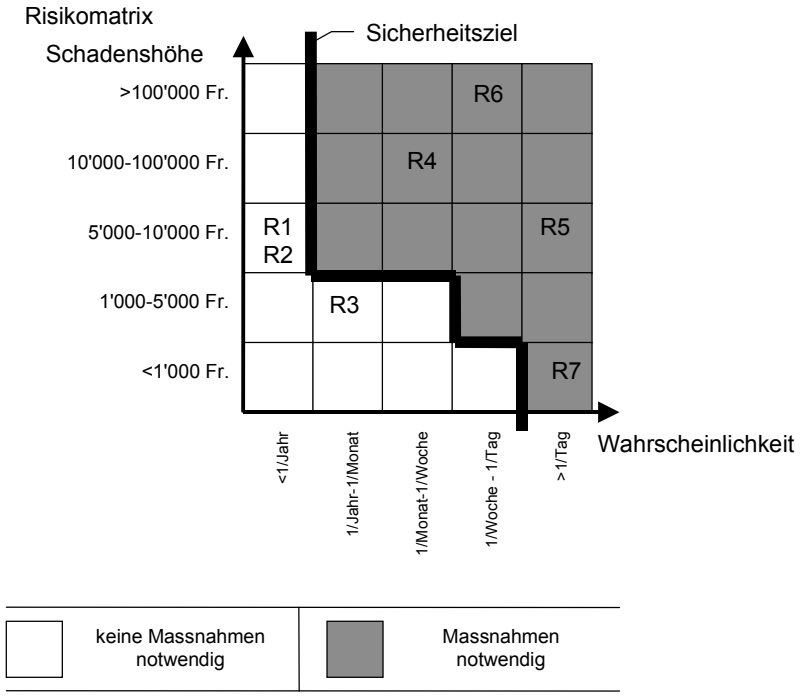


Abbildung 6-2: Risikomatrix mit Sicherheitsziel

Die Bestimmung des Sicherheitsniveaus ist jedoch keine rein analytische Aufgabe, sondern steht in engem Zusammenhang mit der Risikofreude und der Risikokultur der Unternehmung. Sicherheitsmassnahmen ziehen oft nicht nur einmalige, sondern kontinuierliche Mehraufwendungen nach sich und möglicherweise müssen Regeln im Umgang mit den Informationsobjekten befolgt werden, die nicht trivial sind und deren Aufwand nicht vernachlässigt werden kann. Dies schränkt Effizienz und Flexibilität der Informationsverarbeitung im täglichen Betrieb ein. Da Effizienz und Flexibilität allerdings primäre Ziele der Unternehmungsleitung sind, wird die Unternehmung das Sicherheitsniveau tendenziell eher senken als erhöhen wollen. Dabei hängt es stark von der Branche und der individuellen Unternehmungskultur ab, wie gross die Risikobereitschaft ist.[73] Vollständige Sicherheit kann ohnehin

---

72 Inwieweit Risiken, welche seltener als einmal jährlich auftreten, aber Schäden von mehr als 100'000 Fr. verursachen, für die Unternehmung tolerierbar sind (linkes oberes Feld in Abbildung 6-1), ist fragwürdig. Es könnte argumentiert werden, Risiken ab einer bestimmten Höhe (also z.B. ab 100'000 Fr.) seien nie tolerierbar; dann müssten allerdings auch entsprechend extreme Massnahmen getroffen werden. In der Regel bestehen keine Risiken in den Extremfeldern links oben und rechts unten in der Risikomatrix, weil sie als nicht relevant betrachtet werden.

73 In Abbildung 2-1 ist die Risikobereitschaft direkt als Linie *Risiko-Break-Even* eingetragen, deren Neigung mit steigender Risikofreude steigt (und so das Sicherheitsziel nach links verschiebt).Dabei muss jedoch beachtet werden, dass die Risikofreude das *subjektive*

nicht erreicht werden. Der Aufwand zur Erreichung eines höheren Sicherheitsniveau steigt überproportional an, je näher man sich der vollständigen Sicherheit nähert (vgl. Abschnitt 2.2).

Mathematisch erzeugt das Produkt aus Wahrscheinlichkeit und Schadenswert einen Erwartungswert. Diesen berechnen zu können, setzt aber einerseits numerische Skalen voraus. Ausserdem bedingt es, dass die Wahrscheinlichkeitsklassen (`1/Jahr` *etc.*) eindeutig auf einen numerischen Wert (z.B. im Bereich von 0 bis 100%) abgebildet werden können. Letzteres ist aufgrund der Unterschiedlichkeit der Bedrohungen nicht immer möglich. Das Sicherheitsniveau bestimmt sich dann als festgelegter Wert im Bereich der Erwartungswerte, unter den alle Erwartungswerte gesenkt werden müssen.

Wenn die Bedrohungs- und Risikoanalyse durchgeführt werden, sind die Risiken, welchen die betrachteten Objekte unterliegen, bekannt und haben zur Schaffung eines *Risikobewusstseins* geführt. Dies ist ein wichtiger Vorteil dieser Vorgehensweise. Ihre Nachteile sind jedoch, dass die Risikoanalyse in Abhängigkeit von der Grösse und Komplexität des Untersuchungsobjektes und der gewählten Betrachtungstiefe (Abstraktionsgrad) sehr aufwendig sein kann, und dass die Erkenntnisse aufgrund technischen Fortschritts und der Entwicklung der Unternehmung und ihrer Umwelt sehr schnell überholt sind.

Der Ansatz der Bedrohungs- und Risikoanalyse wird hier auch als *Out-In-Ansatz* bezeichnet, weil er primär die von aussen auf die Unternehmung und ihre Informationsverarbeitung einwirkenden Bedrohungen betrachtet. Damit soll nicht ausgeschlossen werden, dass einzelne Bedrohungen aus der Informationsverarbeitung selbst entstehen können.

2.d Kombinierter Ansatz (Combined Approach)

Bei diesem Ansatz wird versucht, die Vorteile von Grundschutzansatz und Bedrohungsansatz durch Kombination zu vereinen.

Die Informationsobjekte werden dabei zunächst gesamthaft erhoben, und es werden allgemeine Massnahmen unabhängig von Bedrohungen und Werten festgelegt und umgesetzt. In einer erneuten, nach Abschluss der Umsetzung oder parallel dazu durchgeführten Betrachtung wird versucht, diejenigen Objekte zu identifizieren, welche grossen Bedrohungen unterliegen. Genau diese Objekte werden dann einer detaillierten Risikoanalyse unterzogen.

Vorteil dieses Vorgehens ist, dass der hohe Aufwand der Bedrohungs- und Risikoanalyse nur für diejenigen Objekte durchgeführt wird, für die es sich aufgrund grober Abschätzung auch lohnt, weil sie hohen Risiken unterliegen.

Sicherheitsniveau beeinflusst. Der objektive Risiko-Break-Even – so er denn bestimmbar wäre – bleibt davon unbeeinflusst!

Nachteil ist dabei, dass die Werte der untersuchten Objekte nicht genauer betrachtet werden und auch die Risiken, denen sie unterliegen, erst in einem zweiten Anlauf (also möglicherweise mit erheblicher zeitlicher Verzögerung) betrachtet werden und dies weniger gründlich als bei direkter Risikoanalyse.

2.e Ad-hoc-Ansatz

Dieser Ansatz wird der Vollständigkeit halber erwähnt und umfasst die Tätigkeiten, welche bei unstrukturiertem Vorgehen des Risikomanagements durchgeführt werden. Der Vorteil dabei ist der geringe Aufwand. Nachteil dieses Ansatzes ist seine Unvollständigkeit per Definition. Ein derartiges Vorgehen scheint so verbreitet zu sein, dass es in [ISO13335-2] Erwähnung findet. Es wird dort als ungeeignet bezeichnet.

2.f Do-Nothing-Ansatz

Ebenfalls der Vollständigkeit halber soll erwähnt werden, dass der Verzicht auf Sicherheitsmanagement auch als mögliche Vorgehensweise gelten kann. Dieser Ansatz wird in der Literatur nicht explizit erwähnt, es kann jedoch nicht ausgeschlossen werden, dass in einzelnen Unternehmungen kein explizites Informationssicherheitsmanagement stattfindet.

Der Vorteil dieses Ansatzes liegt sicherlich in der Minimierung des direkten Sicherheitsaufwandes. Der Nachteil besteht in der Unvorhersehbarkeit der Sicherheit und in der starken Reaktion der schützenswerten Objekte auf Umwelteinflüsse.

Die zweite Phase der Sicherheitskonzeption endet mit einer Zusammenstellung der identifizierten schützenswerten Informationsobjekte und

- im Fall des Grundschutzes ohne weitere Angaben,
- im Fall der Werteanalyse den ihnen zugewiesenen Werten, welche erhalten werden müssen,
- im Fall der Bedrohungsanalyse mit einer Zusammenstellung der Bedrohungen und Risiken (mitsamt erwarteter Schadenshöhe und Eintrittswahrscheinlichkeit), denen die Objekte unterliegen,
- im Fall des kombinierten Ansatzes mit den Ergebnissen der Bedrohungsanalyse für die spezifisch untersuchten Teilobjekte.

6.5 Massnahmen

Die Auswahl geeigneter Massnahmen zur Umsetzung soll dazu führen, dass die Sicherheit der Informationsobjekte langfristig erhalten wird oder steigt[74] und dass sich das tatsächliche Sicherheitsniveau dem angestrebten nähert.

Die umzusetzenden Massnahmen stammen

- aus allgemeinen Massnahmenkatalogen, welche für die Erhöhung der Informationssicherheit der betrachteten Objekte geeignet sind (z.B. in Abhängigkeit von Technologie oder Branche),
- im Falle des Grundschutzes aus besonderen Grundschutzmassnahmen-katalogen, welche zu Beginn der Durchführung des Verfahrens bestimmt wurden. Es bestehen derartige Kataloge, die allgemein verfügbar sind und deren Massnahmen anstreben, möglichst viele Bereiche abzudecken (z.B. das IT-Grundschutzhandbuch [BSI-IT-GSHB97]). Sie sind jedoch oft so abstrakt, dass sie hohen Interpretationsbedarf aufweisen und mehr als „Themen-kataloge“ der Informationssicherheit bezeichnet werden können (z.B. der Code of Practice [BSI-COP95]).
- aus spezifischen Massnahmen, welche durch Initianten oder Leiter der Durchführung, Betreiber, Benutzer oder andere Beteiligte aufgrund der konkreten sich stellenden Aufgabe hergeleitet werden.

Welche Tätigkeiten müssen in dieser Phase durchgeführt werden?

- Im Fall des Grundschutzansatzes ist es Aufgabe dieser Phase, die im entsprechenden Grundschutzmassnahmenkatalog enthaltenen Massnahmen möglichst vollständig für alle betroffenen Objekte umzusetzen.
- Im Fall der Werteanalyse müssen Massnahmen ausgewählt und umgesetzt werden, welche dazu führen, dass die Werte erhalten bleiben.
- Im Fall der Bedrohungsanalyse müssen Massnahmen ausgewählt und umgesetzt werden, welche die identifizierten Risiken bis unterhalb des als angestrebten Sicherheitsniveaus identifizierten Wert senken.

Die Massnahmenauswahl wird primär durch die zu erfüllenden Anforderungen bestimmt. Die Umsetzung jeder einzelnen Massnahme erzeugt jedoch Aufwand, der in der Unternehmung budgetiert und beschlossen werden muss. Dazu bedarf es Diskussionen über Kosten und Nutzen jeder Massnahme. Letztendlich müssen alle an der Informationsverarbeitung Beteiligten gemeinsam über die Umsetzung der sie betreffenden Massnahmen beschliessen.

---

74 Grundsätzlich ist auch eine Durchführung zur *Senkung* des bestehenden Sicherheitsniveaus denkbar. Dies wird hier nicht weiter berücksichtigt.

Beim Werteansatz muss zu bis diesem Zeitpunkt festgestellt werden, ob die Anforderungen, welche an die Informationsobjekte gestellt werden, auch erfüllt werden können. Das ist insbesondere deshalb wichtig, weil es sich bei Anforderungsstellern und Anforderungserfüllern oft um verschiedene Parteien handelt. Wenn beispielsweise an eine Informationssammlung hohe Anforderungen der Vertraulichkeit gestellt werden, dann müssen diese Anforderungen von allen verarbeitenden Systemen, also auch den betroffenen Komponenten des IT-Systems, eingehalten werden. Um dies festzustellen, können durchaus eigene Bedrohungs- und Risikoanalysen der Systembetreiber notwendig sein, welche jedoch nicht so aufwendig sind wie in Abschnitt 6.4 beschrieben, da das zu erreichende Sicherheitsniveau zuvor als *Erhaltung der identifizierten Werte* implizit feststeht. Als Prioritäten der Umsetzung können dabei die absoluten Werte der Differenzen zwischen Anforderung und Erfüllung verwendet werden.

Beim Grundschutzansatz wird die Priorität der Umsetzung sich an allgemeinen Rahmenbedingungen innerhalb der Unternehmung orientieren, da sie sich nicht aus dem Verfahren herleiten lässt. Beim Werteansatz leitet sich aus der Differenz zwischen bestehender und angestrebter Sicherheitsleistung her. Beim Bedrohung- und Risikoansatz kann die Priorität aufgrund der Entfernung der einzelnen Risiken vom angestrebten Sicherheitsniveau gewählt werden.

Der Risikoansatz (vgl. Abbildung 6-3) geht davon aus, dass vor Beginn einer Risikoanalyse Risiken bestehen. Diese werden zunächst soweit wie möglich identifiziert, wobei diese Identifikation aus Aufwands- und Komplexitätsgründen immer unvollständig bleibt. Die einzelnen Massnahmen werden einem *Sicherheitsdispositiv* untergeordnet. Dieser Begriff umfasst die verschiedenen Kategorien, in welche Massnahmen aufgrund ihrer risikobezogenen Wirkung eingeteilt werden können. Diese Kategorien sind:

- Vermeidung:
  Die bedrohten Objekte werden aus der Bedrohung herausgenommen, so dass gar kein Risiko mehr entstehen kann (z.B. durch Aufgabe eines Geschäftsfeldes oder durch Stillegung eines betroffenen Systems)
- Senken der Häufigkeit / Wahrscheinlichkeit:

  Die Wahrscheinlichkeit, dass ein Schaden entsteht, wird durch Anwendung entsprechender Massnahmen gesenkt (z.B. durch Verwendung von redundanten Systemen)
- Senken der Schadenshöhe:

  Der Schaden, der entstehen kann, wird durch Anwendung entsprechender Massnahmen gesenkt (z.B. feinere Aufteilung der Verarbeitung auf mehrere, kleinere Systeme)
- Überwälzen des Risikos:

Durch das Abschliessen von Versicherungen, Verträgen oder ähnlichen Vorkehrungen wird erreicht, dass der Schaden, wenn er entsteht, nicht oder nicht vollständig getragen werden muss.

Jede dieser Massnahmen beabsichtigt, die identifizierten Risiken zu senken. Potentiell werden immer auch die unidentifizierten Risiken beeinflusst. In jedem Fall bleiben Teil-Risiken zurück, die akzeptiert werden müssen. Dies betrifft insbesondere den Selbstbehalt, der bei der Überwälzung von Risiken an Versicherungen notwendig ist. Doch auch die Schadenshöhe oder die Wahrscheinlichkeit eines einzelnen Risikos können nie auf Null gesenkt werden.

Ziel des Sicherheitsdispositivs ist eine Senkung unter den durch das angestrebte Sicherheitsniveau (Sicherheitsziel) festgelegten Wert. Dies ist nicht immer möglich. Wenn keine Massnahmen zur (weiteren) Senkung des Risikos mehr eingesetzt werden können oder sollen, muss das Risiko getragen werden. Dies kann auf einen von drei Gründen zurückgeführt werden:

- Es besteht keine Massnahme, welche das Risiko weiter senken kann,
- die verfügbaren Massnahmen sind zu teuer (erzeugen zuviel Aufwand), so dass das Kosten-Nutzen-Verhältnis zu klein wird,
- die verfügbaren Massnahmen sollen aus unternehmerischen Gründen nicht eingesetzt werden (risikofreudige Entscheidung).

Das selbst getragene Risiko wird *Restrisiko* genannt. Es setzt sich aus den nicht behandelbaren, den nicht behandelten und den unbekannten Risiken zusammen und bleibt in der Regel grösser als vom Sicherheitsziel her vorgegeben (anders formuliert: das Sicherheitsziel wird in der Regel nicht ganz erreicht).

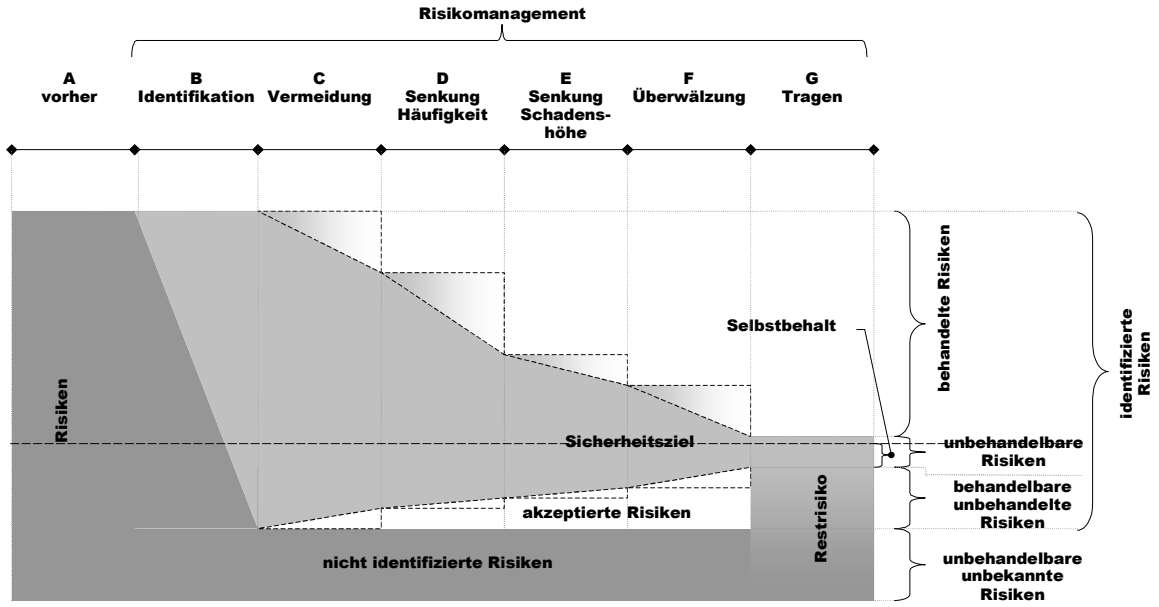


Abbildung 6-3: Sicherheitsdispositiv [in Anlehnung an Winterthur90, S. 10]

Massnahmen und Sicherheitsarchitektur

Die Massnahmen können in organisatorische, personelle, technische und bauliche Massnahmen unterschieden werden (vgl. Abschnitt 4.5). Die Anordnung der Massnahmen auf strategischer, taktischer und operativer Ebene wird als *Sicherheitsarchitektur* (*security architecture*) bezeichnet. Die Sicherheitsarchitektur ist ebenfalls das Ergebnis der Sicherheitskonzeption. Während das Sicherheitskonzept beschreibt, *was* zu tun ist, beschreibt die Sicherheitsarchitektur das Zusammenwirken der einzelnen Komponenten.

Eine mögliche Struktur des einer Sicherheitsarchitektur für *IT-Systeme* hat Sherwood vorgestellt (vgl. Abbildung 6-4).

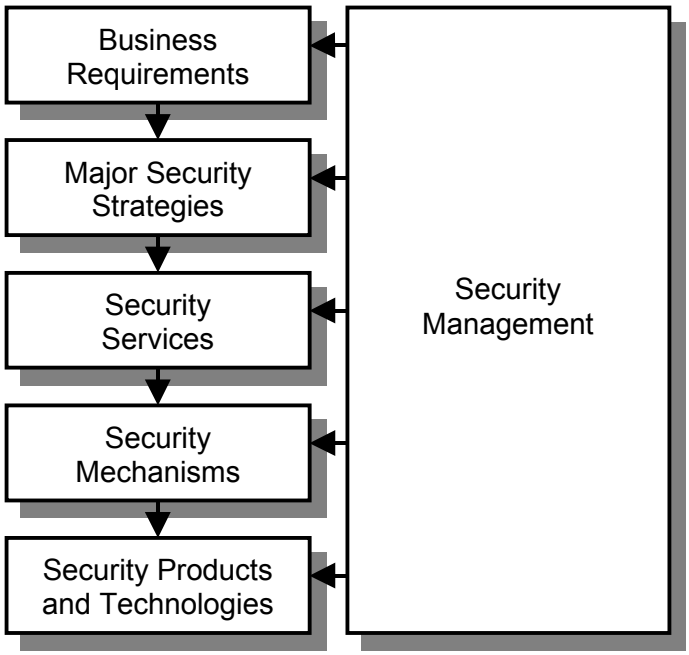


Abbildung 6-4: IT-Sicherheitsarchitektur [Sherwood96]

- Auf der obersten Ebene werden die geschäftlichen Anforderungen (*business requirements*) an die Sicherheitsbedürfnisse der Geschäftsleitung festgelegt. Dies entspricht der Entwicklung und Festlegung der Informationssicherheits-politik.
- Auf der strategischen Ebene werden Sicherheitsstrategien festgelegt, welche die Wege und Mittel beschreibt, um IT-Sicherheit zu erreichen. Das in diesem Kapitel beschriebene Verfahren ist eine solche übergeordnete Strategie.
- Auf taktischer Ebene werden Sicherheitsdienste definiert, mit Hilfe derer die IT-Sicherheit hergestellt werden kann. Darunter versteht er beispielsweise die *security services* gemäss X.800 [ISO7498-2 oder Holbein96 S. 210f]: *peer entity authentication, traffic flow confidentiality, connectionless integrity* etc.,

- Auf operativer Ebene werden diese Dienste durch Sicherheitsmechanismen implementiert, z.B. gemäss X.800 durch *digital signatures, traffic padding, encipherment* etc.
- Auf der untersten Ebene werden Produkte ausgewählt und eingesetzt, in welchen die Sicherheitsmechanismen durch konkrete Funktionalitäten zur Verfügung gestellt werden.

Ein die Ebenen übergreifendes *Sicherheitsmanagement* überwacht und steuert die Tätigkeiten.

Sicherheitskonzept, Sicherheitsarchitektur und die hier beschriebene Vorgehensweise werden hier gemeinsam als *Sicherheitsstrategie* bezeichnet, weil sie festlegen, *wie* Informationssicherheit in der Unternehmung erreicht werden soll. Es ist beabsichtigt, dass die Sicherheitsarchitektur, welche als Resultat der Sicherheitskonzeption entsteht, wiederum Aussagen über die Sicherheitskonzeption und die ihr zugrundeliegenden Strukturen enthalten kann (Sicherheitscontrolling vs. Controller-Funktion des Sicherheitsbeauftragten, vgl. Abschnitte 4.2 und 6.2) und so die wiederholte Durchführung von Informationssicherheitsprojekten zur Anpassung der dabei verwendeten Projektstrukturen führen kann. Dies ist durchaus beabsichtigt und erlaubt die Reaktion auf Veränderungen der organisatorischen Strukturen und der Anforderungen der Informationssicherheit in der Unternehmung. Das Management von Informationssicherheit kann also selbstmodifizierende Elemente enthalten.

6.6 Umsetzung und Kontrolle

Die zur Umsetzung beschlossenen Massnahmen müssen anschliessend durch die davon betroffenen Bereiche der Unternehmung implementiert werden. In dieser Umsetzungsphase können Probleme entstehen, welche die Implementation einzelner Massnahmen verzögern, verteuern oder verhindern. Ausserdem kann festgestellt werden, dass die zu erhaltenden Werte oder die zu senkenden Risiken von der Massnahme nicht beeinflusst werden, die Massnahme also nicht angemessen bzw. nicht wirksam ist. Im letzteren Fall ist ein Verzicht auf die Umsetzung sinnvoll. Ansonsten muss sichergestellt werden, dass die beschlossenen Massnahmen früher oder später zur Anwendung gelangen.

Die Kontrolle (als letzte Phase jedes Führungsprozesses) muss deshalb die festgelegten Ziele mit dem Erreichten vergleichen. Diese Kontrolle muss durch die Leitung der Untersuchung erfolgen; ausschliessliche Selbstkontrolle der betroffenen Bereiche ist nicht sinnvoll. In grossen Unternehmungen besteht i.d.R. eine interne Revisionsstelle, welche diese Kontrollaufgabe wahrnehmen kann (vgl. auch Institutionen in Abschnitt 4.1 und 4.2). Die Ergebnisse der Kontrolle sind Aussagen über den Umsetzungsgrad der einzelnen Massnahmen; Feststellung von Erfüllung oder Nichterreichung der gesetzten Ziele und Begründungen dafür.

Die Ergebnisse der Kontrolle müssen in einen erneuten Durchlauf des Informationssicherheitsverfahrens einfliessen.

6.7 Aufwand für Informationssicherheitsbetrachtungen

Bei der Durchführung einer Informationssicherheitsuntersuchung nach dem oben genannten Schema entsteht Aufwand für die beteiligten Personen. Wieviel Aufwand entsteht, hängt von den im konkreten Fall vorhandenen Rahmenbedingungen ab. Es können folgende Einflussfaktoren identifiziert werden:

- Motivation und Koordination:

  Informationssicherheit ist in vielen Unternehmungen ein unbeliebtes Thema. Das führt dazu, dass hohes Engagement notwendig ist, um eine Untersuchung nur schon *auszulösen*. Andererseits führt es auch dazu, dass viele Personen beteiligt werden *müssen* und zum Teil auch beteiligt werden *wollen* (dies erhöht den für die Kommunikation notwendigen Aufwand). Auch kann es vorkommen, dass wichtige Personen *nicht* beteiligt werden *wollen*. Schon vor dem Start eines Projektes kann demnach hoher Koordinationsaufwand entstehen, um die richtigen Parteien zu identifizieren und zu involvieren. Im allgemeinen sinkt also der Aufwand mit steigender Motivation der Betroffenen.

- Qualität der Basis:

  Das Management der Informationssicherheit beruht auf dem Informatik- und Informationsmanagement. Falls in diesen Bereichen Probleme bestehen – etwa aufgrund mangelnder Kommunikation zwischen Informatik und Fachbereichen oder aufgrund unterschiedlicher Auffassungen – so muss das Management der Informationssicherheit die notwendigen Grundlagen zuerst selbst aufbauen, bevor die eigentliche Sicherheitsarbeit geleistet werden kann. Zentral ist dabei, dass die schützenswerten Objekte und Informationen zuerst einmal *bekannt* sein müssen, d.h. es muss einmal erhoben werden, was zu schützen ist. Der Aufwand für das Management der Informationssicherheit ist also um so geringer, desto besser die Grundlagen sind, auf welchen aufgebaut werden kann.

- Komplexität des Informationssystems:

  Die in den Unternehmungen verwendeten Informationssysteme werden immer komplexer. Zahlreiche Betriebssysteme, Schnittstellen, Zugriffs- und Abfragemöglichkeiten haben die Flexibilität der Systeme stark erhöht, jedoch auch viele Sicherheitslücken aufgerissen. Es ist deshalb zuerst notwendig, ein durchgängiges Verständnis des Informationssystems aufzubauen, um so die einzelnen Schwachstellen überhaupt erst identifizieren zu können. Dies bedingt Erhebungs- und Verwaltungsaufwand. Der Aufwand für das

Management der Informationssicherheit steigt also mit der Komplexität des Informationssystems.

- Klarheit der Anforderungen:

  Die Anforderungen an die Informationssysteme und die verwendeten Informationen steigen in dem Masse, in dem die Abhängigkeit von ihnen zunimmt. Die Anforderungen werden jedoch selten klar und formal nachvollziehbar geäussert, sondern oft nur allgemein formuliert. Um jedoch anforderungsgerechte Informationssicherheit erreichen zu können, müssen die Anforderungen klar spezifiziert werden, was mit Aufwand verbunden ist. Dabei müssen diejenigen Systeme, von denen die höchste Abhängigkeit besteht, prioritär behandelt werden. Bei höherer Abhängigkeit ist deren Anzahl grösser oder die einzelnen Anforderungen sind höher (oder beides). Der Aufwand für das Management der Informationssicherheit steigt also mit der Abhängigkeit vom Informationssystem.

6.8 Fazit aus Teil II

Mit diesem Abschnitt endet die Betrachtung der einzelnen Komponenten des Rahmenwerks der Informationssicherheit. Hier werden einige zentrale Punkte des Textes nochmals betont zusammengefasst.

Was ist Informationssicherheit?

Informationssicherheit ist zunächst derjenige Zustand von Informationen, in welchem sie die Anforderungen erfüllt, welche eine Person daran stellt. Dieser Zustand kann aus mehreren Gründen nie ganz erreicht werden: Vollständige Sicherheit ist nicht beweisbar erreichbar, Sicherheitsanforderungen und die davon betroffene Information ändern sich, Informationssicherheit ist von der Sicherheit der verarbeitenden Informationssystems abhängig, Sicherheit hemmt Flexibilität und Effizienz der Unternehmung.

Informationssicherheit ist also vor allem ein erstrebenswertes Ziel. Wieviel Sicherheit notwendig ist, muss individuell, d.h. subjektiv bestimmt werden. Dazu kann ein anzustrebendes Sicherheitsniveau festgelegt werden. Informationssicherheit umfasst aber auch den Prozess, welcher zur Verfolgung dieses Zieles durchlaufen wird. Schliesslich ist Informationssicherheit auch die Bezeichnung für das Fachgebiet, welches sich mit den drei genannten Bedeutungen (Zustand, Ziel, Prozess) auseinandersetzt.

Warum soll eine Unternehmung Informationssicherheit anstreben?

Informationssicherheit trägt wie die unternehmerische Sicherheit dazu bei, den Ablauf der Geschäftsprozesse vorhersagbarer zu gestalten, da sie die Anzahl und die Stärke der Störfälle reduziert. Die Informationen, die Informationsverarbeitungsprozesse und die darauf beruhenden Entscheidungen werden zuverlässiger, was langfristig zu mehr Erfolg der Unternehmung führt.

Welche Priorität sollte die Informationssicherheit haben?

Informationssicherheit sollte mindestens zweite Priorität nach den unternehmerischen Zielen haben. Es ist nicht sinnvoll, Sicherheit über diejenigen Ziele zu stellen, welche das langfristige Überleben der Unternehmung erst ermöglichen. Der Ausdruck "*mindestens"* bedeutet jedoch, dass Sicherheit möglichst früh betrachtet werden muss und nicht hinter anderen Zielen wie z.B. Optimierungen zurückstehen darf.

Was ist für erfolgreiches Informationssicherheitsmanagement notwendig?

Zentrale Elemente eines erfolgreichen Informationssicherheitsmanagements sind der *Wille der Unternehmungsführung*, Sicherheit bewusst zu gestalten, ein auf die Unternehmung angepasstes *Rollenmodell*, welches die Verantwortungen, Aufgaben und Kompetenzen jedes Einzelnen in der Unternehmung definieren und eine möglichst standardisierte Vorgehensweise: der Informationssicherheits*prozess*.

Die anderen hier erwähnten und beschriebenen Elemente folgen daraus. Wichtige Institutionen sind der Informationssicherheits*beauftragte*, dem die Gesamtführung der Informationssicherheit obliegt, und der Informationssicherheits*koordinator*, der in der einzelnen Abteilung die Informationssicherheit vorantreibt. Zentrale Informationen sind die Informationssicherheits*politik*, die in der Unternehmung als verbindlicher Text verteilt werden sollte und die allgemeine Informationssicherheits*strategie*, die zu verfolgen ist. Diese umfasst wiederum die Vorgehensweise, die Architektur und das Rahmenwerk der Informationssicherheit. Auch ist es unabdingbar, die schützenswerten Objekte zu identifizieren; ohne diese Informationen ist Sicherheit nicht erreichbar. Die baulichen, technischen, organisatorischen und personellen Massnahmen bilden die Instrumente der Informationssicherheit. Hier ist es wichtig, einen möglichst umfassenden Massnahmenkatalog schon früh bereitzustellen bzw. auszuwählen. Für die effiziente Durchführung des Informationssicherheitsmanagements empfiehlt sich die Verwendung computergestützter Werkzeuge.

Welche Bedrohungen sind wichtig?

Eine allgemeine Aussage über Prioritäten von Bedrohungen ist nicht möglich; dies muss anhand einer Risikoanalyse unternehmensspezifisch herausgefunden werden. Allerdings können gemäss einer Umfrage [InfoWeekD98.19] mehr als die Hälfte der Sicherheitsvorfälle auf menschliche Fehler zurückgeführt werden, so dass der Beeinflussung sicheren individuellen Verhaltens und der Sicherheitskultur Potential innewohnt. Dies ist auch darauf zurückzuführen, dass in den weitaus meisten Unternehmungen bereits vielfältige technische Sicherheitsmassnahmen umgesetzt wurden. Die Beherrschung der personellen Probleme ist jedoch ungleich schwieriger, da Personen sich (im Gegensatz zu Technologien) indeterministisch verhalten.

Welche Grundbedrohungen sollen berücksichtigt werden?

Langfristig ist anzustreben, alle Grundanforderungen gleichermassen zu erfüllen. Allerdings bestehen heute nur für die Grundanforderungen auf technischer Ebene (Verfügbarkeit, Vertraulichkeit, innere Integrität) anerkannte und nachvollziehbare Verfahrensweisen. Sie umzusetzen und zu beherrschen ist Grundlage für die Erfüllung weiterer Anforderungen.

Für die Anforderungen auf ökonomischer Ebene (Effektivität, Effizienz, Zuverlässigkeit und beabsichtige Verwendung) bestehen nur betriebswirtschaftliche Beeinflussungs- und Kontrollmöglichkeiten. Diese werden selten im Verbund mit Informationssicherheitsanforderungen gesehen. Beispielsweise ist im allgemeinen betriebswirtschaftlichen Umfeld oft nachvollziehbar, wieviel Aufwand für einen bestimmten Dienst erbracht werden musste, so dass sich die Effizienz bestimmen lässt. In Bezug auf Informationsverarbeitung gelingt die Bestimmung der Effizienz jedoch nur selten. Die beabsichtigte Verwendung von Information ist heute praktisch nicht sicherzustellen und es kann – beispielsweise beim Datenschutz – nur durch Androhung von Sanktionen versucht werden, sie zu erreichen.

Für die sozialen Anforderungen (Ordnungsmässigkeit, Verbindlichkeit, externe Integrität) sind ebenfalls noch keine durchgängigen Lösungen vorhanden. Ordnungsmässigkeit prüft zwar die Übereinstimmung der Informationsverarbeitungsprozesse mit den geltenden Normen, dazu ist aber in der Regel viel manuelle Arbeit notwendig. Für die Verbindlichkeit beginnen sich jedoch erste technikbasierte Lösungen durchzusetzen (Anwendung von Verschlüsselungstechnologien etc.).

Gesamthaft sollten also mindestens die technischen Anforderungen erfüllt werden, danach diejenigen, für welche gültige Rechtsnormen bestehen. Schliesslich wird die Wahrung der Verbindlichkeit eine der nächsten Anforderungen sein, deren Erfüllung für die Unternehmungen wichtig sein wird.

Wie kann von IT-Sicherheit zu Informationssicherheit gewechselt werden?

Eine ganzheitliche Betrachtung von Informationssicherheit kann nur gelingen, wenn die *Inhalte* in den Vordergrund der Betrachtung gestellt werden. Dies ist um so schwieriger, als beim aktuell stattfindenden Wechsel von der Industrie- zur Informationsgesellschaft noch immer die tradierten Werte im Vordergrund stehen: Die Beherrschung von Technologien war mehrere Jahrzehnte lang einer der zentralen Erfolgsfaktoren. In Zukunft wird Information im Zentrum stehen und höheren Stellenwert erlangen als die technologischen Ressourcen, welche viele Unternehmungen noch heute als wichtigste Anlage betrachten.

Ein Wechsel bedingt also, dass *Information* als schützenswertes Gut betrachtet wird -- und nicht die Informationstechnik. Informatik und Informationstechnik sind letztlich ein Mittel zum Zweck.

CONVENTIONAL ENGINEERING IS ABOUT MAKING THINGS WORK. [...] SECURITY IS DIFFERENT; IT'S ABOUT MAKING SURE THINGS DON'T NOT WORK. IT'S MAKING SURE SECURITY ISN'T BROKEN, EVEN IN THE PRESENCE OF A MALICIOUS ADVERSARY WHO DOES EVERYTHING IN HIS POWER TO MAKE SURE THAT THINGS DON'T WORK IN THE WORST POSSIBLE WAY AT THE WORST POSSIBLE TIMES. A GOOD ATTACK IS ONE THAT THE ENGINEERS NEVER EVEN THOUGHT ABOUT.

– BRUCE SCHNEIER
PRESIDENT, COUNTERPANE SYSTEMS
IN: CRYPTO-GRAM, JULY 15, 1999

Teil III: Implementation

In Teil II wurde Informationssicherheit definiert, indem ihre einzelnen Elemente hergeleitet und zu einem Rahmenwerk mit einem generischen Prozess verbunden wurden. In Teil III interessiert nun im besonderen, wie anforderungsgerechte Informationssicherheit innerhalb einer Unternehmung hergeleitet und erreicht werden kann. Dazu wird auf den in Kapitel 6 generisch definierten *Prozess* fokussiert und aus ihm ein spezifischer Informationssicherheitsprozess hergeleitet.

7 Vergleichende Evaluation

In diesem Kapitel sollen zuerst die heute gebräuchlichen Verfahren (als Konkretisierungen des Informationssicherheitsprozesses) beschrieben, analysiert und beurteilt werden. Die *Beschreibung* umfasst jeweils die Darlegung von Ursprung, Ziel und Ablauf eines Verfahrens. Die *Analyse* untersucht, welche Komponenten ein Verfahren aufweist, und in welchem Zusammenhang diese stehen. Die *Beurteilung* basiert auf einer Bewertung dieser Verfahrenskomponenten anhand eines hier entwickelten *Schemas*. Durch die Bewertung wird jedem Verfahren ein *Profil* zugewiesen. Am Ende dieses Kapitels wird mit Hilfe derselben Kriterien ein weiteres Profil definiert, welches die Eigenschaften eines neuen, in Kapitel 8 zu entwickelnden Verfahrens umfasst.

7.1 Bewertungsschema

Terminologie

Die Tatsache, dass hier *Verfahren* zur Erreichung von Informationssicherheit mit Hilfe eines Bewertungs*verfahrens* evaluiert werden, kann zu Missverständnissen in der Interpretation dieses Textes führen. Es wird deshalb konsequent von *ISi-Verfahren* oder *ISi-Prozess* gesprochen, wenn die bewerteten Verfahren gemeint sind, und von *Bewertungsverfahren*, wenn das Verfahren gemeint ist, mit welchem die Bewertung der ISi-Verfahren durchgeführt wird.

Dasselbe gilt für die Begriffe *Anforderungen* und *Kriterien.* In den anderen Kapiteln dieser Dissertation werden darunter die Anforderungen verstanden, welche an die Sicherheit der unternehmerischen Information und Informationsverarbeitung gestellt werden. Dies wird in diesem Kapitel konsequent als *ISi-Anforderung* oder *ISi-Kriterium* bezeichnet. Die Anforderungen, welche an die ISi-Verfahren gestellt werden, um Ansprüchen derjenigen Personen zu genügen, welche diese ISi-Verfahren verwenden, werden hier *Bewertungskriterien* oder *Bewertungs-anforderungen* genannt und sogenannten *Variablen* zugeteilt.

Unter *Bewertung* wird in den anderen Kapiteln dieser Dissertation die Zuteilung eines Wertes zu einer ISi-Anforderung (in einem ISi-Kriterium) verstanden, welche v.a. beim In-Out-Ansatz (vgl. Abschnitt 6.4) angewendet wird und eine Aussage über die gewünschte Höhe der Sicherheit einer Information beschreibt. Dies wird in Kapitel 7 als *ISi-Bewertung* bezeichnet. Die Zuteilung eines Wertes zu einer *Variablen*, welche eine Aussage über die Erfüllung einer Bewertungsanforderung durch das bewertete ISi-Verfahren beschreibt, wird in Kapitel 7 als *Verfahrensbewertung* bezeichnet.

Dokumentationsbasis

Bei den hier bewerteten Bezugsobjekten handelt es sich um *Verfahren der Informationssicherheit* (*ISi-Verfahren*). Bewertungsgrundlage bildet dabei die gedruckte Dokumentation des jeweiligen ISi-Verfahrens, welche einer Textanalyse unterzogen wird. Diese Dokumentationen unterscheiden sich aufgrund ihrer verschiedenen Herkunft und Zielsetzung stark, sowohl bezüglich inhaltlicher Breite und Tiefe als auch durch die gewählte Sprache und den Umfang des Textes.

Zusätzliche Literatur, wie z.B. Umsetzungshinweise und Richtlinien, welche für verschiedene ISi-Verfahren existieren, aber nicht Teil der eigentlichen Dokumentation sind und teilweise von anderen Autoren stammen, wurde nicht berücksichtigt. Selbst wenn diese hinzugezogen würde, bliebe der Unterschied in der Ausrichtung der ISi-Verfahren bestehen. Eine Erweiterung der betrachteten Dokumentationsbasis würde also keinen weiteren Erkenntnisgewinn zulassen.

Da hier eine *unabhängige* Bewertung vorgenommen werden soll, sind auch Kritiken anderer Autoren, welche die hier evaluierten ISi-Verfahren untersucht haben, nicht Gegenstand der hier berücksichtigten Dokumentationsbasis, denn diese Kritiken sind für die betrachteten ISi-Verfahren in unterschiedlicher Zahl vorhanden und definieren jeweils eigene Variablen, die mit den hier zu definierenden Variablen nur teilweise übereinstimmen. Eine derartige Berücksichtigung wäre also problematisch.

Die Beurteilung und Evaluation von Hilfsmitteln (z.B. Formulare, computergestützte Werkzeuge etc.) kann ebenfalls nur ansatzweise erfolgen, da auch diese Hilfsmittel sich zwischen den ISi-Verfahren sehr unterscheidet.

Die Verfahrensbewertung basiert also ausschliesslich auf der direkt zum jeweiligen ISi-Verfahren gehörenden papiergebundenen Dokumentation und den direkt dazugehörenden Anlagen.

Bewertungsverfahren

Die Verfahrensbewertung der einzelnen ISi-Verfahren geschieht, indem *Fragen*[75] formuliert werden, und versucht wird, diese Fragen durch Studium der Dokumentation zu beantworten. Dabei wird zwischen drei Fragetypen unterschieden: *Quantitativen*, *qualitativen* und *spekulativen* Fragen. Quantitative Fragen beziehen sich auf Angaben, welche als Mengen- und Grössenwerte aus den beurteilten Dokumenten hervorgehen oder hergeleitet werden können. Qualitative Fragen werden durch strenge und möglichst objektive Interpretationen des Textes beantwortet. Spekulative Fragen verlangen eine Einschätzung, wie ein ISi-Verfahren sich in einer bestimmten Situation oder unter konkreten Rahmenbedingungen verhielte und unterliegen damit der persönlichen Interpretation des Bewertenden. Sie stellen also nicht nur eine Bewertung, sondern eine *Beurteilung* dar.

Struktur des Bewertungsschemas

Die Variablen werden in vier Bewertungsbereiche aufgeteilt: Zum Ersten wird bewertet, wie die *Auslösung* des Verfahrens geschieht. Der zweite Bereich umfasst die *Organisation*. In einem dritten Bereich wird untersucht, wie das ISi-Verfahren *durchgeführt* wird und ein vierter Bereich untersucht die Einflüsse der einzelnen *Fachbereiche* des ISi-Verfahrens auf das untersuchte Informationssystem. Die vier Variablen werden dementsprechend (gemäss der sequentiellen Abfolge) mit *V1: Auslösung*, *V2: Organisation*, *V3: Durchführung* und *V4: Fachbereiche* bezeichnet. [76]

---

75 Die Begriffe „Frage“ und „Fragestellung“ werden hier synonym verwendet.

76 In Abschnitt 3.1, Absatz "Dynamische Betrachtung" werden drei Problembereiche unterschieden: die *Organisation*, die *inhaltlichen Themenbereiche* und der *Ablauf*. Beim Ablauf

Die Variablen für die vier Bewertungsbereiche erhalten ihre Werte durch die Beantwortung von *Fragen an die Dokumentation*. Dabei interessiert die konkrete inhaltliche Antwort aber nur sekundär. Primär ist es relevant, *ob* die Frage durch das Studium der Dokumentation beantwortet werden kann. Die Höhe der Bewertung (und damit der Wert, welcher der entsprechenden Variable zugeteilt wird) hängt also davon ab, *ob und in welchem Masse* die Dokumentation auf die durch die Fragestellung abgedeckte Thematik eingeht, und nicht *wie* die Antwort lautet!

Bei der Beantwortung dieser Fragestellungen entstehen für jedes ISi-Verfahren unterschiedliche Werte. Die verschiedenen Werte eines ISi-Verfahrens werden gesamthaft als *Profil* dieses ISi-Verfahrens bezeichnet.

Herleitung der Struktur des Schemas

In Kapitel 6 wurden die Phasen eines generischen ISi-Verfahrens identifiziert und mit *Inventur*, *Analyse*, *Massnahmen* sowie *Umsetzung und Kontrolle* bezeichnet. Jedes der in diesem Kapitel zu betrachtenden bestehenden ISi-Verfahren baut diesen Prozess anders auf. Hier soll einheitlich untersucht werden, welche Eigenschaften dieser Aufbau jeweils hat. Deshalb wird hier ein Bewertungsbereich *Durchführung* definiert, welcher die konkrete Anwendung dieser vier Phasen auf ein Untersuchungsobjekt umfasst.

Auch das Objekt, auf welches sich die ISi-Untersuchung bezieht (also z.B. das IT-System, das Informationssystem oder die ganze Unternehmung), wird von jedem ISi-Verfahren anders betrachtet. Dabei variieren sowohl die Tiefe der Betrachtung (die vom ISi-Verfahren berücksichtigten inhaltlichen Fragestellungen) als auch die Breite (die Wahl der Elemente des Untersuchungsobjektes, die betrachtet werden). Das Untersuchungsobjekt stellt also einen weiteren Bewertungsbereich des Schemas dar. Es wird anhand der *Fachbereiche* betrachtet, welche die betrachteten Teile beeinflussen.

Ebenfalls in Kapitel 6 wurde eine weitere Phase 0 *Vorbereitungen* identifiziert. Es wurde kurz umschrieben, dass in dieser Phase die Auslösung des Prozesses betrachtet wird und die organisatorischen Strukturen, welche er umfasst, genauer definiert werden. Beides soll hier jeweils als Bewertungsbereich des Schemas verstanden werden. Die *Auslösung* umfasst alle Tätigkeiten und Informationsflüsse, welche die erstmalige und die weiteren Initialisierungen eines ISi-Prozesses umfassen. Die *Organisation* umfasst all diejenigen Angaben des ISi-Verfahrens, welche die organisatorische An- und Einordnung[77] der Institutionen festlegt, welche

---

wird im besonderen noch die *Auslösung* betrachtet. Die hier gewählte Betrachtung entspricht dieser Dreiteilung und stellt die *Auslösung* als vierten Teil dazu.

77 Mit *Anordnung* ist die Ordnung der Institutionen untereinander gemeint, mit *Einordnung* die Unterordnung der Institutionen der Informationssicherheit unter andere unternehmerische Institutionen.

für die Durchführung des Prozesses von einem konkreten ISi-Verfahren definiert werden.

Das hier verwendete Schema besteht also aus 4 Bewertungsbereichen (vgl. Abbildung 7-1):

1 *Auslösung* umfasst die Feststellung, dass ein Bedarf zur Untersuchung oder Verbesserung der Informationssicherheit besteht, sowie die Initiierung einer solchen Untersuchung,

2 *Organisation* beschreibt Bildung, Aufbau und Beauftragung eines Projektteams zur Erarbeitung einer Lösung zur Befriedigung des zuvor festgestellten Bedarfs,

3 *Durchführung* umfasst alle Fragestellungen des konkreten Ablaufs der Untersuchung, also beispielsweise die Abfolge der Phasen und Schritte und den Dokumentenfluss. Die Durchführung kann weiter in eine *Analyse-*, eine *Beeinflussungs-* und eine *Kontrollphase* unterteilt werden.

4 *Fachbereiche* bezeichnet die inhaltlichen Fragestellungen und konkreten Elemente des Bezugsobjektes, auf welches die Durchführung sich bezieht. Es wird dabei zwischen *Prozessen*, *Institutionen* und *Instrumenten* des Untersuchungsobjekts unterschieden.

Dabei stehen die ersten drei Bewertungsbereiche in einer direkten zeitlichen Abfolge.

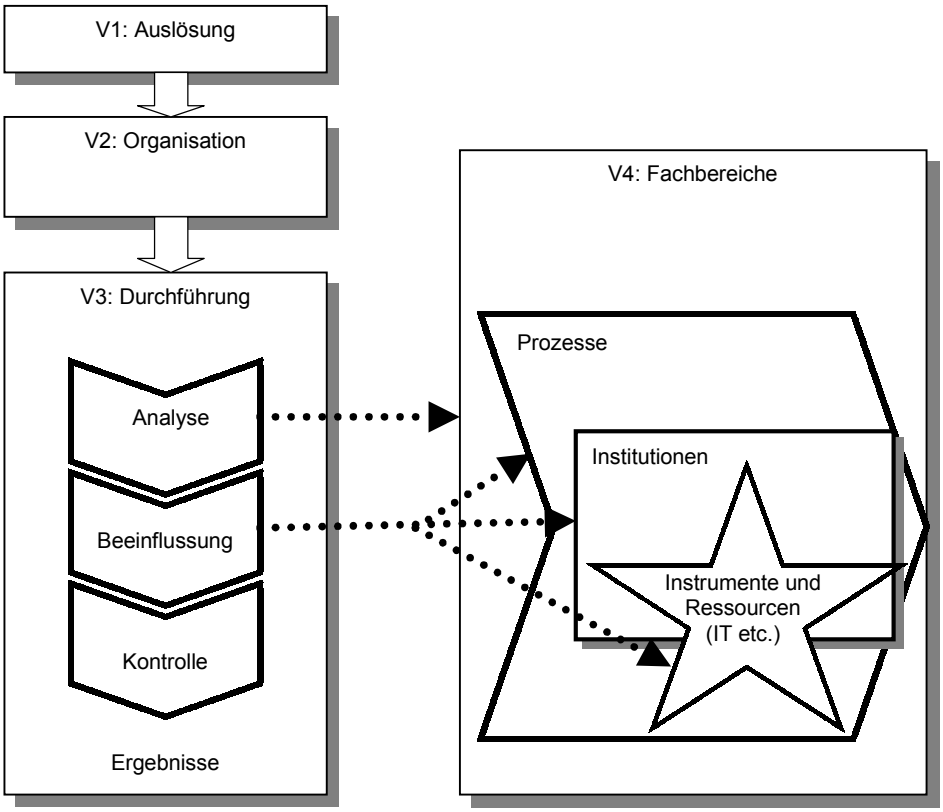


Abbildung 7-1: Schema für Informationssicherheitsverfahren mit den vier Bewertungsbereichen

Variablen der Auslösung

Der Variablen 1 wird das Resultat der Bewertung der *Auslösung* zugeteilt. Diese Variable umfasst folgende Teilvariablen:

V1a: Initianten, Ereignisse und Methoden der *Bedarfsfeststellung* der Informationssicherheit,

V1b: Bezug des ISi-Verfahrens zum *Projektmanagement* anderer Projekte,

V1c: Berücksichtigung von unternehmerischen Veränderungen als Auslöser des Informationssicherheitsmanagements (*Change Management*).

Variablen der Organisation

Das Resultat der Bewertung der *Organisation* wird in Variable 2 festgehalten. Sie umfasst folgende Teilvariablen:

V2a: Struktur, Dauer des Bestehens und Teilnehmer des *Projektteams*, organisatorische Einordnung des ISi-Managements,

V2b: Eignung des ISi-Verfahrens für das *Projektmanagement*, Zielfestlegung, Abgrenzung des Betrachtungsobjekts und der Inhalte,

V2c: *Dauer* des Informationssicherheitsprozesses,

V2d: *Kooperation und Koordination* der Teilprozesse des ISi-Managements.

Variablen der Durchführung

Die *Durchführung* wird in Variable 3 bewertet und umfasst folgende Teilvariablen:

V3a: *Beschreibung des allgemeinen Ablaufs* des Informationssicherheitsprozesses

V3b: Berücksichtigung der verschiedenen *Ansätze* gemäss Kapitel 6

V3c: Beschreibung der einzelnen *Phasen* des Informationssicherheitsprozesses

V3d: Möglichkeiten der *Skalierung* des Informationssicherheitsprozesses

V3e: Beschreibung der Typen und der Darstellung der *Ergebnisse*

V3f: *Aufwand* für die Durchführung

V3g: Beschreibung von *Nutzen- und Ertrag*sbetrachtungen

V3h: Verwendung oder Wiedergabe von *Massnahmenkatalogen*

V3i: Wiedergabe von *Fragenkatalogen* und *Checklisten*

V3j: *Computergestützte Hilfsmittel*

Variablen der Fachbereiche

Das Resultat der Bewertung der *Fachbereiche*, von denen die Beeinflussung des Untersuchungsobjekts ausgeht, wird Variable 4 zugewiesen. Sie umfasst folgende Teilvariablen:

V4a: *Analyse* des Untersuchungsobjektes

V4b: *Beeinflussung* des Untersuchungsobjektes

V4c: *Inhalte* der Bewertung der Fachbereiche

Der Wert jeder Variablen wird durch eine oder mehrere Fragestellungen bestimmt. Diese Fragen sind im Einzelnen in Tabelle B-0 in Anhang B (ab Seite 281) aufgeführt.

Kooperation und Koordination

Kooperation und Koordination bilden zusammen mit der Kommunikation die drei Grundelemente der Gruppenarbeit (vgl. [Teufel95, S. 11f]) *"Koordination bezeichnet jene Kommunikation, welche zur Abstimmung aufgabenbezogener Tätigkeiten, die im Rahmen von Gruppenarbeit ausgeführt werden, notwendig ist." "Kooperation bezeichnet jede Kommunikation, die zur Koordination und zur Vereinbarung gemeinsamer Ziele notwendig ist."*

Die Untersuchung von Informationssicherheit und Informationssicherheits-management im allgemeinen lassen sich als gruppenbezogene Tätigkeit auffassen. Im hier interessierenden Zusammenhang von ISi-Verfahren werden beide Begriffe wie folgt verwendet:

Koordination verschiedener ISi-Untersuchungen bedeutet, dass eine Kommunikation zwischen verschiedenen Untersuchungen stattfinden kann, weil dieselbe Vorgehensweise gewählt wurde, die Ergebnisse standardisiert dargestellt wurden und Schnittstellen der Ergebnisübergabe definiert wurden.

Kooperation von ISi-Untersuchungen bedeutet, dass diese zeitgleich ablaufen, und dass eine gemeinsame Institution besteht, welche die Kooperation koordiniert, indem sie den Ergebnisaustausch fördert.

Wertmassstab und Werte des Schemas

Ziel der Bewertung der verschiedenen ISi-Verfahren ist es, festzustellen, *ob* die verschiedenen Fragestellungen vom ISi-Verfahren behandelt werden. Die Fragen, welche an die Dokumentation gestellt und durch Studium der Dokumentation beantwortet werden, geben also Aufschluss darüber, ob das ISi-Verfahren den durch die Frage abgedeckten Inhalt behandelt oder nicht. Es geht also weniger um die *Beantwortung* der Fragen als um die Feststellung, *ob* die Frage aus dem Studium der Dokumentation heraus beantwortet werden kann.

Ein Teil der Fragen des Fragenkatalogs ist so formuliert, dass sie sich mit *Ja* oder *Nein* beantworten lassen. Eine so eindeutige Aussage ist jedoch in vielen Fällen nicht möglich oder nicht angemessen. Deshalb werden hier für jede der formulierten Fragen fünf mögliche Antworten definiert, welche mit ganzzahligen Werten im Bereich 0 bis 4 gekennzeichnet werden (diskrete Skala). Die Bedeutung der fünf Werte für die verschiedenen Fragetypen ist wie folgt:

Quantitative Fragestellungen (N)

Quantitative Fragestellungen beziehen sich auf Mengen oder Anteile, welche im ISi-Verfahren festgelegt werden oder sich daraus herleiten lassen. Es wird nach *wieviel* oder *wieviel von* gefragt. Die Werte haben die in Tabelle 7-1 angegebene Bedeutung.

Wert	Bedeutung
0	Nein, keine (0%)
1	Ja, aber nur eine Minderheit (>0-33%)
2	Ja, etwa zur Hälfte (>33-67%)
3	Ja, viele und die Mehrheit aller (>67-<100%)
4	Ja, alle (100%)

Tabelle 7-1: Bedeutungen der Werte bei quantitativen Fragestellungen

Qualitative Fragestellungen (L)

Qualitative Fragestellungen beziehen sich auf dokumentierte Eigenschaften des ISi-Verfahrens, welche objektiv aus der Beschreibung hergeleitet werden können. Sie fragen nach der *Existenz einer Beschreibung einer Eigenschaft des ISi-Verfahrens.* Die Werte haben die in Tabelle 7-2 angegebene Bedeutung.

Wert	Bedeutung
0	Die Antwort wird in der Dokumentation nicht beschrieben und die Eigenschaft ist im ISi-Verfahren nicht enthalten und nicht vorgesehen und kann auch nicht aus den bestehenden Angaben interpretiert werden.
1	Die Antwort wird in der Dokumentation nicht explizit beschrieben und die Eigenschaft ist nicht explizit vorgesehen, es kann aber aus den bestehenden Angaben interpretiert werden, dass entsprechende Überlegungen bei der Erstellung des ISi-Verfahrens vorgenommen wurden.
2	Die Antwort ist in der Dokumentation teilweise oder ansatzweise enthalten, die entsprechende Eigenschaft des ISi-Verfahrens ist grundlegend beschrieben und die fehlenden Angaben können interpretatorisch und durch essentiellen Beizug anderer Quellen ergänzt werden.
3	Die Antwort ist grösstenteils in der Dokumentation enthalten und die entsprechende Eigenschaft des ISi-Verfahrens ist vorgesehen, muss aber noch teilweise interpretiert oder mit anderen Quellen vertieft werden.
4	Die Antwort ist in der Dokumentation enthalten und die Eigenschaft ist im ISi-Verfahren vorgesehen und wird vollständig und detailliert beschrieben.

Tabelle 7-2: Bedeutungen der Werte bei qualitativen Fragestellungen

Spekulative Fragestellungen (S)

Spekulative Fragestellungen beziehen sich auf die Beurteilung eines ISi-Verfahrens bei der Anwendung. Dazu werden Rahmenbedingungen vorgegeben oder angenommen oder die Veränderung einzelner Eigenschaften des ISi-Verfahrens diskutiert. Die Werte haben die in Tabelle 7-3 angegebenen Bedeutungen.

Wert	Bedeutung
0	Nein, die Spekulation trifft nicht zu
1	Die Spekulation trifft wahrscheinlich nicht oder nur in geringem Ausmass zu.
2	Die Spekulation trifft möglicherweise zu.
3	Die Spekulation trifft wahrscheinlich zu.
4	Ja, die Spekulation trifft zu.

Tabelle 7-3: Bedeutungen der Werte bei spekulativen Fragestellungen

Die Summe der einzelnen vergebenen Werte pro Teilvariable entspricht dem Wert der Variablen.

7.2 Bewertete Informationssicherheitsverfahren

In dieser Dissertation werden die folgenden ISi-Verfahren bewertet:

1) [78] IT-Sicherheitshandbuch des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI-D) [BSI-IT-SHB92, BSI-IT-SHB94]

2) Grundschutz-Verfahren des schweizerischen Bundesamts für Informatik (BFI) [BFIWS02.95.4, BFIWS02HB1.96.6]

3) IT-Grundschutzhandbuch des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI-D) [BSI-IT-GSHB97]

4) Code of Practice (BS 7799) der British Standards Institution (BSI-GB) [BSI-COP95]

5) Control Objectives for Information and Related Technology (COBIT) der Information Systems Audit and Control Foundation (ISACF) [COBIT96.1-5]

6) Guidelines for the Management of IT Security (GMITS) der International Organization for Standardisation (ISO) (ISO/IEC TR 13335) [ISO13335-1-4]

---

[78] Diese Nummerierung entspricht der nachfolgenden Abschnittsnummerierung (z.B. „7.2.***1***“) sowie der Nummerierung der entsprechenden Tabellen (z.B. „B-***1***“) in den Anhängen (z.B. „B.***1***“).

7.2.1 IT-Sicherheitshandbuch (BSI-D)

Dokument

Das IT-Sicherheitshandbuch des *deutschen Bundesamts für Sicherheit in der Informationstechnik* BSI (D) war 1992 eines der ersten ISi-Verfahren, welches für den deutschsprachigen Raum zur Verfügung stand und Verbreitung fand. Es umfasst auf mehr als 300 Seiten primär ein Verfahren zur Risikoanalyse und zum Risikomanagement und richtet sich an Behörden der deutschen staatlichen Verwaltung. Eine Nutzung ausserhalb dieses Kreises wird jedoch nicht ausgeschlossen. Es baut teilweise auf den „IT-Sicherheitskriterien“ [BSI-IT-SK89] auf, welche bei der Spezifikation von Anforderungen an sichere informationstechnische Systeme und der Auswahl solcher Systeme unterstützen, ist jedoch auch unabhängig davon verwendbar. Es wird hier in der Version 1.1C vom Juli 1994 betrachtet.[79]

Inhalt

Das IT-Sicherheitshandbuch enthält (nach einer einführenden Motivation) v.a. ein *Verfahren zur Gewährleistung der IT-Sicherheit*, welches in vier Stufen mit total zwölf Schritten aufgeteilt ist. Es ist in Abbildung 7-2 dargestellt.

[79] Version 1.1c [BSI-IT-SHB94] lag nur in einer digitalen Form vor. Sie unterscheidet sich von der Version 1.0 [BSI-IT-SHB92] nur geringfügig, weist jedoch aufgrund des Datenformates keine eindeutige Seitennummerierung auf. Alle Seitenreferenzen beziehen sich deshalb auf die Version 1.0.

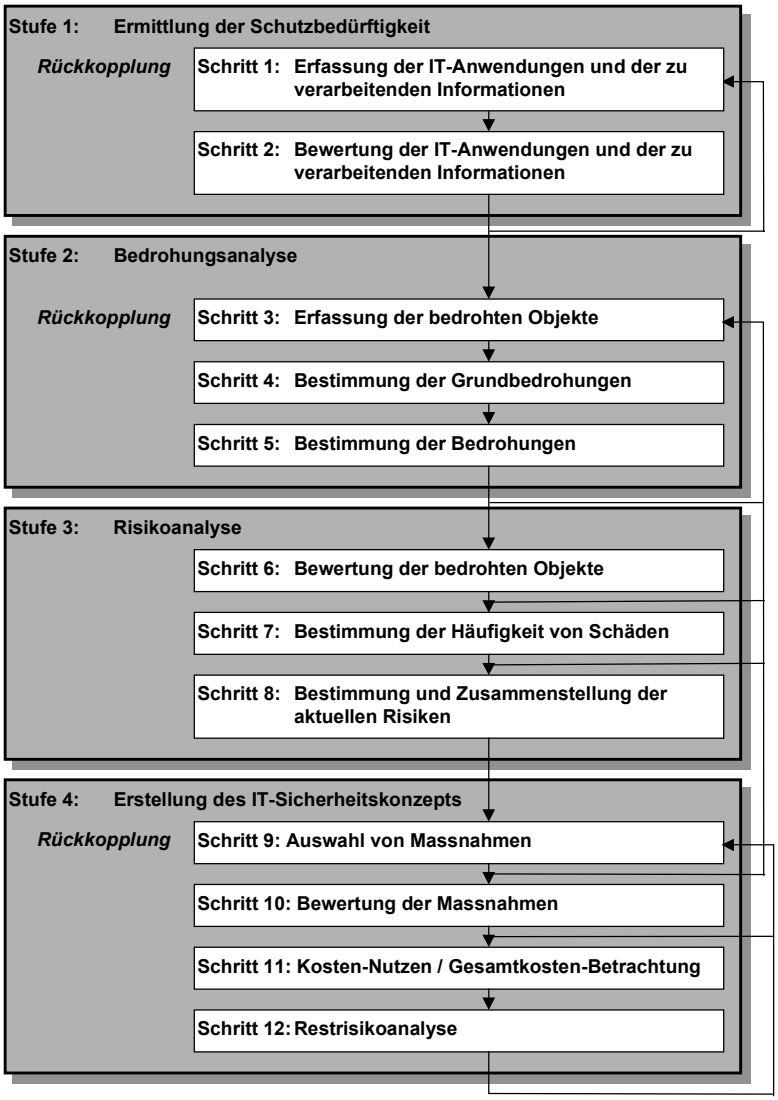


Abbildung 7-2: Verfahren zur Gewährleistung der IT-Sicherheit [BSI-IT-SHB92, S. 35]

Ferner wird auch der Fluss der Informationen zwischen den einzelnen Schritten des Verfahrens geregelt, was in Abbildung 7-3 dargestellt wird.

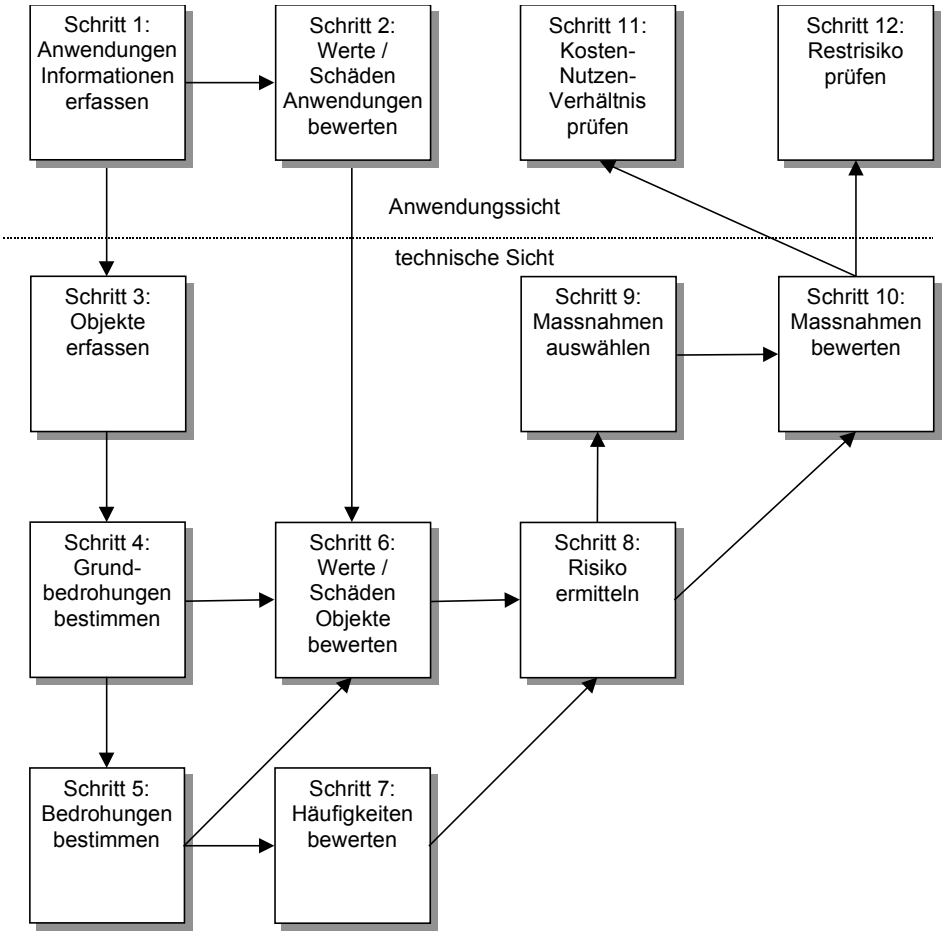


Abbildung 7-3: Abhängigkeiten zwischen den 12 Schritten [BSI-IT-SHB92, S. 37]

Bewertung

Die Tabelle mit der detaillierten Bewertung dieses ISi-Verfahrens findet sich in Anhang B.1, Tabelle B-1. Die Gegenüberstellung der Profile ist in den Tabellen B-9 bis B-12 wiedergegeben. Hier werden die wichtigsten Aussagen kurz zusammengefasst.

Die Stärken des ISi-Verfahrens des IT-Sicherheitshandbuchs liegen in der Beschreibung der Durchführung. Der Prozess wird abstrakt und übersichtlich dargestellt. Zusätzlich ist auch eine konkrete und detaillierte Beschreibung des Prozesses enthalten. Er umfasst einen Risikoanalyseansatz und greift Elemente des Grundschutzes auf. Massnahmenkataloge und weitere Hilfsmittel ergänzen die Dokumentation. Die Kontrolle dieses ISi-Verfahrens ist nur wenig ausgeprägt. Es entsteht hoher Aufwand bei der Durchführung. Abgrenzung sowie Bestimmung von Untersuchungsbreite und -tiefe werden nur ansatzweise behandelt. Ein computerbasiertes Hilfsmittel fehlt, würde die Durchführung dieses ISi-Verfahrens jedoch stark unterstützen.

Die Auslösung ist nur grundlegend beschrieben, und auch die Projektorganisation ist nicht sehr ausführlich. Es fällt jedoch auf, dass sich dieses ISi-Verfahren gut als

Basis für das Projektmanagement eignet und das Ziel klar vorgegeben ist. Auch bildet es eine gute Grundlage für die Koordination verschiedener Untersuchungen.

Beurteilung

Beim IT-Sicherheitshandbuch handelt es sich um eine ausführliche und detaillierte Dokumentation eines Risikoanalyseverfahrens, welches durch seine einheitliche Struktur überzeugt. Die Fokussierung auf Informationstechnik anstatt auf Inhalte und der enorme Aufwand, welcher bei seiner Anwendung entsteht und nicht durch die Mitlieferung eines computerbasierten Werkzeugs aufgefangen wird, sind seine grössten Schwächen. Bei den Massnahmen überwiegen technische, in einzelnen Bereichen organisatorische Komponenten, die jedoch wenig detailliert ausgeführt werden. Die in der Praxis geforderte Erzeugung vergleichbarer quantitativer Ergebnisse wird in einigen Bereichen erfüllt.

7.2.2 Grundschutz-Verfahren (BFI)

Dokument

Das Grundschutzverfahren des schweizerischen Bundesamtes für Informatik ist für den Einsatz in der schweizerischen Bundesverwaltung vorgesehen. Es umfasst die Umsetzung eines „adaptiven" Grundschutzes, indem es die Umsetzung von Massnahmen aus einem vorgegebenen Katalog in Abhängigkeit von der Beurteilung der betroffenen Objekte vorsieht[80]. Es ist in einer Weisung (einer operationalisierbaren Umsetzung der strategischen Vorgabe der Informationssicherheitsziele) 1995 erstmals publiziert worden. Der Massnahmenkatalog wurde mehrmals überarbeitet und wird hier in der 1996 publizierten Version betrachtet.

Inhalt

Das im BFI-Verfahren verwendete Vorgehen ist in Abbildung 7-4 dargestellt. Es umfasst nach vorbereitenden Massnahmen eine Erhebung von Schutzobjekten und einen vierstufigen Zyklus. Dieser beinhaltet die Einstufung von Schutzobjekten in sieben, von der jeweiligen Kategorie des Objekts abhängigen Anforderungskriterien. Es werden drei Objektkategorien gebildet: Hardware, Anwendungen und Daten. Bei der Hardware wird der Wert des Systems in drei Stufen (1 bis 3) bewertet. Bei den Anwendungen werden die Anforderungen an Finanzrelevanz (wenn mit dem System Finanzdaten verarbeitet werden) und maximal zulässige Ausfalldauer in

---

80 Obwohl "Grundschutz von Informatiksystemen und -anwendungen" genannt, entspricht dieses Verfahren eher dem in Abschnitt 6.4 (2.b) beschriebenen *Werteansatz* (In-Out-Ansatz) als dem *Grundschutzansatz*.

zwei bzw. drei Stufen bewertet. Für Daten werden in den Kriterien Datenschutz, Wiederbeschaffungswert, Klassifizierung und Archivierungspflicht die Werte 1 bis 3 vergeben. Welche Massnahmen für ein Objekt zur Anwendung kommen, wird durch die höchsten Anforderungen bestimmt, welche an eines der beteiligten Teilobjekte gestellt werden. Die Massnahmen werden schliesslich umgesetzt; ihre Einhaltung wird kontrolliert und darüber Bericht erstattet. Dies kann zur Anpassung der Einstufung und der Massnahmen führen.

Darüber hinaus werden auch weitergehende Massnahmen angeregt, deren Betrachtung und Umsetzung allerdings nicht Teil dieses ISi-Verfahrens, sondern Betrachtungsgegenstand einer weiterführenden, durch das BFI jeweils individuell vorgenommenen Untersuchung sind.

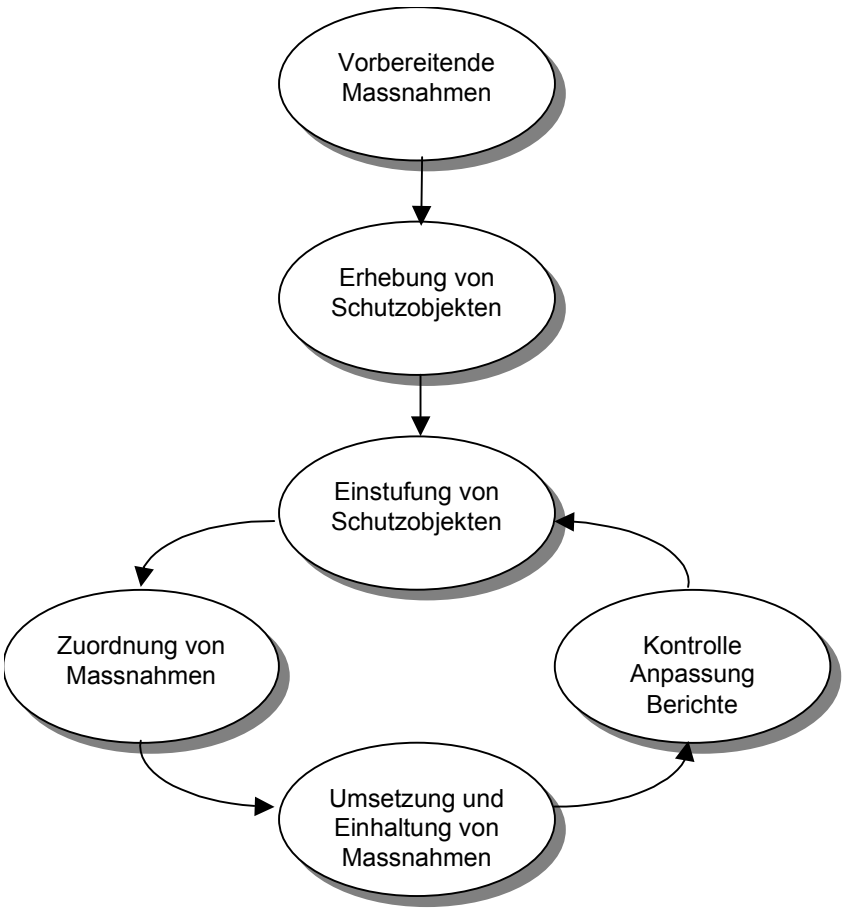


Abbildung 7-4: BFI-Verfahren

Bewertung

Die Bewertung des Grundschutzverfahrens des BFI zeigt deutliche Stärken in der Organisation: Weisungsbefugnis, hierarchische Einordnung sowie zu beteiligende Personen und Institutionen werden klar beschrieben. Koordination und Kooperation werden durch standardisierte Formularschnittstellen unterstützt. Auch die Auslösung des Projektes wird aufgrund der gesetzlichen und auf einer Verordnung

basierenden Grundlagen genügend beschrieben. Die Durchführung hingegen ist nur teilweise beschrieben und wird vom umfangreichen Massnahmenkatalog dominiert, den es in Abhängigkeit der Bewertungen der Objekte umzusetzen gilt. Risikoanalyse wird nicht betrachtet, jedoch sind Grundschutz- und Werteansatz berücksichtigt. Dieses ISi-Verfahren ist nicht skalierbar, dafür jedoch leicht erlernbar. Die Verwaltung der Objekte erzeugt hohen Aufwand und würde von der Verfügbarkeit eines Werkzeugs profitieren. Beim Untersuchungsobjekt wird technikzentriert vorgegangen, wenngleich vier Kriterien für die Bewertung von Datensammlungen definiert werden, allerdings in unklarem Zusammenhang zu den Grundanforderungen Verfügbarkeit, Integrität und Vertraulichkeit. Die Tabelle mit der detaillierten Bewertung dieses ISi-Verfahrens findet sich in Anhang B.2, Tabelle B-2. Die Gegenüberstellung der Profile geschieht in den Tabellen B-9 bis B-12.

Beurteilung

Das ISi-Verfahren des Bundesamtes für Informatik ist anwendungsbezogen, denn es erlaubt mit relativ geringem Aufwand die Feststellung der notwendigen Massnahmen zur Gewährleistung von IT-Sicherheit. Es zeigt jedoch Schwächen im konzeptionellen Bereich, da es grössere Zusammenhänge ganz und personelle Aspekte teilweise ausklammert, sich auf die Betrachtung des IT-Systems beschränkt, die Beurteilungskriterien unüblich sind und ihre Herleitung nicht eindeutig nachvollziehbar ist. Gesamthaft erzeugt es jedoch quantitative und teilweise vergleichbare Daten, die eine Grundlage für Zertifizierungen darstellen könnten und die Koordination und Kooperation erlauben.

7.2.3 IT-Grundschutzhandbuch (BSI-D)

Dokument

Das Grundschutzhandbuch des BSI ist erstmals 1995 erschienen und hat zum Ziel, konkrete und verbindliche Hinweise und ein ISi-Verfahren für den Grundschutz von informationstechnologischen Systemen mit mittlerem Schutzbedarf zur Verfügung zu stellen. Die hier betrachtete dritte Auflage von 1997 umfasst auf mehr als 600 Seiten mehr als tausend Einzelmassnahmen in zwölf Bereichen. Es soll weiterhin jährlich erscheinen und durch Berücksichtigung jeweils aktueller Technologie konkrete Hinweise zur Sicherung der informationstechnischen Systeme bieten. Es richtete sich ursprünglich an Behörden, wurde 1996 jedoch „sowohl auf Bundes-, Landes- und Kommunalebene als auch im Bereich der Wirtschaft breit angenommen.“ [BSI-IT-GSHB97, Kapitel "Neues in Version 1997" - S. 1].

Inhalt

Der IT-Sicherheitsprozess des IT-Grundschutzhandbuches ist in Abbildung 7-5 dargestellt. Dieser Ablauf geht von einer Initiative des Managements aus, welches in einem ersten Schritt das gewünschte Sicherheitsniveau festlegen muss und die grundsätzliche Verantwortung für die IT-Sicherheit übernimmt. Das Sicherheitskonzept wird mit Hilfe von Risikoanalysen und Grundschutzhandbuch erstellt und durch Setzen von Prioritäten und konkrete Zuteilung zu Personen technisch realisiert.[81] Die nachhaltige Beeinflussung von Personen wird ebenfalls intensiv betrachtet und schliesslich sorgen laufende Kontrollen der Umsetzung und erneutes Durchlaufen des Prozesses für bleibende Sicherheit.

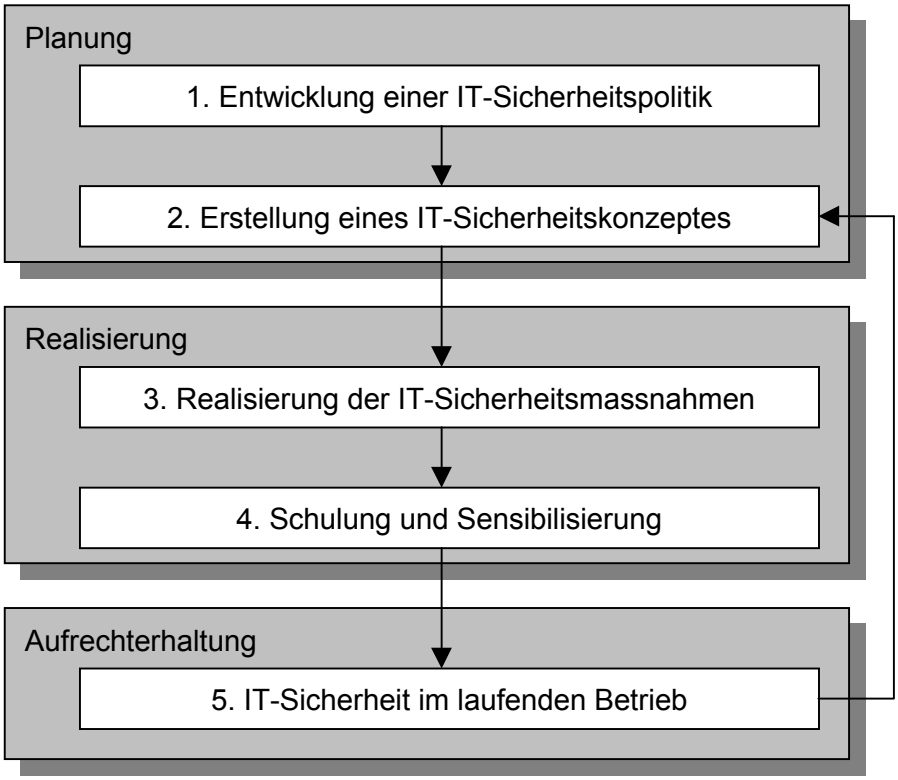


Abbildung 7-5: Aktionsplan für den IT-Sicherheitsprozess [82]

Des weiteren schlägt das IT-Grundschutzhandbuch Organisationsformen für die nachhaltige Gewährleistung der IT-Sicherheit vor. Diese können in einer grossen Unternehmung z.B. gemäss Abbildung 7-6 aufgebaut werden.

---

81 Dabei entsteht für die IT-Sicherheit in der Privatwirtschaft ein Aufwand in der Grössenordnung von 5% der IT-Investitionssumme.[BSI-IT-GSHB97], Teil 1, Kapitel 1, Seite 7

82 [BSI-IT-GSHB97], Teil 1, Kapitel 1, Seite 2

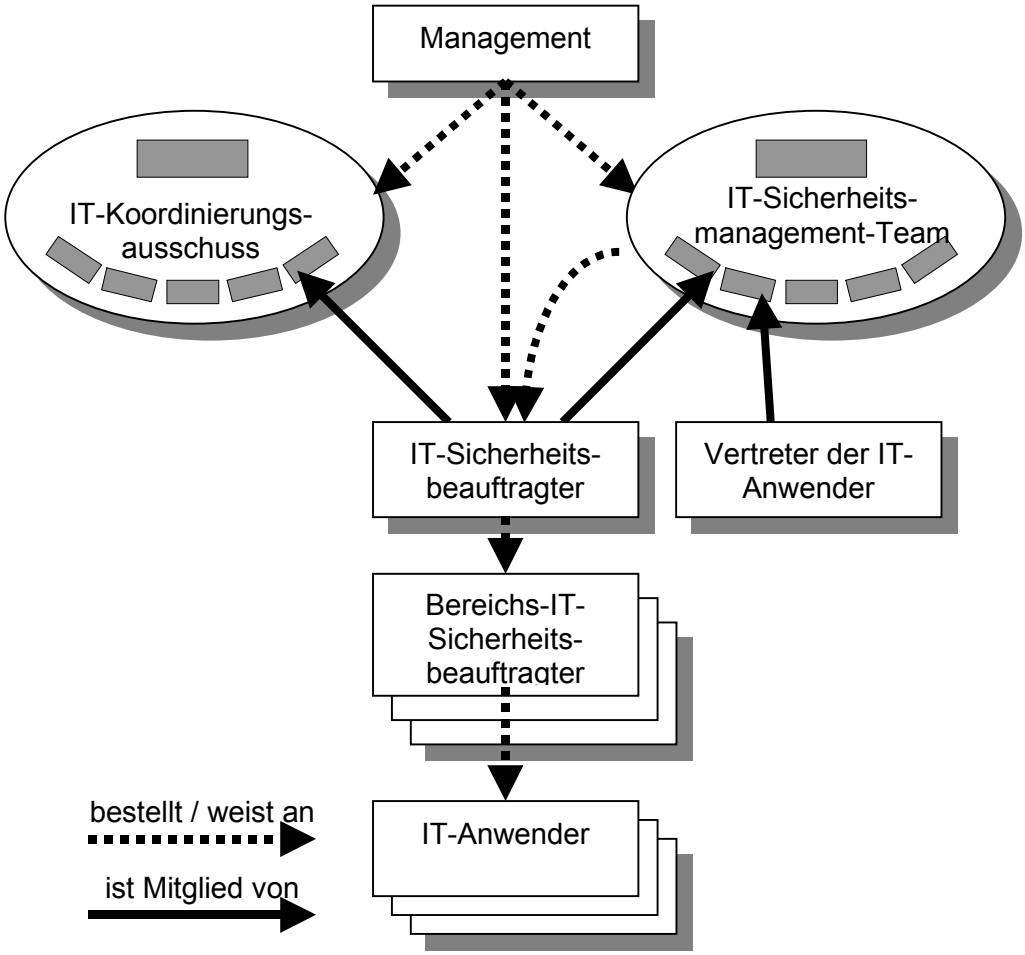


Abbildung 7-6: Beispiel zur Organisation des IT-Sicherheitsmanagements [83]

Im Anschluss an allgemeine Hinweise in Kapitel 1 und 2 des Grundschutzhandbuches werden in sieben weiteren Kapiteln gesamthaft 29 weitere generische „Bausteine" von IT-Sytemen identifiziert und ihnen jeweils einzelne Gefährdungen und Massnahmen aus dem hinteren Teil des Buches zugewiesen. Dort sind in fünf Kapiteln Gefährdungskataloge für die Bereiche Höhere Gewalt, Organisatorische Mängel, Menschliche Fehlhandlungen, Technisches Versagen und Vorsätzliche Handlungen aufgeführt. Sechs weitere Kaptitel enthalten Massnahmen für die Bereiche Infrastruktur, Organisation, Personal, Hardware und Software, Kommunikation und Notfallvorsorge. Abschliessend werden Zuordnungen zwischen Gefährdungen und Massnahmen in Tabellenform dargestellt. Anhänge mit Referenzmaterialien, Bezugsquellen sowie eine CD mit dem kompletten Inhalt des Buches im HTML-Format und im Format für *MICROSOFT WORD* schliessen das IT-Sicherheitshandbuch ab.

---

83 [BSI-IT-GSHB97], Teil 1, Kapitel 1, Seite 15

Bewertung

Die Stärke des IT-Sicherheitshandbuchs liegt im umfangreichen Massnahmenkatalog zur Beeinflussung des Untersuchungsobjektes. Auch wenn ein stark technikzentrierter Ansatz im Vordergrund steht, der noch dazu nur ansatzweise auf Risikoanalysen eingeht und sich fast nur auf Grundschutz bezieht, ist dieses ISi-Verfahren aufgrund der Beschreibung der Projektauslösung und der Organisation für die Verwendung in Informationssicherheitsprojekten geeignet. Die fehlende Koordinations- und Kooperationsmöglichkeit über die Festlegung vergleichbarer Ergebnisse sowie die Vernachlässigung der Kontrolle sind die grössten Schwachstellen dieses Verfahrens. Die Tabelle mit der detaillierten Bewertung dieses ISi-Verfahrens findet sich in Anhang B.3, Tabelle B-3. Die Gegenüberstellung der Profile geschieht in den Tabellen B-9 bis B-12.

Gesamtbeurteilung

Das IT-Grundschutzhandbuch ist in erster Linie ein Referenzwerk für konkrete Massnahmen für verschiedenste technische Systeme. Es wird durch organisatorische und bauliche Massnahmenbereiche sowie durch das ISi-Verfahren ergänzt, wobei dieser Zusätze inhaltlich nicht so ausgefeilt sind wie die technischen Beschreibungen. Trotzdem bietet das Werk eine solide Grundlage für den Aufbau sicherer Systeme. Einer konsequenten einheitlich durchgängigen Anwendung, welche die Voraussetzung für eine Zertifizierung oder Benchmarking wäre, steht der Umfang des Werks und die fehlende einheitliche Ergebnispräsentation entgegen. Das IT-Sicherheitshandbuch erhält in vielen Einzelbewertungen extreme Werte, da es konsequent auf den Umfang des Massnahmenkataloges setzt.

7.2.4 Code of Practice (BSI-GB)

Dokument

Der „Leitfaden zum Management von Informationssicherheit“[84] (COP) wurde 1995 vom British Standards Institute, als British Standard 7799 publiziert. Er umfasst auf ca. 50 Seiten 109 Massnahmen in zehn Bereichen, wobei zehn der Massnahmen als „Key Controls“ bezeichnet werden. Die Erarbeitung dieses Standards wurde von 13 grossen britischen Unternehmungen und britischen Ablegern internationaler Konzerne vorgenommen und soll ein minimales Set von Massnahmen zur Erreichung eines Grundschutzes zur Verfügung stellen. Der BS richtet sich dabei generell an das Management. Eine Überarbeitung des COP wurde 1997 begonnen und soll 1999 publiziert werden.

---

84 Titel der deutschen Übersetzung von [BSI-COP95]; alle Angaben beziehen sich jedoch auf die englische Originalversion.

Der COP wurde in der Wirtschaft breit akzeptiert. Dies ist einerseits auf seine Kürze zurückzuführen, andererseits auf die pragmatische Formulierung der Massnahmen und auf den Aufbau des Dokumentes: die letzten 6 Seiten enthalten eine Zusammenfassung aller Massnahmen.

Inhalt

Der COP unterteilt Sicherheitsmassnahmen in zehn Kategorien gemäss Tabelle 7-4.

Section	Titel	Anzahl Massnahmen-bereiche	Titel der Massnahmenbereiche	Anzahl Teilmass-nahmen
1	Security Policy	1	Information security policy	1
2	Security Organisation	2	Information security infrastructure Security of third party access	7 2
3	Asset classification and control	2	Accountability for assets Information classification	1 2
4	Personnel security	3	Security in job definition and recruiting User training Responding to incidents	3 1 4
5	Physical and environmental security	2	Secure areas Equipment security	6 6
6	Computer and network management	7	Operational procedures and responsibilities System planning and acceptance Protection from malicious software Housekeeping Network management Media handling and security Data and software exchange	5 4 1 4 1 4 5
7	System access control	7	Business requirement for system access User access management User responsibilities Network access control Computer access control Application access control Monitoring system access and use	1 4 2 9 7 4 3
8	Systems development and maintenance	4	Security requirements of systems Security in application systems Security of application system files Security in development and support environments	1 4 2 3
9	Business continuity planning	1	Aspects of business continuity planning	4
10	Compliance	3	Compliance with legal requirements Security reviews of IT systems System audit considerations	4 2 2
10	Total	32		109

Bewertung

Die Stärke des COP liegt in der Beeinflussung des Untersuchungsobjekts. Sehr viele der hier beurteilten Anforderungen an ISi-Verfahren können bei der Studie der COP-Dokumentation nicht beantwortet werden, da der COP praktisch nur aus einer Zusammenstellung von Massnahmenbereichen besteht. Die Durchführung geschieht durch direkte, vom Anwender vollständig selbst zu gestaltende Umsetzung der Massnahmen in den verschiedenen Bereichen. Die Massnahmen sind mehrheitlich abstrakt gehalten, müssen deshalb interpretiert werden und stellen eher inhaltliche Themenbereiche dar. Die Tabelle mit der detaillierten Bewertung dieses ISi-Verfahrens findet sich in Anhang B.4, Tabelle B-4. Die Gegenüberstellung der Profile geschieht in den Tabellen B-9 bis B-12.

Beurteilung

Der erste naheliegende Schluss, der COP sei wegen der im Mittel tiefen Beurteilung grundsätzlich für das Management der Informationssicherheit ungeeignet, ist nicht korrekt. Der COP wird unter anderem auch deshalb hier bewertet und beurteilt, weil er ein in der Praxis verbreitetes "Verfahren" zur Erreichung von Informationssicherheit darstellt. Seine Stärke liegt in der Beschränkung auf wesentliche inhaltliche Bereiche.

Der COP ist kein eigentliches ISi-Verfahren, sondern eignet sich zur unkomplizierten und pragmatischen Betrachtung der Informationssicherheit. Er identifiziert die wichtigsten Betrachtungsgebiete und ist übersichtlich und handlich aufgebaut. In der praktischen Umsetzung erfordert er allerdings viel Interpretation und lässt viele Fragen offen, gerade in Bezug auf den Informationssicherheits-prozess und in Bezug auf die konkrete Beeinflussung der technologischen Komponenten. Er kann daher als gutes Übersichts- und Einstiegswerk angesehen werden, bedarf allerdings weiterer Literatur zur Ergänzung.

7.2.5 COBIT (ISACF)

Dokument

Die *Control Objectives for Information and Related Technology* (COBIT) ist eine Publikation der *Information Systems Audit and Control Association.* Sie ist 1996 erschienen und umfasst ca. 400 Seiten. Die Dokumentation wird in vier verschiedenen Detaillierungsstufen geliefert (*Executive Summary, Framework*, *Control Objectives* und *Audit Guidelines*). COBIT richtet sich v.a. an die internen

und externen Revisoren von Informationssystemen, aber auch an das betroffene Top- und Linienmanagement.

Inhalt

COBIT umfasst einen ganzheitlichen Ansatz zur Betrachtung der Anforderungen an eine sichere Informationsverarbeitung. Erklärtes Ziel dabei ist, die Lücke zwischen Sicherheitsnormen und technischen Verfahren einerseits und den unternehmerischen Anforderungen andererseits zu schliessen, indem konsequent die Prozesse betrachtet werden, welche die Informationstechnik unterstützen. Dazu werden *Control Objectives* aufgestellt, welche sich auf (generisch definierte) Geschäftsprozesse in vier Bereichen (*Domains*) beziehen. Dabei werden jeweils einzelne oder mehrere Anforderungen an die Information (*Information Criteria*) auf einzelne oder mehrere Elemente des Betrachtungsobjekts (*IT Ressourcen*) bezogen. Zur Untersuchung der Erfüllung der Anforderungen werden Prozesse beschrieben, welche die Feststellung des bestehenden Zustandes anhand von Fragen und Beschreibungen erlauben (davon ist eine detaillierte umfangreiche Liste vorhanden) und übergeordnete Prozesse beschrieben, welche den Soll-Ist-Vergleich beinhalten.

Bewertung

Die Stärke von COBIT liegt darin, dass die gesamte Unternehmung mit ihren Geschäftsprozessen und den verarbeiteten Informationen im Zentrum steht, und dass deshalb von den geschäftlichen Anforderungen ausgegangen wird. Informationstechnologie wird sekundär betrachtet. Allerdings beschränkt sich COBIT auf die Betrachtung, denn es umfasst keine Massnahmen. Es soll der Revision helfen, bestehende Mängel aufzudecken und notwendigen Schutzbedarf zu deklarieren. Es ist jedoch Aufgabe des Managements (und nicht der Revision), die Mängel zu beseitigen; dies geschieht unabhängig von COBIT. Da COBIT im Rahmen des Audit verwendet wird, ist die Organisation nur am Rande beschrieben. Die Tabelle mit der detaillierten Bewertung dieses ISi-Verfahrens findet sich in Anhang B.5, Tabelle B-5. Die Gegenüberstellung der Profile geschieht in den Tabellen B-9 bis B-12.

Gesamtbeurteilung

COBIT ist ein umfangreiches, auf die unternehmerischen Bedürfnisse zugeschnittenes Werk. Es eignet sich sehr gut für die Anwendung in Audits (also in nachgelagerten, prozessunabhängigen Betrachtungen). Für die prozessintegrierte Kontrolle kann es ebenfalls verwendet werden. Es enthält jedoch kein eigenes ISi-Verfahren, welches detailliert die Schritte bezeichnen würde, die zu durchlaufen sind, um eine solche Untersuchung durchzuführen, und dient nur zur Feststellung des Zustandes, nicht zur Beeinflussung der Informationssicherheit. Self-Assessment, also die Selbstbeurteilung des geprüften Bereichs, wird unterstützt.

7.2.6 GMITS (ISO)

Dokument

Die *Guidelines for the Management of IT Security* (GMITS) ist ein Technical Report des ISO / IEC Joint Technical Committee 1, der die wichtigsten Vorgehensweisen und Betrachtungsobjekte der Informationssicherheit auf total ca. 200 Seiten beschreibt. Der erste Teil erschien 1996, weitere folgten 1997 und 1998; Teil 4 und 5 sind noch nicht veröffentlicht und beschreiben den Grundschutz und die technischen Sicherheitsanforderungen an Netzwerkverbindungen[85]. GMITS richtet sich an die Personen, welche mit dem Management der Informationssicherheit beauftragt sind.

Inhalt

GMITS enthält Vorgehensweisen und ein Verfahren zur Anwendung auf verschiedenen Ebenen der Unternehmung. Neben strategisch-organisatorischen Elementen (Definition von Sicherheitspolitik) wird ein ISi-Verfahren beschrieben, welches neben Risikoanalysen auch Grundschutz berücksichtigt. Die Grundbetrachtung ist dabei jedoch eher technisch.

Bewertung

Die Stärken von GMITS liegen in der allgemeinen, auf verschiedenen Abstraktionsebenen vorgenommenen, Beschreibung der Durchführung und der detaillierten Beschreibung der Auslösung von Informationssicherheitsprojekten und der Integration verschiedener Ansätze. Obwohl der Technical Report sich im Titel auf Informationstechnologie bezieht, ist er informations- und nicht technikzentriert. Er identifiziert viele Beeinflussungsbereiche der Informationssicherheit. Zu seinen Schwächen zählen die Vernachlässigung von Budget- und Kostenfragen und der Verzicht auf eine detaillierte formale Beschreibung des Untersuchungsprozesses mit Identifikation der einzelnen Aktivitäten, sowie die teilweise sehr abstrakte Formulierung von Massnahmen in verschiedenen Massnahmenbereichen. Die detaillierte Beurteilung befindet sich in Anhang B.6, Tabelle B-6. Die Gegenüberstellung der Profile geschieht in den Tabellen B-9 bis B-12.

---

85 Die Inhalte sind in den bereits publizierten Teilen kurz umrissen. Aufgrund seiner Mitarbeit im Normierungsprozess hat der Autor Kenntnis von den Inhalten. Die hier vorgenommene Bewertung und Beurteilung stützt sich nur auf die publizierten Dokumente.

Beurteilung

GMITS ist ein gutes Rahmenwerk zur Gestaltung des Untersuchungsprozesses der Informationssicherheit, identifiziert einzelne Inhalte der Betrachtung und bleibt, trotz vordergründiger technischer Ausrichtung, offen für eine weiter gefasste Betrachtung von Informationssystemen. Es eignet sich als Leitfaden („Guideline“) für die grundsätzliche Organisation, bedarf aber zur Umsetzung weiterer Hilfsmittel, da es keinen konkreten Massnahmenkatalog enthält. Es referenziert allerdings solche Kataloge.

Gesamthaft entspricht GMITS am ehesten den hier an ISi-Verfahren gestellten Anforderungen, was durch die höchste Bewertung belegt wird.

7.3 Vergleichende Bewertung und Beurteilung

Bewertung

Bei der vergleichenden Bewertung der verschiedenen ISi-Verfahren kann festgestellt werden, dass jedes der ISi-Verfahren seine Stärken und Schwächen aufweist und dass die Bewertungen sich zum Teil stark, zum Teil kaum unterscheiden. Minimal- und Maximalwerte werden erreicht.

Die *Auslösung* wird von GMITS am besten beschrieben. Wenngleich der Bezug zu neuen Projekten vernachlässigt wird, werden die meisten der hier bewerteten Anforderungen von GMITS weitgehend erfüllt. Im Gegensatz dazu enthält der Code of Practice praktisch keine Aussagen zur Auslösung des ISi-Verfahrens.

Die *Organisation* der Durchführung wird vom Grundschutzverfahren des BFI am aussagekräftigsten beschrieben. Wenngleich bei diesem ISi-Verfahren – wie bei den meisten anderen – keine Aussagen zur Dauer der Phasen gemacht werden, und wie bei den meisten anderen Koordination und Kooperation vernachlässigt dargestellt werden, ist dieses ISi-Verfahren aufgrund seiner Einfachheit für das Projektmanagement geeignet. Praktisch keine Aussage zur Organisation macht der Code of Practice.

Bei der *Durchführung* ist GMITS am aussagekräftigsten. Da es sowohl eine abstrakte wie auch eine konkrete Beschreibung des Prozesses enthält, verschiedene Ansätze berücksichtigt und die Identifikation verschiedener inhaltlicher Fachgebiete vornimmt, kann es als gute Grundlage für die Durchführung eines ISi-Verfahrens verwendet werden. Ebenfalls hoch bewertet wurde das IT-Sicherheitshandbuch. Es ist in einigen Bereichen, v.a. bei der Definition der einzelnen Aktivitäten und der Ergebnisse, noch konkreter als GMITS, fällt jedoch durch den bei der Durchführung notwendigen Aufwand zurück. Am schlechtesten wird auch hier der Code of Practice bewertet. Lediglich die Verfügbarkeit der Massnahmen und die einfache Erlernbarkeit zählen zu seinen Stärken.

Bei der *fachbereich*bezogenen Betrachtung liegt der Code of Practice dafür weit vorne, da er die Analyse und Beeinflussung aller wichtigen Bereiche des Untersuchungsobjektes erlaubt. ISACF COBIT übertrifft ihn allerdings in der Analysephase. Das IT-Grundschutzhandbuch ist aufgrund der sehr vielen konkreten Massnahmen in der Beeinflussung stärker, allerdings nur im technischen, produktspezifischen Bereich. Auch ISO GMITS kann aufgrund der gleichmässigen und umfassenden Betrachtung hoch bewertet werden.

Beurteilung

Gesamthaft sind fünf der sechs ISi-Verfahren zur Erreichung von Informationssicherheit geeignet. Lediglich COBIT beschränkt sich darauf, die Probleme der Informationssicherheit zu identifizieren. Es umfasst nur die Erhebung des Zustandes, ohne diesen zu verändern.

Aus den Bewertungen kann gefolgert werden, dass der Code of Practice und das BFI-Grundschutzverfahren sich am ehesten für ein einfaches und direktes Informationssicherheitsmanagement eignen. Letzteres aber nur, falls die Anwendung in einem stark hierarchisch organisierten Betrieb stattfindet, bei welchem die in diesem ISi-Verfahren erwähnten Institutionen eindeutig zugeordnet werden können.

Das IT-Grundschutzhandbuch muss als Referenz für jeglichen technisch orientierten, produktbezogenen Grundschutz angesehen werden. Auch wenn das darin erläuterte ISi-Verfahren weniger gut bewertet wurde, bleibt die Menge und Qualität der vorgeschlagenen Massnahmen im Vergleich unerreicht.

Für eine formale, und damit langfristige und nachhaltige Informationssicherheit bietet sich das IT-Sicherheitshandbuch des BSI an. Die detaillierte Prozessbeschreibung ist seine grosse Stärke, und wenn es nicht allein den Risikoanalyseansatz berücksichtigen würde, könnte eine Durchführung mit geringerem Aufwand vorgenommen werden, wodurch die Akzeptanz dieses ISi-Verfahrens erhöht würde. GMITS berücksichtigt mehrere Ansätze und ist gerade deshalb ein gutes ISi-Verfahren für langfristig orientierte Untersuchungen. Allerdings erreicht es nicht die formale Qualität des IT-Sicherheitshandbuchs.

Fazit der Bewertung und Beurteilung

In diesem Kapitel wurden verschiedene bestehende und in der Praxis eingesetzte Verfahren zur Erreichung von Informationssicherheit (ISi-Verfahren) kurz beschrieben und dann mit einem hier aufgestellten Bewertungsschema bewertet. Von den hier untersuchten ISi-Verfahren hat keines eine maximale Bewertung erreicht. Rein theoretisch wurde also kein ideales ISi-Verfahren betrachtet. Dennoch weist jedes ISi-Verfahren Stärken in spezifischen Bereichen auf und hat so auch seinen Platz in der praxisorientierten Anwendung gefunden.

Weiterhin muss berücksichtigt werden, dass die Bewertungskriterien zum Teil sich widersprechende Anforderungen stellen. Zwar wurden alle Kriterien so gewählt, dass eine höhere Bewertung auch eine bessere Beurteilung ergeben soll, aber beispielsweise ist eine einfache Erlernbarkeit bei gleichzeitiger ausführlicher Dokumentation kaum zu erreichen. Ausserdem spezialisiert sich jedes der beschriebenen ISi-Verfahren auf eine oder mehrere konkrete Anwendungen. Die Erfüllung aller Anforderungen würde diese (gewünschte) Spezialisierung zunichte machen.

Ziel ist es also, Anforderungen anhand der hier vorgenommenen Bewertungen nicht nur als Maxima abzuleiten, sondern durch einzelne Betrachtungen der Kriterien und unter Berücksichtigung der strukturellen und inhaltlichen Anforderungen aus den Teilen I und II dieses Textes (Kapitel 1 bis 6) ein wünschenswertes Profil zu definieren und ein entsprechendes ISi-Verfahren zu entwerfen.

Anforderungen an ein neues ISi-Verfahren

Das neue, in dieser Dissertation entwickelte ISi-Verfahren soll

- die bei den betrachteten ISi-Verfahren identifizierten Schwachstellen durch neue Inhalte und Vorgehensweisen ersetzen,
- identifizierte Stärken der betrachteten ISi-Verfahren übernehmen und
- die Integration der unterschiedlichen Ansätze gemäss Abschnitt 6.4 durch gezielte Aufnahme einzelner Elemente der beschriebenen ISi-Verfahren und absichtliche Auslassung anderer Teile erreichen.

Das Profil wird einerseits als Soll erstellt werden, d.h. es wird eine Bewertung der *angestrebten* Eigenschaften vorgenommen. Konkret soll das in der Tabelle B-7 („Anforderungen an *ISIWAY*“) beschriebene Profil angestrebt werden. Am Ende von Kapitel 8 wird dieses dann rückblickend betrachtet.

Die Ansprüche an das neue ISi-Verfahren sind hoch. Es fällt auf, dass das neue ISi-Verfahren in allen vier Variablen eine höhere Bewertung erhalten soll als die zuvor bewerteten etablierten ISi-Verfahren. Dies soll erreicht werden, obwohl Massnahmenkataloge ausgelassen werden sollen, Projekt- und Change Management nur am Rande betrachtet werden sollen und nur einige inhaltliche Teilgebiete identifiziert werden sollen. Gerade in denjenigen Bereichen, in welchen die bestehenden ISi-Verfahren Schwächen aufweisen (Kontrolle, Skalierbarkeit, Koordination und Kooperation) soll dieses neue ISi-Verfahren jedoch Stärken aufweisen. Es muss offen bleiben, ob das neue ISi-Verfahren diese hohe Bewertung auch bei einem unabhängigen Vergleich erreichen kann.

Auslösung

Das neue ISi-Verfahren soll möglichst genau darauf eingehen, wer ein Informationssicherheitsprojekt auslöst und wann dies geschieht. Auch die Methode

der Auslösung (also die Vorgehensweise mit welcher ein neues Projekt gestartet wird) muss beschrieben werden.

Organisation

Eines der zentralen Probleme der betrachteten ISi-Verfahren ist die ungenaue Zusammensetzung des Projektteams und die daraus entstehenden Unklarheiten der Zuordnung von Verantwortungen und Aufgaben. Hier muss das neue ISi-Verfahren genauer sein. Ferner soll sich das neue ISi-Verfahren selbst auch für das Projektmanagement eignen, indem es die einzelnen Phasen, Schritte und Aktivitäten mindestens so genau regelt wie das IT-Sicherheitshandbuch. Weiterhin müssen Hinweise zur Abgrenzung von Inhalt (Tiefe) und Betrachtungsobjekt (Breite) explizit abgegeben werden. Zentral ist, dass das ISi-Verfahren Koordination und Kooperation unterstützen soll.

Durchführung

Für verschiedene Adressaten des ISi-Verfahrens müssen unterschiedlich detaillierte Verfahrensweisen zur Verfügung gestellt werden, um auf übergeordneter Ebene das schnelle Gewinnen des Überblicks zu erlauben und auf unteren Ebenen konkrete Vorgehensweisen angegeben zu können. Weiter müssen die verschiedenen Ansätze berücksichtigt werden. Einfache Erlernbarkeit ist ein weiteres Ziel, welches unter anderem durch einheitlichen Aufbau und ein Werkzeug erreicht werden soll, welches den Anwender durch das ISi-Verfahren führt. Schliesslich sollen auch Kosten- und Budgetfragen behandelt werden.

Fachbereiche

Das ISi-Verfahren soll ganz deutlich *Information* ins Zentrum der Betrachtung stellen und sich so von den meist Informatik-zentrischen Betrachtungsweisen der anderen ISi-Verfahren abheben. Massnahmenkatalog sollen nicht bereitgestellt werden, da schon viele Kataloge bestehen, auf welche verwiesen werden kann.

Die Anforderungen sind im Detail in Tabelle B-7 beschrieben; das entsprechende Profil ist in den Tabellen B-9 bis B-12 enthalten. Die Anforderungen sind zum Teil sehr hoch. Es kann aber nicht theoretisch erklärt werden, ob sie sich erreichen lassen. Die Beurteilung am Ende von Kapitel 8 zeigt, in welchen Punkten hier Beiträge geleistet werden konnten.

8 Verfahren *ISiWAY*

In den Kapiteln 3 bis 6 wurden das Bezugsobjekt, die Institutionen, Informationen, Instrumente und der Prozess der Informationssicherheit als Teile des Rahmenwerks der Informationssicherheit beschrieben. In diesem Kapitel soll nun ein konkreter *Vorschlag* dargelegt werden, wie das Management der Informationssicherheit in einer Unternehmung ablaufen kann. Dieser Vorschlag wird als *erste Konkretisierung des Informationssicherheitsprozesses* bezeichnet[86].

Kern dieses Vorschlags ist ein neues Verfahren, *ISiWAY* genannt, welches hier entwickelt wird. Dieses Verfahren soll den Ansprüchen genügen, die im Kapitel 7 formuliert wurden (vgl. Tabelle B-7 „Anforderungen an *ISiWAY*“ in Anhang B.7).

Zunächst wird in diesem Kapitel das zugrundeliegende Konzept von *ISiWAY* beschrieben (Abschnitt 8.1). Danach wird vertieft auf die Struktur von *ISiWAY* eingegangen (Abschnitt 8.2). *ISiWAY* verwendet ein Rollenmodell, welches in Abschnitt 8.3 beschrieben wird. In Abschnitt 8.4 wird die Durchführung von *ISiWAY* im Rahmen eines Projektes genauer betrachtet. Schliesslich beinhaltet Abschnitt 8.5 eine Evaluation des Verfahrens mit Hilfe des in Kapitel 7 erstellten Schemas.

8.1 *ISiWAY* Konzept

Idee und Zielsetzung

ISiWAY ist ein *Verfahren zum Management der Informationssicherheit* in Unternehmungen. *ISiWAY* umfasst eine einfache Vorgehensweise und beruht auf dem Dialog zwischen den informationsverarbeitenden Personen innerhalb der Unternehmung. Es stellt dabei die *Inhalte* der Informationsverarbeitung ins Zentrum.

Ziel der Definition von *ISiWAY* war es, ein Verfahren zu erstellen, welches die Anforderungen gemäss Tabelle B-7 in Anhang B.7 erfüllt. Einerseits sollte *ISiWAY* dabei eine Konkretisierung des in Kapitel 6 beschriebenen, generischen Prozesses der Informationssicherheit sein und die verschiedenen Aspekte des Rahmenwerks der Informationssicherheit, welches in Teil II dieser Dissertation beschrieben wurde, abdecken. Andererseits sollte es die Stärken der in Kapitel 7 evaluierten Verfahren integrieren und deren Schwächen meiden; dies ist durch das in Tabelle B-7 definierte Anforderungsprofil gegeben.

---

86 Eine zweite Konkretisierung findet in Kapitel 10 statt.

Ziel der Anwendung von *ISIWAY* ist es, den Zustand der Informationssicherheit in der Unternehmung zu erheben, ein gemeinsames anzustrebendes Sicherheitsniveau zu definieren und dieses Niveau durch gemeinsame Arbeit mit *allen* Beteiligten *langfristig* zu erreichen und zu halten.

ISIWAY enthält konkrete Angaben zur Organisation des Managements der Informationssicherheit innerhalb einer Unternehmung, ohne sich dabei auf einen Einzelfall zu beschränken. Der Vorschlag bleibt also insofern theoretisch und *generisch*, als er sich nicht auf eine konkrete Unternehmung bezieht – dies wäre auch nicht sinnvoll. Er ist aber insofern *konkret*, als er versucht, die zur Umsetzung der Informationssicherheit notwendigen Elemente innerhalb der Unternehmung hinreichend genau festzulegen, um eine möglichst einfache und einheitliche Umsetzung zu erlauben.

Dokumentation

Dieses Kapitel und die Detailergänzungen in Anhang C.1 stellen die vollständige Dokumentation des Verfahrens dar. Die Grundlagen und Begriffe, auf denen *ISIWAY* aufbaut, wurden in den vorherigen Kapiteln dieser Dissertation einzeln erwähnt und erklärt. Sie sind nochmals in einem Glossar in Anhang E ausgeführt. Diese Textteile (Kapitel 8, Anhänge C.1 und E) können gesamthaft als konkrete Handlungsanleitung für diejenigen Personen verwendet werden, welche *ISIWAY* anwenden möchten.

Aufbau

ISIWAY ist als Prozess definiert und enthält deshalb klare Spezifikationen der einzelnen notwendigen Aufgabenstellungen und Aktivitäten, ihrer Reihenfolge, der jeweiligen dabei involvierten Rollen und der jeweiligen Ergebnisse. Dieser Prozess läuft in mehreren Zyklen ab, welche *Detaillierungsgrade (DGs)* genannt werden. Einzelne Schritte dieser Zyklen wiederholen sich, um Veränderungen, die im Laufe der Zeit in der Unternehmung und ihrer Umgebung entstehen, berücksichtigen zu können. Die notwendigen organisatorischen Strukturen (d.h. ihre erstmalige Einrichtung, ihre Aufgaben etc.) werden ebenfalls innerhalb des Verfahrens festgelegt.

ISIWAY umfasst Tätigkeiten auf *strategischer, taktischer und operativer Ebene* der Unternehmung. Grundsätzlich wird dabei *top-down* vorgegangen, d.h. von den grundsätzlichen, auf strategischer Ebene der Unternehmung zu fällenden Entscheidungen wird im Laufe des Verfahrens immer mehr detailliert und konkretisiert, bis schliesslich einzelne operative Handlungsanweisungen entstehen. Im Haupttext werden die übergeordneten Strukturen von *ISIWAY* beschrieben. Die Details sind in Anhang C.1 enthalten.

Da die benötigte Detaillierung von der jeweiligen konkreten Umgebung abhängig ist, in welcher *ISIWAY* eingesetzt wird, werden nicht in jedem Zyklus alle Aufgaben

ausgeführt, sondern jeweils nur eine Teilmenge. *ISIWAY* ist dazu in vier Detaillierungsgrade (DG1 bis DG4) aufgeteilt, umfasst darüber hinaus eine Vorbereitungsphase (DG0) und einen spezifischen Krisenzyklus (DG3.5). Diese *Detaillierungsgrade* werden in aufsteigender Reihenfolge durchlaufen (mit Ausnahme des Krisenmanagements von DG3.5). Detaillierungsgrad 0 umfasst die *Vorbereitung* der Durchführung des Informationssicherheitsmanagements und die notwendige Motivation. Die Erreichung *minimaler Informationssicherheit* mit *ISIWAY* wird in Detaillierungsgrad 1 beschrieben und umfasst vor allem den Grundschutz. Die *angepasste Informationssicherheit* mit Wertekonzept wird in Detaillierungsgrad 2 behandelt. Detaillierungsgrad 3 beschreibt, wie *risikogerechte Informationssicherheit* mit *ISIWAY* erreicht werden kann. Welche weiteren Inhalte für die Betrachtung der Informationssicherheit relevant sind und wie zur Erreichung von *umfassender Informationssicherheit* mit *ISIWAY* vorgegangen werden soll, wird in Detaillierungsgrad 4 beschrieben. Schliesslich wird *Krisenmanagement* mit *ISIWAY* in Detaillierungsgrad 3.5 behandelt.

Durch die Aufteilung in Detaillierungsgrade ist *ISIWAY* skalierbar, d.h. in Abhängigkeit von den konkreten Bedürfnissen des Anwenders können verschiedene Inhalte und Detaillierungsgrade berücksichtigt werden. Die definierten Aktivitäten werden also nicht immer in derselben Breite und Tiefe ausgeführt, sondern umfassen je nach konkreter Anforderung und Situation mehr oder weniger Details. Wenn *ISIWAY* jedoch von DG0 bis DG4 vollständig durchlaufen wird, kann damit umfassende Informationssicherheit erreicht werden.

Komponenten

ISIWAY enthält folgende Komponenten zum Management der Informationssicherheit:

- Festlegung des Ziels der Informationssicherheit und *Auslösung*:

  Da Informationssicherheit personenbezogen ist, wird beschrieben, wie die einzelnen involvierten Personen und Personengruppen Informationssicherheit als Ziel definieren können und wie vorgegangen wird, um *ISIWAY* erstmals auszulösen.

- Schaffung der organisatorischen Voraussetzungen (*Organisation*):

  Die erfolgreiche Umsetzung von Informationssicherheit muss von einer Person getragen werden, die für dieses Ziels langfristig verantwortlich ist. Es wird beschrieben, welche Qualifikationen diese Person aufweisen muss und wie sie erreichen kann, dass weitere Personen in der Unternehmung dieses Ziel ebenfalls verfolgen. Dazu werden weitere Institutionen, Informationen und Instrumente definiert.

- *Durchführung* des Prozesses:

ISIWAY definiert, welche Tätigkeiten von welchen Personen in welcher Reihenfolge unter welchen Bedingungen aufgrund welcher Ausgangsdaten durchgeführt werden sollen, welches konkrete Ziel dabei verfolgt wird und welche Daten dabei produziert werden.

- Beeinflussung des Bezugsobjektes in den verschiedenen *Fachgebieten*:

  ISIWAY umfasst die Identifikation wichtiger Teil- und Fachgebiete der Informationssicherheit und enthält Verweise auf weiterführende Informationen.

Diese Liste zeigt, dass der Aufbau von *ISIWAY* demjenigen des Bewertungsschemas aus Kapitel 7 entspricht.

Betrachtungsgegenstand

Betrachtungsgegenstand des Informationssicherheitsmanagements gemäss *ISIWAY* ist das Informationssystem der Unternehmung; es wird hier konsequent als *Betrachtungsobjekt, Bezugsobjekt* oder einfach als *Objekt* bezeichnet, welches *Teilobjekte* umfasst und sich hierarchisch gliedern lässt (vgl. auch Abschnitte 3.2ff). Die feinsten hier vorgenommenen Unterteilungen von Teilobjekten werden als *Elemente* bezeichnet. Eine Informationssammlung oder ein einzelnes Arbeitsplatzsystem sind jeweils ein solches Element des Betrachtungsobjekts[87]. Diese Elemente können zu Gruppen zusammengefasst werden, deren einzelne Elemente Gemeinsamkeiten aufweisen und deshalb gesamthaft behandelt werden können. Diese Gruppen werden als *Elementegruppen* oder synonym auch als *Objektgruppen* bezeichnet. Die Informatikeinrichtung einer Abteilung ist beispielsweise eine solche Objektgruppe.

8.2 *ISIWAY* Struktur

ISIWAY ist in sechs Detaillierungsgrade (DGs) unterteilt. Sie sind jeweils als Kreise dargestellt, womit verdeutlicht werden soll, dass das Management der Informationssicherheit ein zyklisch ablaufender, kontinuierlicher Prozess ist[88]. Jeder Zyklus wird in einzelne chronologisch aufeinanderfolgende *Phasen* unterteilt. Sie sind an die Phasen des Führungsprozesses gemäss Zürcher Management-Ansatz angelehnt (vgl. Abschnitt 2.6) und werden *Planung, Entscheidung, Anordnung, Durchführung* und *Kontrolle* genannt. Die *Durchführung* umfasst die Arbeiten,

---

87 Bei der Gesamtbetrachtung ist es zwar weiterhin möglich, ein *Dokument* als kleinste unternehmerische Informationseinheit zu betrachten, wie dies in Abschnitt 2.1 festgelegt wurde, doch die *Informationssammlung* ist als kleinste Einheit des Informationssicherheitsmanagements besser geeignet.

88 Diese Ausführungen treffen für das Krisenmanagement (DG3.5) nur teilweise zu.

welche auf der darunterliegenden Managementebene zwischen der *Anordnung* und der *Kontrolle* durchgeführt werden (vgl. Abbildung 8-1). Innerhalb der Phasen werden verschiedene Tätigkeiten ausgeführt, die hier als *Aktivitäten* bezeichnet werden.

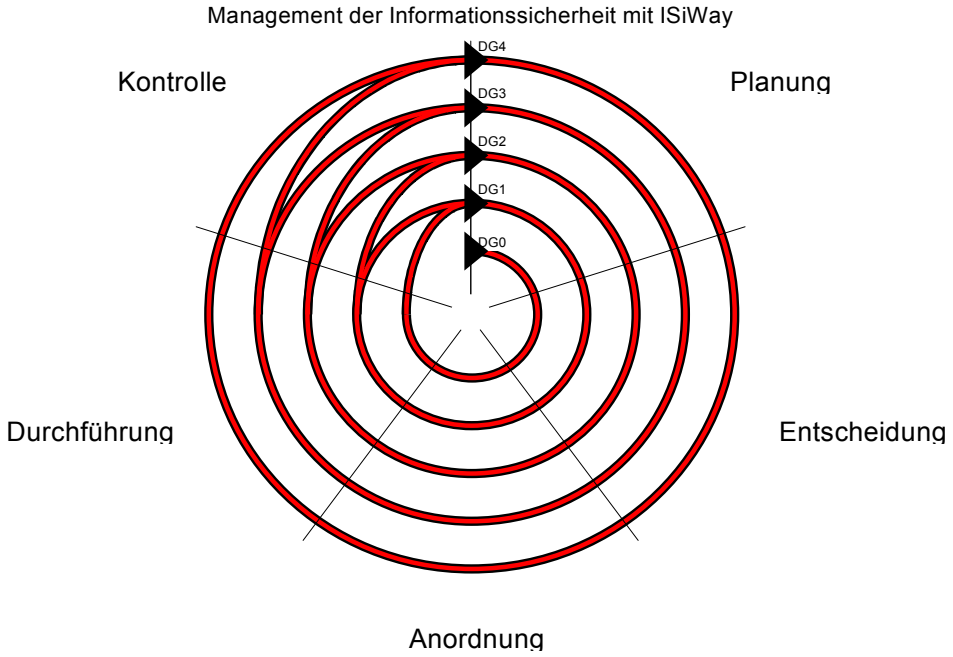


Abbildung 8-1: *ISIWAY* DG0 bis DG4

Bei *ISIWAY* können sich auch innerhalb der Phasen diese fünf Tätigkeiten abwechseln. Deshalb tragen die *ISIWAY*-Phasen andere Bezeichnungen, welche in direkterem Zusammenhang mit den in *ISIWAY* durchzuführenden Tätigkeiten stehen (vgl. Abbildung 8-2).

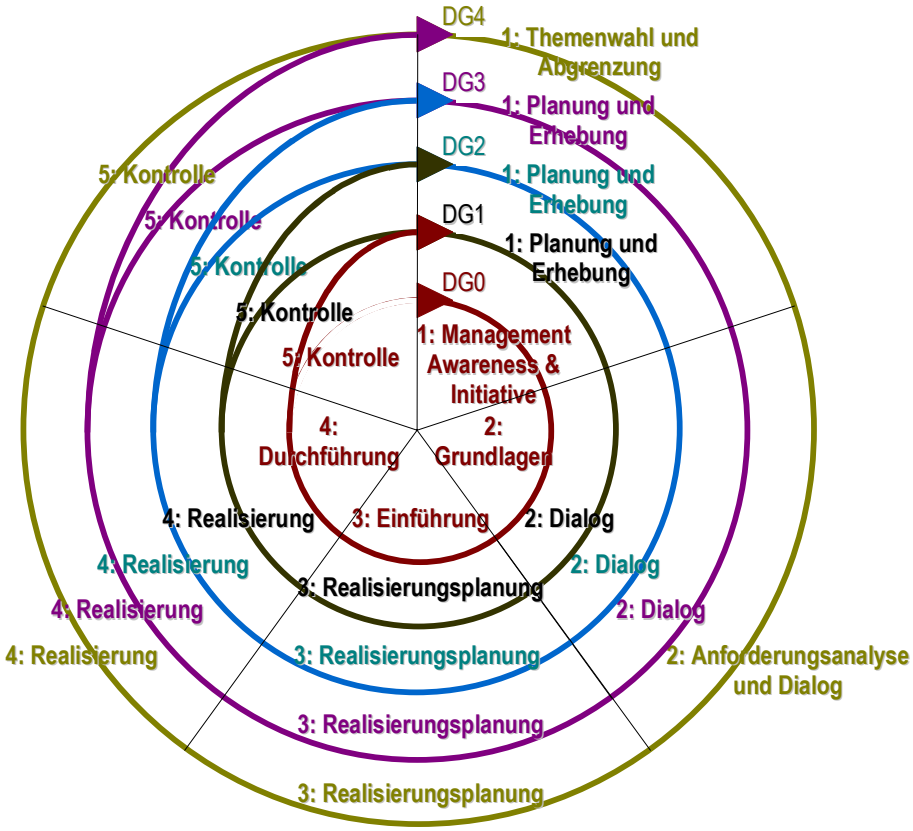


Abbildung 8-2: *ISIWAY* DG0 bis DG4 mit Phasenbezeichnungen

Die sechs Detaillierungsgrade umfassen die nachfolgend beschriebenen Inhalte:

Vorbereitung (Detaillierungsgrad 0)

Vor Beginn eines Projektes der Informationssicherheit sind Vorbereitungsarbeiten notwendig, welche noch keinen eigentlichen Einfluss auf die Informationssicherheit haben, jedoch die Rahmenbedingungen für die Durchführung schaffen. Dabei geht es im besonderen darum, beim Management das Bewusstsein für die Notwendigkeit eines derartigen Projektes zu schaffen, eine Zielsetzung zu formulieren und die Schaffung der notwendigen Institutionen auszulösen. Die wichtigste Institution ist diejenige des Informationssicherheitsbeauftragten (ISiBe), der als oberster Koordinator für Informationssicherheit in der Unternehmung die Auslösung des Prozesses in den einzelnen Bereichen der Unternehmung vornimmt.

Minimale Informationssicherheit (Detaillierungsgrad 1)

DG1 umfasst grundsätzliche erste Erhebungs- und Bewertungsarbeiten, in welchen die Struktur des untersuchten Systems analysiert und dokumentiert wird. Direkt danach können bei groben Unzulänglichkeiten Sofortmassnahmen ergriffen werden. Danach werden Grundschutzmassnahmen aus einem in DG0 vorbereiteten Katalog ausgewählt, umgesetzt und kontrolliert.

Angepasste Informationssicherheit (Detaillierungsgrad 2)

DG2 umfasst einen ersten strukturierten Ansatz zur Erreichung *angepasster Sicherheit*. Dazu wird das Inventar der bestehenden Objekte verfeinert und ergänzt. Die Sicherheitsanforderungen an die erhobenen Objekte werden bewertet. Eine allgemeine Risikoanalyse zeigt die groben Risiken auf, denen die Objekte unterliegen. Dann wird festgestellt, welche der erhobenen Anforderungen erfüllt werden bzw. erfüllt werden können. Es werden Massnahmen aus einem (bestehenden, in DG0 vorbereiteten) Massnahmenkatalog ausgewählt oder situationsspezifisch zusammengestellt, diskutiert, beschlossen, umgesetzt und kontrolliert.

Risikogerechte Informationssicherheit (Detaillierungsgrad 3)

In DG3 werden die Risiken genauer betrachtet, welchen die Objekte unterliegen. Dazu wird eine detaillierte Risikoanalyse für diejenigen Objekte durchgeführt, bei denen hohe Risiken angenommen wurden. Spezifisch daran angepasste bzw. generierte Massnahmen werden diskutiert, beschlossen, umgesetzt und kontrolliert.

Umfassende Informationssicherheit (Detaillierungsgrad 4)

DG4 umfasst weitere inhaltliche Arbeiten, unter anderem die Definition eines Krisenmanagements, die genauere Betrachtung des Sicherheitsdispositivs, und weitere Zusatzarbeiten zur Abrundung der Sicherheitsanstrengungen sowie inhaltliche Arbeiten, welche in Kapitel 5 als Inhalte der Informationssicherheit definiert wurden.

Krisenmanagement (Detaillierungsgrad 3.5)

Das Durchlaufen von DG3.5 wird durch Krisensituationen ausgelöst. Welche Kriterien angewendet werden müssen, um einen Störfall als Krise zu bezeichnen, wer in einer Krisensituation welche Kompetenzen erhält, wie vorgegangen werden muss, um den Normalzustand wiederherzustellen etc. muss zuvor festgelegt werden. DG3.5 definiert lediglich das Muster, nach welchem vorgegangen werden soll; die Festlegung der Details der dabei anzuwendenden Richtlinien (konkrete Institutionen, Informationen, Instrumente der Unternehmung) geschieht durch eine darauf ausrichtete Anwendung von DG4.

Einheitlicher Aufbau der Detaillierungsgrade

Obwohl die Detaillierungsgrade unterschiedliche Inhalte haben, sind sie ähnlich aufgebaut: Sie sind in fünf Phasen unterteilt (mit Ausnahme des Krisenmanagements in DG3.5). Daraus entstehen auch Ähnlichkeiten bei den einzelnen Aktivitäten: Sie lassen sich zu *Aktivitätengruppen* zusammenfassen.

- So lassen sich in der Planungsphase eines jeden Detaillierungsgrades grundsätzlich die Aktivitätengruppen *Auslösung des Teilprojektes, Zielvereinbarung, Abgrenzung, Organisation, Vorbereitung der Durchführung, Ressourcenplanung, Erhebung, Konsolidierung* und *Abschluss* unterscheiden.
- In der Entscheidungsphase können *Sofortmassnahmen, Entscheidungs-spielraum, Dialog vorbereiten, Dialog führen, Dokumentation* und *Abschluss* unterschieden werden.
- In der Anordnungsphase lassen sich die einzelnen Aktivitäten zu *Evaluation der Entscheidung, Erstellung, Diskussion und Beschluss der Realisierungs-planung* sowie *Abschluss* zusammenfassen.
- Die Durchführungsphase ist in *Realisierungsplanung detaillieren, Durchführung der Realisierung, Dokumentation der Realisierung, Publikation der Realisierungsdokumentation, Schulung* und *Abschluss* unterteilbar.
- Schliesslich kann die Kontrollphase in *Review, Respawn, Relaunch, Synchronisation, Report, Audit* und *Abschluss* unterteilt werden.

Diese Aktivitätengruppen sind in Anhang C.1.1 genauer erläutert. Bezogen auf die Inhalte der Detaillierungsgrade sind die einzelnen Aktivitäten in den Anhängen C.1.2ff detailliert beschrieben.

Die Reihenfolge der Tätigkeiten und Aufgaben *innerhalb der jeweiligen Aktivität* ist nicht festgelegt. *Die Aktivitäten selbst* stehen jedoch in einer festen, streng sequentiellen Reihenfolge, weil jede Aktivität auf den Ergebnissen der vorherigen Aktivität aufbaut. Ebenso stehen die Phasen in einer streng sequentiellen Reihenfolge. Die Detaillierungsgrade stehen in aufsteigender Reihenfolge, d.h. nach dem Durchlaufen eines Detaillierungsgrades sollte derselbe oder der darüberliegende durchlaufen werden.

Die strenge Reihenfolge schliesst nicht aus, dass mit Teilergebnissen, welche sich beispielsweise auf einen inhaltlichen Teilbereich oder ein Teil des betrachteten Objektes beziehen, in einer nachfolgenden Aktivität weitergearbeitet werden kann, ohne das Vorliegen sämtlicher Teilergebnisse abzuwarten.

Horizontale und vertikale Betrachtung

Detaillierungsgrade 1 bis 3 umfassen eine *horizontale* Betrachtung: Das identifizierte und zu untersuchende Teilobjekt wird *ganzheitlich* betrachtet. Es wird zunächst ein zu erreichendes Sicherheitsniveau festgelegt. Dieses wird entweder durch Anwendung von festgelegten, einheitlichen Grundschutzmassnahmen (DG1) erreicht oder mit darüber hinausgehenden Massnahmen, die aufgrund der Ergebnisse von Wert- (DG2) und Risikoanalysen (DG3) definiert wurden.

Dabei wird das angestrebte Sicherheitsniveau idealerweise direkt erreicht. Aufgrund des Aufwands der ganzheitlichen Betrachtung und der aus Kosten- und Aufwandsrestriktionen entstehenden Beschränkungen, Pauschalisierungen und

Kompromisse wird das Sicherheitsniveau jedoch nicht in allen Bereichen genügend nah getroffen.

Detaillierungsgrad 4 umfasst eine *vertikale* Betrachtung: Das zu sichernde Teilobjekt wird nicht mehr gesamthaft betrachtet, sondern nur noch einzelne Elemente davon, diese dafür im Detail. Diese Elemente können nach verschiedenen Kriterien ausgewählt werden, z.B. nach Standort (für lokalitätsbezogene Gefährdungen), nach Inhalt (für Datenschutzfragen) oder nach Technologie (für Risiken einer Online-Anbindung). Danach werden der jeweiligen Bedrohungssituation angemessene Massnahmen ergriffen, welche die Sicherheit möglichst nah an das angestrebte Niveau erhöhen. Auch die konkrete Spezifikation der Richtlinien für das Krisenmanagement (DG3.5) geschieht in Detaillierungsgrad 4.

In realer Umgebung könnte beispielsweise das Informationssystem einer Unternehmung in verschiedene Teilsysteme unterteilt werden, die der Gliederung der Unternehmung entsprechen (Marketing, Verkauf und Logistik, Produktion, Beschaffung etc., oder nach Regionen oder Sparten). In DG 1 bis 3 wird jedes dieser Teilsysteme (z.B. das Marketinginformationssystem) von einem jeweils dafür Zuständigen *Koordinator für Informationssicherheit* genauer untersucht und gesichert. In DG4 wird jedoch ein inhaltlicher Teilbereich, z.B. das Outsourcing oder Versicherungen, genauer analysiert. Dazu werden nur diejenigen Elemente des Teilsystems betrachtet, welche vom Outsourcing betroffen sind, also z.B. Büroautomation, logistische Informationssysteme, Netzwerke. Alle Fragen, welche dabei Teilsysteme betreffen, die ausserhalb der konkreten Betrachtung liegen, werden an den Zuständigen des übergeordneten Objekts (d.h. den übergeordneten Koordinator für Informationssicherheit oder direkt an den Beauftragten für Informationssicherheit) weitergegeben, welcher wiederum alle Zuständigen der betroffenen Objekte involviert. Beispielsweise kann die Vereinbarung von Versicherungspolicen für einzelne Teilbereiche gut vom Informationssicherheits-beauftragten koordiniert werden. Die Teilprozesse liefern ihm dann die Anforderungen und konkrete Objekt- und Risikoabgrenzungen, er sammelt diese und treibt die Policenselektion voran.

8.3 Rollen

Personen werden in *ISIWAY* nicht *direkt* berücksichtigt, sondern über die *Rolle* erfasst, welche sie einnehmen. Eine Rolle umfasst Aufgabe, Kompetenz und Verantwortung. Sie ist damit immer einer Institution innerhalb der Unternehmung zugeordnet; diese Zuordnung ist jedoch nicht eindeutig[89]. Die Konzeption der Rollen für *Geschäftsleitung (GL), Beauftragtem für Informationssicherheit (ISiBe),*

[89] Eine Institution kann mehrere Rollen innehaben und eine Rolle kann von mehreren Institutionen wahrgenommen werden, wobei eine Hierarchie entsteht.

Übergeordnetem Management (ÜM), Koordinator für Informationssicherheit (ISiKo), Ansprechpartner für Informationssammlungen (Info Owner), Ansprechpartner für IT-Systeme (Verwalter), Benutzer, Sponsoren und *Berater* geschieht wie in Abschnitt 4.2.3 erklärt.[90]

Zusammenarbeit

ISIWAY baut auf der Kooperation der verschiedenen Fachbereiche auf, welche an der Informationsverarbeitung beteiligt sind (vgl. Abbildung 8-3). Die *Informatikabteilung* verwaltet die Mehrheit der technischen Informationssysteme (IT-Systeme) für die *Fachabteilungen*, welche diese IT-Systeme für ihre inhaltliche Informationsverarbeitung nutzen. In vielen Unternehmungen beauftragt die *Geschäftsleitung* die Informatikabteilung, sich mit Informatik-Sicherheit zu beschäftigen und diese zu erreichen, also ein sicheres IT-System aufzubauen bzw. das bestehende System zu sichern. Es ist für die Informatikabteilung jedoch unmöglich, Informationssicherheit in *eigener* Regie zu erreichen. Einerseits betreibt die Informatikabteilung ihre Systeme nicht für sich selbst, sondern für die Fachabteilungen. Entsprechend müssen die Sicherheitsanforderungen in den Fachabteilungen erhoben werden. Auch wenn dies geschieht, so sind die Sicherheitsanforderungen oft nicht genau genug spezifiziert (z.B. aufgrund technischer Unkenntnis und fehlender Vermittlung) und deshalb nicht direkt operationalisierbar.

Rein technische Betrachtungen können beispielsweise dazu führen, dass aus technischer Sicht sinnvolle Einschränkungen vorgenommen werden – z.B. Verhinderung oder Einschränkung eines direkten Internet-Zugangs, Beschränkung von Zugriffszeiten etc. – welche in den Fachabteilungen auf Unverständnis stossen und nicht akzeptiert werden. Ebenso ist es möglich, dass inhaltlich notwendige Sicherungen nicht geschehen – z.B. der spezielle Schutz von Personaldaten – weil die Informatikabteilung diese Notwendigkeit nicht selbständig erkennt. Es ist also wichtig, dass der Anstoss zur Untersuchung der Informationssicherheit von den Fachabteilungen ausgeht.

Zum Austausch der Sicherheitsanforderungen bestimmen Fachabteilungen und Informatikabteilung jeweils einen *Ansprechpartner*. Es ist prinzipiell offen, ob die Fachabteilungen gesamthaft *einen* Ansprechpartner bestimmen, der dann seinerseits die Aufteilung der entstehenden Arbeiten innerhalb der Fachabteilungen organisiert oder *jede* Abteilung einen eigenen Ansprechpartner ernennt. Diese Ansprechpartner müssen die Anforderungen dann gemeinsam operationalisierbar formulieren. Dabei vertreten die Ansprechpartner der Fachabteilungen alle Info-Owner und Benutzer ihrer Abteilung.

---

90 In der Folge und im Anhang C werden die in Klammern angegebenen Abkürzungen verwendet, um v.a. in den Tabellen eine effiziente Darstellung zu erreichen.

Damit die notwendigen Gespräche nicht an unterschiedlichem Verständnis scheitern – schliesslich sind die Fachabteilungen nicht an technischen Details interessiert und die Informatiker oft nicht an der geschäftlichen Bedeutung der Informationen – ist es Aufgabe des *Koordinators,* den Dialog vorzubereiten und zwischen beiden Parteien zu vermitteln. Es ist vorteilhaft, wenn dieser Koordinator sowohl die geschäftlichen Tätigkeiten beurteilen kann wie auch grundlegendes Wissen im Informatikbereich mitbringt. Dies hilft ihm, von allen Ansprechpartnern als kompetenter Gesprächspartner akzeptiert zu werden. Im Zweifelsfalle sollte der Koordinator näher bei den Fachbereichen als bei der Informatik stehen. Es ist auch möglich, dass der Koordinator einer der Ansprechpartner der Fachbereiche ist (Personalunion). Von einer Personalunion von Koordinator und *Verwalter* wird jedoch dringend abgeraten, da dann eine technikzentrierter Blickwinkel entstehen kann, der vermieden werden soll.

Der Koordinator ist dafür *verantwortlich, dass das Verfahren durchgeführt wird* und die einzelnen Aktivitäten stattfinden. Es ist *jedoch nicht für das Resultat* des Verfahrens verantwortlich. Die Verantwortung für die Sicherheit der schützenswerten Objekte liegt im Management und ist Teil der Verantwortung für die unternehmerischen Teilbereiche.

Um das Projekt zum Erfolg zu führen, ist es ausserdem sinnvoll, *Sponsoren* zu finden. Dies sind Personen, welche ein besonderes Interesse an den Zielen der Informationssicherheit in der Unternehmung haben, beispielsweise der Datenschutzbeauftragte des Unternehmens, ein IT-Sicherheits*verantwortlicher*, oder Personen mit Qualitätsmanagement-Aufgaben. Die Unterstützung dieser Personen kann auch deshalb sinnvoll sein, weil sie über Hintergrund-Informationen über die Unternehmung verfügen oder weil sie zusätzliche Ressourcen bereitstellen können. Sponsoren sind jedoch am Projektablauf nicht direkt beteiligt, es sei denn, dass sie ausserdem noch eine der anderen Rollen einnehmen.

In Einzelfällen ist es darüber hinaus sinnvoll, weitere, unabhängige Ansprechpartner zur Verfügung zu haben, welche Stellungnahmen zu einzelnen Sicherheitsfragen abgeben können, unabhängig beobachten können und den Koordinator bei der Vorbereitung der Berichterstattung an die Geschäftsleitung unterstützen (*unabhängige Berater).*

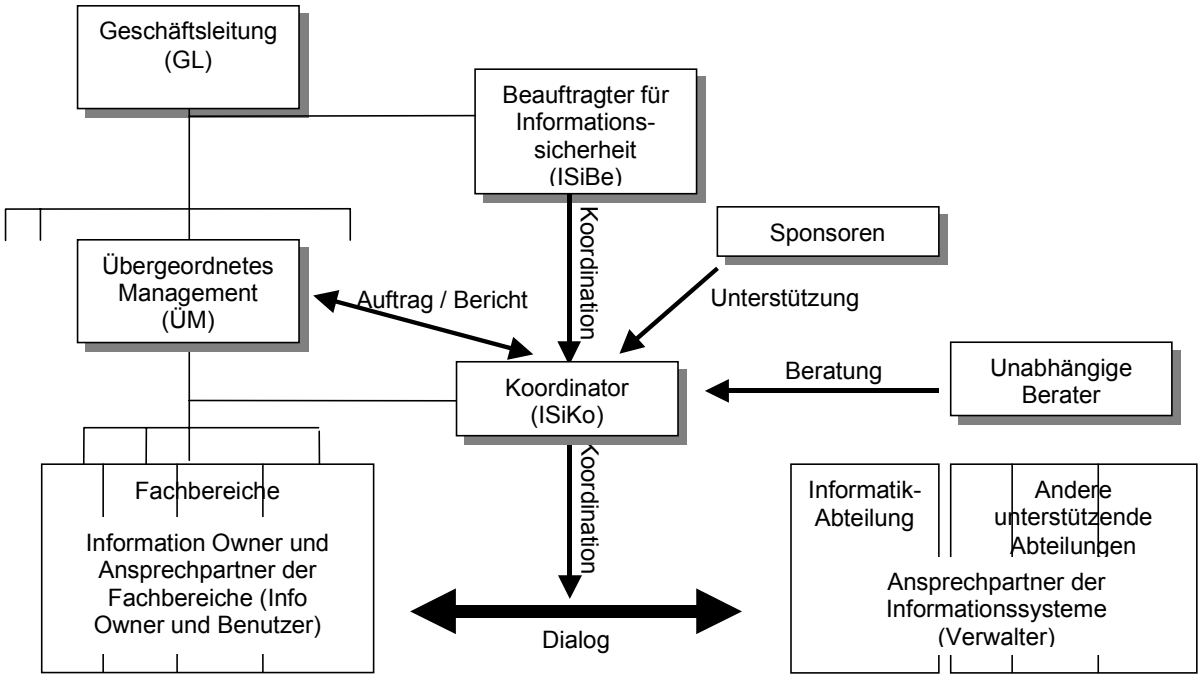


Abbildung 8-3: Zusammenarbeit der Rollen

8.4 Projekt

Verantwortung für ISiWAY

Das Verfahren *ISiWAY* ist für eine möglichst dezentrale Durchführung ausgelegt. Dies äussert sich einerseits dadurch, dass den Mitarbeitern, welche die *inhaltliche Informationsverarbeitung* durchführen, direkt und persönlich die Verantwortung für die Informationssicherheit der von ihnen verarbeiteten Informationen zugeteilt wird, und nicht eine zentrale Institution zum Träger der Verantwortung gemacht wird. Zum Zweiten werden die hier angegebenen Aktivitäten und Massnahmen als Vorschläge formuliert, so dass die Betroffenen freie Hand haben, wie sie die vom übergeordneten Management festgelegten Ziele erfüllen möchten. *ISiWAY* versteht sich als Leitfaden und Richtlinie. Wenn das übergeordnete Management zur Vereinheitlichung des Vorgehens – und damit zur Erzeugung vergleichbarer Resultate – eine Verabschiedung von *ISiWAY* in Form einer Umsetzungsvorschrift beschliesst, so lässt dies den Betroffenen weiterhin freie Hand in der konkreten Ausgestaltung der Massnahmen.

ISiWAY wird idealerweise von der hierarchisch obersten Institution innerhalb der Unternehmung zur Umsetzung empfohlen oder angeordnet. Dies führt dann mit dem Durchlaufen der verschiedenen DGs nach und nach zur einheitlichen Umsetzung der Sicherheitsanforderungen innerhalb der Unternehmung.

Doch auch eine einzelne untergeordnete Einheit innerhalb einer Unternehmung kann *ISiWAY* ausführen. Auch wenn dadurch eine Einschränkung auf ein konkretes,

im Vergleich zur Gesamtunternehmung kleines Bezugsobjekt besteht, so gelingt die Synchronisation mit den übergeordneten Sicherheitsanstrengungen in den meisten Fällen dennoch. Viele Unternehmungen legen im Rahmen einer Sicherheitspolitik oder eines „Code of Practice“[91] Anweisungen zur Umsetzung von Sicherheitsmassnahmen für den internen Gebrauch fest. Diese können als der (normalerweise in DG0 entwickelte) Massnahmenkatalog angesehen werden. Darüber hinaus ermöglicht *ISIWAY* jedoch ein Controlling, welches übergeordnete Sicherheitspolitiken meist nicht bieten.

Für einen föderalistischen bzw. subsidiären Einsatz ist *ISIWAY* ebenfalls geeignet, da es sowohl die übergeordneten Funktionen zur Bildung neuer Teilprozesse für abgegrenzte Teilobjekte als auch die Übermittlung von Resultaten (Reporting) an eine übergeordnete Institution erlaubt.

Projektorganisation

Das Verfahren *ISIWAY* wird innerhalb einer Unternehmung als Projekt organisiert und durchgeführt. Dabei wird strukturiert vorgegangen, um eine improvisierte Problembetrachtung bzw. Lösungsherleitung zu vermeiden (vgl. "Ad-hoc-Ansatz" in Abschnitt 6.4). Dieses Projekt beginnt mit dem Durchlaufen von DG0 des *ISiWay-Prozesses* und endet mit dem Durchlaufen von DG4.

In Abbildung 8-1 ist erkennbar, dass von jedem Zyklus aus die Möglichkeit besteht, in den darüberliegenden Zyklus zu wechseln, oder aber denselben Zyklus nochmals zu durchlaufen. Ersteres ist sinnvoll, wenn alle Aufgaben und Ziele des unteren Detaillierungsgrades erledigt bzw. erreicht wurden. Falls dies nicht geschehen konnte, ist eine Wiederholung desselben Zyklus möglich.

Projekthierarchie

Weiterhin bietet *ISIWAY* die Möglichkeit, *untergeordnete* Teilprojekte auszulösen, die dann in parallel in unterschiedlichen Abteilungen der Unternehmung ablaufen oder unterschiedliche inhaltliche Fragestellungen untersuchen. Die Koordination dieser Teilprojekte geschieht aber zentral, weshalb immer von *einem* Gesamtprojekt gesprochen wird.

Der oberste Projektleiter führt dazu eine erste Gliederung des Betrachtungsobjektes durch. Dies ist i.d.R. die Gesamtunternehmung, welche anhand der bestehenden Organisationsstruktur (nach Funktionen, Regionen etc.) aufgeteilt werden kann. Jeder Teil dieses Bezugsobjektes bildet ein Unterprojekt, welches von der untergeordneten Stelle wieder strukturiert und delegiert werden kann; es entsteht also eine hierarchische Gliederung des Betrachtungsobjekts und eine

---

91 „Code of Practice“ wird hier als allgemeine Bezeichnung für einen Typ von Weisung verwendet und bezieht sich nicht auf die Publikation [BSI-COP95].

dazugehörende Projekthierarchie, welche der Hierarchie der Organisation entsprechen kann und der jeweiligen Aufgabe angepasst ist. Mehrere Unterprojekte können parallel laufen, der jeweils direkt übergeordnete Projektleiter koordiniert den allenfalls notwendigen Informationsaustausch.

Jedes der Teilprojekte folgt dem Aufbau eines der *ISIWAY*-Detaillierungsgrade (DGs).

Abbildung 8-1, (Seite 221) stellt die Detaillierungsgrade 0 bis 4 von *ISIWAY* dar. In dieser Vollständigkeit präsentiert es sich jedoch nur dem Informationssicherheits-beauftragten (ISiBe) der Unternehmung, welcher als oberster Projektleiter agieren sollte. Dieser führt die Tätigkeiten allerdings nicht alle selbst aus, sondern übergibt nach einer anfänglichen Aufteilung des Betrachtungsobjekts in mehrere Teilobjekte die jeweilige Kontrolle einem lokalen (d.h. betrachtungsobjektspezifischen) Koordinator für Informationssicherheit (ISiKo). Der ISiBe koordiniert dann die Tätigkeiten der einzelnen ISiKos, in dem er den Informationsaustausch zwischen den Teilprojekten fördert und regelt. Der Gesamtprozess wird also in verschiedene Unterprozesse aufgeteilt.

Es entstehen so mehrere Sicherheitsprozesse in der Unternehmung, welche alle demselben *ISIWAY*-Aufbau folgen, und jeweils durch zwei Variablen charakterisiert sind:

- Die *Breite* eines Teilprojekt wird durch seine Abgrenzung zu anderen Teilprojekten bestimmt (es bezieht sich immer nur auf einen Teilbereich der Unternehmung) sowie durch die Anzahl der Attribute (Eigenschaften der betrachteten Objekte), welche berücksichtigt werden.
- Die *Tiefe* ist einerseits durch den Detaillierungsgrad bestimmt, andererseits aber individuell durch die Präferenzen und Interessen der jeweiligen Projektleiter.

Abbildung 8-4 zeigt diese Projekthierarchie beispielhaft. Der ISiBe befindet sich im Detaillierungsgrad 0, von wo aus er die Auslösung untergeordneter Projekte steuert und diese während ihrer Laufzeit unterstützt. Er betreut ein Projekt im Personalbereich, welches gerade den Detaillierungsgrad 2 durchläuft (angepasste Sicherheit), eines im Bereich Produktion, welches Detaillierungsgrad 1 bearbeitet (minimale Sicherheit) und ein weiteres im Bereich Verkauf, welches schon Detaillierungsgrad 4 erreicht hat. Jedes dieser Teilprojekte wird von einem Koordinator für Informationssicherheit (ISiKo) aus dem jeweiligen Bereich geleitet.

Im Bereich Verkauf hat der dortige Projektleiter wieder zwei Teilprojekte ausgelöst: eines, welches sich mit rechtlichen Aspekten der Informationsverarbeitung im Verkauf beschäftigt (denkbar etwa sind Datenschutzfragen) und eines, welches die Pflege der Kundendaten betrachtet (denkbar: Sicherstellen der Übereinstimmung zwischen Eigenschaften der Personen und ihrer Beschreibung durch Daten, sog. Kongruenz).

Jedes der Teilprojekte endet nach Durchlaufen aller Phasen. Die Ergebnisse werden dann durch das Team des übergeordneten Projektes kontrolliert. Wenn notwendig, kann der jeweils übergeordnete Projektleiter veranlassen, dass derselbe Zyklus nochmals durchlaufen wird (also z.B. erneut DG2 im Personalbereich), oder in den darüberliegenden Zyklus gewechselt wird (also z.B. DG2 in der Produktion), oder er kann Betrachtungsobjekt und Zielsetzungen neu festlegen.

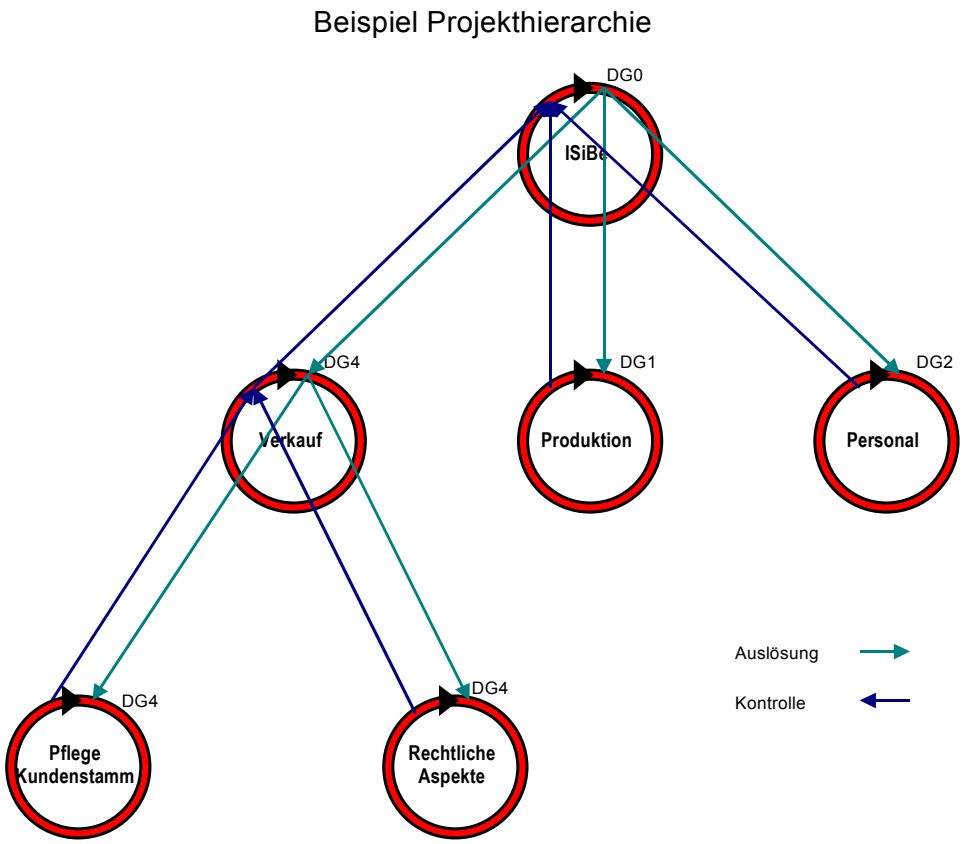


Abbildung 8-4: *ISIWAY*-Projekthierarchie

Status der Teilprojekte

Jedes Teilprojekt befindet sich zu jedem Zeitpunkt in einem definierten Zustand, welcher durch die ausgeführte Aktivität innerhalb der aktuellen Projektphase definiert ist. Innerhalb einer Phase ist die Parallelisierung verschiedener Aufgaben i.d.R. nicht möglich, da nachfolgende Phasen von den Ergebnissen der jeweils vorhergehenden Phasen abhängig sind.

Der erreichte Sicherheitszustand kann für jedes Unterprojekt als Resultat des letzten vollständig durchlaufenen DGs angegeben werden.

Dauer

Die Zeitdauer, welche für das Durchlaufen eines Zyklus notwendig ist, hängt stark von der Priorität des Projektes in der Unternehmung ab. Wie in Abschnitt 6.7 dargelegt wurde, ist der Aufwand für die Umsetzung der Informationssicherheit von der in der Unternehmung bestehenden *Motivation* abhängig, von der *Qualität des Informationsmanagements*, von der *Komplexität des Informationssystems* sowie der *Klarheit der* an das IS gestellten *Anforderungen*. Diese vier Rahmenbedingungen können zwischen Unternehmungen stark variieren, so dass *keine* konkrete Aussage über den Aufwand eines Projektes nach *ISIWAY* abgegeben werden kann. Allerdings ist es möglich, den aus konkret festgelegten Rahmenbedingungen folgenden Aufwand auf verschiedene Weise über einen Zeitraum zu verteilen, indem der Durchführung von *ISIWAY* die entsprechende Priorität eingeräumt wird.

Kopplung mit periodischen Abläufen in der Unternehmung

Die Dauer eines *ISIWAY*-Projektes kann an die Dauer parallel stattfindender Projekte bzw. anderweitig ablaufender wichtiger unternehmerischer Zyklen angepasst werden. Beispielsweise wird in vielen Unternehmungen die strategische und taktische Ausrichtung des Informationsmanagements jährlich überprüft. Ebenfalls finden Investitions- und Beschaffungsplanung (und die damit verbundene Kosten- bzw. Budgetplanung) sowie finanzielle Konsolidierungen oft im jährlichen Rhythmus statt. Auch die Tätigkeiten der internen und externen Revision werden oft auf Jahresbasis geplant und durchgeführt. Diese Faktoren sprechen dafür, auch für *ISIWAY* einen jährlichen Turnus als Basis für die Durchführung der einzelnen Zyklen festzulegen.

Dies kann bedeuten, dass die Durchführung eines Zyklus über ein Jahr verteilt wird, indem die Meilensteine (als Abschluss bzw. Beginn der einzelnen Phasen) angemessen verteilt werden und dem Projekt eine entsprechende Priorität zugeordnet wird. Es kann auch bedeuten, dass ein Zyklus einmal jährlich (z.B. in den Sommermonaten) so schnell wie möglich durchlaufen wird.

Wird ein Jahr als Basis für die Dauer eines Zyklus festgelegt, so werden vier Jahre benötigt, um den vierten Detaillierungsgrad von *ISIWAY* zu erreichen. Das scheint auf den ersten Blick sehr lange. Wenn man jedoch bedenkt, dass gerade in grossen Unternehmungen mit komplexer Infrastruktur schon die konsequente Einführung eines minimalen Sicherheitsniveaus (sog. Grundschutz) einen hohen Aufwand bedeuten kann, und dass gerade in grossen Unternehmungen Informationssicherheit als langfristige Aufgabe betrachtet wird, so kann die Möglichkeit einer von Jahr zu Jahr zunehmenden Vertiefung als Potential von *ISIWAY* gewertet werden.

Projektbezogener Einsatz von ISIWAY

ISIWAY eignet sich ebenfalls für den Einsatz in Projekten, welche sich nicht zentral mit Informationssicherheit beschäftigen. Beispielsweise können die Einführung einer neuen Software, die Erstellung eines Produktes oder die Reorganisation interner Abläufe als Projekte innerhalb der Unternehmung ablaufen. Dabei können Sicherheitsfragen auftauchen. Der Einsatz von *ISIWAY* geschieht dann vollkommen analog: Der Bezugsrahmen des Projektes bildet die Abgrenzung der Breite des *ISIWAY*-Teilprojektes.

Beispiel: Die Unternehmung entwickelt ein Produkt für ein Umfeld, in welchem besondere Sicherheitsanforderungen gelten. Die Projektleitung bestimmt (allenfalls in Zusammenarbeit mit dem ISiBe der Unternehmung) einen Sicherheits-koordinator für das Projekt. Dieser wird idealerweise direkt dem Projektleiter unterstellt und sorgt innerhalb des Projektes dafür, dass Sicherheitsfragen behandelt werden. Die Verantwortung für die Sicherheit bleibt beim Projektleiter. Die einzelnen Zyklen (minimaler Schutz, angepasster Schutz etc.) können ebenfalls analog durchgeführt werden, sobald die einzelnen Komponenten des zu erstellenden Produktes und die damit zu verwaltenden Informationen bekannt sind (dies folgt aus der Spezifikation des Produkts).

Im allgemeinen können die Zyklen von *ISIWAY* direkt mit den Projektphasen eines Systemerstellungs- und Einführungsprojektes gekoppelt werden. Es soll hier angenommen werden, ein derartiges Projekt setze sich aus den Phasen *Projektumriss, Konzept, Detailspezifikation, Systemtest* und *Einführung* zusammen [vgl. Zehnder91, S. 24ff].

Während sich der Detaillierungsgrad 0 (Vorbereitungen) gut mit der Projektumrissphase verbinden lässt (es werden v.a. die Rahmenbedingungen für die Informationssicherheit festgelegt), fällt die Definition und Erreichung der minimalen Informationssicherheit (Detaillierungsgrad 1) mit der Erstellung des Konzeptes zusammen. So können allgemeine Sicherheitsüberlegungen schon vor Beginn der Implementationsarbeiten einfliessen.

Die angepasste Informationssicherheit (Detaillierungsgrad 2) beruht auf der Zuteilung von Werten zu einzelnen Informationsobjekten. Da die Festlegung dieser Objekte Teil der Detailspezifikation eines Informatik-Projektes ist, funktioniert die Koppelung auch in dieser Phase.

Der Systemtest fällt mit der Betrachtung der risikogerechten Informations-sicherheit (Detaillierungsgrad 3) zusammen. Da es Ziel des Systemtests ist, die „korrekte Funktionsfähigkeit der zukünftigen Anwendung“ nachzuweisen und Fehler zu erkennen und zu eliminieren [Zehnder91, S. 119], lässt sich diese Projektphase gut mit der spezifischen Betrachtung einiger besonderer Projektrisiken verbinden. Die dabei gewonnenen Erkenntnisse können als „Sicherheitsfehler“ des Systems betrachtet werden und somit wie die anderen erkannten Probleme korrigiert werden.

Schliesslich fällt die Phase Einführung mit dem Detaillierungsgrad 4 (Umfassende Informationssicherheit) von *ISIWAY* zusammen. Hier sollen spezifische Inhalte vertieft betrachtet werden, was durch die in der Einführung entstehenden Probleme ausgelöst werden kann.

Die Kopplung einer *ISIWAY*-Durchführung an die Phasen eines Systemerstellungsprojektes ist also möglich. *ISIWAY* kann dabei als Teil der projektbezogenen Qualitätssicherungsarbeiten oder als zusätzliche parallele Tätigkeit betrachtet werden.

Während des Betriebes des Systems kann Detaillierungsgrad 4 von *ISIWAY* wiederholt durchlaufen werden, um so stets aufs Neue die Informationssicherheit des Systems zu gewährleisten.

Durchführung mit maximaler Geschwindigkeit

Es ist möglich, die einzelnen Detaillierungsgrade von *ISIWAY* so schnell wie möglich zu durchlaufen. Dies kann angebracht sein, wenn eine dedizierte Person oder Personengruppe damit beauftragt wird, umfassende Informationssicherheit in einer Unternehmung (oder bezogen auf einen Teil davon oder auf ein konkretes Produkt) so schnell wie möglich zu erreichen. Dabei muss allerdings bedacht werden, dass gerade die Etablierung von Institutionen, die Erarbeitung gemeinsamer Ziele (Informationssicherheitspolitik und –strategie) oder die Förderung des sicheren Verhaltens nicht nur Aufwand benötigen, sondern an die Struktur und Kultur der Unternehmung angepasst werden müssen. Die möglicherweise notwendigen tiefgreifenden Veränderungen benötigen Zeit, welche die maximale Geschwindigkeit der *ISIWAY*-Durchführung senkt.

Controlling

Der Informationssicherheitsbeauftragte (ISiBe) der Unternehmung ist der übergeordnete Controller des gesamten Projektes. Durch die starke Unterteilung der Aufgaben in die verschiedenen Teilprojekte der einzelnen Verantwortlichen ist es dem ISiBe nicht möglich, jederzeit alle einzelnen Aktivitäten zu überwachen. Dies ist auch nicht angestrebt. Es führt allerdings dazu, dass neben dem Hauptprozess, den der ISiBe steuert, viele Teilprozesse ablaufen, die demselben Muster folgen. Die Teilprozesse können auf demselben Detaillierungsgrad stattfinden und unterscheiden sich durch die Person des Durchführenden durch seine Rolle, oder durch das Bezugsobjekt. So kann ein Verantwortlicher in seinem eigenen Bereich durchaus mehrere parallele Prozesse initiieren, mehrere Koordinatoren bestimmen etc. wenn dies aufgrund geographischer Trennung oder der Unterschiedlichkeit der Prozesse angemessen ist. Dies hat dann jeweils die Trennung der jeweiligen Bezugsobjekte (Abgrenzung untereinander) zur Folge. Es ist auch möglich, dass verschiedene inhaltliche Bereiche in DG4 parallel betrachtet werden, dass es sich bei mehreren dieser Prozesse jedoch um unterschiedliche

Betrachtungsobjekte und / oder Inhalte handelt, z.B. die Untersuchung von Versicherungsmöglichkeiten der Informationsrisiken eines Bereiches, oder die parallele Untersuchung der Sicherheit beim Outsourcing. Der Informationssicherheitsbeauftragte der Unternehmung könnte also auch als Information Security Controller bezeichnet werden.

Der Verantwortliche für ein Teilobjekt ist auch Controller des jeweiligen Teilprozesses oder bestimmt einen ihm direkt untergeordneten Koordinator, mit welchem er sich Management- und Controlling-Aufgaben teilt. Der Controller gibt die Informationen über seinen Teilprozess jeweils an den Controller des übergeordneten Prozesses weiter. Dieses Controlling wird durch einen regen Informationsaustausch zwischen den einzelnen Teilprozessen und dem übergeordneten Prozess vereinfacht. Wenn in einem Teilprozess aufgrund politischer oder anders motivierter Autonomiebestrebungen jedoch beschlossen werden sollte, kein Controlling zuzulassen, agiert der übergeordnete Controller lediglich als (zu diesem Projektes externe) Revisionsstelle und führt nach abgeschlossener Selbstkontrolle des Unterprojektes eine Revision (Audit) durch.

Darüber hinaus geschieht eine laufende Zielerreichungskontrolle durch den jeweiligen Controller des untersuchten Objektes sowie die Leitung des Gesamtprozesses. Die abschliessende oder sporadische Kontrolle geschieht durch prozessunabhängige Stellen. Zusätzlich umfasst jeder Detaillierungsgrad ein Review und allenfalls ein Neuauslösen (Respawn) der Aktivitäten desselben oder darunterliegenden Detaillierungsgrades.

Die Kommunikation zwischen diesen Teilprozessen und dem Hauptprozess geschieht, indem für die erstellten Dokumente eine einheitliche Form festgelegt wird. Die übergebenen Daten haben

- qualitative Inhalte, d.h. ein Teilprozess gibt Beschreibungen des Ablaufes und der Ergebnisse zurück,
- quantitative Inhalte, d.h. ein Teilprozess gibt konkrete Untersuchungsresultate zurück. Diese können
  - detailliert sein. Dafür spricht, dass der übergeordnete Prozess eine vollständige Kontrolle über die durchlaufenen Aufgaben und Inhalte erhält. Entsprechend gut kann er seine Argumentation bei direkter Einflussnahme oder im Rahmen des übergeordneten Reporting vorbereiten. Nachteil ist der Transfer von Informationen mit potentiell hohen Vertraulichkeitsanforderungen,
  - summarisch sein. Dafür spricht, dass die Steuerung so effektiv auf der Ebene des Teilprozesses belassen wird und dass nur die Kennzahlen des Teilprozesses übermittelt werden. Dies sollte jedoch von qualitativen Aussagen begleitet werden.

Der ISiBe kann beim Dialog unterstützen. Dabei muss er als Moderator auftreten, d.h. er darf selbst keine eigene Meinung vertreten, sondern muss versuchen, die Argumente der beteiligten Parteien zu ordnen und einen Konsens herbeizuführen.

Er darf allerdings Fachwissen einfliessen lassen, jedoch nur so, dass daraus nicht implizit schon eine der vorhandenen Meinungen unterstützt wird. Der Moderator sollte Zurückhaltung üben, um sich nicht durch einseitige Meinungsunterstützung für die andere Seite unglaubwürdig zu machen.

Obwohl er in den Prozess des Sicherheitsmanagements involviert ist, muss er in dieser Stellung nicht unbedingt der Unternehmung angehören. Die Aktionen des Sicherheitsmanagements sind zwar prinzipiell in die Arbeitsabläufe jedes einzelnen Mitarbeiters integriert, gesamthaft ist die Steuerung des Informationssicherheits-prozesses jedoch unabhängig von der konkreten Informationsverarbeitung möglich.

Werkzeugunterstützung

Der formalisierte Ablauf von *ISIWAY* erlaubt den Einsatz eines computer-unterstützten Werkzeuges, welches als Steuerungs- und Dokumentationsmittel dienen kann. Ein solches Tool namens *ISIGO* ist in Kapitel 9 spezifiziert. Im Einzelnen kann ein solches Werkzeug

- Ein- und Ausgabeformulare zur Generierung der Ergebnisse jedes einzelnen Schrittes von *ISIWAY* umfassen, da die Form dieser Ein- und Ausgaben genau spezifiziert sein kann,
- Steuerungsinformationen wie die nächsten notwendigen Aktionen oder Informations- oder Koordinationsbedarf anzeigen, weil die einzelnen Schritte formell genau spezifiziert sind und sich durch den Inhalt der Eingabe-parameter bestimmen lassen.

Effektives übergeordnetes prozessintegriertes Controlling ist nur durch intensiven Informationsaustausch möglich. Auch dies kann durch ein Werkzeug unterstützt werden, indem die notwendigen Schnittstellen innerhalb des Werkzeugs so geschaffen werden, dass verschiedene Instanzen verschiedener Teilprozesse miteinander kommunizieren können

Zertifizierung

Aufgrund der in *ISIWAY* generierten Informationen über Ziel und Stand der Umsetzung bzw. Erreichungsgrad können externe Anforderungen nach Vergleichbarkeit nur durch Erstellung eines übersetzenden Massnahmenkataloges erreicht werden. Das bedeutet, dass eine Zertifizierung einzelner Teilbereiche der Unternehmung durch *ISIWAY* ermöglicht wird.

Ideal ist die einheitliche Verwendung dieses Verfahrens in der gesamten Unternehmung, weil dadurch vergleichbare Ergebnisse und Vorteile in der Ausbildung der Personen (und so letztendlich in der Akzeptanz) erreicht werden.

8.5 Evaluation von *ISIWAY*

Abschliessend soll das hier definierte Verfahren *ISIWAY* mit dem Schema bewertet werden, welches in Kapitel 7 entwickelt und verwendet wurde. Dabei interessiert insbesondere, ob und wie *ISIWAY* die in Kapitel 7 formulierten (und in Anhang B.7, Tabelle B-7 wiedergegebenen) Anforderungen erfüllen konnte.

Die detaillierte Bewertung von *ISIWAY* ist in Anhang B.8, Tabelle B-8 wiedergegeben. Hier werden einzelne wichtige Punkte herausgehoben sowie daraus eine Beurteilung abgeleitet.

Bewertung

Grundsätzlich zeigt die Bewertung von *ISIWAY*, dass auf die wesentlichen Anforderungen gemäss Anhang B.7 eingegangen wurde, und diese weitgehend erfüllt werden konnten. Teilweise bestehen leichte Abweichungen.

Im Bereich Auslösung wurden die Anforderungen vollständig erreicht. Der Bereich Organisation übertrifft die Anforderungen zum Teil sogar leicht, so bei den Aussagen über die Dauer des Bestehens des Projektteams, bei der Abgrenzung von Breite und Tiefe der Untersuchung, bei der Kontrolle und der Korrektur der Projektdauer. Gesamthaft erreicht *ISIWAY* hier beinahe die Maximalbewertung.

Im Bereich Durchführung können gesamthaft nur leicht tiefere Werte vergeben werden als in den Anforderungen verlangt. Die Verweise auf andere Verfahren konnten (und sollten auch) nicht vollständig in *ISIWAY* integriert werden, und die Ergebniserarbeitung und -darstellung steht aufgrund der von *ISIWAY* angestrebten Breite etwas hinter den Forderungen zurück. Aufgrund des Umfangs und der Integration in diese Dissertation ist *ISIWAY* jedoch nicht so leicht erlernbar wie gefordert. Das Werkzeug *ISIGO* hingegen, welches im folgenden Kapitel definiert wird, erfüllt die daran gestellten Anforderungen.

Bei den Fachbereichen schliesslich fällt die Bewertung wieder höher aus als die Anforderungen. Zwar musste die Prozessbetrachtung etwas vernachlässigt werden, jedoch ist die Breite der Betrachtung und Beeinflussung von *ISIWAY* durch die Integration, den föderalistischen Aufbau und die Möglichkeit einer detaillierten Untersuchung deutlich höher als ursprünglich gefordert.

Beurteilung

ISIWAY hat die Mehrheit der aufgestellten Anforderungen erfüllt, bleibt jedoch in einzelnen Punkten leicht hinter den Erwartungen zurück. Insbesondere die Erlernbarkeit des Verfahrens ist nicht so einfach wie angestrebt, wodurch die Durchführung leicht tiefer bewertet wird. Auch bei Organisation und Fachbereichen werden höhere Werte erreicht. Hier profitiert *ISIWAY* von der Integration in die Gesamtbetrachtung dieser Dissertation.

Gesamthaft ist *ISIWAY* ein Verfahren, dass sich zur Durchführung von Informationssicherheitsprojekten eignet und die Anforderungen aus Kapitel 7 weitgehend erfüllt.

ISIWAY im Vergleich

Mit *ISIWAY* ist ein Verfahren entstanden, welches im Vergleich mit den anderen Verfahren in allen Bereichen relativ hoch bewertet wurde. Im Bereich Auslösung liegt *ISIWAY* zwar nur an Platz 2 der betrachteten Verfahren, erfüllt hier aber die Anforderungen, die daran gestellt wurden. In den anderen Bewertungen erreicht *ISIWAY* die höchste Bewertung der betrachteten Verfahren.[92]

Gesamthaft betrachtet ist *ISIWAY* jedoch sehr viel spezifischer und konkreter in der Beschreibung der einzelnen Aktivitäten und der Koordination des Verfahrens, als dies die anderen Verfahren sind. Auch wenn dies bei den anderen Verfahren nicht so notwendig erscheint, da sie sich allesamt an Fachleute der Informatik und Informationssicherheit richten, so ist es doch für *ISIWAY* um so wichtiger: *ISIWAY* richtet sich an die Sachbearbeiter innerhalb der Unternehmung, welche nicht über besondere Vorkenntnisse in Informatik und Informationssicherheit verfügen müssen sollen, um *ISIWAY* anwenden zu können.

Die *Auslösung* der Untersuchung ist in *ISIWAY* einiges umfangreicher und detaillierter beschrieben als in den anderen betrachteten Verfahren. Auch wenn nicht im Detail auf den Zusammenhang neuer Softwareprojekte oder –produkte oder auf Änderungen im unternehmerischen Umfeld eingegangen wurde, hat *ISIWAY* die hohe Bewertung verdient, welche gefordert war.

Auch die *Organisation* ist sehr viel konkreter beschrieben als in anderen Verfahren, und zwar in allen Punkten, in denen dies in der Bewertung der Anforderung verlangt war. Insbesondere die Koordination und Kooperation sowie die Skalierung von Breite und Tiefe sind mit *ISIWAY* viel eher möglich als mit einem der anderen betrachteten Verfahren.

---

92 Daraus zu folgern, dass *ISIWAY* das objektiv in jedem Fall beste der betrachteten Verfahren ist, wäre voreilig. Wenngleich es Ziel des Autors war, alle relevanten Eigenschaften von Verfahren möglichst gut separiert zu beurteilen, sind sowohl Kriterienkatalog wie Bewertung subjektiv. Dies ist jedoch ein prinzipielles Problem einer Einzelbewertung.

Dafür entspricht die *Durchführung* nicht ganz den formulierten Anforderungen. Dies hängt aber v.a. damit zusammen, dass *ISIWAY* hier im Kontext einer Dissertation und nicht für sich alleine betrachtet wurde und sehr viel umfangreicher ist als die meisten der anderen betrachteten Verfahren. Darunter leidet die Erlernbarkeit und der Aufwand für die Einarbeitung. Die für die Verwendung in Kapitel 10 vorgesehene *zweite Konkretisierung* kann hier möglicherweise positiver bewertet werden.

Auch die *Beeinflussung des Untersuchungsobjektes* kann aufgrund der Integration von *ISIWAY* in die Dissertation nicht abschliessend bewertet werden, erfüllt aber die daran gestellten Anforderungen grösstenteils.

Mit *ISIWAY* wurde also ein Verfahren geschaffen, welches die Umsetzung von Informationssicherheit in Unternehmungen weitestgehend unterstützt und formal detailliert beschreibt und sich dadurch von den anderen betrachteten Verfahren deutlich abhebt.

ISIWAY 1.5

ISIWAY ist ein Gesamtkonzept, welches im Rahmen dieser Dissertation entwickelt und beschrieben wurde. Das hat zur Folge, dass zum Verständnis von *ISIWAY* grosse Teile dieser Dissertation gelesen werden müssen, denn in Kapitel 8 sind vielfältige Verweise auf andere Kapitel enthalten. Dies beeinträchtigt insbesondere die Erlernbarkeit von *ISIWAY* und ist mit ein Grund dafür, dass *ISIWAY* in dieser Anforderung (Teilvariable V3f1) tief bewertet wird.

Um das Ziel einer leichten Erlernbarkeit dennoch zu erreichen, wird in dieser Dissertation eine zusätzliche, im Umfang stark reduzierte Variante von *ISIWAY* definiert. Diese kann als einzelne Dokumentation in einem Projekt abgegeben werden und referenziert keine Inhalte dieser Dissertation.[93]

Zusätzlich soll das Verfahren sich als "Einstieg" in *ISIWAY* eignen. Es liegt also nahe, nicht die gesamte *ISIWAY*-Komplexität zu wiederholen, sondern nur die grundlegenden Teile: Detaillierungsgrade 0 (Vorbereitungen), 1 (Grundschutz) und 2 (angepasste Sicherheit). Um die Erlernbarkeit weiter zu fördern, wird zudem nur von einem einzigen Zyklus ausgegangen, welcher die Tätigkeiten der genannten drei integriert.

Das neue Verfahren wird *ISIWAY 1.5* genannt. Es umfasst die sogenannte *zweite Konkretisierung* des Informationssicherheitsprozesses, nachdem *ISIWAY* in Kapitel 8 die erste Konkretisierung darstellte. *ISIWAY 1.5* wird in Kapitel 10 beschrieben.

---

93 Daraus folgt, dass zu dieser Arbeit Redundanzen entstehen. Ebenso folgt daraus aber eine erleichterte Erlernbarkeit sowie ein deutlich geringerer Umfang.

Fazit

In Kapitel 8 wurde der Prozess der Informationssicherheit, welcher in Kapitel 6 generisch definiert wurde, erstmals konkretisiert. Dazu wurde ein Verfahren namens *ISIWAY* entworfen, welches aus verschiedenen Zyklen aufgebaut ist. Es erlaubt einen einfachen Einstieg, da der innerste Zyklus (Detaillierungsgrad 1) nur gerade die minimale Informationssicherheit abdeckt. Mit fortschreitender Betrachtungstiefe wird von jedem Zyklus in den nächsthöheren gewechselt, was jeweils eine Zunahme der Betrachtungsbreite und -tiefe zur Folge hat. Schliesslich führt dies am Ende zur umfassenden Betrachtung der Informationssicherheit.

Zusätzlich wurde ein Vorbereitungszyklus (Detaillierungsgrad 0) definiert, welcher sich spezifisch mit der Auslösung des Informationssicherheitsprozesses befasst. Ausserdem konnte das Krisenmanagement in einem Detaillierungsgrad 3.5 zusammengefasst werden.

ISIWAY wurde abschliessend mit demselben Schema bewertet, welches auch für die Bewertung der anderen Verfahren in Kapitel 7 verwendet wurde. Dabei zeigte sich, dass *ISIWAY* die weitaus meisten der daran gestellten Anforderungen zu erfüllen vermag. Weiterhin erhielt *ISIWAY* die höchste Bewertung von allen betrachteten Verfahren. Die mit der Definition von *ISIWAY* verbundenen Zielsetzungen wurden weitgehend erreicht. Es fehlt noch die Unterstützung mit einem computergestützten Hilfsmittel. Ein solches Werkzeug wird in Kapitel 9 entworfen und *ISIGO* genannt.

9 Prototyp *ISIGO*

ISIGO ist ein *internes Instrument* zu *ISIWAY* (vgl. Abschnitt 4.5). Es erlaubt die Verwaltung der informationssicherheitsrelevanten Inhalte (also die Beschreibung der Elemente des Bezugsobjekts) und führt den Benutzer darüber hinaus durch das Verfahren *ISIWAY*, indem es die Phasen und Tätigkeiten des Informationssicherheitsprozesses sowie die dazugehörenden Ziele, Aufgaben und Ergebnisse beschreibt.

In diesem Kapitel wird *ISIGO* zunächst *spezifiziert*, d.h. es wird beschrieben, welche Funktionen *ISIGO* zu erfüllen hat. Dabei werden zwei Varianten von *ISIGO* beschrieben: *ISIGO 1.5* und *ISIGO CENTRAL*. *ISIGO CENTRAL* beruht auf dem Konzept von *ISIWAY* und soll sich für den Einsatz beim Informationssicherheitsbeauftragten der Unternehmung eignen. *ISIGO 1.5* ist für den dezentralen Einsatz beim Koordinator für Informationssicherheit (ISiKo) gedacht, beruht auf dem Konzept vom in Kapitel 10 vorgestellten *ISIWAY 1.5* und ist deshalb weniger komplex.

Zu Beginn wird die grundsätzliche *Architektur* von *ISIGO* erläutert. Das Datenmodell wird anhand einzelner Entitäten erläutert, welche in den Zusammenhang von *ISIWAY* gestellt werden. Schliesslich werden jeweils die Anforderungen an die *Implementation* festgehalten und die konkrete, für *ISIGO 1.5* gewählte Implementation beschrieben und diskutiert.

9.1 Spezifikation

ISIGO soll als technisches Instrument die Durchführung von Informationssicherheitsmanagement gemäss *ISIWAY* unterstützen (sogenannte *Computer Aided Information Security*, CAIS). Dazu umfasst *ISIGO* mehrere Komponenten, welche sich einzeln für abgegrenzte Einsatzbereiche eignen, aber auch miteinander in Beziehung stehen und gesamthaft die von *ISIWAY* geforderte und in Kapitel 8 spezifizierte dezentrale / föderalistische Durchführung erlauben. *ISIWAY* ist von *ISIGO* unabhängig, d.h. dass *ISIWAY* auch ohne *ISIGO* durchgeführt werden kann. Jedoch bilden die in *ISIGO* implementierte Führung durch das Verfahren, die Verwaltung der erarbeiteten Zwischenresultate und das durch die konkrete Festlegung einheitliche Datenformat einen besonderen Anreiz zur Verwendung von *ISIGO*. *ISIGO* kann deshalb die Durchführung von *ISIWAY* erheblich erleichtern.

ISIGO wird in *Daten-* und *Funktions*komponenten unterteilt. Den *Daten*komponenten werden alle Inhalte zugeordnet, welche während der Durchführung von *ISIWAY* entstehen und verarbeitet werden (*Ergebnisdaten*) sowie *Steuerungsdaten* zu dieser Durchführung. Beide basieren auf *Stammdaten*. Die *Funktions*komponenten umfassen die *Steuerung* des Verfahrens selbst, die

Verwaltung der verarbeiteten Daten, die *Auswertung* und als spezielle Komponente die *Kommunikation*. Dabei wird jeweils zwischen problembezogenen Funktionen von *ISIGO* und den verwendeten Basisfunktionen der Anwendungsumgebung unterschieden.

Informationen und Daten[94]

Ergebnisdaten

Ergebnisdaten entstehen als Resultate der Durchführung der einzelnen Tätigkeiten von *ISIWAY*. Beispielsweise werden die erfassten Prozesse, Informationssammlungen und Informationssysteme, welche bei den einzelnen Beteiligten erhoben und bewertet werden, den Ergebnisdaten zugerechnet. Auch die Zuordnung von Massnahmen zu den schützenswerten Objekten ist Teil der Ergebnisdaten.

Steuerungsdaten

Steuerungsdaten des *ISIWAY*-Prozesses beeinflussen den Informationssicherheitsprozess selbst, wie z.B. die Bestimmung des Bezugsobjektes des aktuellen Projektes. Die Steuerungsdaten umfassen auch den aktuellen Projektzustand, die erledigten und offenen Arbeiten. Auch die Einordnung des Projektes in übergeordnete Projekte oder die Auslösung untergeordneter Projekte (Kommunikation nach oben und unten) wird in den Steuerdaten festgehalten.

Stammdaten

Stammdaten stellen die Grundlage für die Steuerung und Verwaltung von *ISIGO* dar, wie z.B. Firmen- und Adressdaten zur Identifikation der am Informationssicherheitsprozess teilnehmenden Parteien, Bewertungsformulare, Bewertungskriterien, Massnahmenkataloge etc. Grundsätzlich sind alle Daten, welche den Prozess nicht steuern und welche nicht im Rahmen des Durchlaufens des Prozesses erhoben werden, den Stammdaten zuzurechnen.

---

94 Prinzipiell werden gemäss Herleitung der Begriffe in Kapitel 2 in einem technischen System immer nur Daten, nie jedoch Informationen verwaltet. Der Informationsbegriff wird hier dennoch verwendet, um zu betonen, dass die verwalteten Steuerinformationen handlungsrelevant sind.

Funktionen

Steuerung

Die Steuerungsfunktion von *ISIGO* führt den Benutzer durch die einzelnen Schritte. Dazu werden Steuerungsdaten zur Anzeige von *informativen* (Ziele, Ergebnisse) oder *imperativen* Informationen (auszuführende Tätigkeiten) verwendet und die Erhebung und Erfassung der Ergebnisdaten und Stammdaten aus dem aktuellen Kontext heraus vorgeschlagen. Als optionale zentrale Steuerungsfunktion wird eine Funktionsauswahl definiert, welche das direkte Aufrufen der einzelnen Funktionen erlaubt, ohne auf den Kontext des Informationssicherheitsprozesses Rücksicht nehmen zu müssen.

Verwaltung

Die Verwaltungsfunktion erlaubt die Eingabe, Bearbeitung und Verknüpfung der Ergebnisdaten und der Stammdaten sowie die Darstellung und Ausgabe von formatierten Darstellungen dieser Daten.

Auswertung

Die Auswertungsfunktion ermöglicht die Erstellung von summarischen Informationen über Stand der Durchführung und dabei gewonnene Erkenntnisse. Dazu werden sowohl Steuerungsdaten als auch Ergebnisdaten zusammengefasst und zu Mittel- und Durchschnittswerten integriert.

Kommunikation

Die Kommunikationsfunktion umfasst v.a. die Synchronisationsfunktion zur Auslösung von Abgleichungsprozessen mit übergeordneten Projekten (*Synchronisation*) und zum Auslösen untergeordneter Projekte (*Respawn*)[95]. Dabei muss berücksichtigt werden, dass nicht notwendigerweise *alle* Informationen synchronisiert werden müssen. In vielen Fällen genügt die Weitergabe summarischer Informationen oder von Informationen über abteilungsübergreifende Ressourcen mit Notwendigkeit zur Kooperation.

---

[95] Die Aktivitäten Review, Respawn, Relaunch, Synchronisation, Report und Audit werden detailliert in der Behandlung von Phase 5 des Detaillierungsgrades 1 in Anhang C.1 beschrieben.

9.2 Architektur

Architektur von ISIGO

Die Architektur von *ISIGO* ist in Abbildung 9-1 dargestellt.

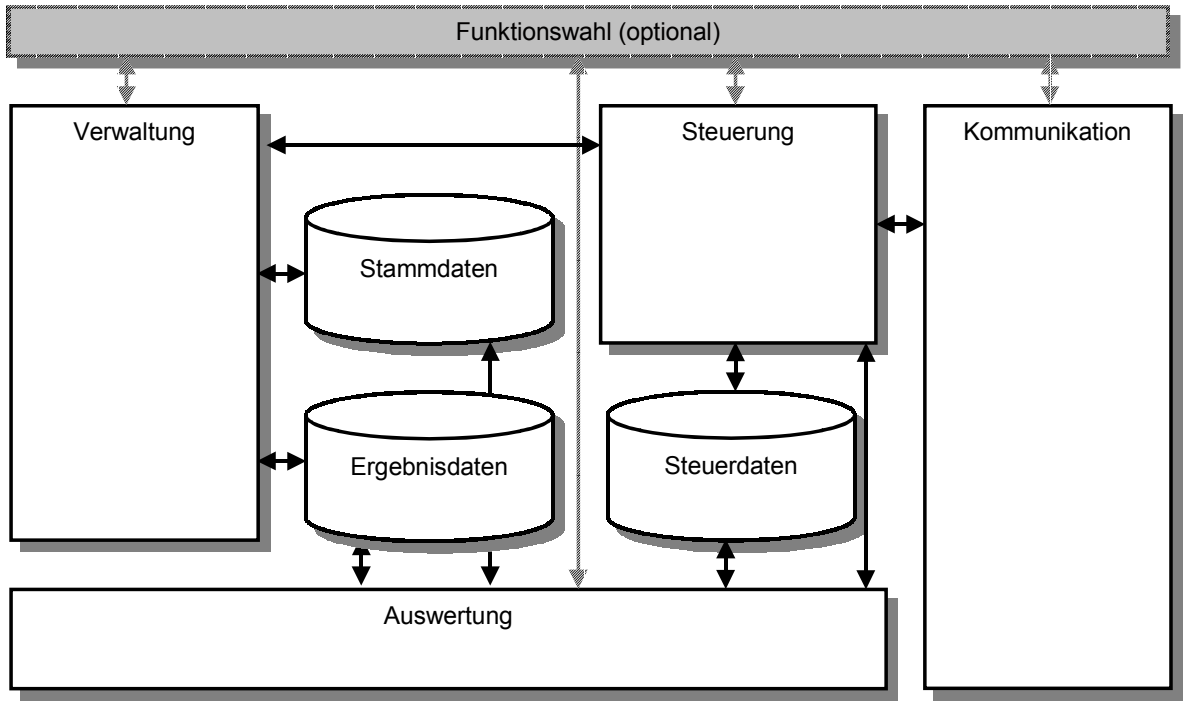


Abbildung 9-1: Blockdiagramm der *ISIGO*-Architektur

Der Einstieg in *ISIGO* findet über die *Steuerung* statt. Dort wird der Informationssicherheitsprozess gemäss *ISIWAY* dargestellt und die aktuelle Prozessphase mit den dabei entstehenden Tätigkeiten angezeigt. Die direkte Bearbeitung der Steuerdaten ist möglich, z.B. der Wechsel in die nachfolgende oder vorhergehende Aktivität oder Phase, aber auch der Sprung in nicht direkt sequentiell verbundene Phasen und Aktivitäten. Vorgesehen ist jedoch, in Abhängigkeit von diesen Tätigkeiten Ergebnisdaten zu bearbeiten, also beispielsweise Prozesse, Informationssammlungen etc. zu erfassen oder zu bewerten und dazu in die Verwaltungsfunktion zu wechseln. Sofern notwendig, können von dort aus die Stammdaten angepasst werden. Von der Verwaltungsfunktion aus ist ein Wechsel in die Auswertungsfunktionen möglich, welche die Zusammenfassung und Ausgabe von Ergebnis-, Steuer- und Stammdaten erlauben.

Die *Steuerung* löst, ebenfalls in Abhängigkeit der Steuerdaten bzw. entsprechend der aktuellen Projektphase und der dabei entstehenden Notwendigkeiten, die Synchronisation mit übergeordneten Projekten oder die Erstellung neuer, untergeordneter Projekte aus und wechselt dazu in die Kommunikations-komponente.

Alternativ (in Abbildung 9-1 grau hinterlegt dargestellt und mit *optional* gekennzeichnet) sind alle Funktionen ebenfalls direkt über eine Funktionsauswahl zugänglich. Dies entspricht jedoch nicht dem normalen Arbeitsablauf.

Basisfunktionen

ISIGO besteht aus den übergeordneten Funktionen *Steuerung, Auswertung, Verwaltung* und *Kommunikation*. Zu ihrer Implementation wird auf Basisfunktionen der Anwendungsumgebung aufgebaut. Aufgrund der dadurch entstehenden Komplexität werden die Funktionen in Ebenen eingeordnet.

- Die Benutzerebene umfasst die *Steuerung, Auswertung, Verwaltung* und *Kommunikation*.
- Die Interaktionsebene implementiert die *Identifikation und Authentisierung, die inhaltliche und steuernde Interaktion,* die *Integration,* und die *Verbindung*.
- In der Abstraktionsebene sind die Funktionen für *Abfrage, Nachführung* und *Synchronisation* angeordnet.
- Die Darstellungsebene umfasst *Darstellung, Formularisierung* und *Formatierung*.
- *Abstraktion, Auswertung, Datenverwaltung* und *Datenkommunikation* sind in der Datenebene angeordnet.

Jede dieser Basisfunktionen muss bei der Implementation als Element der Laufzeitumgebung zur Verfügung stehen oder gestellt werden. Jede Ebene greift nur auf Funktionen der selben oder der darunterliegenden Ebenen zu. Es entsteht ein hierarchischer Aufbau gemäss Abbildung 9-2.

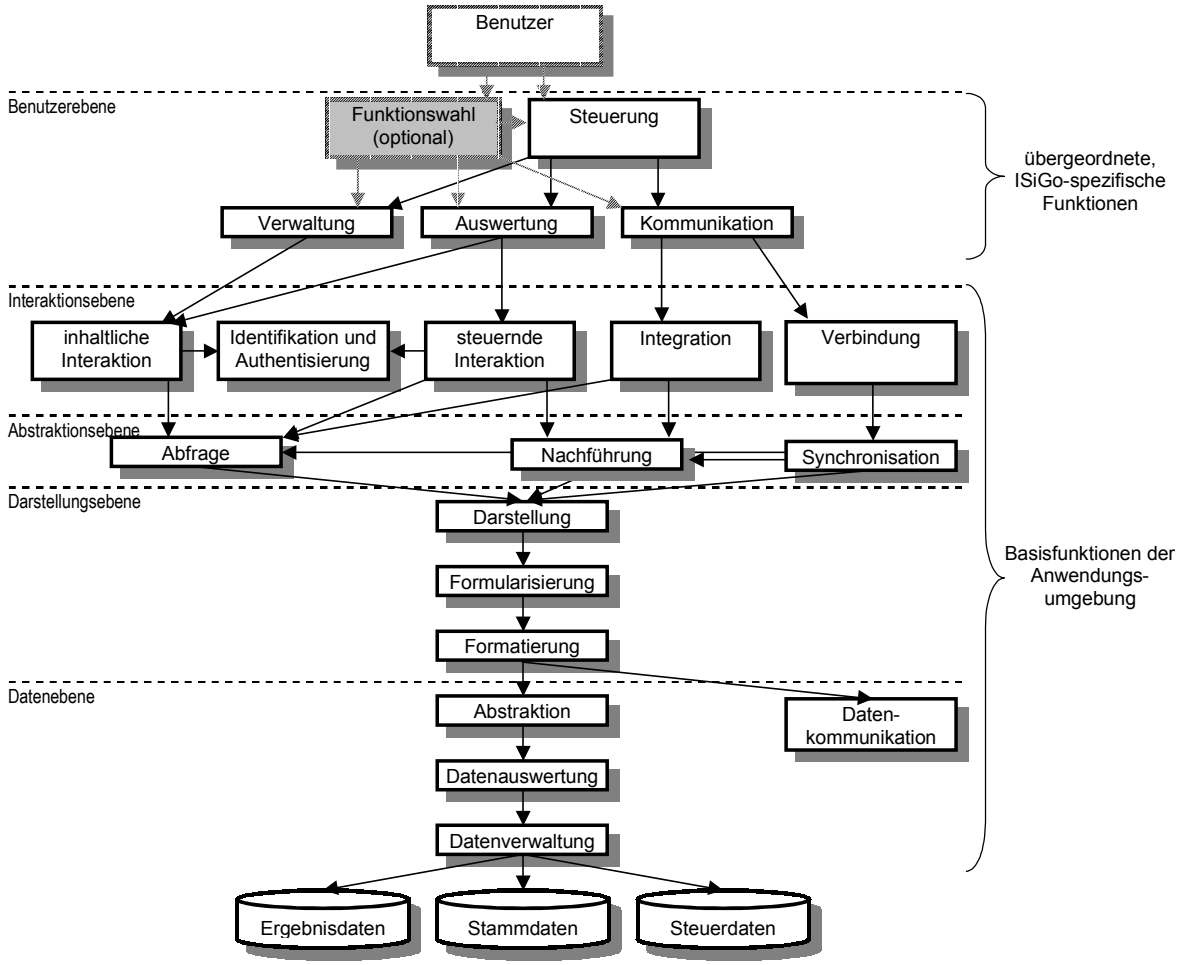


Abbildung 9-2: Funktionenmodell der *ISiGo*-Architektur mit Ebenen

Das Ebenenmodell gemäss Abbildung 9-2 stellt eine ideale, vollständige Lösung dar. Die Basisfunktionen sind in Tabelle 9-1 beschrieben.

Benutzer-ebene	Die Benutzerebene wurde in Abschnitt 9.1 unter dem Titel *Funktionen* bereits beschrieben. *Verwaltung* und *Auswertung* bauen auf steuernden und inhaltlichen Interaktionskomponenten auf, welche ihrerseits auf Identifikations- und Authentisierungsfunktionen zurückgreifen. Die *Kommunikation* beruht auf Integrations- und Verbindungsfunktionen.	
Interaktions-ebene	Die Interaktionsebene umfasst die Bedienungsschnittstelle zwischen Benutzer und System (Benutzerschnittstelle) und stellt dazu alle Datenein- und -ausgabefunktionen zur Verfügung.	
	Inhaltliche Interaktion	Die inhaltlichen Interaktionsfunktionen erlauben die Entgegennahme und Weiterleitung von inhaltlichen Benutzereingaben, z.B. das Auslesen und Weiterleiten von Texten, die ein Benutzer eingegeben hat, aus einem Feld oder die Werte aus einer Auswahl. Sie umfassen auch Konsistenzprüfungen (Datentypen und Wertebereiche).
	Identifikation und Authentifikation	Die Identifikation und Authentisierung dient zur Ermittlung und Vergabe der Berechtigung eines Benutzers, die Interaktion vornehmen zu dürfen, also

		ISIGO benutzen und auf in *ISIGO* erfasste Daten zugreifen zu dürfen. Dazu müssen Login- oder andere Anmeldeaufforderungen, Verwaltung von Benutzerdaten und Vergleich, Management dieser Daten etc. implementiert werden.
	Steuernde Interaktion	Die steuernden Interaktionsfunktionen stellen Möglichkeiten zur Entgegennahme und Weiterleitung von steuernden Benutzereingaben zur Verfügung, z.B. Menüs, Schaltflächen etc.
	Integration	Die Integrationsfunktion erlaubt die Weitergabe von Daten einer *ISIGO*-Instanz an eine andere, also die Übernahme von Daten, und stellt Vorgehensweisen zur Bewältigung der dabei entstehenden Konflikte zur Verfügung. Dies dient v.a. zur Synchronisation von Daten.
	Verbindung	Die Verbindungsfunktionen erlauben die Auswahl der Instanzen (von *ISIGO* oder anderer Applikationen), mit welchen Daten ausgetauscht werden sollen.
Abstraktionsebene	Die Abstraktionsebene umfasst alle Funktionen, welche der Ein- und Ausgabe von Daten in den und aus dem erfassten Bestand erlauben.	
	Abfrage	Unter Abfrage wird allgemein die Erzeugung formatierter Darstellungen von gespeicherten Daten verstanden, also der passive (nur-lesende) Zugriff auf *ISIGO*-Daten in einem benutzerlesbaren Format.
	Nachführung	Nachführung bedeutet, dass diese Daten verändert werden, stellt also einen aktiven (schreibenden und lesenden) Zugriff dar.
	Synchronisation	Die Synchronisationsfunktionen erlauben die Übernahme von Daten von anderen *ISIGO*-Instanzen und die Integration in den Bestand. Dazu werden sowohl Abfragen ausgeführt, um Konflikte festzustellen, als auch Nachführungen, um den Bestand zu ergänzen oder zu verändern.
Darstellungsebene	Die Darstellungsebene nimmt die Formatierung der Daten gemäss Anforderungen, die Einordnung dieser formatierten Daten in Formulare sowie die Darstellung dieser Formulare vor. Diese drei Funktionen sind nicht streng zu trennen, weshalb sie einander jeweils untergeordnet, aber in derselben Ebene dargestellt sind. Ihre Trennung ist implementationsabhängig. Für die Synchronisation sind spezifische Formatierungen (für Import / Export) vorzusehen.	
	Darstellung	Die Darstellung selbst sorgt für die Aufbereitung von Funktionen für das vom Benutzer verwendete Anzeigeformat, also beispielsweise die Übersetzung fertiger Formulare in HTML oder als "Comma Separated Values (CSV)" für den Import oder Export von Daten.
	Formularisierung	Die Formularisierung umfasst die Einordnung formatierter Inhalte in Interaktionsbereiche, z.B. Formulargenerierung, Bündigkeit, Einfügen von Schaltflächen und editierbaren Textfeldern etc.
	Formatierung	Die übersichtliche Formatierung der Daten geschieht durch einheitliche Darstellung wie z.B.

		Tabellenstrukturierung, Länge von Zeichenketten, Schriftart, Masseinheiten und Rundung etc.
Datenebene	Die Datenebene stellt die im Bestand vorhandenen Daten zur Verfügung und nimmt die technische Speicherung vor.	
	Datenverwaltung	Die Datenverwaltung umfasst alle Funktionen, um Daten in einer nachvollziehbaren Weise innerhalb des Systems zu speichern und wieder aufzufinden. Dies wird in der Regel als *Datenbankmanagement* bezeichnet. Es muss sich jedoch nicht um ein vollständiges, z.B. auf dem relationalen Ansatz aufbauendes Datenbankmanagementsystem handeln, sondern für die erwarteten Datenmengen sind zumindest in einer kleinen Lösung einfache Storage- und Retrievalmechanismen genügend. Allerdings müssen auch Datenbank-Systemmanage-mentfunktionen zur Verfügung stehen, um die Beeinflussung der Strukturen und Abläufe des Datenbankmanagementsystems zu erlauben, z.B. zur Erzeugung neuer Tabellen und zur Manipulation von Tabellenstrukturen.
	Datenauswertung	Die von der Datenverwaltung bereitgestellten Daten werden grob ausgewertet, indem Auswahlfunktionen zur Selektion, Sortierung und Verknüpfung (Kombination und Filterung) von Daten aufgrund der von weiter oben geforderten Filterung angewendet werden.
	Abstraktion	Die Abstraktionsfunktionen dienen zur zusammenfassenden Auswertung von Daten, z.B. zur Berechnung von Mittel- und Summenwerten.
	Datenkommunikation	Die Datenkommunikationsfunktionen umfassen alle Funktionen, welche den Datenaustausch zwischen den verschiedenen Komponenten von *ISIGO* erlauben (innere Kommunikation) und die Weitergabe von Daten zwischen verschiedenen Instanzen (gleichzeitig ablaufenden Kopien) des Programmes regeln. Dabei kann es sich um Import- und Exportfunktionen handeln, um die Synchronisation zwischen einer über- und einer untergeordneten Instanz oder um die Erstellung von neuen Instanzen von *ISIGO*. *ISIGO* kann als verteiltes System mit asynchronen und synchronen Prozessen betrachtet werden. Die Kommunikationskomponente muss alle Funktionen zur Identifikation des Kommunikationspartners unterstützen und kann dazu beispielsweise Protokolle wie TCP/IP oder ODBC[96] implementieren.

Tabelle 9-1: Beschreibung der *ISIGO*-Basisfunktionen

96 ODBC: Open Database Connectivity: Von Microsoft und anderen Unternehmen entwickelte Schnittstelle zur Anbindung von Anwendungen unter Microsoft Windows-Betriebssystemen an SQL-Datenquellen.

9.3 Technologievarianten

Zur Implementation von *ISIGO* wurden verschiedene Technologien betrachtet, welche die zuvor besprochenen Funktionen zur Verfügung stellen bzw. ihre Implementation ermöglichen. Nachfolgend werden drei geeignete *Technologievarianten* besprochen, welche verschiedene der betrachteten Technologien vereinen. Aufbauend auf der gewählten Variante kann ein konkretes *Implementationskonzept* erstellt werden.

Aufgrund der Komplexität von *ISIWAY* und im Hinblick auf die erste und zweite Konkretisierung, welche in Kapiteln 8 und 10 dieser Dissertation beschrieben sind, wurde eine Aufteilung von *ISIWAY* in zwei Produkte vorgenommen, welche *ISIGO CENTRAL* und *ISIGO 1.5* genannt werden sollen.

ISIGO CENTRAL soll das Gesamtkonzept von *ISIWAY* unterstützen, sich zum Einsatz durch den Informationssicherheitsbeauftragten der Unternehmung eignen und alle Detaillierungsgrade (DGs) von *ISIWAY* abbilden. *ISIGO 1.5* ist hingegen speziell für den Einsatz bei den jeweiligen Koordinatoren für Informationssicherheit konzipiert und auf *ISIWAY 1.5* abgestimmt (vgl. Kapitel 10 und Anhang C.2). Beide Produkte verbindet ein gemeinsames Datenmodell, auf dessen Basis sie miteinander kommunizieren können. Sie verwenden jedoch unterschiedliche Basistechnologien.

LAMP-System

Beschreibung

Das Akronym LAMP [Kunze98] steht für *LINUX-APACHE-MYSQL-PHP* und identifiziert so die vier wesentlichen Produkte-Komponenten[97]. *LINUX* bildet die IT-Plattform mit *UNIX*-üblichen Systemschnittstellen, welche die grundlegende Kommunikation und Speicherverwaltung bereitstellen.

APACHE ist ein auf *LINUX* (und anderen IT-Plattformen) verfügbarer Webserver, welcher über nachladbare Module frei mit Funktionen erweitert werden kann. Er verwaltet in HTML codierte Dateien und stellt diese auf Anfrage eines WWW-Clients diesem zur Darstellung zur Verfügung.

Die Interaktionsebene von *ISIGO* kann also über die standardisierten Funktionen von HTML (z.B. Darstellung von Feldern, Weiterleitung von Eingaben und

---

97 Die hier genannten Produkte stehen stellvertretend für entsprechende Technologien. Prinzipiell ist es möglich, das hier beschriebene Linux durch ein anderes UNIX-artiges Betriebssystem zu ersetzen. Auch Apache steht hier nur für den Typus Webserver-Software. MySQL kann prinzipiell ebenfalls gegen ein anderes relationales Datenbankmanagementsystem ausgetauscht werden, da die weitaus meisten dieser Systeme eine SQL-Implementationn. Schliesslich ist auch PHP nur *eine* Möglichkeit, Server-basierte Applikationen ausführen zu lassen.

Steuerungsaktionen) implementiert werden. Auch die Identifikation und Authentisierung von Benutzern kann über in *APACHE* verfügbare oder als Module nachrüstbare Funktionen realisiert werden.

PHP ist eine Skriptingsprache, mit welcher alle Funktionen der *LINUX*-Plattform gesteuert werden können, dessen Module in HTML-Dokumente integriert werden können und so die Steuerung von Abfrage und Nachführung der Daten in Abhängigkeit der Interaktion vornehmen kann (also die Codierung der Datenbanksteuerungsfunktionen). Ebenfalls in *PHP* zu implementieren wäre der Aufbau der vom Server zur Verfügung zu stellenden Seiten, also Darstellung, Erstellung von interaktiven Formularen und grundsätzliches Formatieren (alles durch automatisierte Erstellung HTML-codierter Elemente). Prinzipiell könnte dazu auch eine andere auf *LINUX* verfügbare Sprache und Laufzeitumgebung verwendet werden (z.B. *PERL* oder C/C++), welche von *PHP* ausgelöst würde.

MYSQL ist ein Datenbankmanagementsystem nach relationalem Datenbankkonzept, welches über die Structured Query Language (SQL) gesteuert werden kann und über ein nachladbares Modul mit *APACHE* und *PHP* verbunden wird.

Bewertung

Ein LAMP-System vereinigt verschiedene aktuelle Technologien. Mit *nur einem* in das Netz zu integrierenden entsprechend konfigurierten *LINUX*-Gerät könnte schnell eine breite Verfügbarkeit von *ISIGO* in der Unternehmung erreicht werden, da die notwendige Client-Installationen schon heute auf den weitaus meisten Clients im unternehmerischen Umfeld installiert sind: Die Server-Komponenten des LAMP-Systems sind frei oder (bei kommerzieller Nutzung) zu geringen Gebühren verfügbar.

Einer der Voraussetzungen für ein funktionierendes LAMP-System ist jedoch der Anschluss von Clients und Servern an dasselbe Netz. Parallele Installationen in verschiedenen Teilnetzen erzeugen Synchronisationsbedarf der zentral auf dem LAMP-System abgelegten Daten. Die dazu notwendige Suchfunktion ist in *MYSQL* nicht vorhanden und müsste nachgerüstet (bzw. selbst erstellt) werden. Darüber hinaus ist die zentrale Speicherung von informationssicherheitsrelevanten Daten auch aus Sicherheitsüberlegungen problematisch: Bei den erfassten Daten handelt es sich grösstenteils um vertrauliche Inhalte. Da aus diesen Inhalten auf Schwachstellen der durch sie beschriebenen IT-Systeme geschlossen werden kann, muss ein effektiver Zugriffsschutz implementiert werden, welcher durch die sich stark entwickelnden Internet-Technologien ständig in Frage gestellt werden muss. Auch an die Verfügbarkeit des Servers müssten aufgrund der heute nicht vorgefertigt bestehenden koordinierten Replikation hohe Anforderungen gestellt werden.

Access-System

ACCESS ist ein relationales Datenbankmanagementsystem, welches auf IT-Plattformen mit *MICROSOFT WINDOWS* lauffähig ist. Es umfasst neben den datenbankbezogenen Verwaltungs-, Auswertungs- und Abstraktionsfunktionen auch Darstellungselemente, z.B. für die Gestaltung von Berichten und Formularen. Abfrage- und Nachführungsfunktion sind in die Bedienungsoberfläche integriert und lassen sich, ebenso wie alle anderen Funktionen, mit Hilfe von integriertem SQL und der Scripting-Sprache „Visual Basic“ in eigenen Applikationen verwenden. Die Kommunikation mit anderen Systemen geschieht über direkte Verwendung der Kommunikationselemente des Betriebssystems (dynamic link libraries), über definierte Ein- und Ausgabeformate von verschiedenen Datenbanktypen sowie über die von *MICROSOFT* und anderen Herstellern spezifizierte, auf SQL basierende Datenbankschnittstelle *Open DataBase Connectivity* (ODBC). Innerhalb von *WINDOWS*-Systemen können darüber hinaus *Data Access Objects* (DAO) verwendet werden, die auch zur Publikation von Daten auf Webservern von *MICROSOFT* genutzt werden können. *ACCESS* umfasst also alle Basisfunktionen, welche für eine Implementation der Funktionen von *ISIGO* notwendig sind.

Einer der Nachteile von *ACCESS* ist die Plattformgebundenheit: Da es nur für *MICROSOFT WINDOWS* verfügbar ist und die verschiedenen *ACCESS*-Versionen nur teilweise untereinander kompatibel sind[98], werden Anwender anderer Plattformen (z.B. *MACINTOSH*, *UNIX*) ausgeschlossen. Ausserdem verfügte *ACCESS* bis zur Version von 1995 nicht über die Möglichkeit, kontrollierte Redundanz zur Replikation zu erzeugen und auch in der Version von 1997 ist die Replikation schwierig zu beherrschen. Darüber hinaus stellt *ACCESS* hohe Anforderungen an die Rechenleistung der verwendeten IT-Systeme.

Bewertung

ACCESS ist ein sehr leistungsfähiges Werkzeug, welches viele Voraussetzungen für die Verwendung zur *ISIGO*-Implementation enthält. Seine Schwächen liegen in der Beschränkung auf *WINDOWS*-Systeme und die starke Betonung proprietärer Technologien.

---

98 Von Access bestehen die Versionsfamilien 1, 2, 95 und 97. Versionen 1 und 2 können ab Windows 3.1 verwendet werden, alle Versionen funktionieren auf Windows 95, 98 und NT 4. Jede Version kann auf die von ihr erstellten Datenbanken lesend und schreibend zugreifen. Die von einer früheren Version erstellten Datenbanken kann eine nachfolgende Version nur lesend öffnen, sie aber in eine der aktuellen Version entsprechendes Format umwandeln, und dann wieder schreibend darauf zugreifen. Auf eine in ein neueres Format umgewandelte Datenbank kann dann allerdings von früheren Versionen nicht mehr zugegriffen werden. Eine Interaktion verschiedener Versionen auf verschiedenen Systemen auf Dateibasis ist also ausgeschlossen.

Excel-System

EXCEL ist ein Tabellenkalkulationssystem, welches von *MICROSOFT* für *WINDOWS*- und *MACINTOSH*-Plattformen zur Verfügung gestellt wird. Die Funktionen zur Tabellenkalkulation können gesamthaft als einfaches Datenbanksystem betrachtet werden, da Datenverwaltung, Datenauswertung und Abstraktion unterstützt werden. Es wird allerdings keine einfache interne Integritätsprüfung ermöglicht, da kein Datenbankkonzept zugrunde liegt. Zur Darstellung wird auf die auf *WINDOWS*- und *MACINTOSH*-Plattformen üblichen Mechanismen zurückgegriffen. Darüber hinaus ist die Erstellung eigener Formulare mit zusätzlichen Programmen möglich. Die Implementation eigener Anwendungen geschieht wie bei *ACCESS* über „Visual Basic", wobei auch hier prinzipiell jede zur Verfügung stehende Laufzeitbibliothek verwendet werden kann. Weil jedoch zwei Plattformen unterstützt werden, sind nur diejenigen Anwendungen von einer auf die andere Plattform portierbar, welche sich dabei auf die vom Hersteller speziell für *EXCEL* erstellten Bibliotheken beschränken. Dazu gehören allerdings Datenimport- und –exportfunktionen sowie eine ODBC-Schnittstelle.

Bewertung

EXCEL eignet sich für die Implementation von *ISIGO*, allerdings mit der Einschränkung, dass die Verwaltung der Daten aufgrund der fehlenden internen Integritätskontrolle fehleranfällig ist. Dies ist für kleine Datenmengen, wie sie beispielsweise in einem einzelnen *ISIWAY*-Teilprojekt entstehen, nicht problematisch[99]. Für eine Verwendung zur zentralen Koordination durch den ISiBe wird eine *EXCEL*-basierte Lösung nicht empfohlen.

Durch die Verfügbarkeit einer ODBC-Schnittstelle für *EXCEL* kann die Kommunikation mit relationalen Datenbanksystemen gewährleistet werden. Dies erlaubt den kombinierten Einsatz von *EXCEL*-basierten Systemen mit Systemen auf relationaler Basis.

Weitere Systeme

Prinzipiell eignet sich jede beliebige Anwendungsentwicklungsumgebung für die Implementation der hier verlangten Basisfunktionen. Um den Aufwand für die

---

99 Die in einem Teilprojekt von *ISIWAY* entstehenden Daten sind tendenziell nicht sehr umfangreich, so dass auch die einfachen Sortier- und Selektionsfunktionen von Excel noch angemessene Antwortzeiten ermöglichen. Auch qualitativ unterliegen die in einem Teilprojekt entstehenden Daten gesamthaft nicht so hohen Anforderungen wie die kumulierten Daten des Informationssicherheitsbeauftragten (die der Kumulation zugrundeliegenden Teildaten selbstverständlich schon!). Ausserdem hat der Koordinator für Informationssicherheit eine gewisse Vertrautheit mit den erfassten Daten und ist zur Gewährleistung der Konsistenz weniger auf formale Methoden angewiesen.

Implementation gering zu halten, sollte jedoch auf möglichst funktionsstarke Einzelkomponenten zurückgegriffen werden können; die Aufgabe der Entwicklungsumgebung liegt dann in der Verbindung dieser Komponenten. Denkbar wäre beispielsweise eine mit C / C++ implementierte Steuerungsfunktion oder der Zugriff auf ein zentrales Datenbankmanagementsystem mit *EXCEL* über die ODBC-Schnittstelle. Es können zwar nicht alle Möglichkeiten diskutiert werden und es kann auch kein Nachweis erbracht werden, ob eine „ideale" Lösung existiert und welche dies wäre. Vielmehr wurden die drei zuvor beschriebenen Varianten ausgewählt, weil sie in der Praxis Verbreitung erlangt haben und auf etablierten Konzepten beruhen.

Auswahl

Die Auswahl der Technologievarianten für die beiden Produkte *ISIGO CENTRAL* und *ISIGO 1.5* orientiert sich an der Verbreitung und der Möglichkeit, das Produkt in einer realen Umgebung zu verwenden (vgl. Kapitel 10).

Ein grosser Vorteil der drei betrachteten Technologievarianten ist die jeweils grosse Verbreitung, welche die Benutzerschnittstellen aufweisen: Die Bedienung von WWW-Clients und Tabellenkalkulationsprogrammen – insbesondere von *EXCEL* – kann im unternehmerischen Bereich heute als Allgemeinwissen bezeichnet werden. Da viele Unternehmungen auf Basis von *ACCESS* eigene Applikationen entwickelt haben, ist auch die Bedienung dieses Systems vielen Benutzern geläufig. Nur wenige andere Systeme, welche auch Datenbankfunktionen bieten, können eine ähnlich weit verbreitetes Benutzungswissen vorweisen.

Unter dem Gesichtspunkt des Einsatzes muss die Variante „LAMP" ausgeschlossen werden. Einerseits würde die zentrale Datenhaltung nicht auf Akzeptanz stossen, da die betrachteten Einheiten ihre Unabhängigkeit auch bei der Ablage der von ihnen verwalteten Daten behalten möchten. Darüber hinaus besteht für die Einsatzumgebung kein Konzept, welches die Sicherheit der zentralen Speicherung gewährleisten würde. In der Systemumgebung in der angestrebten Einsatzumgebung muss die Unabhängigkeit der verschiedenen, untereinander nicht verbundenen Subnetze berücksichtigt werden, welche nicht alle das für LAMP-Systeme notwendige TCP/IP-Protokoll verwenden. Auch wenn in der in Kapitel 10 beschriebenen Einsatzumgebung pro Netz ein Server vorgesehen würde und auf die Synchronisation der einzelnen Datenbanken verzichtet würde, entstünde hoher Aufwand für Beschaffung, Installation und Wartung der Systeme. Die effiziente Umsetzung wäre also mit einer derartigen Konfiguration nicht durchführbar.

Die *ACCESS*-Variante ist geeignet, um *ISIGO CENTRAL* und *ISIGO 1.5* zu implementieren. Da *ACCESS* jedoch ein *WINDOWS*-System voraussetzt, eignet es sich nicht zur Erfassung und Verwaltung von *MACINTOSH*-basierten Netzwerken vor Ort. Da in der in Kapitel 10 beschriebenen Einsatzumgebung jedoch mehrere *MACINTOSH*-basierte Netzwerke bestehen, scheidet *ACCESS* als Basis für *ISIGO 1.5* aus. Für den Einsatz bei Informationssicherheitsbeauftragten – also als Basis für

ISIGO CENTRAL – ist es aber geeignet, wenn angenommen wird, dass der Informationssicherheitsbeauftragte über ein *WINDOWS*-Gerät verfügt.

Es bleibt *EXCEL* als Basis für *ISIGO 1.5*. Es erlaubt eine dezentrale, benutzerbezogene Speicherung und Bearbeitung der beim Durchlaufen von *ISIWAY* erfassten Daten. Der Zugriff auf die *ISIGO*-Daten (also auf die Datei mit den *EXCEL*-Tabellen) kann wie der Zugriff auf andere vertrauliche Informationen geregelt werden. Die Weitergabe der Daten an den ISiBe oder bzw. an unter- oder übergeordnete Projekte kann über Dateien auf Disketten geschehen. Prinzipiell ist auch die Kommunikation über ODBC möglich, dies verlangt jedoch, dass die beiden miteinander kommunizierenden Systeme in demselben Netz sind, was in der Einsatzumgebung (vgl. Kapitel 10) nicht vorausgesetzt werden kann.

Das *ISIGO CENTRAL* zugrundeliegende Datenmodell sowie die Details der Implementation von *ISIGO 1.5* (mit Bildschirmausdrucken) werden in Anhang D.1 beschrieben. *ISIGO 1.5* ist Teil dieser Dissertation.

9.4 Fazit aus Teil III

In Teil III wurden die Anforderungen an die konkrete Gestaltung eines Informationssicherheitsprozesses erarbeitet (Kapitel 7), darauf aufbauend ein solcher Prozess neu definiert (Kapitel 8 und Anhang C.1) und ein Prototyp spezifiziert, welcher dieses Verfahren unterstützt (Kapitel 9 und Anhang D.1).

In Kapitel 7 wurden verschiedene praxiserprobte Verfahren zur Erreichung von Informationssicherheit beschrieben: Das IT-Sicherheitshandbuch und das IT-Grundschutzhandbuch des deutschen Bundesamts für Sicherheit in der Informationstechnik, das Grundschutzverfahren des schweizerischen Bundesamts für Informatik, der Code of practice der British Standards Institution, COBIT der ISACF sowie ISO GMITS. Sie wurden anhand eines Bewertungsschemas beurteilt, welches spezifisch zu diesem Zweck in Kapitel 7 aufgestellt wurde. Bei dieser Bewertung stellte sich heraus, dass jedes der untersuchten Verfahren spezifische Stärken und Schwächen hat und sich in jeweils einem Bereich überdurchschnittlich eignet. Der Code of Practice weist beispielsweise Stärken in der Umsetzung auf, während das IT-Grundschutzhandbuch v.a. durch seine detaillierten technischen Massnahmen überzeugt.

Keines der Verfahren eignete sich jedoch für die hier angestrebte, aus den inhaltlichen Anforderungen aus Kapitel 7 angestrebte Verwendung durch Benutzer innerhalb der Unternehmung.

Mit der Definition von *ISIWAY* in Kapitel 8 scheint nun ein genau dafür geeignetes Verfahren vorzuliegen. Ein vorsichtige Beurteilung des Autors lässt die Erfüllung der meisten der am Ende von Kapitel 7 aufgestellten Anforderungen vermuten.

ISIWAY zeichnet sich dabei durch einen zyklischen Aufbau in mehreren Detaillierungsgraden aus, welche nacheinander durchlaufen werden. Die

Durchführung geschieht in den Fachbereichen der Unternehmung unter Betreuung durch den Informationssicherheitsbeauftragten. Im Zentrum der Betrachtung stehen jedoch die Informationen und die unternehmerischen Anforderungen, nicht technologische Fragestellungen.

In Kapitel 9 wurde die Spezifikation von *ISIGO* beschrieben, einem internen Instrument des Informationssicherheitsprozesses *ISIWAY*. Es wurden Technologievergleiche vorgenommen und drei mögliche Implementationsvarianten *LAMP*, *ACCESS* und *EXCEL* definiert. *LAMP* bezeichnet ein *LINUX*-basiertes zentrales System, welches die Datenverwaltung auf einem SQL-basierten Datenbankmanagementsystem vornimmt und über HTML-Dateien mit der integrierten Skriptingsprache *PHP* gesteuert wird. Eine derartige Implementation musste in Antizipation des Umfelds der Einsatzumgebung (vgl. Kapitel 10) fallengelassen werden. Eine Implementation unter *MICROSOFT ACCESS* wäre prinzipiell möglich, wurde aber zugunsten einer *EXCEL*-Variante für den dezentralen, förderativen Einsatz in *ISIWAY-1.5*-Projekten zurückgestellt.

Die konkrete Implementation von *ISIGO 1.5* unter *EXCEL* wurde in Anhang D.1 beschrieben. Die ausführliche Dokumentation wurde in die Beschreibung von *ISIWAY 1.5* integriert, welche in Anhang C.2 enthalten ist. Einige beispielhafte Inhalte der Tabellen in der Basis-Version von *ISIGO 1.5* sind in Anhang D.2 wiedergegeben.

Aufgrund der Verwendung des verbreiteten Tabellenkalkulationssystems *EXCEL* als Basis für die Implementation und aufgrund der Integration der Verwendung von *ISIGO 1.5* in das Verfahren *ISIWAY 1.5* wird davon ausgegangen, das beide Komponenten sich ergänzen und die Durchführung von Informationssicherheits-projekten erleichtern. Es konnte demnach gezeigt werden, dass es möglich ist, auf der Basis eines verbreiteten Tabellenkalkulationsprogramms ein internes Werkzeug zur Unterstützung der Durchführung von *ISIWAY 1.5* zu implementieren. Auch wenn Daten- und Funktionsmodell eines solchen Werkzeuges schon schnell hohe Komplexität annehmen, stehen heute auf jedem Arbeitsplatzgerät die Technologien zur Verfügung, die für die Ausführung dieser Werkzeuge notwendig sind. Da nicht nur das Werkzeug *ISIGO 1.5* als Datei weitergegeben werden kann, sondern auch die dazu gehörende Beschreibung des Verfahrens *ISIWAY 1.5* (in Anhang C.2 eingefügt) als HTML-Datei vorliegt, ist eine Verbreitung von Verfahren und Werkzeug innerhalb der Unternehmung einfach. Auch wird davon ausgegangen, dass die Verfügbarkeit eines Werkzeugs die Akzeptanz des Verfahrens und die allgemeine Motivation zur Betrachtung von Informationssicherheit erhöht. Ob das Verfahren und das Werkzeug die Anforderung der einfachen Erlernbarkeit erfüllt, muss zwar offen bleiben, jedoch wirkt sich die Verwendung des verbreiteten und in den Unternehmungen häufig eingesetzten Produktes *EXCEL* wirkt tendenziell erleichternd auf die Einarbeitung in *ISIWAY 1.5* aus.

MIT ZUNEHMENDEM FORTSCHRITT VERLAGERT SICH DAS PHÄNOMEN DES BLACK-BOXING PARADOXERWEISE MEHR UND MEHR IN DEN ALLTAG. WERFEN SIE MAL EINEN BLICK IN DIE EINGEWEIDE IHRES AUTOS, ODER VERSTEHEN SIE NOCH, WIE EIN MODERNER FERNSEHER FUNKTIONIERT? WIR SIND UMGEBEN VON GERÄTEN, DIE UNS DAS LEBEN ERLEICHTERN, DENEN WIR UNS ANVERTRAUEN, VON DENEN WIR ABER NICHT WISSEN, WAS GENAU IN IHNEN VORGEHT. SO IST BLACK-BOXING EIN WESENTLICHER BESTANDTEIL UNSERES MODERNEN LEBENS GEWORDEN.

– PROF. DR. HANS-JÜRGEN QUADBECK-SEEGER
EHEM. FORSCHUNGSVORSTAND DER BASF AG
IN: FASZINATION INNOVATION, S. 49

Teil IV: Umsetzung

Teil IV beschreibt die potentielle Umsetzung des in Teil III definierten spezifischen Informationssicherheitsprozesses (Kapitel 10) und bietet in Kapitel 11 einen Ausblick auf weitere mögliche Arbeiten zum Management der Informationssicherheit.

10 Verwendung von *ISiWAY* und *ISiGO*

In diesem Kapitel wird betrachtet, wie die Umsetzung von *ISiWAY* und die Anwendung von *ISiGO 1.5* in einem konkreten unternehmerischen Umfeld gestaltet werden könnte. Dabei wird eine real existierende unternehmerische Umgebung und das darin ablaufende Projekt SECNET beschrieben. Insbesondere wird betrachtet, wie das Projekt ausgelöst wurde und die Bedarfsbestimmung stattgefunden hat, wie die Kommunikation auf strategischer Ebene geschehen ist und wie die Betroffenen motiviert wurden. Ausserdem wird beschrieben, welche Probleme bei der Auslösung aufgetreten sind und noch erwartet werden.[100]

---

100 Das hier beschriebene Projekt SECNET endete 1998 und wird in der Vergangenheitsform beschrieben. Da es jedoch nur die Voraussetzungen für die Umsetzung bereitstellen sollte, wird die Anwendung der Ergebnisse – also die beginnende Durchführung des Informationssicherheitsprozesses – in der Gegenwarts- oder Zukunftsform geschildert.

10.1 Situation und Zielsetzung

Das Umfeld für das hier beschriebene Projekt SECNET war ein international tätiger Industriekonzern. Mit seinen weltweit mehreren Zehntausend Mitarbeitern stellt er mannigfaltige Produkte v.a. im Investitionsgüterbereich her, erbringt aber auch unterschiedlichste Dienstleistungen. Der Hauptsitz dieses stark diversifizierten und strikt in einzelne Unternehmensbereiche unterteilten Konzerns befindet sich in der Schweiz.

Das Projekt SECNET hatte zum Ziel, das Bewusstsein für die Informationssicherheit in diesem Konzern nachhaltig zu erhöhen, Vorgehensweisen bereitzustellen, mit denen das anzustrebende Sicherheitsniveau für die einzelnen Konzernbereiche individuell bestimmt werden kann, die Erreichung dieses jeweiligen Sicherheitsniveaus voranzutreiben und den davon Betroffenen alle notwendigen Hilfsmittel zur Verfügung zu stellen, um diese bei der selbständigen Erarbeitung einer Lösung zu unterstützen.

Projektleiter von SECNET war der Sicherheitsbeauftragte (SiBe) der Konzernleitung. Er ist dem Chef der Konzernstäbe unterstellt, welche direkt dem Präsidenten der Geschäftsleitung untergeordnet sind. Unternehmerische Aufgabe des SiBe ist es, alle unternehmerischen Bedingungsrisiken zu betrachten, darunter auch diejenigen der Informationssicherheit.

10.2 Auslöser

Auslöser von Projekt SECNET war die Feststellung, dass Information innerhalb des Konzerns eine immer grössere Rolle spielt und dass die Ressource Information deshalb besonders geschützt werden muss.

Ausgehend von der Unternehmenspolitik des Konzerns hatte der Sicherheitsbeauftragte schon vor Beginn von SECNET eine allgemeine Sicherheitspolitik definiert, welche die wichtigsten Rahmenbedingungen für das Management unternehmerischer Bedingungsrisiken enthielt und von der Konzernleitung 1996 in Kraft gesetzt wurde. Diese gültige Sicherheitspolitik definiert unter anderem die Aufgabengebiete des Sicherheitsbeauftragten, darunter auch den *Informationsschutz*. Weiterhin wurden das prinzipielle Vorgehen zur Bestimmung und Erreichung des angestrebten Sicherheitsniveaus (*Schutzziel*) beschrieben, Kontrolldokumente, -stellen und -tätigkeiten definiert sowie der Aufgaben- und Kompetenzbereich des Sicherheitsbeauftragten abgegrenzt.

Im Projekt SECNET ging es nun darum, die allgemein gehaltenen Vorgaben aus der unternehmerischen Sicherheitspolitik für die Informationssicherheit zu konkretisieren, die dazu notwendigen Stellen in den Stabsbereichen des Konzerns einzurichten und möglichst konkrete Hilfestellungen zur Erreichung einer angemessenen Informationssicherheit zu geben. Diese Zielsetzungen und

Tätigkeiten sollten in einer Informationssicherheitspolitik beschrieben werden, deren Verabschiedung wiederum durch die Konzernleitung geschehen sollte.

10.3 Anwendung von *ISIWAY*

Das Projekt SECNET umfasste vor allem die Vorbereitungsphasen des Informationssicherheitsmanagements. Deshalb werden die einzelnen Aktivitäten hier so gegliedert, wie es in der Vorbereitungsphase von *ISIWAY* beschrieben wurde (vgl. Anhang C.2).

Vorbereitung

Anforderungen und Ziele festlegen (Aktivität 1.10)

Die grundsätzlichen Anforderungen an die unternehmerische Informationssicherheit wurden in der unternehmerischen Sicherheitspolitik schon festgehalten: Ziel ist die Minimierung der Anzahl und des Ausmasses von Störungen der unternehmerischen Leistungserbringung. Es soll deshalb als unternehmerisches Ziel definiert werden, dass die bestehenden Risiken zu erkennen sind, Schutzziele definiert werden müssen und die Risiken auf ein tragbares Mass zu senken sind. Informationssicherheit muss in die unternehmerischen Tätigkeiten integriert werden. Die Verantwortung für die Informationssicherheit muss vom Management getragen werden.

Diese Vorgaben wurden vom Sicherheitsbeauftragten formuliert und werden von der Geschäftsleitung durch die Verabschiedung der (allgemeinen) Sicherheitspolitik getragen.

Stelle und Stellung des ISiBe (Aktivität 1.21)

Der unternehmerische Sicherheitsbeauftragte (SiBe), welcher auch Leiter des Projektes SECNET war, hatte durch eine entsprechende Definition in der bestehenden Sicherheitspolitik interimistisch die Stelle des Informationssicherheitsbeauftragten (ISiBe) inne. Deshalb wurden zunächst die für die Informationssicherheit spezifischen Eigenschaften des ISiBe vom SiBe definiert.

Es wurde eine Unterordnung des ISiBe unter den SiBe vorgesehen. Ferner wurde eine Stabsstelle für Informationssicherheit definiert, welche vom ISiBe geleitet werden sollte. Diese Stabsstelle sollte als beratende und unterstützende Stelle innerhalb des Konzerns fungieren und auf diese Weise die Umsetzung der Politik fördern. Ferner sollte sie Vorgehensweisen und fachspezifisches Know-How bereitstellen.

Einordnung identifizieren (Aktivität 1.22)

Es wurde festgelegt, dass der ISiBe keine über die erwähnte Stabstelle hinausgehende Weisungsbefugnis erhalten soll. Er soll lediglich auf Anfrage beratend tätig werden, im Rahmen seiner Kontrollfunktion jedoch auch ungefragt den Zustand der Informationssicherheit in einem Teil des Konzerns aufnehmen können und darüber an den ihm übergeordneten SiBe berichten. Dieser erstattet dem Präsident der Geschäftsleitung Bericht über den erhobenen Zustand und die dabei festgestellten Mängel. Der Präsident der Geschäftsleitung veranlasst dann gegebenenfalls auf Empfehlung des SiBes die Nachfrage nach Beratungsdienstleistungen der Fachstelle für Informationssicherheit.

Es wurde ebenfalls festgelegt, dass Informatik als wichtigstes informationsverarbeitendes Werkzeug zentraler Betrachtungsgegenstand der Informationssicherheit sein muss. Es wurde deshalb in verschiedenen Gremien von Informatik-Führungspersonal bekanntgegeben, dass die Stelle des ISiBe neu besetzt wurde. Ferner erfolgte die Kommunikation über die Erstellung der neuen Informationssicherheitspolitik, indem in den bestehenden Gremien für unternehmerische Sicherheit im Konzern darüber informiert wurde.

Auswahl Projektteam (Aktivität 1.23)

Das Projektteam setzte sich bei SECNET zusammen aus

- dem Projektleiter,
- dem Autor, der als Vertreter des Instituts für Informatik der Universität Zürich für die Sicherstellung der konzeptionellen Vollständigkeit und aktuellen Methodologie zuständig war,
- dem ehemaligen Leiter einer Informationssicherheitsfachstelle einer früheren Tochtergesellschaft des Konzerns, der aufgrund seiner Erfahrung Schwerpunkte in der inhaltlichen Ausgestaltung des Projektes vorschlagen konnte,
- einem externen Berater für unternehmerische Sicherheit, der mit den Sicherheitsstrukturen des Konzerns vertraut war und die Qualifikation der möglichen Ansprechpartner für Informationssicherheit gut kannte,
- einer weiteren Mitarbeiterin der Universität Zürich, welche aufgrund ihrer Erfahrung in ähnlichen Projekten anderer Unternehmungen die Konsistenz der erarbeiteten Inhalte mit vergleichbaren Umgebungen sicherstellen konnte, sowie
- einem führenden Mitarbeiter der Beratungsabteilung der Revisionsgesellschaft des Konzerns, der einerseits über Kenntnisse einzelner Teile des Konzerns verfügte, andererseits Erfahrungen aus anderen vergleichbaren Projekten einfliessen lassen konnte und darüber hinaus für die

Abdeckung der minimalen Komponenten aus Sicht der gesetzlichen Anforderungen sorgte.

Grundlagenerarbeitung planen (Aktivität 2.10)

Erste Aufgabe des Projektteams war es, aus den zuvor geschilderten Elementen eine Informationssicherheitspolitik zu formulieren, welche diese Grundlagen, Ziele, Institutionen, Verantwortungen und generischen Prozesse umfasste. Insbesondere bei der Wahl der Inhalte wurde entschieden, diese an dem international anerkannten Standard [BSI-COP95] auszurichten. So sollte einerseits eine möglichst vollständige Abdeckung der verschiedenen inhaltlichen Anforderungen erreicht werden, andererseits sollte es die Vergleichbarkeit der im Konzern erarbeiteten Resultate untereinander sowie mit denjenigen anderer Unternehmungen ermöglichen, welche sich an demselben Standard ausrichten.

Vorschlag (Aktivität 2.20)

Die Informationssicherheitspolitik wurde in mehreren Runden vom Projektteam erstellt und mit Hilfe weiterer zugezogener Personen (Vertreter der Konzernstäbe Recht, Versicherungen und Revision) konsolidiert. Der Umfang reduzierte sich dabei von über 30 Seiten der ersten Version auf schliesslich 4 Seiten, wobei der nicht-„politische“, "strategische" Teil in ein eigenes Dokument mit 13 Seiten ausgelagert wurde[101].

Der politische Teil des Vorschlags (in der Folge Informationssicherheitspolitik, *ISiPol,* genannt) wurde dem Präsidenten der Geschäftsleitung vom SiBe unterbreitet. Parallel dazu wurde die Erarbeitung des strategischen Teils vorangetrieben (in der Folge Informationssicherheitsstrategie, *ISiStrat,* genannt).

In der ISiPol wurden die Zielsetzungen und die Organisation der Informationssicherheit festgelegt. Die ISiStrat sollte v.a. die Vorgehensweise enthalten, anhand derer die Erreichung der Ziele vorangetrieben werden sollte. Da das Management jedoch die Freiheit hat, die Vorgehensweise zur Erreichung von vereinbarten oder vorgeschriebenen Zielen selbst festzulegen, war die Festlegung einer Vorgehensweise für den gesamten Konzern unangebracht. Aus firmenkulturellen Gründen wurde deshalb vorgesehen, dass diese Vorgehensweise zunächst nur für die Stabsbereiche des Konzerns gelten sollte. Sie sollten diese Vorgehensweise auch als erste anwenden, auf diese Weise mit gutem Beispiel vorangehen und nach einiger Zeit erste Ergebnisse der Verwendbarkeit des Vorgehens zur Verfügung stellen. Die schriftlich festgehaltene Vorgehensweise

---

101 Während eine *Politik* die Ziele und Rahmenbedingungen festlegt und auf strategischer Ebene beschreibt, *was* erreicht werden soll, enthält eine *Strategie* die Vorgehensweise, *wie* zur Erreichung dieser Ziele vorgegangen werden soll. Die Umsetzung der Strategie erfolgt auf strategischer, taktischer und operativer Ebene.

sollte zudem als beispielhafte Umsetzung (Muster) beigelegt werden, wenn die ISiPol verabschiedet und im Konzern verteilt werden würde, jedoch nicht als eigenständige Vorschrift festgelegt werden.

Zur Erarbeitung der ISiStrat wurde die Projektgruppe nochmals erweitert. Neben den schon erwähnten Konzernstabsstellen wurden Vertreter aus den Konzernstäben Patente und Konzerninformation hinzugezogen, um eine möglichst breite Abdeckung der betroffenen Bereiche der Konzernleitung zu erreichen. Ferner wurden aus Kapazitätsgründen und aufgrund ihrer Erfahrung weitere Mitarbeiter der Revisionsgesellschaft involviert.

Die ISiStrat umfasst im Wesentlichen die Kurzbeschreibung eines Verfahrens zur Erreichung von Informationssicherheit. Dieses vom Autor sehr allgemein definierte Verfahren wurde zunächst in Zusammenarbeit mit dem ehemaligen Leiter der Informationssicherheitsstelle an die Einsatzumgebung angepasst. In mehreren Gruppendiskussionen und Arbeitssitzungen erfolgten dann weitere Verfeinerungen. Das Verfahren besteht aus sechs Phasen und ist im Wesentlichen identisch mit dem Verfahren *ISIWAY 1.5*, welches später in Abschnitt 10.4 vorgestellt und in Abschnitt 10.5 evaluiert wird. Es wird in der ISiStrat jedoch nur grob beschrieben.

Diskussion (Aktivität 2.30)

Die Diskussion des Vorschlags wurde unter Einbezug der oben erwähnten Stellen solange fortgeführt, bis ein Konsens erreicht werden konnte. Daraufhin wurde die ISiStrat in den bestehenden Sicherheitsgremien vorgestellt; die einzelnen dort beteiligten Personen wurden zur Mitarbeit aufgefordert. Das entstehende Feedback erforderte eine erneute leichte Überarbeitung des Dokuments.

Verabschiedung (Aktivität 2.40)

Beide Dokumente – die strategisch ausgerichtete, für eine konzernweite Gültigkeit erarbeitete ISiPol sowie die taktisch ausgerichtete, für die Anwendung in den Stabsstellen konzipierte Verfahrensweise ISiStrat – wurden dem Präsidenten der Konzernleitung vom SiBe vorgelegt. Aufgrund der Tatsache, dass beide Dokumente in breit abgestützten Gremien erarbeitet wurden und ein Konsens weitgehend erreicht wurde, steht der Verabschiedung inhaltlich nichts im Wege.

Aus aktuellem Anlass wurde die Verabschiedung jedoch mehrmals aufgeschoben[102]. Dies ist jedoch nicht weiter problematisch, da sowohl ISiPol wie auch *ISIWAY*

---

102 Die Probleme, welche mit dem Anbrechen des Jahres 2000 in den einzelnen Teilbereichen und Tochtergesellschaften des Konzerns entstehen könnten, erfordern Sonderaufwände zur Lokalisierung und Behebung möglicher, aus diesem Jahreswechsel hervorgehender Störungen. Die dabei entstehenden Arbeiten sind ebenfalls als Senkung von Bedingungsrisiken zu betrachten und müssen dementsprechend von denselben Stellen wahrgenommen werden,

weitgehend technologieneutral formuliert sind und auf eine mehrjährige Lebensdauer hin formuliert wurden. Die Arbeit am Projekt SECNET konnte also dennoch fortgesetzt werden.

Was im Anschluss beschrieben wird, sind dementsprechend schon erledigte vorbereitende Teilarbeiten bzw. mit fortschreitendem Text eine Schilderung der geplanten Vorgehensweise und der dabei erwarteten Entwicklungen.

Unterlagen vorbereiten (Aktivität 2.50)

Als Kommunikationskanal zur Verbreitung der ISiPol wurde die Form *Konzernvorschrift* gewählt. Dies bedeutet, dass die Umsetzung der enthaltenen Inhalte für jeden davon betroffenen Mitarbeiter im Konzern verpflichtend ist. Die Verteilung erfolgt über die bestehenden Informationskanäle des allgemeinen unternehmerischen Sicherheitsbeauftragten, da in der Vorschrift selbst auch angeregt wird, den Informationssicherheitsbeauftragten jedes einzelnen Konzernbereichs und jeder Tochtergesellschaft dem jeweiligen Sicherheits-beauftragten unterzuordnen.

Für die ISiStrat wurde die Form *Gesellschaftsvorschrift* gewählt. Diese ebenfalls für alle Mitarbeiter verbindliche Festlegung der Umsetzungsverantwortlichkeit beschränkt sich auf die Gesellschaft, für welche diese Vorschrift bestimmt ist. Im konkreten Fall handelt es sich um die Zusammenfassung der Stabsbereiche, welche gemeinsam als Gesellschaft organisiert sind. Die Verbreitung erfolgt dann durch Verteilung der Dokumente, vorgenommen durch den Chef der Stabsbereiche.

Bewertungskriterienkatalog (Aktivität 2.51)

Für die Vorgehensweise im Projekt wurden lediglich die drei Grundanforderungen Verfügbarkeit, Integrität und Vertraulichkeit als Bewertungskriterien definiert. Zu jedem dieser Kriterien wurden die Werte 0, 1, 2 und 3 festgelegt, wobei 3 "hohe Anforderungen" im Kriterium bedeutet, 2 "mittlere", 1 "tiefe" und 0 "keine Anforderung". Die Auswirkungen der Nichterfüllung der damit verbundenen Anforderungen wurde als Text formuliert. Der gesamte Bewertungskriterienkatalog befindet sich im Anhang 3 des Verfahrens *ISIWAY 1.5*, welches in Abschnitt 10.4 dieses Kapitels kurz beschrieben und in Anhang C.2 wiedergegeben ist.

Objektklassifikation (Aktivität 2.52)

Die Objektklassifikation wurde ebenfalls durch einzelne Aktivitäten des Verfahrens festgelegt: Er werden zunächst nur *Informationssammlungen* und *technische Informationssysteme* gesamthaft betrachtet, und diese werden *Personen* zugeordnet.

---

welche die technische Infrastruktur zur Verfügung stellen. Aus diesem Grunde verzögert sich die Verabschiedung (und somit die Anwendung) der ISiPol und ISiStrat.

Allgemeiner Massnahmenkatalog (Aktivität 2.53)

Auf Basis des Code of Practice for Information Security [BSI-COP95], der in der ISiPol als Grundlage für die Informationssicherheit festgelegt wurde, haben die Projektteammitglieder spezifische Massnahmen für die Stabsbereiche des Konzerns zusammengestellt. Darin enthalten sind beispielsweise Massnahmen für die Klassifikation von Informationssammlungen, für das Anlegen redundanter Kopien (Backup) und für den Virenschutz. Ausgeschlossen wurde Massnahmen, welche durch das Vorgehen selbst abgedeckt wurden (z.B. Erstellen einer Informationssicherheitspolitik) oder welche irrelevant für die Stabsbereiche sind (z.B. Massnahmen für die Entwicklung von Software).

Dieser Massnahmenkatalog wurde in die ISiStrat integriert.

Referenzmaterialien erfassen (Aktivität 2.54)

Für die Referenzmaterialien wird grösstenteils auf die schon bestehenden vom Sicherheitsbeauftragten aufgebauten Bibliothek für Informationssicherheit zurückgegriffen. Im besonderen wurde aber das Verfahren *ISIWAY 1.5* selbst elektronisch erfasst und in HTML-Format zur Verfügung gestellt. So kann es auf Diskette weitergegeben, einfach kopiert[103] und auf jedem handelsüblichen PC betrachtet werden. Darüber hinaus gehört auch die Entwicklung und Bereitstellung des elektronischen Hilfsmittels *ISIGO 1.5* zu den Referenzmaterialien. Beides kann später auch über ein Intranet bereitgestellt werden.

Publikationsmedium wählen (Aktivität 2.55)

Als Medium wurden aus rein praktischen Überlegungen zunächst Papierdokumente gewählt. Während der Erstellung dieser Dokumente und Materialien waren jedoch Arbeiten am konzernweiten Intranet im Gang. Dieses würde sich als Publikationsmedium eignen. Zwischenzeitlich werden auch Disketten zur Weitergabe verwendet. Zur Erfassung und Bearbeitung der einzelnen Objekte wurde *ISIGO 1.5* auf Basis von *MICROSOFT EXCEL* implementiert (vgl. Kapitel 9). Die dabei entstehenden Datensammlungen lassen sich ebenfalls einfach weitergeben, woraus für die interne Kommunikation zwischen den Teilprojekten Vorteile entstehen.

Aufteilung des Untersuchungsobjektes (Aktivität 3.10)

Die Durchführung des Informationssicherheitsmanagements nach *ISIWAY* wurde in einzelnen Stabsbereichen des Konzerns schon begonnen. Diese Arbeiten beruhten jedoch auf freiwilliger Basis und auf eigener Überzeugung der Teilnehmer, da

---

103 Es ist beabsichtigt, die Verbreitung von *ISIWAY 1.5* durch einfache Verfügbarkeit und freie Kopierbarkeit zu fördern.

aufgrund der noch ausstehenden Verabschiedung der ISiPol und ISiStrat noch keine Umsetzungspflicht bestand.

Für die konzernweite Einführung wurden drei Stufen vorgesehen: In einer ersten Stufe geschieht sie in den Stabsbereichen der Konzernleitung, in einer zweiten Stufe in allen Gesellschaften der Schweiz und in einer dritten Stufe weltweit.

In der ersten Stufe sollen die Konzernstabsbereiche das Verfahren vollständig umsetzen. Dieser Bereich eignet sich besonders für ein erstes Projekt, da es sich hier grösstenteils um rein informationsverarbeitende Einheiten handelt, welche darüber hinaus zum Teil hoch sensitive Informationen bearbeiten. Ausserdem bestehen vielfältige Kontakte aus den Stabsbereichen in die anderen Bereiche des Konzerns, wodurch eine Vorbildfunktion erzielt würde. Die Leitung der Durchführung würde einer einzigen Person obliegen: dem ISiBe, der gleichzeitig auch als ISiKo der Stabsbereiche agieren würde.

Schulung der Koordinatoren (Aktivität 3.20)

In einer zweiten Stufe soll eine Einführung in den Konzerngesellschaften in der Schweiz erfolgen. Da diese Arbeit schon nicht mehr von einer Person alleine zu bewältigen ist, muss Ausbildungsaufwand getrieben werden. Auf diese Weise können das Wissen um das Verfahren und die Erfahrungen aus der Umsetzung in den Stabsbereichen eingebracht und weitergegeben werden. Da es sich beim Verfahren selbst um eine Vorschrift handelt, welche für die einzelnen Konzerngesellschaft nicht verbindlich ist, kann auf diese Weise eine einheitliche Vorgehensweise nicht zur Pflicht gemacht werden. Durch die einheitliche Ausbildung jedoch, welche zunächst vom Informationssicherheitsverantwortlichen selbst durchgeführt werden wird, kann die Einheitlichkeit zumindest motiviert werden. Dies um so mehr, als den einzelnen Beteiligten so auch die Möglichkeit gegeben werden kann, ihre eigenen Resultate mit denen der anderen Bereiche zu vergleichen. Die prinzipielle Motivation zur Umsetzung besteht aus der unternehmensweit gültigen Vorschrift heraus (ISiPol).

In einer dritten Stufe geschieht eine weltweite Einführung. Hier werden die vormaligen Schüler des ISiBe selbst zu Lehrern in denjenigen Tochter-gesellschaften, welche mit der eigenen Tochtergesellschaft international verbunden sind. Auch hier bleibt die prinzipielle Motivation zur Durchführung dieselbe, ebenso der Anreiz einer einheitlichen Vorgehensweise.

Durchführung planen (Aktivität 4.10)

Der ISiBe wird Prioritäten bei der Betreuung der einzelnen Teilprojekte setzen müssen, da er ab der zweiten Stufe nicht mehr alle Projekte direkt betreuen können wird. Er wird deshalb möglichst schnell die ISi-Koordinatoren als ISi-Beauftragte des jeweiligen Teilbereichs des Konzerns betrachten und auf diese Weise eine fachliche Hierarchie aufbauen. Sodann wird er bei denjenigen der stattfindenden

Teilprojekte, in denen er besonders hohe Risiken vermutet, selbst teilnehmen, die ISi-Koordinatoren bei der Durchführung unterstützen und hier direkt Einfluss zu nehmen versuchen. In den anderen Projekten wird er sich auf die Berichterstattung der jeweiligen ISiKos verlassen müssen und möglicherweise einzelne Stichproben-Kontrollen durchführen, um die Qualität der Umsetzung sicherzustellen.

Teilprojektdurchführung planen (Aktivität 4.20)

Die Durchführung der einzelnen Teilprojekte obliegt den jeweiligen ISi-Koordinatoren. Es wird davon ausgegangen, dass diese sich weitgehend an das vom ISiBe zur Verfügung gestellte Verfahren *ISIWAY 1.5* halten werden. Die bei der konkreten Durchführung erwarteten Probleme sind im Abschnitt 10.5 beschrieben.

Teilprojekt kontrollieren (Aktivität 4.50)

Die Kontrollphase ist in *ISIWAY* ebenfalls detailliert vorgesehen. Eine Rückmeldung des Abschlusses eines Teilprojektes abzuwarten und die Neuauslösung hinzunehmen, ist jedoch nur eine mögliche Reaktion. Wichtiger ist es für den ISiBe, in denjenigen Teilprojekten, in welchen seines Wissens oder aufgrund seiner Vermutungen grosse Risiken behandelt werden müssen, die Kontrolle der Durchführung der einzelnen Phasen vorzunehmen und zu begutachten, ob die Ziele des strategischen Dokumentes erreicht werden.

Review (Aktivität 5.10)

Es wird davon ausgegangen, dass der ISiBe in enger Zusammenarbeit mit dem SiBe des Konzerns regelmässig über den Status der laufenden, abgeschlossenen und geplanten Teilprojekte informiert. Der SiBe wird in seinem periodischen Bericht an die Konzernleitung diese Statusberichte kurz zusammenfassen und einzelne besondere Fälle lobend oder kritisierend herausheben. Möglicherweise wird er auch mit der Aufforderung an das Management herantreten, selbst aktiv zu werden und die Umsetzung des strategischen Dokuments von der betreffenden Konzerngesellschaft zu verlangen.

10.4 Definition von *ISIWAY* 1.5

Das Verfahren *ISIWAY,* so wie es in Kapitel 8 spezifiziert wurde, ist sehr komplex. Auch wenn es nicht prinzipiell ungeeignet für eine empirische Untersuchung[104] ist, müssen folgende Rahmenbedingungen berücksichtigt werden:

---

104 Aus den in der Einleitung (Abschnitt 1.2) und im Absatz "Verabschiedung" in Abschnitt 10.3 erwähnten Gründen konnte die empirische Studie, zu deren Durchführung *ISIWAY 1.5* definiert und verwendet wurde, nicht abgeschlossen werden.

- Eines der Ziele der Dissertation war die Definition eines einfach zu erlernenden und anzuwendenden Verfahrens. *ISiWAY* ist eine Gesamtkonzeption, welche diese Anforderung nur teilweise erfüllt (vgl. Profil in Anhang B.8, Tabelle B-8).
- Eine empirische Untersuchung muss auf verschiedenen vergleichbaren Resultaten beruhen. Es ist deshalb vorteilhaft, verschiedene Anwendungen geringen Umfangs zu betrachten, und nicht eine Anwendung mit hohem Umfang. *ISiWAY* wurde für die gesamthafte Anwendung in einer Unternehmung konzipiert. Es müssten also verschiedene Unternehmungen betrachtet werden, die allesamt *ISiWAY* verwenden.
- Die Komplexität von *ISiWAY* stellt hohe Anforderungen an die Konzeption und Operationalisierung der empirischen Untersuchung.

Aus diesem Grund wurde eine vereinfachte Version von *ISiWAY* definiert. Sie eliminiert viele der in *ISiWAY* bestehenden Freiheitsgrade und besteht nur noch aus einem Zyklus, welcher Elemente der Vorbereitung (DG0), der minimalen (DG1) und der angepassten Informationssicherheit (DG2) integriert und *ISiWAY 1.5* genannt wird. Daraus resultiert auch eine Vereinfachung der empirischen Untersuchung. Diese Vereinfachung ist zugleich eine erneute, *zweite Konkretisierung* des Informationssicherheitsprozesses.

Die Anwendung von *ISiWAY* 1.5 geschieht nicht durch eine Gesamtunternehmung, sondern durch die Koordinatoren für Informationssicherheit auf der Stufe einzelner Abteilungen. So ist es möglich, mehrere Anwendungen von *ISiWAY* 1.5 in derselben Unternehmung empirisch zu betrachten.

Um Aussagen über Erlernbarkeit und Verwendbarkeit von *ISiWAY* 1.5 generieren zu können, genügt die Betrachtung der ersten beiden Phasen von *ISiWAY* 1.5, da hier der Koordinator für Informationssicherheit die Vorbereitungsarbeiten und die Koordination der Erhebung vornehmen muss, also die beiden für ihn aufwendigsten Arbeiten. Diese Beschränkung reduziert den Aufwand für die empirische Untersuchung zusätzlich.

Die komplette Dokumentation zu *ISiWAY* 1.5 ist in Anhang C.2 wiedergegeben. Dieser Anhang kann aus dieser Dissertation extrahiert werden und als selbständige, von dieser Dissertation unabhängige Beschreibung des Verfahrens verwendet werden[105]. Darüber hinaus wurden Bedienungshinweise zur Verwendung von *ISiGO* 1.5 in diese Dokumentation integriert, um die Erlernbarkeit und Verwendbarkeit des Verfahrens weiter zu fördern.

---

105 D.h. es sind keine Verweise auf Kapitel oder Abschnitte dieser Dissertation enthalten.

10.5 Situationsbezogene Evaluation von *ISiWAY 1.5*

Verantwortung

Eines der zentrale Probleme bei der Erhebung und Bewertung von Informationssammlungen ist die korrekte Zuordnung der Ansprechpartner. Idealerweise ist eine eindeutige Zuordnung einer Informationssammlung zu einer Person möglich. Diese Person gilt dann nicht nur als Ansprechpartner, sondern auch als Verantwortlicher für Informationssicherheit. Eine solche eindeutige Zuordnung ist jedoch nicht immer möglich. Beispielsweise kommt es vor, dass eine Informationssammlung von verschiedenen Stellen gleichberechtigt gepflegt wird, in dem beispielsweise ein Adressbestand nach Postleitzahlen sortiert und in verschiedene Teile unterteilt wird, die den PLZ-Zonen entsprechen. In diesem Fall ist die verantwortliche Person (der Information Owner) am ehesten der Vorgesetzte all derer Stellen, welche die Bearbeitung vornehmen. Gerade dann ist dieser Vorgesetzte jedoch soweit von der konkreten Informationssammlung entfernt (d.h. arbeitet nicht persönlich damit), dass die Zuweisung der Verantwortlichkeit an ihn keine Massnahmen auslöst. Er empfindet die Sicherheitsverantwortung als zu abstrakt, da er möglicherweise weder über Erfahrungen im direkten Umgang mir der Informationssammlung verfügt, noch Einflussmöglichkeiten wahrnimmt.

Ebenfalls ist es möglich, dass eine asymmetrische Bearbeitung besteht, wenn beispielsweise die eine Abteilung Daten erfasst (z.B. Versicherungsverkäufer), welche eine andere Abteilung abruft und verändert (z.B. Schadensachbearbeiter). Hier hilft nur eine Funktionstrennung bei der korrekten Zuordnung der Verantwortlichkeit: eine Gruppe ist für die korrekte Erfassung verantwortlich, eine weitere für die korrekte Veränderung etc.

Dies sind jedoch nur zwei mögliche Beispiele für Konflikt- und Problemfälle. Ein radikaler, jedoch praktikabler Vorschlag für eine Lösung dieser Probleme ist die Ankündigung des ISiKos, Informationssammlungen, welche keinen Personen zugeordnet werden konnten, stillzulegen (d.h. sie zu löschen oder den Zugriff darauf zu verhindern). In den auf diese Ankündigung folgenden Diskussionen ist diejenige Person, welche das grösste Interesse am Weiterbestand der Informationssammlung hat, oft eindeutig bestimmbar ("Salomonisches Urteil"). Eine weitere, weniger radikale Lösung besteht darin, allen Personen, welche keine Verantwortung wahrnehmen möchten, den Zugriff auf die Informationen zu entziehen.

Ebenfalls ist oft zu beobachten, dass Personen sich mit der Begründung aus der Verantwortung stehlen möchten, die Notwendigkeit der Existenz einer Informationssammlung entstehe direkt aus den geschäftlichen Anforderungen und sei ihnen deshalb nicht persönlich zuzuordnen. Hier hilft ein Verweis auf die Treue- und Sorgfaltspflicht des Arbeitnehmers, welche aus dem Obligationenrecht hervorgeht und besagt, dass jeder Arbeitnehmer die ihm übertragenen Aufgaben

sorgfältig auszuführen hat und die ihm anvertrauten Firmengeheimnisse zu wahren hat [vgl. OR92 Art. 321a].

Weitere besondere Fälle stellen die Informationsverarbeitungen im Auftrag durch Dritte dar (Outsourcing oder Consulting). Auch im Auftragsverhältnis besteht zwar eine Sorgfaltspflicht, die Kontrolle ihrer Einhaltung ist jedoch schwieriger als bei Arbeitnehmern.

Gesamthaft kann gefolgert werden, dass die eindeutige und tragfähige Zuordnung der Verantwortung eine aufwendige Aufgabe sein kann, welche starken geäusserten oder ungeäusserten Auffassungen der Betroffenen unterliegt und für deren Lösung *ISIWAY* Anhaltspunkte bieten kann.

Organisatorische Einbindung des ISiBe

Als Koordinator für Informationssicherheit wird oft eine Person aus der Informatik-Abteilung gewählt, welche von den Inhalten der verarbeiteten Informationssammlungen keine Kenntnis hat[106]. Ziel muss es jedoch sein, eine Person zu finden, welche die Behandlung der Informationssicherheit von der inhaltlichen Seite her forciert. Eine solche Person ist oft Teil des mittleren Kaders des Linienmanagements der Unternehmung. In der Regel delegiert diese Person die Aufgaben der Informationssicherheit an einen Mitarbeiter des unteren Kaders. Geschieht dies, so gestaltet sich eine konstruktive Erarbeitung der Informationssicherheit sehr schwierig, da auf unterer Kaderebene die übergreifenden Geschäftsprozesse weit weniger deutlich erscheinen und eine stark operativ geprägte Arbeitsweise vorherrscht. Es muss also darauf geachtet werden, Informationssicherheitskoordinatoren auszuwählen, welche die unternehmerischen Tätigkeiten und die Werterbringung verstehen und berücksichtigen können.

Eine praktikable Lösung bietet hier die Bildung eines Teams, welches gemeinsam (unter Führung genau einer Person) die Koordination der Informationssicherheit in der Konzerngesellschaft wahrnimmt. Zu diesem Team gehören dann sowohl Personen aus dem mittleren Kader, der Informatik, allenfalls aus Rechtsabteilungen oder aus den Produktionsbereichen (Steuerungstechnik). Sie vereinbaren regelmässige Treffen, um das Teilprojekt der Informationssicherheit, welches in ihrer Konzerngesellschaft abläuft, gemeinsam voranzutreiben.

Kontrolle

Gerade bei der Behandlung von Bedingungsrisiken ist es üblich, dass erst nach dem Auftreten eines Störfalles reaktiv gehandelt wird, anstatt das Auftreten präventiv zu verhindern. Dies ist insbesondere darauf zurückzuführen, dass bei präventivem Handeln der Nachweis für den Handlungsbedarf nie konkret gegeben ist.

---

106 Im Wortsinn verarbeitet sie nur Daten, keine Informationen (vgl. Kap. 2).

Andererseits ist es jedoch gerade die Aufgabe des Managements der Informationssicherheit, diesen Nachweis konzeptionell zu erbringen, indem beispielsweise Risikoanalysen (oder wie in *ISIWAY 1.5* Werteanalysen) durchgeführt werden. Der ISiKo ist in seinem Bereich verantwortlich für die Durchführung des Verfahrens und muss deshalb *kontrollieren*, ob die einzelnen Phasen tatsächlich durchlaufen werden. Er muss seinem direkten Vorgesetzen Bericht über Status und Fortschritt erstatten und von diesem gegebenenfalls Unterstützung bei der Umsetzung verlangen. Zusätzlich kann der ISiBe ein Assessment durchführen und so bestimmen, ob die vom ISiKo wahrgenommenen Umsetzungsdiskrepanzen eine übergeordnete Intervention erfordern.

Motivation

Die Motivation der Betroffenen zur Umsetzung der Informationssicherheit steigt oft nur beim Eintritt von Störfällen. Für die rechtzeitige Entwicklung einer bleibenden Sicherheitskultur und die Förderung sicheren Verhaltens werden oft zu geringe Mittel aufgewendet. Dies ist insofern inkonsequent, als in den eigenen Mitarbeitern das grösste Potential steckt, um Störfälle zu verhindern (vgl. Abschnitt 5.3). Die sozialpsychologischen Aspekte menschlichen Verhaltens, welche hier zu beeinflussen wären, lassen sich jedoch nur schwer verändern. Dies wird deshalb oft vernachlässigt.

Auch für die Umsetzung von *ISIWAY* in den Tochtergesellschaften des Konzerns muss davon ausgegangen werden, dass die ausgebildeten ISiKos nur eine limitierte Ausbildung im sozialpsychologischen Bereich besitzen. Um so mehr muss die Übertragung der Sicherheitsmotivation auf diese Personen stattfinden, damit sie selbst mit einem sicheren Verhalten vorangehen können und auf diese Weise die Sicherheitskultur fördern.

Zielsetzung

Die Zielsetzungen, welche mit der Informationssicherheit verbunden werden, sind in der ISiPol (vgl. Abschnitt 10.3) nur abstrakt formuliert. Bei der Umsetzung ist es jedoch essentiell, dass die theoretischen Anforderungen in konkrete Handlungsanweisungen umgesetzt werden können. Der ISiKo ist dafür verantwortlich, diese Konkretisierung vorzunehmen und bei Zweifeln über die Interpretationsspielräume den ISiBe um Klärung zu bitten.

Bewertung

Das zentrale Problem der Bewertungsphase ist das Finden des angemessenen Wertes für das beurteilte Objekt. Zwar wurden in einer der ersten Aktivitäten die Beurteilungskriterien ausgewählt und Argumentationen für die Zuweisung eines Wertes angegeben. In der Umsetzung stellt sich jedoch immer wieder heraus, dass die festgelegte Argumentation unvollständig ist und auf wichtige, im konkreten

Zusammenhang interessierende Fragen keine Antworten bereithält. In diesem Fall muss die Argumentation vervollständigt werden, entweder durch Rückfrage beim Ersteller des Bewertungskriterienkatalogs (i.d.R. dem ISiBe) oder durch eigenmächtiges Festlegen von Argumenten, um so die begründete Zuweisung eines Wertes zu erlauben. Wichtig ist dabei nur, dass diese neue Argumentation auch bei zukünftigen Bewertungen konsequent verwendet wird.

Ebenfalls ist es in der Praxis oft notwendig, Zwischenwerte zu vergeben, z.B. den Wert 2.5 bei einer Skala von 0 bis 3. Die Nachfrage nach Zwischenwerten wird darauf zurückgeführt, dass sich einzelne Personen nicht auf einen genauen Wert festlegen möchten, da sie sich von der angegebenen Argumentation nicht genau betroffen fühlen. Der naheliegende Schluss, einfach mehr Werte zu definieren, ist also übereilt, da dies die Ausarbeitung einer höheren Zahl von Argumentationen notwendig machen würde, welche gegenseitig voneinander unabhängig sein müssen. Sehr wohl können die Befragten jedoch meistens angegeben, ob ihre Anforderungen an die entsprechende Informationssammlung höher oder niedriger als einer der definierten Werte sind. Die Zuteilung von Zwischenwerten sollte also prinzipiell erlaubt werden.

In der Praxis ist häufig zu beobachten, dass nur die Informationssammlungen mit den hohen Bewertungen berücksichtigt werden (z.B. mit 2.5 und 3 im Vertraulichkeitskriterium). Dies ist oft das Ergebnis einer falschen Priorisierung: Nicht die absolute *Höhe* der Bewertung ist massgebend, sondern die *Differenz*, welche zwischen den Anforderungen an die Information und der Sicherheitsleistung der verarbeitenden Systeme besteht. Auch eine als *intern* bewertete Informationssammlung *Kundenstamm* mit einer Vertraulichkeitsanforderung von 1 darf nicht mit einem System bearbeitet werden, welches als offen zugänglicher Server mit dem Internet verbunden ist (die Vertraulichkeitsleistung ist 0, die Differenz beträgt also 1).

Hingegen kann es durchaus sein, dass eine als hoch vertraulich bewertete Lohn- und Honorartabelle (die Vertraulichkeitsanforderung ist 3), welche beispielsweise nur auf Disketten gespeichert wird und nur auf einem Einzelgerät ohne Netzanschluss bearbeitet wird (die Vertraulichkeitsleistung ist ebenfalls 3) als sicher genug gilt (die Differenz beträgt 0) und nicht mehr zusätzlich gesichert werden muss. Prioritäten müssen also anhand der Differenzen und nicht anhand der absoluten Höhe festgelegt werden. Missachtung dieser korrekten Priorisierung kann also zu fehlerhafter, unvollständiger Behandlung der informationellen Risiken führen.

Fazit

Die Umsetzung von *ISIWAY 1.5* im betrachteten Konzern kann gelingen, wenn die notwendige Unterstützung durch die Konzernleitung und durch die Sicherheitsbeauftragten der einzelnen Konzerngesellschaften vorhanden ist. Durch die Einbindung des Verfahrens *ISIWAY 1.5* in die Phase 0 des Verfahrens *ISIWAY*

(gemäss Kapitel 8) können so vergleichbare, parallel und koordiniert ablaufende Sicherheitsteilprojekte entstehen, in welchen die einzelnen Personen wegen der absichtlich nicht vorhandenen zentralen Weisungsbefugnis Informationssicherheit im eigenen Interesse verfolgen. Die Umsetzung von *ISIWAY 1.5* im Konzern ist dabei nur der erste Schritt. Ein Wechsel auf den übergeordneten *ISIWAY*-Zyklus sollte später möglich sein (je nach Resultat des Teilprojektes erfolgt der Wechsel in den *ISIWAY*-Detaillierungsgrad 1 oder 2), so dass langfristig eine umfassende Informationssicherheit erreicht werden kann.

Dies wird ohnehin notwendig werden, da durch den langsamen Wandel der Industrie- zur Informationsgesellschaft (vgl. Kapitel 4) Information einen immer höheren Stellenwert bekommen wird. *ISIWAY* kann also den Anfang einer konsequenten, nachhaltigen Umsetzung der Informationssicherheit im Konzern bilden.

11 Ausblick

11.1 Erarbeitete Komponenten

Beitrag

Diese Dissertation umfasst vier grosse Beiträge (vgl. Abschnitt 1.1): Zum Ersten wurde ein *Rahmenwerk* für das Management der Informationssicherheit erarbeitet, welches Führungskonzeption, Informationsmanagement und Informatik-Sicherheit verbindet. Zum Zweiten wurden einige Verfahren, welche heute in der Praxis zur Anwendung kommen, anhand eines einheitlichen Schemas *bewertet, beurteilt und verglichen*. Dieses Schema wurde für genau diesen Zweck geschaffen, indem ein Superset der Konzepte erstellt wurde, auf denen die bewerteten Verfahren basieren. Das Schema kann prinzipiell zur Bewertung und Beurteilung weiterer Verfahren verwendet werden. Drittens konnten aus dieser vergleichenden Bewertung Anforderungen hergeleitet werden, welche für die Spezifikation eines neuen Verfahrens berücksichtigt wurden, mit dessen Hilfe sich umfassende Informationssicherheit in einer Unternehmung erreichen lässt. Viertens wurde der Prototyp eines Werkzeugs bereitgestellt, der die Anwendung dieses neuen Verfahrens vereinfacht.

Rahmenwerk

Informationssicherheit ist kein homogenes, einfach strukturierbares Gebiet. Es bestehen vielfältige Konzepte, Ideen und Fachgebiete, deren gegenseitige Beziehungen zueinander nicht sofort offensichtlich sind. In dieser Dissertation wurden deshalb die einzelnen Komponenten der Informationssicherheit unter den Oberbegriffen *Grundlagen*, *Elemente*, *Tätigkeiten* und *Prozesse* identifiziert, in einen gesamthaften Zusammenhang gestellt und so ein Rahmenwerk für die Informationssicherheit geschaffen. Dabei wurde von der unternehmerischen Information als primär schützenswerter Ressource ausgegangen. Das Bezugsobjekt der Informationssicherheit wurde strukturiert und identifiziert die (sekundär schützenswerten) Informationstechnologien. Das entstandene Rahmenwerk der Informationssicherheit gibt nicht nur Aufschluss über die vielfältigen Beziehungen und die Einordnung so unterschiedlicher Sachgebiete wie Controlling, Netzwerksicherheit, Sicherheitskultur etc., sondern es erlaubt auch, weitere und neu entstehende Fachgebiete anhand der dargestellten Unterteilung einzuordnen. Es konnte eine theoretische einheitliche Basis für weitere managementorientierte Arbeiten im Informationssicherheitsbereich geschaffen werden.

Vergleichende Bewertung

In der Literatur existieren verschiedene Publikationen, welche die Umsetzung von Informationssicherheit in Unternehmungen betrachten und Lösungsvorschläge enthalten. Diese unterscheiden sich nicht nur in Betrachtungsbreite und –tiefe, sondern bauen auf völlig unterschiedlichen Ansätzen, Zielsetzungen und Verfahren auf. Um den Vergleich dieser bestehenden Verfahren zu ermöglichen und so die Unterschiede ausweisen zu können, war zunächst die Definition eines einheitlichen, übergreifenden Schemas notwendig. Dieses stellt den Massstab dar, an welchem die bestehenden Verfahren gemessen werden. Mit etwas Aufwand liesse sich dieses Schema zu einem Zertifizierungsinstrument für Informationssicherheitsverfahren erweitern.

Eine anschliessende Beurteilung dieser Verfahren mit dem Schema führte zu einem breiten Katalog von Anforderungen, welche an ein „ideales" Verfahrens zu stellen wären. Innerhalb des Schemas wurden jedoch sich widersprechende Anforderungen definiert– die Ausgeprägteste darunter der gleichzeitige Anspruch auf Vollständigkeit und einfache Erlernbarkeit. Deshalb wurde als Anforderung an das neue Verfahren nicht Vollständigkeit angestrebt, sondern gezielt die Erfüllung derjeningen Anforderungen, bei denen mehrere der beurteilten Verfahren Schwächen zeigten.

Verfahren

Aufbauend auf dem Rahmenwerk und seinen verschiedenen Komponenten sowie dem Anforderungsprofil aus der vergleichenden Bewertung wurde der Prozess der Informationssicherheit zu einem Verfahren namens *ISiWAY* konkretisiert. Dessen Besonderheit ist die konsequente Einbeziehung der Personen, welche informationelle Inhalte innerhalb der Unternehmung verarbeiten. Ihnen wird nicht nur direkt oder indirekt die Verantwortung für die Sicherheit der ihnen anvertrauten Informationen übergeben, sondern sie werden zudem dazu verpflichtet, Informationssicherheitsmanagement gemäss Vorgaben der Unternehmungsführung zu gestalten. Für die vorbereitenden und betreuenden Aufgaben wurde die Position des *Informationssicherheitsbeauftragten* spezifiziert und seine Verantwortung, Koordinations- und Kooperationssteuerungstätigkeiten beschrieben. Im gesamten Prozess *ISiWAY* wird Informatik als reines Mittel zum Zweck betrachtet, wobei die hohe Bedeutung der Informationstechnologien für moderne Unternehmungen konsequent berücksichtigt wird.

Ferner zeichnet sich das Verfahren durch eine inkrementell steigende Betrachtungsbreite und –tiefe aus. Dies erlaubt einerseits einen schnellen, unkomplizierten und relativ einfach durchzuführenden Einstieg bis hin zu Erreichung der minimalen Informationssicherheit mit Grundschutz. In einem erweiterten, zweiten Detaillierungsgrad werden wertbezogene Analysen und Massnahmenzuteilungen vorgenommen, um auf diese Weise eine angemessenere

Umsetzung der Informationssicherheit zu erreichen. Für die Betrachtung und Senkung grösserer bestehender Risiken wurde ein dritter Detaillierungsgrad geschaffen, mit welchem sich die Risiken identifizieren lassen, spezifische risikosenkende Massnahmen festgelegt werden können und so risikogerechte Informationssicherheit erreicht werden kann. Schliesslich dient ein vierter Detaillierungsgrad dazu, einzelne Fachbereiche genauer zu betrachten (z.B. spezifische Technologien oder rechtliche Fragestellungen) und Informationssicherheit auf diese Weise umfassend zu erreichen. Ebenfalls im vierten Detaillierungsgrad geschieht die Betrachtung des Krisenmanagements, welches in einem weiteren, mit dem Wert 3.5 bezeichneten Detaillierungsgrad generisch definiert wurde. Aufgrund der vier Zyklen wird dieses Verfahren auch *ISIWAY 4* genannt.

Das hier definierte Verfahren umfasst also nicht nur die relevanten Inhalte und Vorgehensweisen des Managements der Informationssicherheit, sondern eignet sich auch durch die verschiedenen Betrachtungsbreiten und –tiefen für unterschiedliche Anwender und Anwendungsbereiche.

Prototyp

Zur Unterstützung der Durchführung dieses Prozesses wurde ein Hilfsmittel entworfen und implementiert. Vom Prozess selbst wurde dazu eine zusätzliche Variante namens *ISIWAY 1.5* angefertigt, welche eine noch einfachere Behandlung der Informationssicherheit (z.B. für kleine Projekte oder zum erstmaligen Einstieg) durch Beschränkung auf einen einzigen Zyklus erlaubt. Entsprechend wurde ein gemeinsames Datenmodell entwickelt, welches alle Entitäten von *ISIWAY 4* und *ISIWAY 1.5* umfasst und welches die Erfassung und Verwaltung aller bei der Durchführung der Verfahren entstehenden Daten erlaubt. Die Implementation des Datenmodells erfolgte mit dem Datenbankmanagementsystem *MICROSOFT ACCESS* als Basis für *ISIGO CENTRAL*. Aufgrund der Anforderungen im Umsetzungsprojekt wurde *ISIGO CENTRAL* funktionell nicht implementiert. Jedoch wurde konkret für die Unterstützung von *ISIWAY 1.5* das Hilfsmittel *ISIGO 1.5* definiert und auf Basis des Tabellenkalkulationsprogramms *MICROSOFT EXCEL* als Prototyp erstellt, mit dem Datenmodell von *ISIGO CENTRAL* über SQL-basierte Selektionsbefehle verknüpft und durch Makros zu einem voll funktionsfähigen Werkzeug ausgebaut.

Sowohl die Beschreibung von *ISIWAY 1.5* als auch das Hilfsmittel *ISIGO 1.5* sind Teil dieser Dissertation und können in Informationssicherheitsprojekten eingesetzt werden.

Es war beabsichtigt, mit den hier vorgestellten Konzepten und Ideen die Strukturierung der Informationssicherheit in der Unternehmung zu erleichtern. Es ist jedoch unerlässlich, dass eine prinzipielle, minimale Motivation der Unternehmungen zur Umsetzung der Informationssicherheit besteht, bevor dieses Thema überhaupt betrachtet wird. Es muss klar verstanden und allen Beteiligten

immer bewusst sein, dass der Informationssicherheit in der Unternehmung mindestens zweite Priorität nach den Zielen der Leistungserbringung zugeordnet werden muss. Entsprechend versteht sich diese Dissertation auch als Charakterisierung des Gesamtgebietes und soll einen Beitrag zum Verständnis dieses Gebietes liefern.

11.2 Folgeprojekte

Wie können die Ergebnisse dieser Dissertation weiter verwendet werden?

Im Rahmen dieser Dissertation konnten bei weitem nicht alle Probleme gelöst werden, welche in dem breiten Spektrum zwischen Informatiksicherheit, Informationsverarbeitung und unternehmerischem Handeln bestehen und der Informationssicherheit zugeordnet werden müssen. Insbesondere sind folgende Einzel-Thematiken für weitere Arbeiten denkbar:

- Die Abgrenzung zwischen Bedingungs- und Wagnisrisiken müsste genauer geklärt werden. Wenngleich in dieser Arbeit eine breite Grundlage von Begriffen gelegt wurde, könnte die Berücksichtigung weiterer relevanter Gebiete des Risikomanagements – z.B. aus dem Finanzbereich – dazu verwendet werden, genauer zwischen den willentlich und den unwillentlich eingegangenen Risiken zu unterscheiden. Vielleicht könnte eine derartige Arbeit auch konkrete Variablen definieren, welche die Berechenbarkeit von Teilrisiken beeinflussen und die quantitative Feststellung (formale Berechnung) der Sicherheit eines Systems ermöglichen.
- Die unter dem Stichwort "Information Warfare" zusammengefassten Entwicklungen der Spionage und Sabotage bieten ebenfalls genügend Ausgangsmaterial für die Erstellung weiterer Arbeiten. Es könnte beispielsweise betrachtet werden, welchen Einfluss politische oder makroökonomische Entwicklungen auf den Umfang derartiger Tätigkeiten haben. Es müsste sicherlich definiert werden, welche Einzeltätigkeiten zu diesem Bereich gehören und wie sie voneinander abgrenzbar sind. Auch die Bestimmung der Erkennbarkeit solcher Vorfälle, die notwendigen Erhebungsmethoden sowie die Identifikation aller Anforderungen, welche an diese Informationen gestellt werden, geordnet nach Träger der Anforderungen, müssten in einer solchen Arbeit detaillierter untersucht werden. Als Ergebnis könnten beispielsweise Aussagen über die Gefährdung einzelner Unternehmungen, Branchen oder ganzer Staaten entstehen.
- Nur ansatzweise konnten die soziokulturellen Probleme betrachtet werden, welche innerhalb einer Unternehmung aus der Einflussnahme von Personen auf die Sicherheit der unternehmerischen Informationsverarbeitung entstehen. Es ist relativ einfach, die ohnehin deterministische Verhaltensweise technischer Systeme durch gezielte Anwendung technischer Massnahmen zu

beeinflussen. Die Beeinflussung der Verhaltensweisen der Menschen, welche mit diesen technischen Systemen interagieren und zu deren Nutzen die Systeme gebaut wurden, ist jedoch ungleich schwieriger. Zwar bietet die Sozialpsychologie vielfältige Ansatzpunkte für die Erarbeitung einer Sicherheitskultur, doch da in vielen Unternehmungen Informationsverarbeitung immer noch mit Datenverarbeitung gleichgesetzt wird, besteht heute noch nicht genügend Bewusstsein, um in diesem Bereich die notwendigen Mittel bereitzustellen. Auch wäre es interessant, den Aufbau einer unternehmerischen Informationssicherheitskultur ins Zentrum einer wissenschaftlichen Arbeit zu stellen und, weitgehend frei von der Berücksichtigung technischer Gegebenheiten, Vorgehensweisen und Massnahmen zur gezielten Beeinflussung des menschlichen Verhaltens zu definieren.

- Neben den kulturellen, auf dem Verhalten mehrerer Personen aufbauender Effekte, könnten auch die individuellen Verhaltensweisen der Einzelpersonen genauer betrachtet werden. Information wird auch für jeden Einzelnen immer mehr zu einem schützenswerten Gut und deshalb müssten die Prämissen und Konzepte des *persönlichen Informationsmanagements*, das sich im Rahmen der zunehmenden Informationsorientierung in Wirtschaft und Gesellschaft zu entwickeln beginnt, untersucht und strukturiert werden.
- Aus wissenschaftlicher und praktischer Sicht wäre es interessant, die Eignung von *ISIWAY* und die Bewertung des hier vorgeschlagenen sowie anderer Verfahren empirisch genauer zu untersuchen. Aufgrund der Erkenntnis, dass für Projekte mit *ISIWAY 1.5* eine mehrmonatige, für solche mit *ISIWAY 4* eine mehrjährige Durchführungsdauer veranschlagt werden muss, sind derartige Untersuchungen im Rahmen einer einzigen Dissertation kaum möglich. Dem Autor ist nicht bekannt, dass heute empirische Untersuchungen bestehen, die sich mit der Eignung von Verfahren von Informationssicherheit beschäftigen.
- Interessant wäre es aus praktischer Hinsicht weiterhin, den hier entwickelten Prototypen *ISIGO 1.5* zu einem voll funktionsfähigen Produkt weiterzuentwickeln, welches auch *ISIWAY 4* unterstützt, und dabei konsequent zu versuchen, die in Kapitel 7 und 8 festgelegten Anforderungen an *ISIWAY* zu erreichen.
- Als *praxisorientiertes* Projekt muss die Umsetzung im Konzern, welche in Kapitel 10 beschrieben wurde, fortgesetzt werden, denn sie wurde erst begonnen. Auch wenn mit Politik und Strategie der Informationssicherheit die beiden Grundsatzdokumente bestehen und in absehbarer Zeit verabschiedet werden können, so sind die entsprechenden Inhalte noch lange nicht in die einzelnen Tochtergesellschaften vorgedrungen. Hier muss noch umfassende Kommunikations-, Überzeugungs- und Einführungsarbeit geleistet werden.

11.3 Fazit

Die Informatik unterliegt momentan einem starken Wandel, dessen Folgen für Wirtschaft und Gesellschaft noch kaum absehbar sind. Schon längst sind Unternehmungen, Einzelne wie auch die Gesellschaft als Ganzes von der korrekten und zuverlässigen Funktionsweise von Informationstechnologie abhängig. Einer der noch fehlenden Bausteine auf dem Weg zur Informationssgesellschaft ist das Vertrauen der Menschen in diese neue Technologie. Für viele Personen stellen Informatik und Informationsverarbeitung noch stets „Black Boxes" dar, die nur schwer verständlich sind und sich nicht immer kontrollieren lassen. Verständnis ist jedoch eine Voraussetzung für Vertrauen. Wer versteht, kann Verhalten voraussagen und fühlt sich zunehmend sicherer im Umgang mit diesen Technologien. Um dieses Verständnis und das Vertrauen gewinnen zu können, muss jeder Einzelne als Teil einer Unternehmung oder der Gesellschaft Fähigkeiten entwickeln, welche als *persönliches Informationsmanagement* bezeichnet werden können. Mit der zunehmend bewussten Wahrnehmung und Durchführung aktiver Informationsmanagementtätigkeiten werden die verwendeten Informationstechnologien immer mehr Mittel zum Zweck. In Zukunft kann deshalb viel eher auch ein persönliches Informations*sicherheits*management umgesetzt werden, als dies heute der Fall ist. Die explizite Weitergabe der Sicherheitsanforderungen, welche an eine Information gestellt werden, geschieht heute nur in den seltensten Fällen. Sich dieser Anforderungen bewusst zu werden, sie zu formulieren und ihre Einhaltung einzufordern, wird als Verhaltensweise an Bedeutung gewinnen.

Die vorliegende Dissertation identifiziert die Grundlagen eines derartigen Verhaltens und stellt ein mögliches Verfahren zur Durchführung des Informationssicherheitsmanagements zur Verfügung. Aufgrund des starken gesellschaftlichen Wandels muss angenommen werden, dass auch diese Dissertation nur einen Baustein auf dem Wege zu einer langfristigen, tiefgreifenden Veränderung persönlichen Verhaltens – sowohl innerhalb von Unternehmen wie auch als Teile der Gesellschaft – darstellt. Die erarbeiteten Grundsätze und Erkenntnisse stellen einen weiteren Schritt in der Entwicklung der Informatik bzw. Informationssicherheit dar. Der rasche Wandel in der Informationsverarbeitung, die immer weiteren neu entstehenden Anwendungsgebiete und die daraus entstehenden Gefährdungen z.B. für die Privatsphäre werden auch in nächster Zeit kontinuierlich Neuberwertungen und Verhaltensanpassungen erfordern. Aus heutiger Sicht scheint ein Wandel hin zur Informationsorientierung, wie er schon in der Einleitung dieser Arbeit postuliert wurde, unvermeidlich und ein entsprechendes persönliches Informationssicherheitsmanagement scheint notwendig. In diesem Sinne ist die Verwertung der vorliegende Arbeit wahrscheinlich an die Zeit der Jahrtausendwende gebunden und kann später vielleicht noch als Aufzeichnung des gedanklichen Erkenntnisstands dieser Zeit Verwendung finden.

Anhänge

A Exkurs: Informatik, EDV und IT

Die Begriffe *Elektronische Datenverarbeitung (EDV)*, *Informationstechnik (IT)* und *Informatik* werden im deutschsprachigen Raum unterschiedlich verwendet.

In Deutschland wird unter *EDV* die gesamte elektronische Datenverarbeitung als Funktion der Unternehmung verstanden und umfasst neben der Informationstechnik (*IT-* oder *EDV-System*) auch die organisatorischen Strukturen und Abläufe. Dasselbe wird in der Schweiz *Informatik* genannt. *Informatik* hat in Deutschland eine vornehmlich akademische Bedeutung und bezeichnet ein Fachgebiet oder eine Studienrichtung, welche sich mit technischen Aspekten von Informations- und Datenverarbeitung beschäftigt.

Das in Deutschland mit *EDV-System* Bezeichnete wird in der Schweiz selten so, sondern eher mit *IT-System* oder *Informatik-System* bezeichnet. Die *deutsche EDV-Sicherheit* entspricht deshalb der *schweizerischen Informatik-Sicherheit*. Die schweizerische *IT-Sicherheit* entspräche der deutschen *EDV-Systemsicherheit*, wird aber *EDV-Sicherheit* genannt. Der in der Schweiz *IT-Betrieb* oder *Informatik-Betrieb* genannte Betrieb und Unterhalt der technische IT-Systeme heisst in Deutschland *EDV-Betrieb*.

Es bestehen also drei Bedeutungen:

(1) Bezeichnung der wissenschaftlichen bzw. akademischen *Disziplin*, welche sich mit allen Aspekten der digitalen Verarbeitung von Informationen beschäftigt; Verwendung im akademischen Umfeld,

(2) Bezeichnung der *Abteilung oder Organisationseinheit*, deren Aufgabe innerhalb einer Unternehmung die Bereitstellung und Wartung aller digitalen informationstechnologischen Werkzeuge ist; dies umfasst die Prozesse und die Personen, welche für die Erfüllung dieser Aufgabe notwendig ist,

(3) Bezeichnung der *technischen Infrastruktur*, deren Bereitstellung und Wartung die Aufgabe der in (2) genannten Abteilung ist; ohne Prozesse und Personen.

Die Zuordnung dieser Bedeutungen zu den Begriffen wird in Tabelle A-1 und Tabelle A-2 dargestellt. Ein ✓ bedeutet, dass die entsprechende Bedeutung im Begriff enthalten ist; ein (✓) stellt dar, dass die Bedeutung je nach Zusammenhang enthalten sein kann.

Deutschland	**EDV**	**Informatik**	**Informations-technik, IT**	**EDV-System**	**Informatik-System**	**IT-System**	**Informations-system. IS**
1 akademische Disziplin		✓	(✓)				
2 Abteilung oder Organisationseinheit	✓						
3 Technische Infrastruktur	✓		✓	✓	✓	✓	✓

Tabelle A-1: Informatik, EDV und IT in Deutschland

Schweiz	**EDV**	**Informatik**	**Informations-technik, IT**	**EDV-System**	**Informatik-System**	**IT-System**	**Informations-system. IS**
1 akademische Disziplin		✓	(✓)				
2 Abteilung oder Organisationseinheit		✓					(✓)
3 Technische Infrastruktur	✓	✓	✓	(✓)	✓	(✓)	✓

Tabelle A-2: Informatik, EDV und IT in der Schweiz

In dieser Dissertation werden hauptsächlich die in der Schweiz gebräuchlichen Bedeutungen verwendet. Eine deutsche Entsprechung wird nach einem Schrägstrich beigefügt, wo dies dem Verständnis dient.

B Tabellen zur vergleichenden Evaluation

Auf den folgenden Seiten sind die Tabellen zur vergleichenden Evaluation in Kapitel 7 abgebildet.

B.0 Fragenkatalog

Tabelle B-0 enthält die Fragestellungen für die Bewertung von Informationssicherheitsverfahren. Es interessiert dabei nicht die konkrete inhaltliche Antwort auf die verschiedenen Fragen, sondern die Tatsache, ob und in welchem Masse die Frage aus dem Studium der Dokumentation heraus beantwortet werden kann!

Legende Typ: N: Quantitative Fragestellung
L: Qualitative Fragestellung
S: Spekulative Fragestellung

Variable			Formulierung	Typ
V1	**Auslösung**			
	a	***Bedarfsfeststellung***		
	a1	*Auslösende Institution oder Person*	Wer löst die ISi-Untersuchung aus?	L
	a2	*Auslösendes Ereignis*		
		Zeit	Wird die ISi-Untersuchung in einem zyklischen / repetitiven / regelmässigen Turnus ausgelöst?	L
		Vorfall	Wird die ISi-Untersuchung durch Vorfälle ausgelöst?	L
	a3	*Methode der Auslösung*	Wie geschieht die Auslösung der ISi-Untersuchung?	L
	b	***Projektmanagement***		
	b1	*Neue Projekte*		
		Auslösung	Wird die ISi-Untersuchung durch neue Softwareprojekte oder -produkte ausgelöst?	L
		Unterstützung	Unterstützt das Verfahren die Untersuchung noch nicht bestehender, geplanter Objekte?	L
	c	***Change Management***		
	c1	*Unternehmerische Veränderungen*	Wird die ISi-Untersuchung durch neue Veränderungen der Unternehmung ausgelöst?	L

Variable				Formulierung	Typ
V2	**Organisation**				
	a	***Projektteam***			
		a1	*Struktur*		
			Weisungsbefugnis	Haben die Projektmitglieder weisende Funktion?	L
			Verantwortlichkeit	Wer ist für den Erfolg des Projektes verantwortlich?	L
		a2	*Organisatorische Einordnung*	Wie ist das Projektteam in die Unternehmung eingeordnet?	L
		a3	*Dauer des Bestehens*	Wie lange bleibt das Projektteam bestehen?	L
		a4	*Teilnehmer*		
			Projektleiter	Wer leitet das Untersuchungsteam?	L
			Auswahl	Wie werden die Projektteammitglieder ausgewählt?	L
			Qualifikationen	Welche Qualifikationen müssen die Projektteammitglieder aufweisen?	L
	b	***Projektmanagement***			
		b1	*Eignung*	Ist das Verfahren als Grundlage des Projektmanagements geeignet?	L
		b2	*Zielfestlegung*	Wie wird das Projektziel festgelegt?	L
		b3	*Abgrenzung Breite*	Wie wird das Betrachtungsobjekt abgegrenzt?	L
		b4	*Abgrenzung Tiefe*	Wie werden die zu betrachtenden Inhalte abgegrenzt?	L
	c	***Projektdauer***			
		c1	*Planung*	Wie lange dauert die Planungsphase?	L
		c2	*Kontrolle*	Wie lange dauert die Kontrollphase?	L
		c3	*Anpassung*	Wie wird die Projektdauer den Anforderungen angepasst?	L
	d	***Kooperation und Koordination***			
		d1	*Koordination*	Wie geschieht die Koordination zwischen verschiedenen Informations-sicherheitsprojekten?	L
		d2	*Kooperation*	Wie geschieht die Kooperation zwischen (gleichzeitig laufenden) Informationssicherheitsprojekten?	L

Variable				Formulierung	Typ
V3	**Durchführung**				
	a	***Beschreibung allgemeiner Ablauf***			
		a1	*Abstraktion*	Wird der Ablauf der Untersuchung abstrakt beschrieben?	L
		a2	*Detaillierung*	Wird der Ablauf der Untersuchung konkret und detailliert beschrieben?	L
		a3	*Umfang*	Wie umfangreich ist die Dokumentation im Verhältnis zum Inhalt?	N
		a4	*Skalierung*	Bestehen verschiedene Teil-Dokumentationen je nach Adressaten des Verfahrens?	N
		a5	*Verfahren*	Werden Verweise auf andere Verfahren abgegeben?	N
		a6	*Literatur*	Werden Hinweise auf weiterführende Literatur abgegeben?	N
	b	***Ansätze***			
		b1	*Ad-Hoc*	Wird der ad-Hoc-Ansatz vertieft dargestellt?	L
		b2	*Grundschutz*	Wird der Grundschutz-Ansatz vertieft dargestellt?	L
		b3	*Bewertungsansatz*	Wird der Bewertungsansatz vertieft dargestellt?	L
		b4	*Risikoanalyse*	Wird der Risikoanalyse-Ansatz vertieft dargestellt?	L
		b5	*Vertiefung*	Werden weitere Vertiefungsmöglichkeiten vorgeschlagen?	L
	c	***Phasen***			
		c1	*Analyse*		
			Beschreibung	Wird die Analysephase beschrieben?	L
			Aktivitäten	Welche Aktivitäten umfasst die Analyse?	L
		c2	*Beeinflussung*		
			Beschreibung	Wird die Beeinflussungsphase beschrieben?	L
			Aktivitäten	Welche Aktivitäten umfasst die Beeinflussung?	L
		c3	*Kontrolle*		
			Beschreibung	Wird die Kontrollphase beschrieben?	L
			Aktivitäten	Welche Aktivitäten umfasst die Kontrolle?	L
		c4	*Daten*		
			Ein- / Ausgabe	Werden Ein- und Ausgabedaten der Phasen beschrieben?	L
			Datenfluss	Wird die Datenweitergabe innerhalb des Prozesses beschrieben?	L
		c5	*Tätigkeiten / Aktivitäten*		
			Beschreibung	Werden die einzelnen Aktivitäten beschrieben?	L
			Zuordnung zu Personen	Werden die Aktivitäten Personen zugeordnet?	L
			Abfolge	Wird der Ablauf der Aktivitäten beschreiben?	L
	d	***Skalierbarkeit***			
		d1	*Breite*	Wie geschieht die Anpassung der Grösse des Untersuchungsobjektes?	L

Variable				Formulierung	Typ
	d2	*Tiefe*		Wie geschieht die Anpassung der inhaltlichen Tiefe der Untersuchung?	L
e	***Ergebnisse***				
	e1	*Qualitative Ergebnisse*		Welche qualitativen Ergebnisse liefert die Untersuchung?	L
	e2	*Quantitative Ergebnisse*		Welche quantitativen Ergebnisse liefert die Untersuchung?	L
f	***Aufwand***				
	f1	*Erlernbarkeit*		Kann das Verfahren mit geringem Aufwand erlernt werden?	L
	f2	*Budgetierung*		Wie geschieht die Budgetierung und der Nachweis von Aufwand und Kosten?	L
	f3	*Integration in Arbeitsablauf*		Werden Aufwandsüberlegungen in die Untersuchung integriert?	L
	f4	*Kontrolle*		Wie wird der Aufwand kontrolliert?	L
	f5	*Entstehender Aufwand*		Kann das Verfahren mit geringem Aufwand durchgeführt werden?	S
g	***Nutzen und Ertrag***			Wie werden Nutzen und Ertrag der Untersuchung dargestellt?	L
h	***Massnahmenkataloge***				
	h1	*Existenz*		Bestehen Massnahmenkataloge als Teil der Dokumentation?	L
	h2	*Konkretisierung*		Sind die Massnahmenkataloge konkret gehalten?	L
	h3	*Inhalte*			
			Personelle Massnahmen	Werden personelle Massnahmen vorgeschlagen?	N
			Organisatorische Massnahmen	Werden organisatorische Massnahmen vorgeschlagen?	N
			Technische Massnahmen	Werden technische Massnahmen vorgeschlagen?	N
			Bauliche Massnahmen	Werden bauliche Massnahmen vorgeschlagen?	N
i	***Fragenkataloge und Checklisten***				
	i1	*Existenz*		Bestehen Fragenkataloge als Teil der Dokumentation?	N
	i2	*Checklisten*		Bestehen Checklisten als Teil der Dokumentation?	N
j	***Computergestützte Hilfsmittel***				
	j1	*Existenz*		Welches Hilfsmittel besteht zum ISi-Verfahren?	L
	j2	*Vereinfachung Verwaltung*		Wie vereinfacht dieses Hilfsmittel die Verwaltung der Daten, bzw. würde es sie vereinfachen?	S
	j3	*Vereinfachung Ergebnisproduktion*		Wie vereinfacht dieses Hilfsmittel die Erzeugung und Präsentation von Ergebnissen, bzw. wie würde es sie vereinfachen?	S
	j4	*Akzeptanz Verfahren*		Fördert dieses Hilfsmittel die Akzeptanz des Verfahrens, bzw. würde es sie fördern?	S

Variable				Formulierung	Typ
V4	**Fachbereiche**				
	a	***Analyse***			
		a1	*Prozesse*		
			Betrachtung	Wie werden die unternehmerischen Prozesse des Untersuchungsobjektes betrachtet?	L
			Revision	Werden die unternehmerischen Prozesse nachträglich kontrollierend betrachtet?	L
			Controlling	Werden die unternehmerischen Prozesse während des Ablaufs steuernd und kontrollierend betrachtet?	L
		a2	*Inhalte und Informationen*		
			Informations-zentrierter Ansatz	Wie wird Information als zentrales schützenswertes Objekt betrachtet?	L
		a3	*Institutionen*	Wie werden die Institutionen des Untersuchungsobjektes betrachtet?	L
			Gesellschaft und soziale Rahmenbedingungen	Werden Gesellschaft und soziale Rahmenbedingungen berücksichtigt?	L
			Unternehmung	Wird die Unternehmung als Ganzes betrachtet?	L
			Informationssystem	Wird das unternehmerische Informationssystem als Ganzes betrachtet?	L
			Rollen	Werden Personen und Rollen betrachtet?	L
		a4	*Instrumente*		
			Werkzeuge	Werden die Werkzeuge zur Datenverarbeitung betrachtet?	L
			IT- / EDV-System	Wird das IT- / EDV-System betrachtet?	L
			Principals	Werden die aktiven Elemente des IT- / EDV-Systems betrachtet?	L
			IT- / EDV-Ressourcen	Werden die IT- / EDV-Ressourcen betrachtet?	L
			IT-Plattformen	Werden die IT-Plattformen betrachtet?	L
			Anwendungs-systeme	Werden die Anwendungssysteme betrachtet?	L
			Kommunikations-systeme	Werden die Kommunikationssysteme betrachtet?	L
	b	***Beeinflussung***			
		b1	*Prozesse*		
			Neue Prozesse	Wie sind neue Prozesse zu etablieren?	L
			Prozessanpassungen	Wie sind die bestehenden Prozesse anzupassen?	L
			Budget und Kosten	Wie sind Budget- und Kostenbetrachtungen in die Prozesse zu integrieren?	L
			Komplexität und Interdependenzen	Wie werden Komplexität und Interdependenzen in den Prozessen berücksichtigt?	L
		b2	*Institutionen*		
			Neue Institutionen	Wie sind neue Institutionen zu etablieren?	L
			Motivation	Wie geschieht die Motivation der Mitarbeiter?	L

Variable				Formulierung	Typ
			Verantwortung		
			Eigentümer-prinzip	Wie werden die Informationsobjekte den Personen zugeordnet?	L
			Verantwort-lichkeit	Wer trägt die operative Verantwortung für die Informationssicherheit?	L
	b3	*Instrumente (Breite)*			
		Elemente des Bezugsobjekts		Wie werden die Bezugsobjekte abgegrenzt (Breite der Untersuchung)	L
c	***Inhalte (Tiefe)***				
	c1	*Teilgebiete*		Welche Teilgebiete der Betrachtung werden beschrieben?	L
	c2	*Kriterien*			
		Verfügbarkeit, Integrität, Vertraulichkeit		Werden die grundlegenden drei ISi-Kriterien berücksichtigt?	L
		Verbindlichkeit, Authentizität		Werden die beiden ISi-Kriterien Verbindlichkeit und Authentizität berücksichtigt?	
		Weitere vordefinierte Kriterien		Werden weitere vorgegebene ISi-Kriterien berücksichtigt?	L
		Selbst definierte Kriterien		Besteht die Möglichkeit, weitere Kriterien selbst zu definieren?	L

Tabelle B-0: Fragenkatalog

B.1 Bewertung BSI (D) IT-Sicherheitshandbuch

Variable	Wert	Bemerkungen und Beschreibung
V1	**∅=1.2**	**Auslösung**
a1	1	Es wird nur die allgemeine Verantwortung der Führungskräfte beschrieben, nicht die konkrete Auslösung.
a2	1	Der ursprüngliche Auslöser der Untersuchung wird nur ansatzweise erwähnt. Es werden einzelne allgemein bekannte Vorfälle geschildert.
a3	1	Es wird nur allgemeine Sensibilisierung im Vorwort erwähnt. Es besteht kein Verfahren und keine Methodik zur Auslösung.
b1	2	Die Auslösung bei neuen Softwareprojekten oder -produkten wird nicht beschrieben. Die Verwendung des IT-Sicherheitshandbuchs im Rahmen der Planung und Implementation eines neu entstehenden Systems ist zwar möglich, aber nicht konkret unterstützt. Um es dennoch zu tun, ist eine detaillierte Kenntnis des zu bauenden Systems notwendig. Da jedoch nicht immer in der Planung schon alle Details des Systems bekannt sind, ist auch dies problematisch. Lediglich die Evaluation von sicheren Systemen wird in Kapitel 7 beschrieben und baut auf dem IT-Evaluationshandbuch und den IT-Sicherheitskriterien auf.
c1	1	Die gesamte Betrachtung ist auf eine Erhebung und Beurteilung von Objekten ausgerichtet, die sich während der Erhebung nicht verändern. Zwar ist eine abgegrenzte Betrachtung von neuen oder veränderten Systemkomponenten denkbar und wird auch angeregt; Schnittstellen dazu oder Koordinationsverfahren werden indessen nicht vorgesehen.
V2	**∅=1.3**	**Organisation**
a1	1	Weisungsbefugnis und Organisation sind teilweise beschrieben, indem die generelle Verantwortung der Führungskräfte erläutert wird.
a2	1	Die organisatorische Einordnung wird teilweise beschrieben, indem die generelle Verantwortung der Führungskräfte und die Delegation erläutert werden.
a3	0	Es besteht keine Beschreibung der Dauer des Projektteambestandes. Die Dauer der Untersuchung (ein komplettes Durchlaufen des Zyklus) wird implizit angenommen..
a4	2	In Abschnitt 4.3 wird kurz beschrieben, aus welchen Bereichen Mitarbeiter teilnehmen müssen. Wie sie ausgesucht werden oder welche Qualifikationen sie aufweisen müssen, wird nicht erwähnt. Dies ergibt sich indirekt teilweise aus den Adressaten des Verfahrens.
b1	4	Aufgrund der klaren Struktur eignet sich das Verfahren als Grundlage des Projektmanagements.
b2	4	Die Festlegung des Projektziels ist einerseits durch die beschriebene Zielsetzung des IT-Sicherheitshandbuchs vorgegeben, andererseits entsteht sie als "Senkung der Risiken auf ein tragbares Mass".
b3	0	Keine Beschreibung der Abgrenzung der Breite der Untersuchung; sie bezieht sich implizit auf die gesamte Unternehmung.
b4	0	Keine Beschreibung der Abgrenzung der Tiefe der Untersuchung; alle zur Risikoreduktion notwendigen Inhalte sind relevant.
c1	0	Keine Beschreibung der Dauer der Planungsphase; implizit sind die Stufen 1 bis 3 (also 8 von 12 Schritten) der Planung zuzurechnen.
c2	0	Keine Beschreibung der Dauer der Kontrollphase; implizit sind die Stufen 11 und 12 (also 2 von 12 Schritten) der Kontrolle zuzurechnen.
c3	0	Keine Beschreibung der Korrektur der Projektdauer.

Variable	Wert	Bemerkungen und Beschreibung
d1	3	Durch den einheitlichen Aufbau des Verfahrens und die z.T. detaillierte Beschreibung der Ergebnisse besteht die Möglichkeit, Informationen zwischen verschiedenen Untersuchungen auszutauschen und diese so zu koordinieren.
d2	1	Im Prozess selbst werden keine Aussagen über die Kooperation verschiedener Projekte oder über Zentralisierung gemacht. In der Anwendung wird jedoch von einem Projektteam ausgegangen, welches unter einheitlicher Führung die Informationssicherheit untersucht und zu verbessern versucht, wobei verschiedene Personen mit einbezogen werden. Eine rein zentrale Steuerung liegt durch die Involvierung der IT-Nutzer in die Entscheidungsprozesse jedoch nicht vor, sie wird aber in mindestens einem Fall verlangt ([BSI-IT-SHB92], S. 101).
V3	**∅=2.5**	**Durchführung**
a1	4	Der gesamte Prozess wird abstrakt und übersichtlich dargestellt und beschrieben. Die Beschreibung ist gut nachvollziehbar und bietet eine gute Einführung.
a2	4	Die einzelnen Phasen, Schritte und Aktivitäten des Verfahrens werden konkret und detailliert beschrieben.
a3	4	Ca. 90% der Dokumentation enthalten die ausführliche Dokumentation und Beschreibung des Verfahrens.
a4	1	Einzelne Abschnitte wenden sich an unterschiedliche Adressaten, es wird jedoch keine konsequente Trennung.
a5	2	Es wird v.a. auf das IT-Evaluationshandbuch und die IT-Sicherheitskriterien hingewiesen, welche zur Zeit der Veröffentlichung des Verfahrens wichtige weitere Dokumentationen darstellten.
a6	4	In der ausführlichen Literaturliste wird weiterführende Literatur in den relevanten Bereichen genannt.
b1	0	Der Ad-Hoc-Ansatz wird nicht beschrieben.
b2	2	Der Grundschutz wird ansatzweise in Kapitel 11 berücksichtigt.
b3	0	Der Bewertungsansatz wird nicht beschrieben.
b4	4	Das beschriebene Verfahren entspricht gesamthaft dem Risikoanalyse-Ansatz.
b5	3	Es werden mit der Angabe unterschiedlicher Fachgebiete verschiedene ablaufbezogene und inhaltliche Vertiefungsmöglichkeiten vorgeschlagen.
c1	4	Die Analysephase ist ausführlich und detailliert beschrieben.
c2	3	Die Beeinflussungsphase ist beschrieben, die Beeinflussung geschieht mehrheitlich über die Massnahmen, welche separat beschrieben sind.
c3	1	Die Kontrolle der Umsetzung der Massnahmen, in der Aussagen über die Folgen einer mangelhaften Umsetzung zu finden wären, wird in der Beschreibung nur ansatzweise beschrieben. Es finden sich allerdings Rückkopplungsschritte, welche eine Annahme der Kontrolle erlauben.
c4	4	Die Beschreibung des Prozesses definiert sowohl Ein- als auch Ausgabedokumente, ist einheitlich für jeden Betrachtungsschritt und definiert die Datenweitergabe.
c5	4	Die einzelnen Aktivitäten werden grösstenteils detailliert beschrieben und mit Arbeitsmaterial ergänzt. Sie werden einzelnen Rollen im Projekt zugeordnet und in einen Ablauf gestellt.
d1	0	Die Anpassung der Untersuchungsbreite wird nicht beschrieben. Das Verfahren folgt unabhängig von der Grösse oder Komplexität des Betrachtungsobjekts, der Kenntnis der beteiligten Personen oder der Abhängigkeit des Unternehmens vom betrachteten Objekt immer demselben Schema. Lediglich die bestehenden Schutzmassnahmen werden in einem frühen Schritt des Verfahrens erhoben, beeinflussen den Ablauf ansonsten aber nicht.

Variable	Wert	Bemerkungen und Beschreibung
d2	2	Das IT-Sicherheitshandbuch umfasst genau einen Lösungsansatz zum Problemkreis der Informationssicherheit (Risikoanalyse und -management). Auch wenn es wichtige inhaltliche Bereiche (wie Versicherungen, Organisation, Notfallkonzeption, Sicherheitskriterien, Evaluationshandbuch und Grundschutzverfahren) identifiziert, beschreibt es sie doch nicht gesamtheitlich, stellt sie nicht in einen grösseren Zusammenhang und beschreibt nicht, wie sie im Verfahren behandelt werden sollen.
e1	3	Die im Prozess erzeugten qualitativen Ergebnisse insbesondere bzgl. der Risiken sind im Verfahren mehrheitlich beschrieben.
e2	2	Die quantitativen Ergebnisse geben einerseits über Anzahl und Gefährdung der erhobenen Objekte Auskunft, andererseits können auch Aussagen über Höhe und Veränderung des Risikos abgeleitet werden. Sicherheit selbst wird jedoch nicht quantitativ messbar.
f1	4	Durch die sowohl abstrakte als auch konkrete Beschreibung ist das Verfahren gut erlernbar.
f2	3	Zur Kosten-Nutzen-Betrachtung wird ein eigener Schritt durchlaufen. Die Sammlung der dazu notwendigen Daten ist nur knapp dokumentiert.
f3	1	Es werden nur wenige Aussagen über den entstehenden Aufwand der Durchführung abgegeben.
f4	0	Die Kontrolle erfolgt durch die Rückkopplungsprozesse, ist jedoch nicht beschreiben.
f5	0	Die zum Teil detailliert notwendige Erhebung der Objekte und die Erhebung der Vielzahl von möglichen Risiken, die unerlässlich ist, um realistisches Risikomanagement vornehmen zu können, führen zu hohem Aufwand bei der Durchführung des Verfahrens. Für einzelne, gut abgegrenzte Bereiche kann es jedoch zur realistischen Umsetzung empfohlen werden.
g	1	Die konkrete Darstellung des Ertrags (Nutzens) wird nur ansatzweise beschrieben.
h1	4	Die Dokumentation umfasst 178 (auf ein bis zwei Zeilen zusammengefassten und nicht weiter erläuterten) Massnahmen in 12 Bereichen, welche als Anhaltspunkt für den Grundschutz oder risikogerechten Schutz verwendet werden können.
h2	3	Die Massnahmenkataloge sind konkret, aber technologieneutral formuliert.
h3	4	Es werden alle vier Massnahmenbereiche berücksichtigt.
i1	4	Es sind ausführliche Fragenkataloge enthalten.
i2	3	Es sind Checklisten enthalten.
j1	0	Es bestehen keine Hilfsmittel als Teil der Dokumentation.
j2	3	Aufgrund der hohen Mengen an Erhebungsdaten bei der Erfassung der einzelnen Objekte ist eine Werkzeugunterstützung erforderlich. Eine auf Tabellenkalkulationen basierende Lösung ist dabei zuwenig leistungsfähig, sondern es sollte wegen der vielfältigen Abhängigkeiten muss ein Datenbanksystem verwendet werden. Eine manuelle Bearbeitung des Verfahrens ist – von Ausnahmefällen oder sehr kleinen Projekten – sehr schwierig.
j3	2	Die Erzeugung und Präsentation von Ergebnissen würde vereinfacht.
j4	4	Ein Hilfsmittel würde die Akzeptanz massiv fördern, da der sonst manuell zu tragende Aufwand massiv reduziert wird.
V4	**∅=1.8**	**Fachbereiche**
a1	1	Das IT-Sicherheitshandbuch orientiert sich nur ansatzweise an unternehmerischen Prozessen und berücksichtigt Verarbeitungsvorgänge oder Informationsflüsse zwischen verschiedenen unternehmerischen Abteilungen nur ansatzweise.

Variable	Wert	Bemerkungen und Beschreibung
a2	2	Im Sicherheitsprozess wird die Information von Nutzern bewertet, was auf eine inhaltliche Betrachtung schliessen lässt. Die Bewertung geschieht jedoch nur im Hinblick auf den potentiellen Schaden und Information wird nicht als unternehmerischer Wert betrachtet.
a3	2	Im IT-Sicherheitshandbuch finden sich zwar einzelne Verweise auf die rechtlichen und gesellschaftlichen Rahmenbedingungen, auch eine Kurzbeschreibung in Anhang C und eine Verzeichnis in Anhang D. Inhaltlich werden dies jedoch nicht im Detail betrachtet. Der technische Aspekt des IT-Systems steht im Vordergrund. Es wird immer von einem behördlichen (oder unternehmerischen) Einsatz des Systems ausgegangen. Personen sind als operative oder taktisch steuernde Institutionen erwähnt und berücksichtigt, jedoch wird Informationssicherheit niemals unabhängig vom IT-System betrachtet.
a4	4	Das IT-Sicherheitshandbuch beschäftigt sich in erster Linie mit dem technischen Aspekt von Informationen und ihrer Verarbeitung. Die gesamte Betrachtung ist auf eine Erhebung von Objekten ausgerichtet, welche zwar im Detail in acht Kategorien betrachtet werden, deren Abhängigkeit auch erwähnt und ansatzweise modelliert wird, allerdings nicht konsequent betrachtet wird. Dabei wird zwar nicht auf einzelne Dateien eingegangen, jedoch auf technische Komponenten wie z.B. Diskettenlaufwerke und Bandarchiv ([BSI-IT-SHB92], S. 159)
b1	1	Die Abläufe der Informationsverarbeitung und der Informationssicherheit werden durch das IT-Sicherheitshandbuch nicht nachhaltig verändert. Einzig die erwähnten Massnahmen können solche Veränderungen auslösen, sind jedoch nicht genau genug spezifiziert. Das IT-Sicherheitshandbuch macht keine konkreten Angaben über aufzubauende oder zu verändernde Prozesse, welche nach Durchführung einer Untersuchung bestehen bleiben oder als ihre Folge errichtet werden.
b2	1	Das Eigentümerprinzip ist im Prozess des IT-Sicherheitshandbuches nicht erwähnt und wird auch nicht konsequent umgesetzt. Lediglich eine Zuweisung an die involvierten Personen der betrachteten Abteilungen wird angestrebt. Der Informationssicherheitsprozess als Ganzes ist eher extern zum Linienmanagement zu sehen; Selbstverantwortung wird nicht gefördert. Revisionsfähigkeit wird auch nur am Rande betrachtet.
b3	1	Das Verfahren des IT-Sicherheitshandbuch orientiert sich an Personen und berücksichtigt zwei Rollen: die der Anforderungssteller an die Informationsverarbeitung (Nutzer und Inhaber) und die des Projektleiters für die gesamthafte Gewährleistung. Die Rolle des Verwalters von Informationsobjekten, also derjenigen Person, die konkret die auf Einhaltung der beschlossenen Massnahmen im operativen Betrieb achten muss, wird nicht berücksichtigt. Es wird keine Aussage zur Motivation der betroffenen Personen abgegeben.
c1	2	Es besteht keine direkte Beschreibung, welche inhaltlichen Thematiken wann behandelt werden sollen.
c2	2	Das IT-Sicherheitshandbuch definiert nur die drei Anforderungen an Verfügbarkeit, Integrität und Vertraulichkeit. Diese werden als Grundbedrohungen des Verlusts der jeweiligen Eigenschaft definiert. Es wird keine darüber hinausgehende Betrachtung der Anforderungen motiviert. [Die Qualitätsanforderungen, wie sie in den im IT-Sicherheitshandbuch referenzierten und beschriebenen IT-Sicherheitskriterien gefordert werden, sind hier nicht berücksichtigt, da sie anders hergeleitet und aufgebaut sind]. Weitergehende Inhalte werden definiert, aber nicht genau spezifiziert.

Tabelle B-1: Bewertung BSI (D) IT-Sicherheitshandbuch

B.2 Bewertung BFI Grundschutzverfahren

Variable	Wert	Bemerkungen und Beschreibung
V1	**∅=2**	**Auslösung**
a1	3	Die Auslösung geschieht auf gesetzlicher Grundlage (Verordnung) und ist kurz beschrieben.
a2	3	Das beschriebene Verfahren enthält einen Zyklus. Vorfallbezogene Auslösung ist im Massnahmenkatalog enthalten.
a3	0	Die Methode der Auslösung ist nicht beschrieben.
b1	2	Die Auslösung des Verfahrens bei neuen Softwareprojekten oder -produkten und seine Anwendung dabei ist in den Massnahmen rudimentär beschrieben.
c1	2	Die Auslösung des Verfahrens aufgrund unternehmerischer Veränderungen ist in den Massnahmen rudimentär beschrieben.
V2	**∅=2.1**	**Organisation**
a1	4	Die Weisungsbefugnis und Verantwortung ist detailliert beschrieben. Sie bezieht sich konkret auf die angestrebte Einsatzumgebung und berücksichtigt deshalb die organisatorischen Regelungen der schweizerischen Bundesverwaltung.
a2	4	Die organisatorische Einordnung des Projektteams ist detailliert beschrieben.
a3	0	Es werden keine Angaben über Dauer der Untersuchung oder Bestehen des Projektteams gemacht.
a4	3	Leitung des Projektteams und Qualifikation werden nur am Rande behandelt; implizit ist die verantwortliche Person auch Projektleiter. Die Auswahl der Teilnehmer ist durch die organisatorischen Rahmenbedingungen weitgehend gegeben.
b1	2	Das Verfahren ist teilweise als Projektmanagementverfahren geeignet, definiert die Phasen aber nur rudimentär und beinhaltet keine Ergebnisdefinition.
b2	4	Die Zielfestlegung ist durch die Einhaltung der Verordnung gegeben. Das Ziel des Verfahrens wird beschrieben.
b3	3	Die Betrachtungsbreite wird implizit durch die Beschränkung auf den Verantwortungsbereich des Projektleiters abgegrenzt.
b4	3	Die Abgrenzung der Inhalte geschieht durch die speziellen Bewertungskriterien und die Massnahmen.
c1	0	Die Dauer der Planungsphase wird nicht beschrieben.
c2	0	Die Dauer der Kontrollphase wird nicht beschrieben.
c3	0	Die Korrektur der Projektdauer wird nicht beschrieben.
d1	2	Durch einheitliche, standardisierte, ausführlich beschriebene Formulare ist Koordination prinzipiell möglich. Es wird jedoch nicht beschrieben, wie dies durchgeführt wird. Sie geschieht in der Anwendung des Verfahrens durch das Bundesamt für Informatik selbst.
d2	2	Die Koordination geschieht zentral durch das Bundesamtes für Informatik auf Anfrage oder bei übergreifenden Problemen, ist aber inhaltlich nur ansatzweise beschrieben.

V3	∅=1.7	Durchführung
a1	4	Es besteht eine abstrakte Beschreibung des Verfahrens mit den relevanten Inhalten.
a2	2	Die konkrete Beschreibung erschöpft sich in den Hinweisen zum Ausfüllen der Erhebungsformulare.
a3	2	Die Beschreibung des Verfahrens umfasst ca. 25% der Dokumentation.
a4	0	Es besteht nur eine Beschreibung, also keine adressatenspezifische Dokumentation.
a5	1	Es werden nur allgemeine Hinweise auf vertiefte Risikobetrachtungen abgegeben.
a6	1	Es werden nur Hinweise auf allgemeine gesetzliche Rahmenbedingungen und Verordnungen bzw. weitere Weisungen abgegeben.
b1	0	Der Ad-Hoc-Ansatz wird nicht beschrieben.
b2	3	Der Grundschutzansatz wird nicht vertieft dargestellt, das Verfahren behandelt ihn jedoch implizit.
b3	3	Der Werteansatz wird beschrieben, indem die Umsetzung von Schutzmassnahmen von der Bewertung abhängig gemacht werden.
b4	0	Der Risikoanalyseansatz wird nicht beschrieben.
b5	0	Es werden keine weiteren Vertiefungsmöglichkeiten angegeben.
c1	2	Die Analyse umfasst nur die Erhebung und Bewertung der Objekte und wird inhaltlich rudimentär beschrieben.
c2	2	Die Beeinflussung besteht v.a. aus der Umsetzung der Massnahmenkataloge in Abhängigkeit der Bewertung und wird inhaltlich nur grundlegend ausgeführt.
c3	0	Die Kontrollphase wird nicht beschrieben.
c4	3	Die Ausgabedaten sind durch die Erhebungsformulare gegeben. Die Datenweitergabe ist nur im Hinblick auf die Kooperation geregelt. Eingabedaten werden nicht beschrieben.
c5	4	Die einzelnen Aktivitäten innerhalb der Phasen werden kurz beschrieben. Die Zuordnung geht eindeutig aus der Beteiligung am Projektteam hervor.
d1	0	Die Anpassung der Untersuchungsbreite wird nicht beschrieben.
d2	0	Die Anpassung der Untersuchungstiefe wird nicht beschrieben.
e1	1	Die qualitativen Ergebnisse werden nicht beschrieben. Durch die formalisierte Erfassung ist eine Herleitung qualitativer Aussagen möglich.
e2	3	Die quantitativen Resultate der Erhebung bestehen aus der Zusammenstellung umzusetzender Massnahmen.
f1	4	Das Verfahren ist durch den einfachen Ablauf, die kurze Beschreibung und die Beschränkung auf wenige Objektklassen gut erlernbar.
f2	0	Die Budgetierung und der Nachweis von Aufwand und Kosten ist nicht beschrieben.
f3	0	Die Integration von Aufwandsüberlegungen in den Arbeitsablauf wird nicht beschrieben.
f4	0	Die Kontrolle des Aufwands wird nicht beschrieben.
f5	2	Bei der Anwendung des Verfahrens kann aufgrund der teilweise komplexen Zusammenhänge (Vererbung) zwischen den Systemen hoher Aufwand entstehen, aufgrund des einfachen Objektmodells ist dies jedoch unwahrscheinlich.
g	0	Keine Beschreibung.
h1	4	Es bestehen umfangreiche Massnahmenkataloge als Teil der Dokumentation.

h2	4	Alle Massnahmen werden konkret und zum Teil technologiespezifisch beschrieben.
h3	4	Alle Massnahmenbereiche werden abgedeckt.
i1	1	Die Erhebungsformulare können als rudimentäre Fragenkataloge betrachtet werden.
i2	0	Die Massnahmen können als Checklisten verwendet werden (vgl. oben), ansonsten keine Kataloge.
j1	1	Im BFI besteht ein Hilfsmittel "Chac", welches nicht publiziert wird und dort zur Erfassung und Beurteilung der Objekte verwendet wird.
j2	4	Die Verwaltung der Daten und die Berechnung der Vererbung würde durch die Verfügbarkeit eines einfachen Hilfsmittels stark vereinfacht.
j3	4	Die Darstellung der Ergebnisse würde durch die Verfügbarkeit eines einfachen Hilfsmittels stark vereinfacht.
j4	2	Die Motivation für die Anwendung des Verfahrens basiert v.a. auf der Kürze und Einfachheit des Verfahrens und auf der Verpflichtung zur Anwendung. Ein Hilfsmittel hätte nur beschränkte Motivationswirkung.
V4	**∅=1.7**	**Fachbereiche**
a1	0	Unternehmerische Prozesse werden nicht berücksichtigt.
a2	2	Es geschieht eine inhaltlich differenzierte Bewertung der Datensammlungen, ansonsten handelt es sich aber um einen technikzentrierten Ansatz.
a3	1	Institutionen der Unternehmung werden nicht berücksichtigt, sondern aufgrund der einheitlichen Strukturen der Untersuchungsumgebung (Bundesverwaltung) vorausgesetzt.
a4	4	Die technischen Elemente der Informationsverarbeitung werden durch die Erhebung und die Massnahmen vollständig abgedeckt.
b1	2	Die Etablierung neuer Prozesse wird nur in den Massnahmenkatalogen beschrieben.
b2	3	Die Einrichtung neuer Institutionen wird in den Massnahmenkatalogen beschrieben bzw. vorausgesetzt (Informationssicherheitsbeauftragter der Organisationseinheit, Datenschutzbeauftragter, etc.). Das Eigentümerprinzip wird umgesetzt.
b3	0	Die Breite der untersuchten Elemente wird nicht abgegrenzt.
c1	1	Es werden keine inhaltlichen Teilgebiete beschrieben; Datenschutz wird als einzige Vertiefung erklärt.
c2	2	Es werden spezielle Kriterien definiert (vier davon für Daten), die Definitionen weiterer Kriterien ist nicht vorgesehen und die definierten können nicht eindeutig auf die drei üblichen Grundbedrohungen der Verfügbarkeit, Integrität und Vertraulichkeit abgebildet werden.

Tabelle B-2: Bewertung BFI Grundschutzverfahren

B.3 Bewertung BSI (D) IT-Grundschutzhandbuch

Variable	Wert	Bemerkungen und Beschreibung
V1	**∅=1.8**	**Auslösung**
a1	2	Es wird kurz beschrieben, dass die Initiative für die Auslösung vom Management ausgehen muss.
a2	2	Das Verfahren ist zyklisch aufgebaut, und die Feststellung des Sicherheitsbedarfs wird berücksichtigt.
a3	3	Der "Aktionsplan zur Initiierung des IT-Sicherheitsprozesses" wird beschrieben und umfasst eine Methodik zur Auslösung der ISi-Untersuchung.
b1	1	Die Möglichkeit, das IT-Grundschutzhandbuch bei neuen Softwareprojekten oder -produkten zu verwenden, wird erwähnt.
c1	1	Die Notwendigkeit, bei Veränderungen des unternehmerischen Umfelds das IT-Grundschutzhandbuch einzusetzen, wird erwähnt.
V2	**∅=1.8**	**Organisation**
a1	4	Die Strukturen des Projektteams werden detailliert dargestellt.
a2	4	Die organisatorische Einordnung des Projektteams wird detailliert beschrieben.
a3	1	Die Dauer des Bestehens des Projektteams wird nicht beschreiben. Implizit wird die Dauer der Durchführung des Verfahrens angenommen.
a4	4	Anforderungen, Auswahl und Qualifikationen der Projektteamteilnehmer werden detailliert beschrieben.
b1	2	Das Verfahren ist bedingt für das Projektmanagement geeignet, da Phasen und Ziele der Phasen festgelegt werden. Es ist allerdings nicht projektorientiert dargestellt.
b2	3	Das Ziel der "Schutzbedarfsfeststellung" wird in einer eigenen Phase behandelt.
b3	1	Die Abgrenzung des Betrachtungsobjekts wird nicht beschrieben. Das Verfahren bezieht sich auf die "gesamte IT".
b4	3	Die zu betrachtenden Inhalte werden gemäss Bedarfsfeststellung im Projekt abgegrenzt, dies ist beschrieben.
c1	0	Die Dauer der Planungsphase ist nicht beschrieben.
c2	0	Die Dauer der Durchführungsphase ist nicht beschrieben.
c3	0	Die Dauer der Kontrollphase ist nicht beschrieben.
d1	0	Die Koordination und Kooperation zwischen verschiedenen Projekten wird nicht beschrieben. Die Formate der Ergebnisse sind nicht festgelegt, deshalb ist eine Koordination nur durch individuelle Absprachen möglich.
d2	0	vgl. d1
V3	**∅=2**	**Durchführung**
a1	3	Es besteht eine abstrakte Beschreibung der Vorgehensweise.
a2	2	Die einzelnen Phasen werden weitgehend detailliert, ohne jedoch einzelne Aktivitäten zu identifizieren.
a3	1	Das Verfahren belegt nur einen geringen Anteil (ca. 5%) des gesamten Dokumentationsumfangs, der hauptsächlich aus Massnahmen besteht.
a4	1	Es bestehen keine auf bestimmte Ansprechsgruppen bezogenen Dokumentationen. Implizit wird eine Eignung für verschiedene Gruppen angestrebt.
a5	3	Es wird auf die Risikoanalyse als Ergänzung verwiesen.

Variable	Wert	Bemerkungen und Beschreibung
a6	4	Es werden einzelne Bezugsdokumente, Literaturlisten und weiteres ausführliches Referenzmaterial angegeben.
b1	0	Der Ad-Hoc-Ansatz wird nicht beschrieben.
b2	4	Das Verfahren implementiert den Grundschutzansatz.
b3	0	Der Werteansatz wird nicht beschrieben.
b4	1	Der Risikoanalyse-Ansatz wird kurz beschreiben und es sind Verweise darauf enthalten.
b5	0	Es werden keine weiteren Vertiefungsmöglichkeiten beschrieben.
c1	3	Die Analysephase wird in zwei Schritten beschrieben.
c2	4	Die Beeinflussung wird detailliert beschrieben.
c3	2	Die Kontrolle wird grundlegend beschrieben.
c4	0	Ein- und Ausgabedaten der Phasen werden nicht beschrieben.
c5	2	Einzelne Tätigkeiten in den Phasen werden teilweise und grundlegend beschrieben.
d1	0	Die Anpassung der Breite des Untersuchungsobjektes wird nicht beschrieben.
d2	1	Die Anpassung der Untersuchungstiefe geschieht implizit über den festgestellten Schutzbedarf.
e1	4	Als qualitative Ergebnisse entstehen die umgesetzten Schutzmassnahmen mit Berücksichtigung der Details der verwendeten Technologien.
e2	0	Die Generierung quantitativer Ergebnisse wird nicht beschrieben.
f1	4	Das Verfahren ist einfach dargestellt und beschrieben und deshalb gut erlernbar.
f2	0	Budgetierung und Nachweis der Kosten und Auswände wird nicht beschrieben.
f3	2	Die Integration des Arbeitsaufwands in die Untersuchung wird in der Planungsphase ansatzweise beschrieben.
f4	0	Es wird keine Aufwandskontrolle beschrieben.
f5	3	Der entstehende Aufwand ist in starkem Mass abhängig von der Komplexität des betrachteten Systems, aber prinzipiell gering.
g	0	Nutzen und Ertrag der Untersuchung werden nicht dargestellt.
h1	4	Der überwiegende Teil des IT-Grundschutzhandbuchs besteht aus Massnahmenvorschlägen.
h2	4	Alle Massnahmen sind sehr konkret und grösstenteils technologiespezifisch.
h3	4	Alle Massnahmenbereiche werden berücksichtigt.
i1	3	Fragenkataloge sind enthalten.
i2	3	Checklisten sind enthalten und können darüber hinaus auf Basis der Dokumentation erstellt werden.
j1	3	Es wird eine CD mit dem gesamten Text des Grundschutzhandbuches mitgeliefert, jedoch kein Verwaltungswerkzeug.
j2	2	Die Verwaltung würde nur teilweise vereinfacht, da das Grundschutzhandbuch stark technisch orientiert ist und so von vielen technischen Angaben abhängt.
j3	0	Die Erzeugung belegbarer Ergebnisse wird von der CD-ROM nicht direkt gestützt.
j4	3	Die Verfügbarkeit der Referenz auf CD-ROM unterstützt die Suche und fördert die Verwendung.

Variable	Wert	Bemerkungen und Beschreibung
V4	**∅=2.4**	**Fachbereiche**
a1	2	Prozesse werden durch die Massnahmen behandelt, jedoch nicht im Verfahren selbst.
a2	0	Die Betrachtung ist stark auf die Technik zentriert. Inhalte werden nicht berücksichtigt.
a3	2	Umgebung der Unternehmung und die Unternehmung als Ganzes werden nur ansatzweise berücksichtigt. Rollen und inhaltliche Informationen werden v.a. in den Massnahmen berücksichtigt.
a4	4	Alle aktuellen Instrumente zur Informationsverarbeitung werden betrachtet.
b1	4	Die Schaffung neuer Prozesse wird in den Massnahmen beschrieben.
b2	4	Die Schaffung neuer Strukturen wird in den Massnahmen beschrieben.
b3	1	Es erfolgt keine direkte Abgrenzung der Untersuchungsobjekte, sondern nur in Zusammenhang mit der Verantwortlichkeit der leitenden Personen.
c1	4	Es werden viele Rand- und Teilgebiete der Informationssicherheit behandelt.
c2	1	Es werden nur die drei grundlegenden Grundbedrohungen der Verfügbarkeit, Integrität und Vertraulichkeit behandelt. Die Spezifikation weiterer Anforderungen ist nicht beschrieben.

Tabelle B-3: Bewertung BSI (D) IT-Grundschutzhandbuch

B.4 Bewertung BSI (GB) Code of Practice

Variable	Wert	Bemerkungen und Beschreibung
V1	**∅=0.4**	**Auslösung**
a1	0	Die Auslösung der Untersuchung wird nicht beschrieben.
a2	1	Die auslösenden Ereignisse, zyklische oder repetitive Auslösung werden nicht beschreiben aber ansatzweise in Vorwort und Einleitung erwähnt.
a3	0	Es wird keine Methode der Auslösung oder Bedarfsfeststellung beschrieben.
b1	1	Es besteht keine Beschreibung der Auslösung durch neue Softwareprojekte oder -produkte; dies wird ansatzweise in Vorwort und Einleitung erwähnt.
c1	0	Es besteht keine Beschreibung der Auslösung durch Veränderungen im unternehmerischen Umfeld.
V2	**∅=0.3**	**Organisation**
a1	0	Die Struktur des Projektteams wird nicht beschrieben.
a2	0	Die organisatorische Einordnung des Projektteams wird nicht beschrieben.
a3	0	Die Dauer des Bestehens des Projektteams wird nicht beschrieben.
a4	0	Die Auswahl und Qualifikation der Projektteammitglieder wird nicht beschrieben.
b1	0	Das Verfahrens ist nicht als Grundlage des Projektmanagements geeignet, da keine Beschreibung des Vorgehens enthalten ist.
b2	2	Die Zielfestlegung wird durch Beschreibung der Motivation und der Feststellung des Handlungsbedarfs grundlegend beschrieben.
b3	0	Die Abgrenzung der Untersuchungsbreite wird nicht beschrieben.
b4	0	Die Abgrenzung der Untersuchungstiefe geschieht nur durch den geringen inhaltlichen Umfang des COP selbst.
c1	0	Die Dauer der Planungsphase ist nicht beschrieben.
c2	0	Die Dauer der Kontrollphase ist nicht beschrieben.
c3	0	Die Anpassung der Projektdauer ist nicht beschrieben.
d1	1	Die Koordination und Kooperation zwischen verschiedenen Projekten wird nicht beschrieben. Aufgrund der Beschränkung auf wenige Massnahmen kann der COP jedoch als Grundlage für eine gesamtheitlichen Zertifizierung und damit als Basis für den Austausch vergleichbarer Informationen verwendet werden.
d2	1	vgl. d1
V3	**∅=1.1**	**Durchführung**
a1	0	Der Ablauf der Untersuchung wird weder abstrakt noch konkret beschrieben.
a2	0	vgl. a1
a3	0	vgl. a1
a4	0	vgl. a1
a5	1	Es wird auf die Risikoanalyse verwiesen, ihre Anwendung aber nicht beschrieben.
a6	1	Es werden nur minimale Hinweise auf weiterführende Informationen abgegeben.
b1	0	Der Ad-Hoc-Ansatz wird nicht beschrieben.
b2	2	Der Grundschutzansatz wird nicht beschrieben, implizit durch den COP aber umgesetzt.
b3	0	Der Bewertungsansatz wird nicht beschrieben.
b4	0	Der Risikoanalyse-Ansatz wird nicht beschrieben.
b5	0	Es werden keine weiteren Vertiefungsmöglichkeiten angegeben.

Variable	Wert	Bemerkungen und Beschreibung
c1	0	vgl. a1
c2	3	vgl. a1; die Beeinflussung geschieht jedoch implizit durch die Anwendung der Massnahmen.
c3	0	vgl. a1
c4	0	Die Ein- und Ausgabedaten der Phasen und der Informationsfluss werden nicht beschrieben.
c5	2	Die einzelnen Aktivitäten werden kurz im Massnahmenkatalog beschrieben.
d1	0	Die Anpassung der Breite des Untersuchungsobjekts wird nicht beschrieben.
d2	0	Die Anpassung der Tiefe der Untersuchung wird nicht beschrieben.
e1	4	Die qualitativen Ergebnisse bestehen aus den umgesetzten Massnahmen.
e2	0	Es werden keine quantitativen Ergebnisse oder ihre Herleitung beschrieben.
f1	4	Der COP ist auf aufgrund linearer Abfolge der inhaltlichen Teilbereiche sehr einfach erlernbar und anwendbar.
f2	0	Die Budgetierung und der Nachweis von Kosten ist nicht beschrieben.
f3	0	Die Integration von Aufwandsüberlegungen in den Arbeitsablauf ist nicht beschrieben.
f4	0	Der Aufwand wird nicht kontrolliert.
f5	3	Da nur Massnahmenbereiche identifiziert werden, kann der Aufwand durch Variation der inhaltlichen Tiefe gut beeinflusst werden.
g	0	Die Darstellung von Nutzen und Ertrag wird nicht beschrieben.
h1	3	Der COP ist mehrheitlich ein Katalog von Massnahmenbereichen.
h2	1	Nur wenige Massnahmen sind so konkret, dass sie direkt angewendet werden können. Alle Massnahmen sind technologieneutral.
h3	4	Alle Massnahmenbereiche werden berücksichtigt.
i1	2	Der COP kann als Fragenkatalog verwendet werden.
i2	2	Der COP kann als Checkliste verwendet werden.
j1	0	Es wird kein Hilfsmittel als Bestandteil des COP mitgeliefert.
j2	2	Die Verwaltung der Massnahmen würde sich durch die Verfügbarkeit eines Werkzeuges vereinfachen.
j3	1	Ergebnisgenerierung und Präsentation würden durch ein Werkzeug ansatzweise verbessert, aber das Ausmass der möglichen Unterstützung ist unklar.
j4	2	Der COP überzeugt durch seinen geringen Umfang und würde mit einem Werkzeug (welches Dokumentation erforderte) grösser. Der Einfluss ist unklar.

Variable	Wert	Bemerkungen und Beschreibung
V4	**∅=2.8**	**Fachbereiche**
a1	3	Die Betrachtung der Prozesse geschieht als Teil der Umsetzung des Massnahmenkatalogs.
a2	4	Die Betrachtung von Inhalten und Informationen geschieht zentral als Teil der Umsetzung des Massnahmenkatalogs.
a3	3	Die Betrachtung der Institutionen geschieht als Teil der Umsetzung des Massnahmenkatalogs.
a4	2	Die Betrachtung der Instrumente geschieht als Teil der Umsetzung des Massnahmenkatalogs.
b1	3	Die Etablierung neuer Prozesse, Institutionen und Instrumente geschieht als Teil der Umsetzung des Massnahmenkatalogs, zum Teil jedoch sehr abstrakt. Das Eigentümerkonzept wird umgesetzt.
b2	3	vgl. b1
b3	3	vgl. b1
c1	3	Die Abdeckung verschiedener Inhalte geschieht durch Ein- oder Ausschluss der verschiedenen beschriebenen Massnahmenbereiche.
c2	1	Es werden nur die drei grundlegenden Kriterien betrachtet, die Definition von weiteren ist nicht vorgesehen.

Tabelle B-4: Bewertung BSI (GB) Code of Practice

B.5 Bewertung ISACF COBIT

Variable	Wert	Bemerkungen und Beschreibung
V1	**Ø=1.8**	**Auslösung**
a1	3	Die auslösende Institution wird nicht explizit genannt, jedoch mit der Detaillierung des "Need for Control [...] by Management" beschrieben.
a2	1	Die auslösenden Ereignisse werden nicht explizit erwähnt, werden aber auf den "audit process" aufgebaut und auf diese Weise in den normalen Revisionszyklus integriert
a3	1	Die Auslösung geschieht über die Revision.
b1	2	Die Auslösung durch neue Softwareprojekte oder -produkte ist nicht explizit beschrieben, wird aber in den "control objectives" grundlegend behandelt.
c1	2	Die Auslösung durch Veränderungen des unternehmerischen Umfelds wird nicht explizit beschrieben, aber in den "control objectives" grundlegend behandelt.
V2	**Ø=1.4**	**Organisation**
a1	1	Über die Struktur des Projektteams werden keine Angaben abgegeben, aber es wird erwähnt, dass sie bestimmt werden muss (vgl. Appendix IV - Audit Process)
a2	1	Die organisatorische Eingliederung wird nicht beschrieben, wird aber implizit als Teil des Audit angesehen.
a3	0	Es werden keine Angaben über die Dauer des Bestehens des Projektteams abgegeben.
a4	1	Die Mitglieder des Projektteams werden nicht grundsätzlich beschrieben, aber implizit als Teil der Revision angenommen.
b1	1	Das Verfahren eignet sich nur für ganz spezifische Betrachtungen, da es v.a. der Gewinnung von Zustandsinformation dient und nicht der Beeinflussung.
b2	4	Das Projektziel ergibt sich aus der Erfüllung der control objectives in den relevanten Bereichen.
b3	2	Die Abgrenzung der Breite ergibt sich implizit aus dem im Rahmen der Revision untersuchten Teil, wird aber nur grundlegend beschrieben.
b4	2	Die Abgrenzung der inhaltlichen Tiefe ergibt sich implizit aus dem im Rahmen der Revision untersuchten Inhalte, wird aber nur grundlegend beschrieben.
c1	1	Die Dauer von Planungs- und Kontrollphase sowie die Anpassung der Projektdauer wird nicht beschrieben, wird jedoch implizit durch die Revision bestimmt (vgl. Appendix IV - Audit Process).
c2	1	vgl. c1
c3	1	vgl. c1
d1	2	Die Koordination und Kooperation ist durch Vergleich der Ergebnisse aufgrund der einheitlichen Anforderungen möglich, wird aber nicht beschrieben.
d2	2	vgl. d1
V3	**Ø=1.6**	**Durchführung**
a1	2	Es ist eine abstrakte Beschreibung des Verfahrens vorhanden, jedoch in einem der hinteren Anhänge (d.h. untergeordnet) wiedergegeben.
a2	0	Das Verfahren selbst wird nicht detailliert beschrieben.
a3	1	Das Verfahren ist nur grundlegend beschrieben und umfasst weniger als 5% des gesamten Dokumentation.
a4	4	Es bestehen verschiedene Dokumentationen je nach Adressat.
a5	2	Verweise auf andere Verfahren werden in den Referenzen abgegeben.

Variable	Wert	Bemerkungen und Beschreibung
a6	4	Es werden ausführliche Referenzlisten für weiterführende Literatur abgegeben.
b1	0	Der Ad-Hoc-Ansatz wird nicht beschrieben.
b2	0	Der Grundschutz-Ansatz wird nicht beschrieben.
b3	0	Der Werte-Ansatz wird nicht beschrieben.
b4	0	Der Risikoanalyse-Ansatz wird nicht beschrieben.
b5	4	Es wird ein allgemeiner Audit-Ansatz zur Erfüllung vorgegebener Einzelanforderungen beschrieben.
c1	4	Der beschriebene Audit-Ansatz umfasst (nur) die Erhebung des Zustandes und somit die Analysephase.
c2	1	Die Beeinflussungsphase wird nur grundlegend beschrieben und umfasst v.a. die Berichterstattung über den Zustand.
c3	0	Die Kontrolle wird als Erfüllung der Anforderungen, nicht als Umsetzung von Massnahmen verstanden, und ist nicht im hier gefragten Sinne beschrieben.
c4	4	Die Ein- und Ausgabedaten sowie die Datenübergabe sind festgelegt aufgrund einheitlicher Struktur der control objectives
c5	2	Die einzelnen Tätigkeiten werden nicht im Detail beschrieben, lassen sich jedoch gut aus den allgemein Revisionstätigkeiten herleiten.
d1	2	Die Anpassung der Breite ergibt sich implizit aus dem im Rahmen der Revision untersuchten Teil, wird aber nur grundlegend beschrieben.
d2	2	Die Anpassung der inhaltlichen Tiefe ergibt sich implizit aus dem im Rahmen der Revision untersuchten Inhalte, wird aber nur grundlegend beschrieben.
e1	2	Als qualitatives Ergebnis entsteht ein Revisionsbericht über den Zustand der Erfüllung der Control objectives.
e2	3	Als quantitative Ergebnis entstehen Einzelinformationen über die Erfüllung der control objectives
f1	3	Das Verfahren selbst ist einfach, die Aufteilung der control objectives ebenso. Die Durchführung beruht weitgehend auf Interpretation. Es ist deshalb leicht erlernbar.
f2	1	Die Budgetierung, die Integration von Aufwand und Kosten sowie die Aufwandskontrolle geschieht implizit über die Integration in der Revision der Unternehmung, wird aber nicht beschrieben.
f3	1	vgl. f2
f4	1	vgl. f2
f5	0	Wenn alle control objektives geprüft werden sollen, entsteht sehr hoher Aufwand.
g	0	Die Darstellung von Nutzen und Ertrag ist nicht beschrieben.
h1	0	Es sind keine Massnahmenkataloge im COBIT enthalten.
h2	0	vgl. h1
h3	0	vgl. h1
i1	4	Die Inhalte lassen sich als Fragebogen verstehen.
i2	3	Teile der Inhalte können als Checklisten verwendet werden.
j1	2	Es werden einzelne Texte aus der Dokumentation im ASCII-Format auf Diskette abgegeben.
j2	0	Durch die abgegebenen Hilfsmittel ergibt sich keine Vereinfachung der Verwaltung.
j3	0	Die Ergebnisproduktion würde durch ein spezifisches Hilfsmittel nicht erleichtert.
j4	3	Die Akzeptanz wird durch die abgegebenen Hilfsmittel erhöht.

Variable	Wert	Bemerkungen und Beschreibung
V4	**∅=2.3**	**Fachbereiche**
a1	4	Im Zentrum der Untersuchung mit COBIT stehen die unternehmerischen Prozesse.
a2	4	Information wird als zentrales Element der unternehmerischen Prozesse betrachtet.
a3	4	Die Unternehmung, ihre Beziehungen zur Aussenwelt sowie die Rollen und verarbeiteten Inhalte werden zentral betrachtet.
a4	3	Informationstechnologie wird als wichtiges Hilfsmittel zur Datenbearbeitung betrachtet, aber nicht konkret beschrieben.
b1	0	COBIT umfasst nur die Analyse, nicht die Beeinflussung des Untersuchungsobjekts.
b2	0	vgl. b1
b3	0	vgl. b1
c1	3	Es werden verschiedene inhaltliche Teilgebiete beschrieben und es wurde bei der Erstellung von COBIT angestrebt, alle relevanten Inhalte zu berücksichtigen.
c2	3	Neben CIA werden Verbindlichkeit, Authentizität und weitere Kriterien vordefiniert. Die Definition eigener Kriterien ist nicht vorgesehen.

Tabelle B-5: Bewertung ISACF COBIT

B.6 Bewertung ISO GMITS

Variable	Wert	Bemerkungen und Beschreibung
V1	**Ø=3.2**	**Auslösung**
a1	4	Die Auslösung wird in den generellen Rahmen der Management-Tätigkeiten gestellt und ist mit Institutionen ausführlich beschrieben.
a2	3	Zur Auslösung wird ein zyklischer Prozess vorgestellt, bei welchem eine Rückkopplung zu jeder Phase stattfinden kann. Vorfallbedingte Auslösung wird nicht beschrieben.
a3	4	Die Auslösung geschieht durch Ableitung von IT-Sicherheitspolitik aus Geschäfts- und Sicherheitspolitik. Der Vorgang ist ausführlich beschrieben.
b1	2	Die Auslösung durch neue Softwareprojekte oder -produkte wird nicht direkt beschrieben, aber in der Einführung und an verschiedenen Stellen im Text erwähnt.
c1	3	Change Management wird in einem eigenen Abschnitt beschrieben (GMITS 1-9.2). Es bezieht sich v.a. auf technische Veränderungen und nur bedingt auf Veränderungen des unternehmerischen Umfelds.
V2	**Ø=1.7**	**Organisation**
a1	3	Das Projektteam selbst wird nicht vorgestellt, aus der Dokumentation kann seine Struktur jedoch entnommen werden.
a2	4	Die organisatorische Einordnung des Projektteams ist detailliert und mit Varianten beschrieben.
a3	1	Die Dauer des Bestehens des Projektteams wird nicht beschrieben. Implizit wird die Dauer des Verfahrens angenommen.
a4	1	Die Qualifikationen, Auswahl und Leitung des Projektteams werden nicht beschrieben. Mehrere Rollen werden ansatzweise beschrieben.
b1	3	Das Verfahren eignet sich für das Projektmanagement: Die einzelnen Phasen und teilweise die Aktivitäten werden spezifiziert, die Ergebnisse der Phasen beschrieben.
b2	4	Die Festlegung der Ziele geschieht direkt aus der Zielfestlegung der Unternehmung (aus Geschäfts- und Sicherheitspolitik) und ist beschrieben.
b3	2	Die Abgrenzung der Untersuchungsbreite ist nicht direkt beschrieben, aber aus des Wahl des Ansatzes (combined) ableitbar.
b4	1	Die Abgrenzung der Untersuchungsbreite ist grundlegend beschrieben, aber inhaltlich nicht detailliert.
c1	0	Die Dauer der Planungsphase wird nicht beschrieben.
c2	0	Die Dauer der Kontrollphase wird nicht beschrieben.
c3	0	Die Anpassung der Phasendauer wird nicht beschrieben.
d1	1	Koordination und Kooperation werden nicht beschrieben. Wegen fehlender Ergebnisbeschreibung wären sie problematisch und müssen auf individuellen Vereinbarungen beruhen. Allerdings ist das Verfahren einheitlich aufgebaut, was die Vergleichbarkeit des Ablaufes erleichtert.
d2	1	vgl. d1
V3	**Ø=2.6**	**Durchführung**
a1	4	Das Verfahren wird in 4 Abstraktionsstufen beschrieben: Übersicht (Part I), Verfahren allgemein (Part II), Verfahren im Detail (Part III), Grundschutz und Massnahmenauswahl (Part IV). Dies umfasst abstrakte und konkrete detaillierte Beschreibungen und richtet sich an verschiedene Personengruppen.
a2	4	vgl. a1

Variable	Wert	Bemerkungen und Beschreibung
a3	4	Die Dokumentation des Verfahrens macht mehr als 80% der Dokumentation aus.
a4	4	vgl. a1
a5	4	Es wird auf Risikoanalyse und verschiedene Grundschutzverfahren (in Anhängen) verwiesen.
a6	2	Literaturhinweise sind v.a. für technische Referenzen enthalten, aber nicht für inhaltliche Teilgebiete.
b1	4	der Ad-Hoc-Ansatz wird als "informal approach" beschrieben.
b2	4	Der Grundschutzansatz wird beschrieben.
b3	0	Der Werteansatz wird nicht beschrieben.
b4	4	Der Risikoanalyse-Ansatz wird beschrieben.
b5	4	Ein weiterer, kombinierter Ansatz ("combined approach") wird beschrieben. Netzwerksicherheit (Part V) wird detailliert betrachtet.
c1	3	Die einzelnen Phasen der Analyse-, Beeinflussungs- und Kontrollphase werden beschreiben, die einzelnen Aktivitäten jedoch nicht formal voneinander abgegrenzt.
c2	3	vgl. c1
c3	4	vgl. c1. Im besonderen werden approval, maintenance und follow-up beschrieben.
c4	1	Die Ein- und Ausgabedaten der einzelnen Phasen werden nur allgemein und informell beschrieben.
c5	1	Die Aktivitäten werden beschrieben, jedoch nicht in konkreten Zusammenhang mit Projektteammitarbeitern und Rollen gebracht.
d1	2	Die Anpassung der Untersuchungsbreite geschieht durch die Zielsetzung, wird aber nicht konkrete beschrieben.
d2	2	Die Anpassung der Untersuchungstiefe wird durch die Auswahl des Ansatzes bestimmt. Nur wenige Fachgebiete werden meist ansatzweise beschrieben.
e1	3	Als qualitative Ergebnisse entstehen die Erfassung der Objekte, Bedrohungen, Risiken sowie die Risikoprioritäten.
e2	2	Die Gewinnung quantitativer Ergebnisse ist nicht konkret beschrieben, aber aufgrund der Schilderung des Verfahrens aus den Phasen ableitbar.
f1	4	Aufgrund der abgestuften Dokumentation und des einheitlichen Aufbaus ist das Verfahren gut erlernbar.
f2	0	Budgetierung und Aufwandsnachweis werden nicht beschrieben.
f3	1	Die Integration von Aufwandsüberlegungen in die Untersuchung wird ansatzweise beschrieben.
f4	1	Die Kontrolle wird ansatzweise in der Kontrollphase beschrieben.
f5	3	Aufgrund der verschiedenen Ansätze kann der Aufwand gut beeinflusst werden. Durchführung mit mässigem Aufwand ist also möglich.
g	0	Die Darstellung von Nutzen und Ertrag ist nicht beschrieben.
h1	2	Es werden keine Massnahmenkataloge als Teil der Dokumentation abgegeben, aber es sind Beschreibungen von Massnahmenbereichen und Verweise auf Massnahmenkataloge enthalten.
h2	1	Die Massnahmenbereiche sind grösstenteils sehr abstrakt beschrieben.
h3	4	Alle Massnahmenbereiche werden berücksichtigt.
i1	4	Fragenkataloge sind enthalten.
i2	4	Checklisten sind enthalten.
j1	0	Es wird kein Hilfsmittel mitgeliefert.
j2	3	Die Verwaltung der erhobenen Informationen würde durch ein Hilfsmittel vereinfacht.

Variable	Wert	Bemerkungen und Beschreibung
j3	3	Die Produktion der Ergebnisse würde v.a. durch eine Führung durch den Prozess vereinfacht.
j4	3	Das Hilfsmittel würde die Akzeptanz fördern, da der Standard in einzelnen Elementen unübersichtlich dargestellt ist.
V4	**∅=2.1**	**Fachbereiche**
a1	1	Unternehmerische Prozesse werden nur implizit betrachtet.
a2	4	Information wird als wichtigste Ressource der Unternehmung zentral betrachtet.
a3	3	Die Umgebung der Unternehmung wird nur am Rande betrachtet, die Unternehmung selbst jedoch ganzheitlich.
a4	3	Die Instrumente werden betrachtet, jedoch nur auf Technologie- nicht auf Produkteebene.
b1	2	Die Etablierung neuer Prozesse ist bei den Massnahmenbereiche teilweise beschrieben.
b2	2	Die Etablierung neuer Institutionen ist bei den Massnahmenbereichen teilweise beschrieben.
b3	0	Die Abgrenzung der Bezugsobjekte wird nicht beschrieben.
c1	2	Es werden verschiedene Teilgebiete sehr allgemein beschrieben.
c2	2	Die grundlegenden Kriterien werden berücksichtigt und ansatzweise weitere drei Kriterien. Die selbst vorgenommene Kriteriendefinition wird nicht beschrieben.

Tabelle B-6: Bewertung ISO GMITS

B.7 Anforderungen an *ISiWAY*

Variable	Wert	Bemerkungen und Beschreibung
V1	**∅=2.8**	**Auslösung**
a1	4	Es muss beschrieben werden, welche Institution die ISi-Untersuchung auslöst.
a2	4	Es muss ein zyklischer Ablauf definiert werden, welcher regelmässige Wiederholungen der Untersuchung verlangt. Ausserdem muss ISiWay periodisch sowie bedarfsweise durchlaufen werden können, da Informationssicherheit keine einmalige Aufgabe ist, sondern bedingt durch Veränderungen im Betrachtungsobjekt, welche durch neue Technologien oder durch veränderte Sicherheitsanforderungen der Benutzer entstehen, ständig neu betrachtet werden muss.
a3	4	Das Vorgehen zur Auslösung der ISi-Untersuchung muss detailliert beschrieben werden.
b1	1	Der Zusammenhang mit neuen Projekten soll nur grundlegend betrachtet werden.
c1	1	vgl. a2; Der Zusammenhang mit Veränderungen des unternehmerischen Umfelds soll nur grundlegend betrachtet werden.
V2	**∅=3.4**	**Organisation**
a1	4	Für die Struktur des Projektteams (Weisungsbefugnis und Verantwortlichkeit) sollen ausführliche Vorschläge abgegeben werden. ISiWay soll rollenorientiert sein, d.h. durch die direkte Zuweisung von Tätigkeiten zu Rollen soll mittel- bis langfristig eine Identifikation mit den Aufgaben der Informationssicherheit gewährleistet werden.
a2	4	Die organisatorische Einordnung des Projektteams muss ausführlich beschrieben werden.
a3	3	Es müssen Aussagen über die Dauer des Bestehens des Projektteams und die Abhängigkeiten gemacht werden.
a4	4	Die Zusammensetzung des Projektteams, die Qualifikationen der Personen und insbesondere die Rollen, welche sie wahrnehmen, muss ausführlich erläutert werden.
b1	4	Das Verfahren muss sich als Grundlage eines Projektmanagements eignen, indem die einzelnen Phasen, Aktivitäten und Ergebnisse formal detailliert und konkret festgelegt werden und denjenigen Personen, welche sie umsetzen müssen, konkrete Handlungsanweisungen zur Verfügung stellen. Dabei muss es dezentral ablaufen. Eine zentrale Kontrolle bei der bestehenden Komplexität des Untersuchungsobjekte ist irrealistisch. Das Verfahren muss Informationssicherheit als Teil der täglichen Arbeit integrieren. Zentral soll lediglich die Zielvorgabe und die Kontrolle der Zielerreichung geschehen.
b2	3	Es muss beschrieben werden, wie das Projektziel festgelegt wird.
b3	3	Es muss beschrieben werden, wie die zu betrachtenden Objekte abgegrenzt werden.
b4	3	Es muss beschrieben werden, wie die zu betrachtenden Inhalte abgegrenzt werden.
c1	3	Die Dauer der Planungsphase muss aufgrund der verfügbaren Informationen bestimmt werden können.
c2	3	Die Dauer der Kontrollphase muss aufgrund der verfügbaren Informationen bestimmt werden können.
c3	3	Die Projektdauer muss aufgrund der Anforderungen angepasst werden können.

Variable	Wert	Bemerkungen und Beschreibung
d1	4	Koordination muss durch formale Festlegung der Ergebnisse und Bestimmung eines Informationsflusses vorgesehen werden. Dazu muss die Kommunikation verschiedener Institutionen der Prozesse, welche bei der Umsetzung des Verfahrens entstehen, untereinander spezifiziert werden (v.a. übergeordnete mit untergeordneten Teilprozessen). Auf diese Weise soll der Einsatz in föderalistisch organisierten Unternehmungen vorbereitet werden.
d2	4	ISiWay muss die gemeinsame Erarbeitung von Informationssicherheit in der Unternehmung fördern, indem Kooperation vorgesehen und beschrieben wird.
V3	**∅=2.9**	**Durchführung**
a1	4	Der Ablauf muss abstrakt beschrieben werden.
a2	4	Der Ablauf muss konkret beschrieben werden.
a3	3	Das Verfahren muss mindestens 70% der Gesamtbeschreibung umfassen.
a4	2	Es müssen mindestens zwei verschiedene Sichtweisen dargestellt werden.
a5	3	Es müssen Hinweise auf und Schnittstellen zu anderen Verfahren aufgenommen werden.
a6	2	Es muss auf die wichtigste weiterführende Literatur verwiesen werden.
b1	1	Der Ad-hoc-Ansatz muss am Rande erwähnt und dargestellt werden.
b2	4	Der Grundschutz-Ansatz soll vertieft dargestellt werden.
b3	4	Der Bewertungs-Ansatz soll vertieft dargestellt werden.
b4	4	Der Risikoanalyse-Ansatz soll vertieft dargestellt werden.
b5	4	Es soll ein eigener Ansatz entwickelt werden, welcher die anderen Ansätze integriert. Darüber hinaus muss ISiWay fachlich integriert sein. Dies bedeutet, dass bestehende Sicherheits- und Risikomanagementverfahren in dieses Verfahren einfliessen müssen, weil es sich dabei um etablierte und bekannte Vorgehensweisen handelt, und so allenfalls schon auf Know-How bei der Durchführung zurückgegriffen werden kann. Es bedeutet auch, dass Vorgehensweisen aus verwandten Bereichen (z.B. unternehmerisches Krisenmanagement) berücksichtigt werden müssen und, wo im konkreten Fall vorhanden, Schnittstellen geschaffen werden müssen.
c1	4	Die einzelnen Phasen und die in ihnen zu durchlaufenden Tätigkeiten sollen detailliert festgelegt, mit formalen Definitionen der Ausgabedaten versehen, einzelnen Rollen zugeordnet und in einen einheitlichen Ablauf eingebettet werden.
c2	4	vgl. c1
c3	4	vgl. c1
c4	4	vgl. c1
c5	4	vgl. c1
d1	4	Das Verfahren soll auf unterschiedlich grosse Objekte während des Durchlaufens angepasst werden können.
d2	4	Das Verfahren soll auf unterschiedliche Inhalte während des Durchlaufens eingehen können. Die inhaltliche Skalierung soll durch die Identifikation der wichtigsten Massnahmenbereiche geschehen. Es muss jedoch eine umfassende Berücksichtigung der Inhalte vorbereiten, indem es Stichworte und Aktionsbereiche identifiziert und auf weiterführende Elemente verweist.
e1	4	Das Verfahren muss möglichst viele qualitative und quantitative, aussagekräftige Ergebnisse erzeugen.
e2	4	vgl. e1

Variable	Wert	Bemerkungen und Beschreibung
f1	4	Das Verfahren muss mit geringem Aufwand erlernt werden können. Dies ist durch die Komplexität des Untersuchungsobjekts eine besondere Herausforderung. Einfachheit ist Voraussetzung für Akzeptanz und deshalb für die Erreichung des Ziels des Verfahrens. Es soll ein Werkzeug implementiert werden, welches diese einfache Erlernbarkeit und Verwendbarkeit fördert. Zur Förderung der Erlernbarkeit muss ISiWay nach einem einheitlichen und möglichst bekannten Ansatz strukturiert sein.
f2	1	Budgetierung und Kostennachweis sollen nur grundlegend beschrieben werden.
f3	1	Das Verfahren muss die Beeinflussung des Arbeitsablaufs durch erhöhten Aufwand grundlegend erlauben.
f4	4	Die Kontrolle des Verfahrens muss detailliert beschrieben werden.
f5	3	Das Verfahren soll mit geringem bis mässigem Aufwand durchgeführt werden können.
g	2	Der Ertrag der Durchführung soll überblicksartig dargestellt werden können.
h1	0	Es sollen keine Massnahmenkataloge entwickelt und aufgenommen werden, sondern nur darauf verwiesen werden.
h2	0	vgl. h1
h3	0	vgl. h1
i1	0	Es sollen keine Fragekataloge entwickelt werden.
i2	0	Es sollen keine Checklisten entwickelt werden.
j1	4	Es soll ein Hilfsmittel erstellt werden.
j2	4	Dieses soll die Verwaltung der entstehenden Daten vereinfachen, um die Beherrschung der Komplexität und der inneren Dependenzen des Informationssystems zu erlauben.
j3	4	Es soll die Erzeugung und Präsentation von Ergebnissen vereinfachen, den Beteiligten die Darstellung ihrer eigenen Situation erleichtern und Aussagen über Handlungsbedarf generieren können. Zusätzlich muss eine einfache Weitergabe der ISi-Anforderungen an die Dienstleistungslieferanten möglich sein.
j4	4	Es soll die Akzeptanz des Verfahrens fördern.
V4	**∅=2.6**	**Fachbereiche**
a1	4	Das Verfahren soll von einer Betrachtung der Prozesse ausgehen.
a2	4	Information soll im Zentrum der Betrachtung stehen. Es muss eine ganzheitliche Sicht gefördert werden, also ein Bezug auf Informationssystem und Prozesse hergestellt werden, nicht nur auf das IT-System. ISiWay muss die Beeinflussung menschlichen Verhaltens umfassen. Menschen sind die wichtigsten Komponenten innerhalb der Informationsverarbeitungsvorgänge innerhalb und ausserhalb der Unternehmung, da sie im Gegensatz zu technischen Systemen auch auf ungeplante Situationen angemessen und konsistent reagieren können.
a3	2	Die unternehmerischen Rahmenbedingungen sollen am Rande betrachtet, das Informationssystem mit allen Komponenten sekundär betrachtet werden. Die Komplexität und Heterogenität von Informationssystemen muss berücksichtigt werden und auch die Betrachtung unternehmensexterner Teilsysteme umfassen.
a4	2	Die verwendeten Technologien sollen sekundär betrachtet werden.

Variable	Wert	Bemerkungen und Beschreibung
b1	2	Die Beeinflussung soll nur über die Etablierung von neuen Informationssicherheitsprozessen, -strukturen und instrumenten erfolgen, bzw. über individuell zusammengestellte oder referenzierte Massnahmenkataloge. Es werden also nur die direkt informationssicherheitsrelevanten Beeinflussungen berücksichtigt. Das Verfahren selbst muss jedoch skalierbar sein. Es muss verschiedenen Bedürfnissen angepasst werden können und darf nicht nur einen starren Weg durchlaufen.
b2	2	vgl. b1
b3	2	vgl. b1
c1	1	Einige Teilgebiete sollen ansatzweise beschrieben werden.
c2	4	Es sollen sowohl die bekannten Kriterien berücksichtigt werden als auch Angaben gemacht werden, wie eigene Kriterien zu definieren sind.

Tabelle B-7: Anforderungen an ISiWay

B.8 Bewertung ISiWay

Variable	Wert	Bemerkungen und Beschreibung
V1	**∅=2.8**	**Auslösung**
a1	4	Die auslösenden Institutionen sind detailliert beschrieben.
a2	4	Es ist detailliert beschrieben, dass Informationssicherheit zyklisch untersucht wird und dass die stets erneute Auslösung einer Untersuchung zyklisch stattfindet. Die Auslösung durch Vorfälle wird durch den spezifischen Zyklus "Krisenmanagement" (Detaillierungsgrad 3.5) abgedeckt.
a3	4	Es wird detailliert beschrieben, wie zur Auslösung der Untersuchung vorgegangen wird; dies nicht nur im Rahmen des repetitiven Zyklus, sondern auch die allererste Auslösung.
b1	1	Der Zusammenhang mit neuen Projekten wird nur grundlegend betrachtet. Es wird lediglich darauf hingewiesen, dass projektbezogener Einsatz den unternehmensbezogenen weitgehend entspricht, ohne dies genauer auszuführen.
c1	1	Es wird darauf hingewiesen, dass der zyklische Aufbau von ISiWay aus der Notwendigkeit erfolgt ist, die entstehenden Veränderungen zu berücksichtigen. Eine Integration von ISiWay in Change-Management-Prozesse ist nicht beschrieben.
V2	**∅=3.8**	**Organisation**
a1	4	Struktur, Weisungsbefugnis und Verantwortlichkeiten der einzelnen Projektteammitglieder werden ausführlich beschrieben und im Rahmen eines Rollenmodells vertieft.
a2	4	Die organisatorische Einordnung der Projektteammitglieder geht eindeutig aus dem Rollenmodell hervor.
a3	4	Die Dauer des Bestehens des Projektteams folgt direkt aus der Dauer der einzelnen Teilprojekte.
a4	4	Die Zusammensetzung des Projektteams, die Leitung, die Auswahl und die Qualifikationen folgen direkt aus den Beschreibungen der einzelnen Rollen gemäss Rollenmodell.
b1	4	Das Verfahren ist als Grundlage des Projektmanagement sehr gut geeignet, da die einzelnen Phasen, Aktivitäten und Ergebnisse formal detailliert und konkret festgelegt wurden und denjenigen Personen, welche sie umsetzen müssen, konkrete Handlungsanweisungen zur Verfügung gestellt werden. Ein dezentraler Ablauf ist vorgesehen. Eine zentrale Kontrolle wird nicht angestrebt, jedoch eine zentrale Koordination. Das Verfahren integriert Informationssicherheit als Teil der täglichen Arbeit. Zielvorgabe und die Kontrolle der Zielerreichung werden zentral vorgegeben. Kontrolle wird in den Teilprojekten gefördert.
b2	3	Der Prozess der Festlegung der unternehmerischen Informationssicherheits-ziele wird detailliert betrachtet. Die einzelnen Zielsetzungen werden jedoch nicht im Verfahren selbst, sondern im Text verstreut betrachtet.
b3	4	Die Abgrenzung der Breite des Betrachtungsobjekts erfolgt eindeutig durch die Wahl der Teilprojekte. Es wird beschrieben, wie der ISiBe und allenfalls der ISiKo dabei vorzugehen haben.
b4	4	Die Abgrenzung der Inhalte erfolgt direkt aus der Wahl des Detaillierungsgrades.

Variable	Wert	Bemerkungen und Beschreibung
c1	3	Es werden Schätzungen und Einflussfaktoren für die Dauer des Projektes abgegeben, aus denen im konkreten Fall Voraussagen und realistische Ziele abgeleitet werden können.
c2	4	Die Dauer der Kontrollphase kann aufgrund der im jeweiligen Teilprojekt erarbeiteten Informationen bestimmt werden.
c3	4	Die Projektdauer kann anforderungsgemäss angepasst werden, indem Teilprojekte verlängert werden oder neue Teilprojekte ausgelöst werden.
d1	4	Die Koordination wird durch formale Festlegung der Ergebnisse und Bestimmung eines Informationsflusses gut unterstützt. Die Kommunikation verschiedener Institutionen der Prozesse, welche bei der Umsetzung des Verfahrens entstehen, wird spezifiziert. Der föderalistisch organisierte Einsatz von ISiWay ist vorgesehen und eines der zentralen Ziele von ISiWay.
d2	4	ISiWay geht von einer zentralen Koordination der einzelnen Teilprojekte aus, wodurch die gemeinsame Erarbeitung von Informationssicherheit in der Unternehmung gefördert wird.
V3	**∅=2.8**	**Durchführung**
a1	4	Der Ablauf wird abstrakt und übersichtlich beschrieben.
a2	4	Der Ablauf wird konkret und detailliert beschrieben.
a3	3	Gemessen an Kapitel 8 und Anhang C umfasst die Beschreibung der einzelnen Phasen ca. 60% der Gesamtbeschreibung, die allgemeine Beschreibung umfasst nochmals ca. 20%. Einzelne Inhalte sind auf den Rest der Arbeit verstreut. Der Umfang kann also nicht eindeutig bestimmt werden.
a4	2	Die einzelnen Sichtweisen resultieren eindeutig aus dem Rollenmodell. Es wird jedoch keine eigene Dokumentation erstellt oder abgegeben, welche für einzelne Rollen gedacht ist. Jeder Benutzer muss seinen Teil separat herausfiltern. Idee ist jedoch, dass der ISiBe und der ISiKo diese Arbeit für die anderen Teilnehmer durchführen.
a5	2	Durch die Behandlung der verschiedenen Verfahren in der Gesamtarbeit wird diese Forderung erfüllt, indem auf Kapitel 6 (generischer Prozess) und Kapitel 7 (vergleichende Bewertung) verwiesen wird. Eine eindeutige Bestimmung dieses Wertes ist jedoch schwierig, da es sich hier um eine Selbstreferenzierung handelt.
a6	2	Dito. Die Literatur ist als Teil dieser Arbeit integriert.
b1	1	Der Ad-hoc-Ansatz wird erwähnt und als schlechtes Vorbild dargestellt (vgl. auch Beschreibung in Kapitel 6).
b2	4	Der Grundschutz-Ansatz wird vertieft dargestellt.
b3	4	Der Bewertungs-Ansatz wird vertieft dargestellt..
b4	4	Der Risikoanalyse-Ansatz wird vertieft dargestellt.
b5	4	Der eigene Ansatz besteht aus der Integration der genannten drei Ansätze in Kombination mit einem Krisenmanagementzyklus. ISiWay wird dabei fachlich integriert. Bestehende Sicherheits- und Risikomanagementverfahren können als Basis von ISiWay verwendet werden; ISiWay baut direkt auf diesem Know-How auf.
c1	4	Die einzelnen Phasen und die in ihnen zu durchlaufenden Tätigkeiten werden detailliert festgelegt, wurden soweit wie möglich mit formalen Definitionen der Ausgabedaten versehen, einzelnen Rollen zugeordnet und in einen einheitlichen Ablauf eingebettet.
c2	4	vgl. c1
c3	4	vgl. c1
c4	4	vgl. c1

Variable	Wert	Bemerkungen und Beschreibung
c5	4	vgl. c1
d1	4	Das Verfahren kann durch Auslösung von Teilprojekten auf unterschiedlich grosse Objekte während des Durchlaufens angepasst werden.
d2	4	Das Verfahren kann durch die Wahl des Detaillierungsgrads auf unterschiedliche Inhalte während des Durchlaufens eingehen. Die inhaltliche Skalierung soll durch die Identifikation der wichtigsten Massnahmenbereiche geschehen. Es muss jedoch eine umfassende Berücksichtigung der Inhalte vorbereiten, indem es Stichworte und Aktionsbereiche identifiziert und auf weiterführende Elemente verweist.
e1	3	Das Verfahren erzeugt qualitative und quantitative, aussagekräftige Ergebnisse, die jedoch nicht alle im Detail spezifiziert werden können, da ISiWay nicht konkret auf einzelne unternehmerische Umgebungen, Sicherheitstechnologien oder Fachgebiete eingehen kann.
e2	3	vgl. e1
f1	1	Die Erlernbarkeit des Verfahrens ist durch die Verstreuung der relevanten Inhalte auf die verschiedenen Kapitel nicht einfach. Die Lektüre des gesamten Verfahrens und der einzelnen weiteren Abschnitte, auf welche verwiesen wird, ist aufwendig. Die verwendete Sprache ist teilweise sehr exakt, dadurch aber nicht leichter verständlich. Ein Erlernen mit geringem Aufwand ist also nicht möglich. Zwar bestehen durch die Anlehnung an einen bewährten Managementansatz Erleichterungen, jedoch nur für Leser, die damit auch vertraut sind.
f2	1	Budgetierung und Kostennachweis werden nur grundlegend beschrieben, da das Verfahren zu allgemein gehalten ist, um konkreter darauf eingehen zu können.
f3	2	Aufwandsplanung und die Beeinflussung des Aufwands der bestehenden Arbeitsabläufe werden erwähnt und so gut wie möglich beschrieben.
f4	4	Die Kontrolle des Verfahrens wird detailliert beschrieben.
f5	3	Das Verfahren kann mit geringem bis mässigem Aufwand durchgeführt werden, indem nur die ersten beiden Detaillierungsgrade durchlaufen werden. Aufgrund des Umfangs der Dokumentation und der daraus folgenden Einarbeitungszeit und Konkretisierungsaufwände ist der Aufwand jedoch nicht minimal.
g	2	Der Ertrag der Durchführung kann überblicksartig dargestellt werden, indem der Status der einzelnen Teilprojekte durch den übergeordneten Informationssicherheitsbeauftragten ständig überwacht wird und Kriterien zur Verfügung gestellt werden, wie der Status bestimmt werden kann.
h1	0	Es wurden keine Massnahmenkataloge entwickelt, sondern nur (in Kapitel 6) darauf verwiesen.
h2	0	vgl. h1
h3	0	vgl. h1
i1	0	Es wurden keine Fragekataloge entwickelt.
i2	0	Es wurden keine Checklisten entwickelt.
j1	4	Ein Hilfsmittel namens ISiGo wurde erstellt. Diese und die folgenden drei Bewertungen beziehen sich auf Kapitel 9.
j2	4	ISiGo vereinfacht die Verwaltung der entstehenden Daten, indem es die wichtigen Daten einheitlich formatiert zur Eingabe verlangt und die Darstellung der inneren Dependenzen des Informationssystems durch automatisierte Herleitung erlaubt.

Variable	Wert	Bemerkungen und Beschreibung
j3	4	ISiGo vereinfacht die Erzeugung und Präsentation von Ergebnissen, und erleichtert den Beteiligten die Darstellung ihrer eigenen Situation. Aussagen über den Handlungsbedarf lassen sich generieren. Eine einfache Weitergabe der ISi-Anforderungen an die Dienstleistungslieferanten ist möglich.
j4	4	ISiGo hat das Potential, die Akzeptanz des Verfahrens zu fördern, indem es die Durchführung vereinfacht.
V4	**∅=3.2**	**Fachbereiche**
a1	2	Das Verfahren geht von einer Betrachtung der Prozesse aus, ist jedoch nicht sehr spezifisch in deren Untersuchung.
a2	4	Information steht im Zentrum der Betrachtung. Eine ganzheitliche Sicht wird gefördert, indem ein Bezug auf Informationssystem, IT-System und Prozesse hergestellt wird. ISiWay umfasst auch die Beeinflussung menschlichen Verhaltens.
a3	3	Die Institutionen der Unternehmung werden vertieft betrachtet und ihr Einfluss bzw. ihre Integration in die Durchführung von ISiWay im Rollenmodell beschrieben. Auch Gesellschaft und soziale Rahmenbedingungen finden Erwähnung. In jedem Fall bezieht sich ISiWay deutlich auf die gesamte Unternehmung, was in der Herleitung der Zielsetzungen zum Ausdruck kommt. Die Komplexität und Heterogenität von Informationssystemen und auch die Betrachtung unternehmensexterner Teilsysteme wird berücksichtigt. Personen und ihre Rollen werden vertieft betrachtet.
a4	2	Die verwendeten Technologien werden als notwendige Komponenten des Informationssystems betrachtet und ihre Erhebung und Spezifikation ist in ISiWay vorgesehen. Das Verfahren selbst geht jedoch nicht auf einzelne Technologien ein.
b1	4	Die Beeinflussung erfolgt über die Etablierung von neuen Informationssicherheitsprozessen, -strukturen und -instrumenten und über individuell zusammengestellte oder referenzierte Massnahmenkataloge. Dabei werden nur die direkt informationssicherheitsrelevanten Beeinflussungen berücksichtigt. Das Verfahren ist dabei stark skalierbar. Es kann verschiedenen Bedürfnissen angepasst werden und durchläuft nicht nur einen starren Weg.
b2	4	vgl. b1
b3	4	vgl. b1
c1	2	In ISiWay selbst werden keine Teilgebiete beschrieben. Es wird jedoch auf die Teilgebiete gemäss Kapitel 5 verwiesen.
c2	4	Die bekannten Kriterien werden (in Kapitel 2, jedoch nicht direkt in ISiWay) beschrieben und es werden auch Angaben gemacht, wie eigene Kriterien zu definieren sind.

Tabelle B-8: Bewertung ISiWay

B.9 Gegenüberstellung der Profile: Variable 1 (Auslösung)

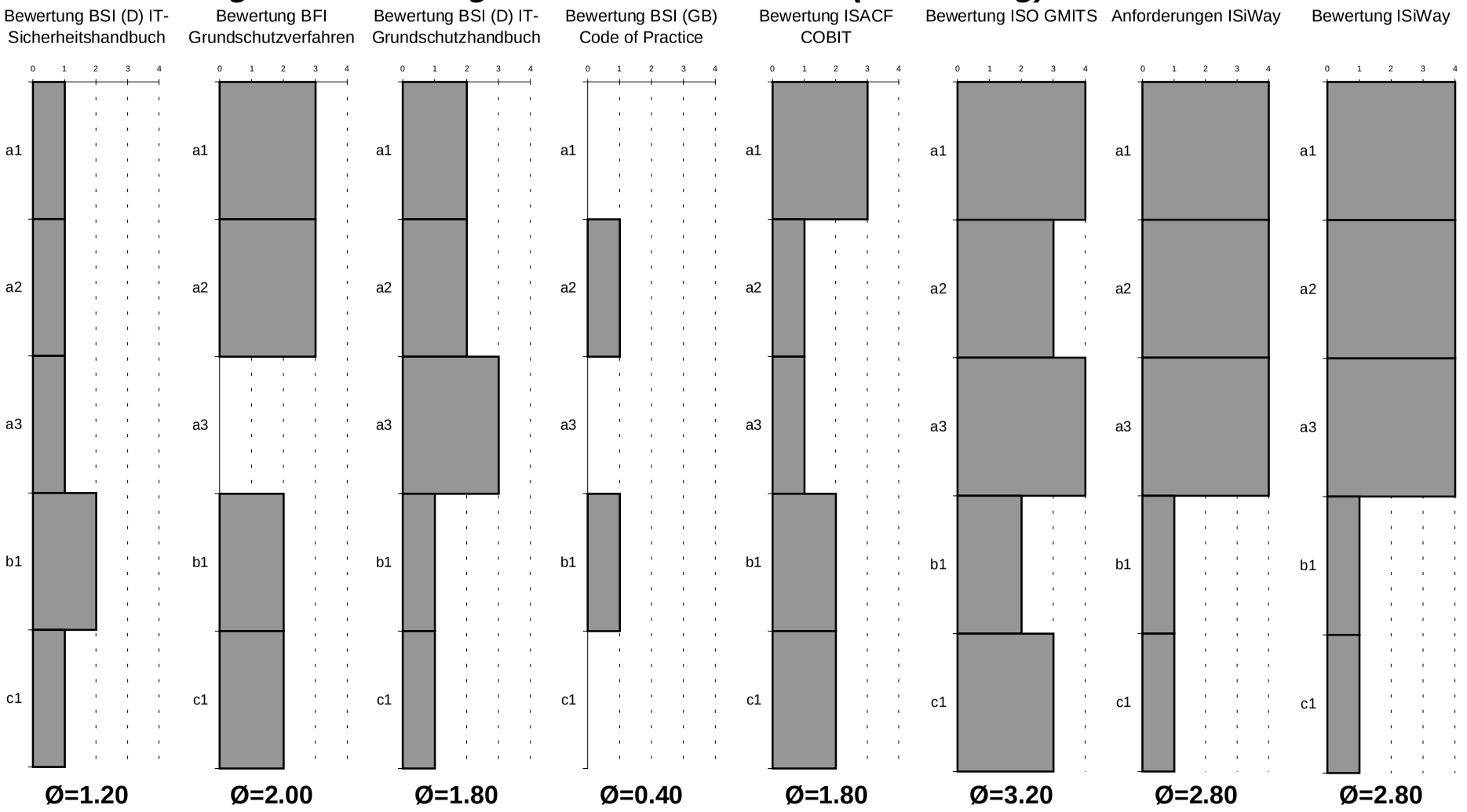


Tabelle B-9: Gegenüberstellung der Profile: Variable 1 (Auslösung)

B.10 Gegenüberstellung der Profile: Variable 2 (Organisation)

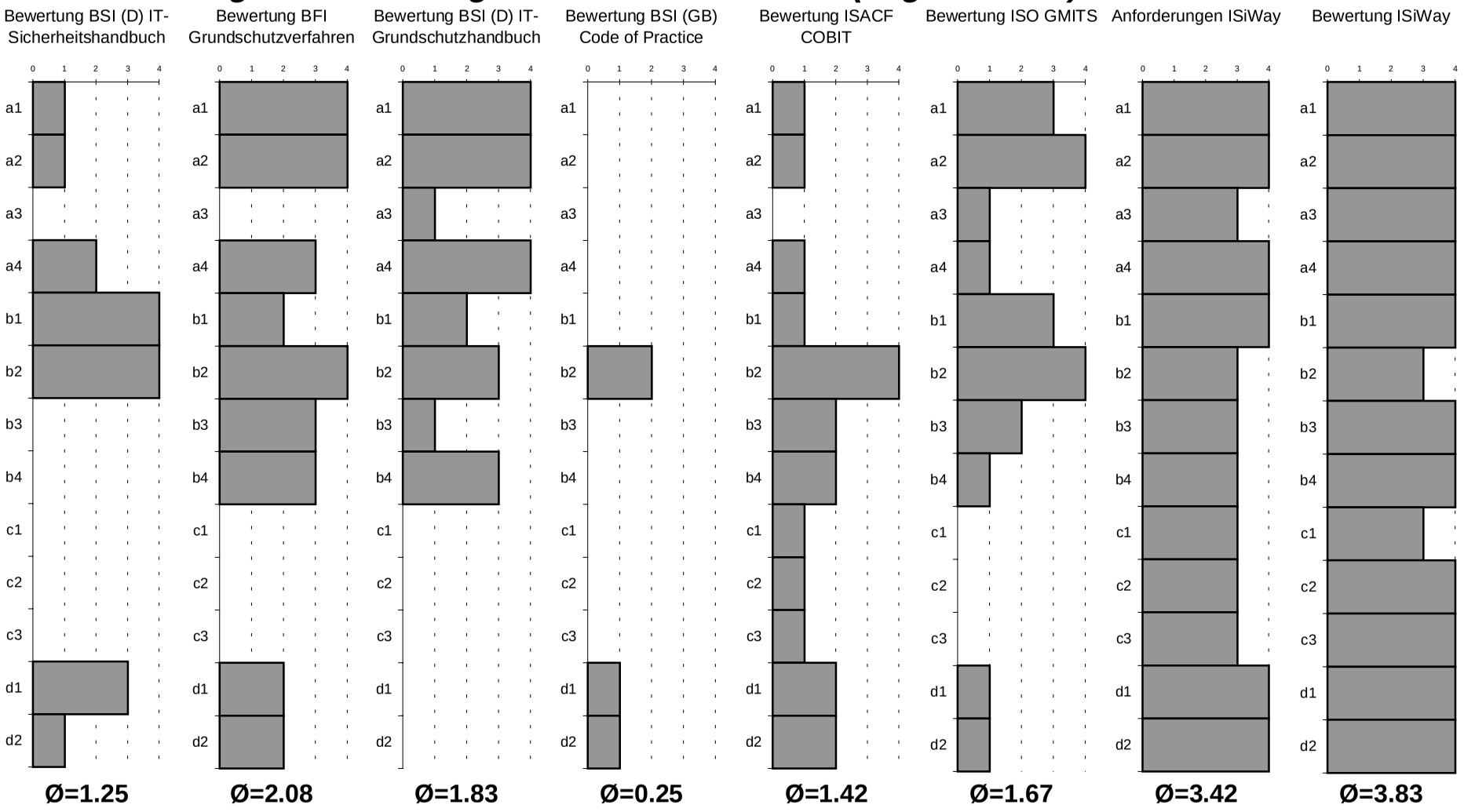


Tabelle B-10: Gegenüberstellung der Profile: Variable 2 (Organisation)

B.11 Gegenüberstellung der Profile: Variable 3 (Durchführung)

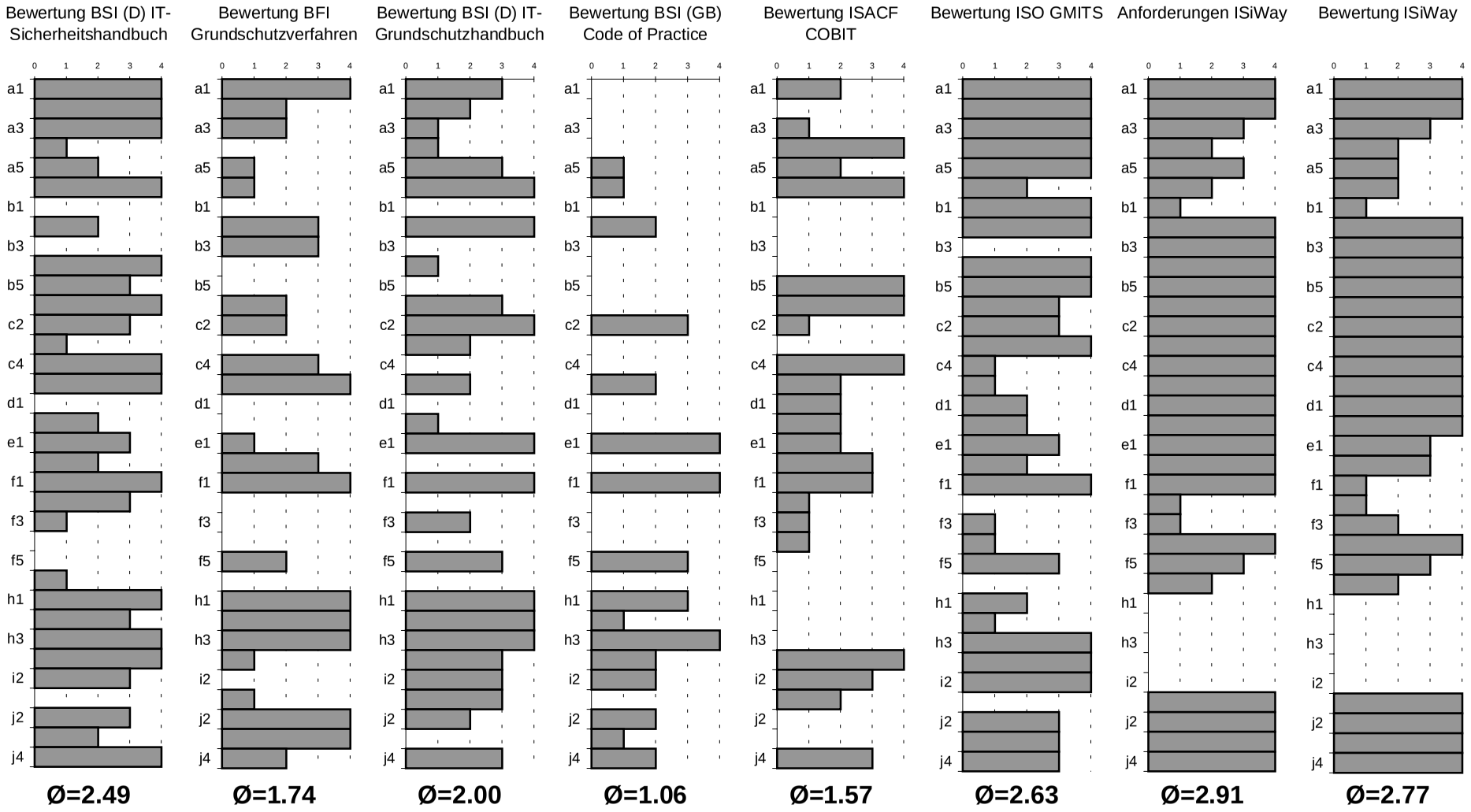


Tabelle B-11: Gegenüberstellung der Profile: Variable 3 (Durchführung)

B.12 Gegenüberstellung der Profile: Variable 4 (Fachbereiche)

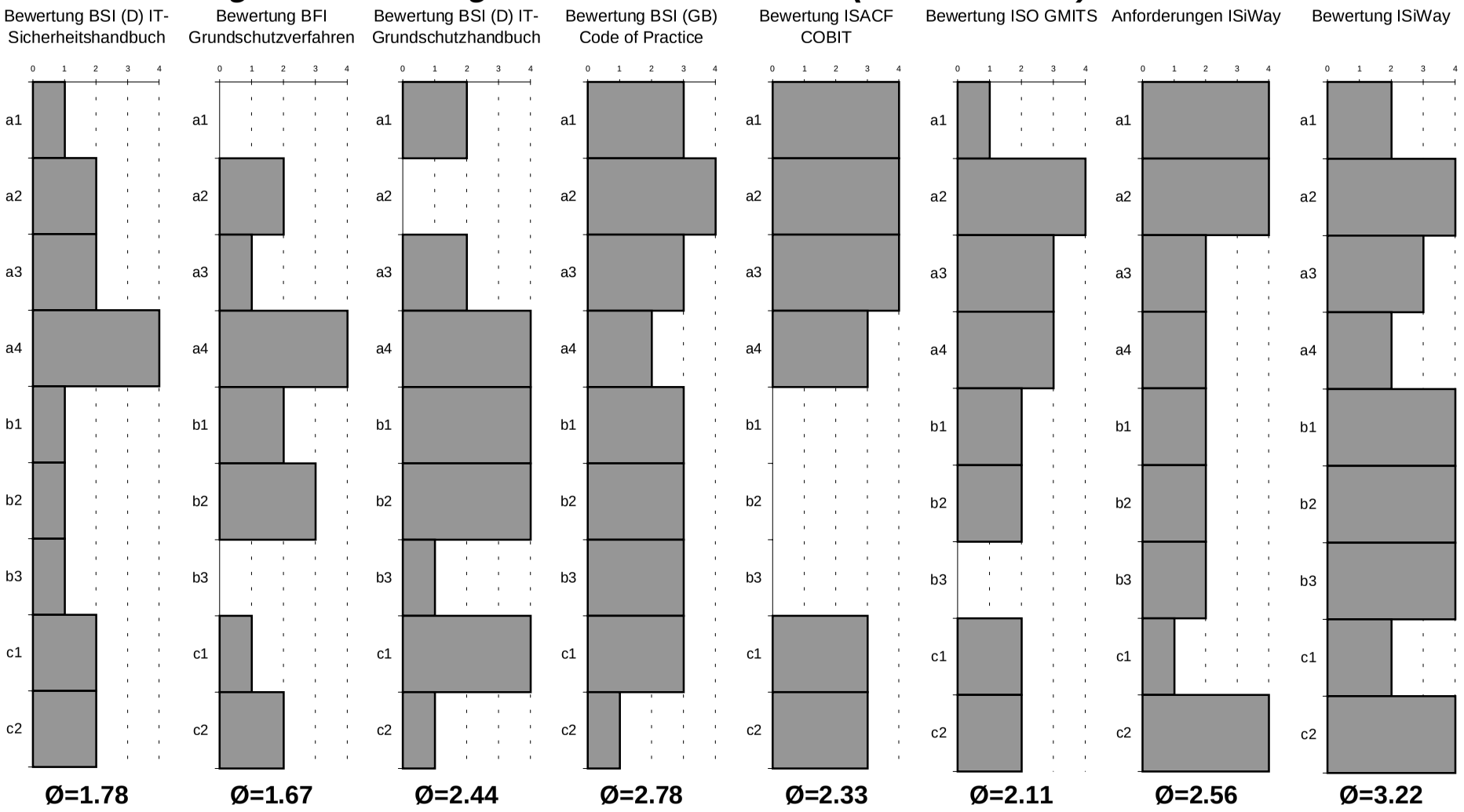
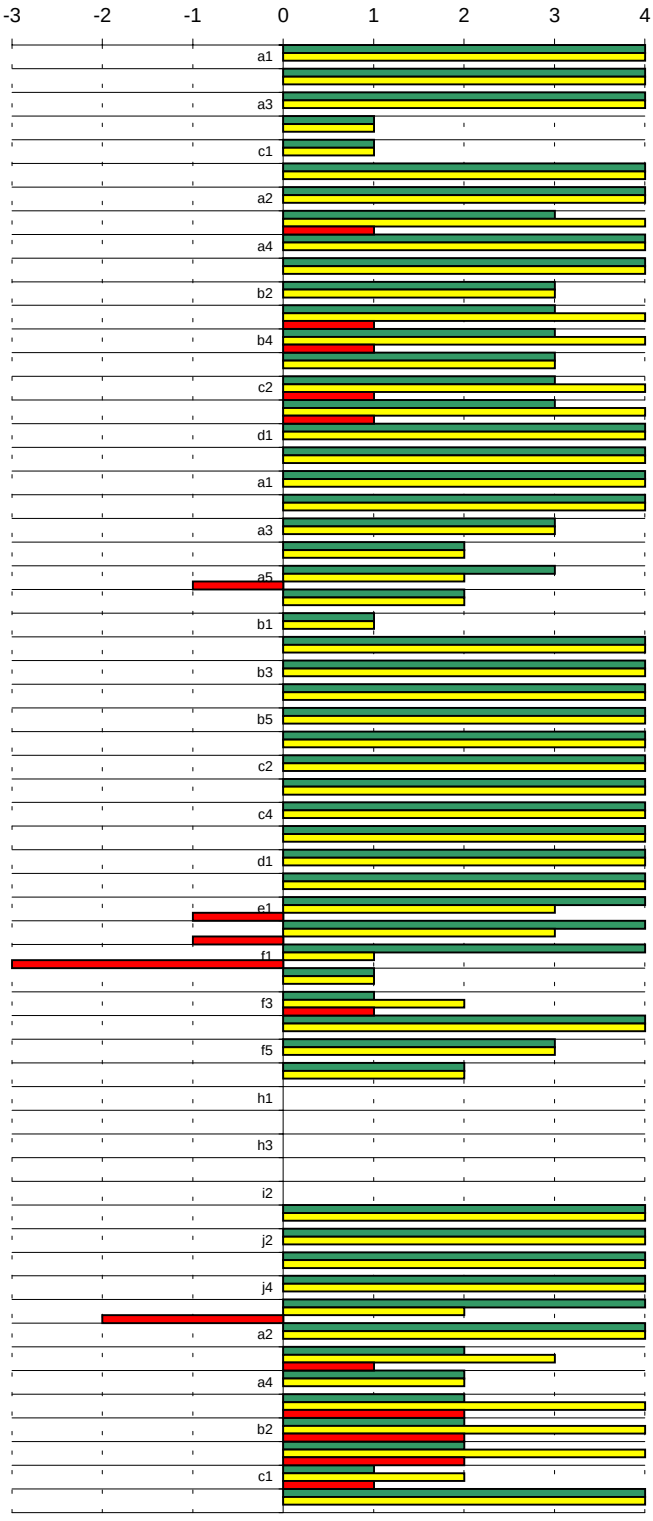


Tabelle B-12: Gegenüberstellung der Profile: Variable 4 (Fachbereiche)

B.13 Differenzen zwischen Anforderungen an und Bewertung von ISiWay

Variable	Teilvar.	Anforderungen an ISiWay: Wert	Bewertung von ISiWay: Wert	Differenzen zwischen Anforderung und Bewertung: Differenz
V1	a1	4	4	0
V1	a2	4	4	0
V1	a3	4	4	0
V1	b1	1	1	0
V1	c1	1	1	0
V2	a1	4	4	0
V2	a2	4	4	0
V2	a3	3	4	1
V2	a4	4	4	0
V2	b1	4	4	0
V2	b2	3	3	0
V2	b3	3	4	1
V2	b4	3	4	1
V2	c1	3	3	0
V2	c2	3	4	1
V2	c3	3	4	1
V2	d1	4	4	0
V2	d2	4	4	0
V3	a1	4	4	0
V3	a2	4	4	0
V3	a3	3	3	0
V3	a4	2	2	0
V3	a5	3	2	-1
V3	a6	2	2	0
V3	b1	1	1	0
V3	b2	4	4	0
V3	b3	4	4	0
V3	b4	4	4	0
V3	b5	4	4	0
V3	c1	4	4	0
V3	c2	4	4	0
V3	c3	4	4	0
V3	c4	4	4	0
V3	c5	4	4	0
V3	d1	4	4	0
V3	d2	4	4	0
V3	e1	4	3	-1
V3	e2	4	3	-1
V3	f1	4	1	-3
V3	f2	1	1	0
V3	f3	1	2	1
V3	f4	4	4	0
V3	f5	3	3	0
V3	g	2	2	0
V3	h1	0	0	0
V3	h2	0	0	0
V3	h3	0	0	0
V3	i1	0	0	0
V3	i2	0	0	0
V3	j1	4	4	0
V3	j2	4	4	0
V3	j3	4	4	0
V3	j4	4	4	0
V4	a1	4	2	-2
V4	a2	4	4	0
V4	a3	2	3	1
V4	a4	2	2	0
V4	b1	2	4	2
V4	b2	2	4	2
V4	b3	2	4	2
V4	c1	1	2	1
V4	c2	4	4	0



C Dokumentation zu *ISIWAY*

Anhang C.1 enthält die Details zur Spezifikation des Prozesses *ISIWAY*, der in Kapitel 8 konzeptionell und ganzheitlich beschrieben und evaluiert wird. Diese Details sind integraler Bestandteil der Dokumentation von *ISIWAY* und stehen nicht für sich alleine. Sie wurden aufgrund ihres Umfangs und aufgrund ihrer operativen Ausrichtung in diesen Anhang ausgelagert.

In Anhang C.2 wurde die Dokumentation zum reduzierten Verfahren *ISIWAY 1.5* eingefügt. Dieses Verfahren stellt eine Vereinfachung des ganzheitlichen Verfahrens *ISIWAY* dar und wird im Text als zweite Konkretisierung des Informationssicherheitsprozesses bezeichnet. Die hier eingefügte Dokumentation ist vollkommen unabhängig von dieser Dissertation verwendbar und kann beim Autor bezogen werden.

C.1 Detaillierte Beschreibung von ISIWAY

Anhang C.1.1 beinhaltet die Beschreibung der Aktivitätengruppen von *ISIWAY*.

Anhänge C.1.2ff umfassen die detaillierte Beschreibung aller einzelnen Aktivitäten von *ISIWAY*, geordnet nach Detaillierungsgrad.

C.1.1 Aktivitätengruppen

Die Aktivitäten, welche als Teil der einzelnen Detaillierungsgrade durchlaufen werden, unterscheiden sich inhaltlich stark, formell jedoch kaum. Sie lassen sich deshalb unabhängig vom Detaillierungsgrad zu Aktivitätengruppen zusammenfassen, die hier in der Folge kurz beschrieben werden.

Aktivitätengruppen der Planungsphase

Es werden Entscheidungsgrundlagen für die Durchführung des aktuellen Zyklus bereitgestellt. Dies umfasst:

10[107]:*Auslösung* des Teilprojektes durch Beauftragung; Übergabe der übergeordneten Ziele, des Zeitrahmens und Budgets,

20: *Zielvereinbarung* mit möglichst konkreter Festlegung der zu erreichenden Ziele und zu erfüllenden Anforderungen,

---

107 Die Aktivitäten sind in Zehner-Schritten nummeriert, um weitere Detaillierungen zuzulassen (Gruppierung). Die in diesem Abschnitt angegebenen Aktivitäten sind allgemein beschrieben. In den einzelnen Detaillierungsgraden werden Aktivitäten definiert, welche zu diesen Gruppen gehören.

30: *Abgrenzung* des zu betrachtenden Objekts bzgl. Breite (Objektkategorien und Verantwortungsbereiche) und Tiefe (Themenwahl, Bewertungskriterien etc.),

40: Festlegen der Verantwortung für dieses Teilprojekt mit Zusammenstellung der beteiligten Personen und Identifikation der Institutionen zur *Organisation* des Teilprojekts,

50: *Vorbereitung der Durchführung* mit Zusammenstellung der Arbeitsunterlagen,

60: *Ressourcenplanung* von Kosten / Budget, Zeit, Personen und Werkzeugen,

70: *Erhebung* oder *Nachführung* des aktuellen Zustands,

80: *Konsolidierung*: Übergeordnete Betrachtung der Verhältnismässigkeit der Erhebung, der vorgenommenen Bewertungen und der Ergebnisse der Teilprojekte sowie der Vollständigkeit (Verhinderung der Auslassung wichtiger Objekte); Feststellen mehrfach (redundant in verschiedenen Teilobjekten) erhobener Objekte und Beheben von Erhebungsunterschieden; evtl. Vornehmen von Korrekturen der Bewertung,

90: *Abschluss* durch Zusammenstellung der Ergebnisse und Zwischenberichterstattung an den ISiBe oder den Koordinator des übergeordneten Teilprojekts.

Aktivitätengruppen der Entscheidungsphase

Aufgrund der Planungsunterlagen wird eine der bestehenden Handlungsalternativen ausgewählt und als angemessen definiert. Dies umfasst:

10: Feststellen, ob *Sofortmassnahmen* notwendig sind; rasche Planung und Umsetzung in der Anordnungsphase,

20: *Entscheidungsspielraum* festlegen: Notwendigkeiten und Budget zusammenstellen,

30: *Dialog vorbereiten*: Entscheidungsrelevante Unterlagen zusammenstellen,

40: *Dialog führen* und *Entscheidung* fällen,

50: *Dokumentation* und Kommunikation der Entscheidung durch Beschreibung und Verteilung der Entscheidungsfindung,

90: *Abschluss* durch Zusammenstellung der Ergebnisse und Zwischenberichterstattung an den ISiBe oder den Koordinator des übergeordneten Teilprojekts.

Aktivitätengruppen der Anordnungsphase

Es wird konkret zusammengestellt und beschlossen, *wie* das entschiedene Ziel erreicht werden soll und welche Tätigkeiten dazu ausgeführt werden sollen:

10: *Evaluation der Entscheidung* zur Einschätzung der konkret entstehenden Aufwände und Nebenwirkungen,

20: *Erstellung* der *Realisierungsplanung* mit der Zusammenstellung und Ausarbeitung von Massnahmen,

30: *Diskussion* der *Realisierungsplanung* zur integrierten Betrachtung möglicher Auswirkungen,

40: *Beschluss* der *Realisierungsplanung* durch das erarbeitende Gremium,

90: *Abschluss* durch Zusammenstellung der Ergebnisse und Zwischenberichterstattung an den ISiBe oder den Koordinator des übergeordneten Teilprojekts.

Aktivitätengruppen der Durchführungsphase

Ausführung der Entscheidung mit Umsetzung dieser Tätigkeiten.

10: *Realisierungsplanung detaillieren* zur technik- und prozessbezogenen Beeinflussung des betroffenen Teilobjekts,

20: *Durchführung der Realisierung* durch Veränderung des Teilobjekts,

50: *Dokumentation der Realisierung* als Basis für die Bekanntgabe der Änderungen,

60: *Publikation der Realisierungsdokumentation,*

70: *Schulung* zur Einführung der Betroffenen in ein verändertes Teilobjekt und sein davon beeinflusstes Umfeld,

90: *Abschluss* durch Zusammenstellung der Ergebnisse und Zwischenberichterstattung an den ISiBe oder den Koordinator des übergeordneten Teilprojekts.

Aktivitätengruppen der Kontrollphase

Kontrolle bedeutet die Überprüfung der Erreichung des Ziels gemäss Entscheidung. Dies umfasst die Überprüfung, ob die Tätigkeiten erfolgreich durchgeführt werden konnten, ob der angestrebte Zustand damit erreicht wurde, ob das in der Planung definierte Ziel damit erreicht ist und die Feststellung, welche Defizite bei dieser Zielerreichung noch bestehen:

10: Im *Review* werden rückblickend Anordnung und Durchführung und die dabei entstandenen Zielerreichung für das aktuelle Projekt und alle möglicherweise laufenden untergeordneten Teilprojekte betrachtet. Dazu werden *Kennzahlen* gesammelt,

20: *Respawn* erlaubt das Neuauslösen weiterer Teilprojekte mit einem veränderten Bezugsobjekt oder Teilen davon (dies führt zur Projekthierarchie),

30: *Relaunch* umfasst die Neuauslösung eines Teilprojektes unter Berücksichtigung veränderter Umwelteinflüsse und unter Überarbeitung der Planung. Im Relaunch wird entschieden, ob die erneute Auslösung desselben

Detaillierungsgrades notwendig oder der Wechsel zum übergeordneten Detaillierungsgrad möglich ist,

40: *Synchronisation* mit anderen Teilprojekten mit Kommunikation, Koordination und Kooperation,

50: *Report* beinhaltet die Berichterstattung über Zielerreichung an die übergeordnete Ebene und einen Vorschlag zum weiteren Vorgehen,

70: *Audit* durch Betroffene, Sponsoren, Koordinatoren, Dritte, das übergeordnete Management oder die interne Revisionsstelle zur Klärung der Mittelverwendung und des Erfolgs,

90: *Abschluss* durch Beendigung des Teilprojektes und Übergabe der erarbeiteten Informationen an den ISiBe oder den Koordinator des übergeordneten Teilprojekts.

C.1.2 Inhalte der Vorbereitung (Detaillierungsgrad 0)

Der Detaillierungsgrad 0 (DG0) von *ISIWAY* umfasst Vorbereitungsarbeiten und führt noch nicht direkt zu einer Verbesserung der Informationssicherheit. Ziel des Vorbereitungszyklus ist es, die Grundlagen für ein funktionierendes Informationssicherheitsmanagement zu erarbeiten. Dies beginnt mit der Erreichung der Unterstützung des obersten Managements (GL) und umfasst die Festlegung und Zusammenstellung aller notwendigen Institutionen, Informationen und Instrumente, um die Durchführung des ISiM innerhalb der Unternehmung zu ermöglichen. Nach der Durchführung von DG0 ist die Unternehmung für eine erste Durchführung von DG1 bereit. DG0 ist also besonders wichtig und wird hier deshalb detaillierter beschrieben als die anderen Detaillierungsgrade.

DG0 umfasst fünf Phasen:

- Die Phase 1 *Management Awareness & Initiative* umfasst die Auslösung der gesamten Informationssicherheit.
- In Phase 2 *Grundlagen* werden die Grundlagen für das ISiM innerhalb der Unternehmung erarbeitet und zusammengestellt.
- Phase 3 *Einführung* beinhaltet die Publikation und Präsentation der Grundlagen innerhalb der Unternehmung und somit eine erste Bewusstseinsbildung für die Probleme der Informationssicherheit.
- Phase 4 *Durchführung* führt zur erstmaligen Auslösung der Informationssicherheit in Teilbereichen der Unternehmung und umfasst die Betreuung der dabei entstehenden Teilprojekte.
- Phase 5 *Kontrolle* beinhaltet die Berichterstattung über die geleisteten Arbeiten an die Geschäftsleitung.

Detaillierungsgrad 0 ist gesamthaft in Abbildung C-1 dargestellt[108].

[108] Diese und die folgenden Abbildungen wurden vom Werkzeug *ISIGO 1.5* generiert, welches im Kapitel 9 vorgestellt wird.

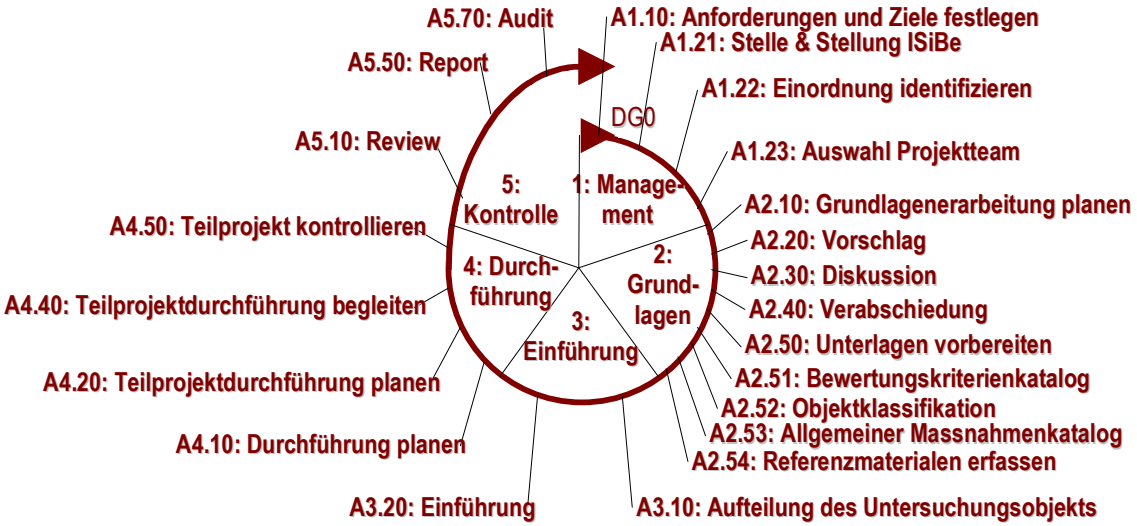


Abbildung C-1: Detaillierungsgrad 0

1: Management Awareness & Initiative

In Phase 1 geht es primär darum, das Informationssicherheitsmanagement (ISiM) erstmals auszulösen und die Stellen des primären Akteurs – des *Informationssicherheitsbeauftragten* (ISiBe) – zu definieren und ihm Handlungsspielraum einzurichten. Dieser muss sodann ein Projektteam zusammenstellen, welches ihn bei der weiteren Arbeit unterstützt.

Aktivität 1.10: Anforderungen und Ziele festlegen

Zu Beginn müssen die Anforderungen und Ziele festgelegt und zusammengestellt werden, welche mit dem ISiM verbunden sind. Diese Ziele müssen der Geschäftsleitung so präsentiert werden, dass sie grundsätzlich über die Auslösung des ISiM entscheiden kann. Ziel ist die Erwirkung eines Grundsatzentscheides der GL, welcher die Sammlung weiterer Fakten und die Erarbeitung weiterer, detaillierter Entscheidungsgrundlagen erlaubt.

Folgende Argumente sind dabei relevant:

- Informationssicherheit ist ein wichtiges Ziel der Unternehmung, da sie die Vorhersagbarkeit der unternehmerischen Prozesse erhöht und die Anzahl und Schwere von Störungen reduziert.
- Informationssicherheit umfasst alle Aspekte der Informationsverarbeitung. Inhalte stehen im Vordergrund, Technik im Hintergrund. Informations- und Datentechnik stellen eine wichtige Komponente dar, aber nur durch sicheres Verhalten von Mitarbeitern und die sichere, d.h. anforderungsgerechte Verwendung von Information kann Informationssicherheit langfristig erreicht werden.

- Informationssicherheit darf nicht mehr kosten als sie nutzt. Es muss also ein angemessenes Sicherheitsniveau festgelegt werden. Dies bedingt ernsthafte und ehrliche Auseinandersetzung mit Anforderungen und Kosten.
- Informationsverarbeitung geschieht dezentral. Deshalb müssen organisatorische Rahmenbedingungen geschaffen werden, um die dezentrale Durchführung des ISiM mit zentraler Koordination und Vergleichbarkeit zu erlauben.
- Informationssicherheit kann von der Informatik-Revision unterstützt werden, geht allerdings inhaltlich darüber hinaus.
- In dieser Aktivität müssen der Auftrag zur Erarbeitung von Entscheidungsgrundlagen, die Vorbereitung der Institutionen, Informationen, Instrumente und Prozesse des Informationssicherheitsmanagements (ISiM) und die Einrichtung einer Institution des Beauftragten für Informations-sicherheit (ISiBe) erreicht werden, der die Arbeiten durchführt und koordiniert.
- Für die Vorbereitung sollten 2 bis 12 Monate veranschlagt werden, 5 bis 50 % der Arbeitskapazität eines leitenden Angestellten aus der Organisations-, Internen Kommunikations- oder Informatikabteilung, welche die ISiBe-Institution besetzt sowie 5 bis 25% jeweils einer Person der teilnehmenden Bereiche[109].

Diese Argumente und weitere sensibilisierende Materialien können zusammengestellt und mit aktuellen Bedrohungen der Informationssicherheit (z.B. aus der Tagespresse) ergänzt werden. Dies kann (z.B. im Rahmen eines Vortrags) dem Management präsentiert werden. Ein Zeit- und Budgetplan kann dabei ebenfalls unterstützen.

Ergebnis dieser Aktivität ist ein Auftrag zur Erarbeitung des ISiM und die Beauftragung einer Person mit dieser Tätigkeit.

Aktivität 1.21: Stelle und Stellung ISiBe

In vielen Fällen ist die von der GL beauftragte Person nicht direkt der ISiBe, sondern der Auftrag wird zunächst (interim) an den Stabschef Sicherheit oder den Leiter der Informatikdienste o. ä. vergeben. Erste Aufgabe dieser Person ist es, die Stelle des Informationssicherheitsbeauftragten (ISiBe) zu definieren. Er erstellt dazu eine Aufgabenbeschreibung. Daraus müssen hervorgehen (gemäss [Rühli85, S. 253])

"1. Bezeichnung der Stelle, Titel des Stelleninhabers

2. Einordnung der Stelle in die Gesamtstruktur

---

109 Diese Zahlen sind allgemeine Richtwerte, welche in der konkreten Umsetzung in Abhängigkeit der Priorität erheblich nach oben oder unten abweichen können.

3. *Interne Gliederung der Stelle*
4. *Standort (räumliche Regelungen)*
5. *Stellvertretungsregelungen*
6. *Unterschriftenregelung (Zeichnungsberechtigung) und Weisungsbefugnis*
7. *Umschreibung der Aufgaben, Kompetenzen und Verantwortlichkeiten des Stelleninhabers; evtl. Umschreibung von Zielsetzungen*
8. *Anforderungen an den Stelleninhaber*
9. *Kriterien für die Beurteilung der Leistung sowie des Sozialverhaltens des Stelleninhabers*
10. *Koordination mit anderen Stellen*
11. *Teilnahme an Konferenzen usw."*

Diese Elemente müssen (von interim bestimmten ISiBe) zusammengestellt und der Geschäftsleitung zur Verabschiedung vorgelegt und verabschiedet werden. Dann ist ein geeigneter Stelleninhaber zu bestimmen. In Abhängigkeit von der Grösse der Unternehmung ist auch eine Personalunion mit der übergeordneten oder einer anderen Stelle möglich. Ein Beispiel zur Stellenbeschreibung des ISiBe ist in Tabelle C-1 wiedergegeben.

Stellenbeschreibung Informationssicherheitsbeauftragter	
1. Bezeichnung der Stelle Titel des Stelleninhabers	Informationssicherheitsbeauftragter (ISiBe) der Geschäftsleitung Beauftragter für Informationssicherheit
2. Einordnung der Stelle in die Gesamtstruktur	Hierarchische Unterordnung und Berichterstattung an den Stabschef Sicherheit der Geschäftsleitung
3. Interne Gliederung der Stelle	Leiter des Stabsbereiches Informationssicherheit der Geschäftsleitung
4. Standort (räumliche Regelungen)	In den Räumen der Stabsbereiche am Hauptsitz der Unternehmung
5. Stellvertretungsregelungen	1. Durch den stv. Leiter des Stabsbereiches Informationssicherheit 2. durch den Vorgesetzten
6. Unterschriftenregelung (Zeichnungsberechtigung) und Weisungsbefugnis	Für Beträge bis 10'000.- einzeln, darüber bis Fr. 100'000.- zu Zweien mit dem direkten Vorgesetzten.
7. Umschreibung der Aufgaben, Kompetenzen und Verantwortlichkeiten des Stelleninhabers; evtl. Umschreibung von Zielsetzungen	Führung des Stabes Informationssicherheit Erarbeitung, Zusammenstellung, Publikation und Präsentation von Handlungs- und Entscheidungsgrundlagen für die übergeordneten Stellen und die von den Inhalten betroffenen Parteien innerhalb der Unternehmung Leitung und Koordination der Informationssicherheitsprojekten innerhalb der Unternehmung in Zusammenarbeit mit den jeweiligen Verantwortlichen

8. Anforderungen an den Stelleninhaber	Organisations- und Informatik-Kenntnisse Freude am Umgang mit Menschen Überzeugungskraft und sicheres Auftreten Führungsqualitäten
9. Kriterien für die Beurteilung der Leistung sowie des Sozialverhaltens des Stelleninhabers	Rückmeldungen aus den Bereichen über Zustand und Fortschritte der Informationssicherheit innerhalb der Unternehmung
10. Koordination mit anderen Stellen	Zusammenarbeit mit anderen Stäben Koordination mit dem Leiter Informatik, dem Leiter Kommunikation und dem Leiter der Revision

Tabelle C-1: Beispiel für Stellenbeschreibung des ISiBE

Ergebnis dieser Aktivität ist die eingerichtete Stelle des ISiBe und damit die Ausgangsbasis für die Durchführung der weiteren Aktivitäten. Die Geschäftsleitung beruft eine Person in diese Stelle.

Aktivität 1.22: Einordnung identifizieren

Zu Beginn seiner Arbeit muss der ISiBe erkennen, welche Stellen innerhalb der Unternehmung die Informations- und Datenverarbeitung und somit die Informationssicherheit beeinflussen. Er muss sich Klarheit darüber verschaffen, in welcher Art und Weise er mit diesen Stellen aufgrund seiner Stellenbeschreibung und der möglicherweise schon geschehenen Einführung zusammenarbeiten kann. Dies hängt insbesondere auch von seiner Weisungsbefugnis ab. Diese Identifikation ist eine Voraussetzung für die zielgerichtete Auswahl des Projektteams für die weitere Arbeit.

Falls der ISiBe den betroffenen Gremien und Stellen nicht vorgestellt worden ist, kann er dies bei Bedarf selbst tun. Eine Einführung über den Projektleiter ist jedoch von Vorteil.

Ergebnis dieser Tätigkeit ist ein (nicht notwendigerweise schriftlich festgehalten) Verzeichnis der die Informationssicherheit beeinflussenden Stellen und Gremien.

Aktivität 1.23: Auswahl Projektteam

Der Informationssicherheitsbeauftragte kann Informationssicherheit in der Unternehmung nicht unabhängig erreichen. Einerseits kann er aufgrund der normalerweise fehlenden Weisungsbefugnis keinen Zwang zur Kooperation herstellen, andererseits muss er die Informationssicherheit in die Arbeit der jeweiligen betrachteten Bereiche integrieren. Es ist für den ISiBe deshalb wichtig, einflussreiche Personen aus den verschiedenen Bereichen der Unternehmung zu einem Projektteam zusammenzustellen, um mit ihnen die Erarbeitung der Grundlagen des ISiM vorzunehmen. Die Berufung einflussreicher Personen ist um so schwieriger, als diese oft selbst in verschiedenen Projekten engagiert sind und den Zielen der Informationssicherheit anfänglich kritisch gegenüberstehen können.

Es sollten Personen aus folgenden Bereichen in das Projektteam aufgenommen werden:

- Ein Geschäftsleitungsmitglied kann einerseits das Bindeglied zur Geschäftsleitung darstellen, andererseits die notwendige Motivation erhöhen,
- leitende Mitarbeiter der Fachbereiche der Unternehmung, in welchen das oder die Hauptgeschäfte / Hauptgeschäftsprozesse der Unternehmung ablaufen,
- einen leitenden Mitarbeiter der Informatik-, EDV- oder Automatisierungsabteilung, da dieser die Verwaltung der technisch erfassten Informationen (Daten) leitet,
- einen Mitarbeiter der internen Kommunikation und / oder der Personalentwicklung, da die Weitergabe der Inhalte und Ziele der Informationssicherheit innerhalb der Unternehmung die Unternehmungskultur beeinflusst,
- bei der Verwaltung personenbezogener Daten eine Person, welche im rechtlichen Bereich (v.a. Datenschutzes) beraten kann,
- bei ganz oder teilweise vollzogenem Outsourcing einen Vertreter des entsprechenden Insourcers,
- bei komplexen oder nicht selbst betriebenen technischen Informationssystemen einen Berater für Technologiefragen,
- bei grösseren wichtigen eingesetzten Fremdprodukten Vertreter der Hersteller oder Händler / Betreuer dieser Systeme,
- bei grösseren Unternehmungen der Leiter der Revision oder der Informatik-Revision, um die Anforderungen der Eigentümer der Unternehmung angemessen berücksichtigen zu können und Transparenz zu erreichen.

Aufgabe dieses Projektteams ist die Erarbeitung von Grundlagen, also nicht die konkrete Durchführung des ISiM, sondern die Organisation dieser Durchführung. Viele der Aufgaben in der Koordinationsphase werden vom ISiBe selbst durchgeführt; dazu greift er auf die Mitarbeit der verschiedenen Projektteammitglieder zurück. Sitzungen im Plenum werden jedoch nur selten notwendig sein. Zentral ist deshalb eine effiziente Kommunikation zwischen diesen Projektteam-Mitgliedern.

Ergebnis dieser Aktivität ist ein gebildetes Projektteam zur Erarbeitung der Grundlagen.

2: Grundlagen

Ziel der zweiten Vorbereitungsphase ist die Zusammenstellung von Grundlagen für die spätere Durchführung des Informationssicherheitsmanagements (ISiM). Hier werden die organisatorischen Institutionen, Prozesse und inhaltlichen Instrumente definiert und zusammengestellt, welche später bei der Durchführung der Informationssicherheit zu Anwendung gelangen sollen. Welche Grundlagen erarbeitet werden müssen, muss dabei erst noch festgelegt werden. Die hier vorgeschlagene Strukturierung in Institutionen, Informationen, Instrumente und

Prozesse kann zur Erstellung einer Agenda dienen. Ziel dabei ist die Einfachheit der Durchführung.

Aktivität 2.10: Grundlagenerarbeitung planen

Die Grundlagen des ISiM können gegliedert werden in:

- Festlegen des *Ziels* und der *Inhalte* des ISiM,
- Definition der *Institutionen und der Verantwortung*: Stellen, Gremien, und Besetzung mit Personen mit Verantwortung, Aufgaben und Kompetenzen,
- Definition der Abläufe und *Prozesse* des ISiM und Bereitstellung der Instrumente.

Ziel dieser Aktivität ist es, die zu definierenden Grundlagen zusammenzustellen. Hier wird ein möglicher Vorschlag abgegeben und weiter betrachtet:

- Festlegen einer *Informationssicherheitspolitik*, welche das Informationssicherheitsmanagement allgemein festlegt und das Ziel beschreibt und die von der Geschäftsleitung verabschiedet wird,
- Festlegen der Institutionen und Aufgaben gemäss der in Abschnitt 4.2.3 definierten Rollen,
- Festlegen der Prozesse des ISiM als Detaillierungsgrade 1 bis 4 von *ISIWAY*.

Aktivität 2.20: Vorschlag

In dieser Aktivität sollen Vorschläge für die Grundlagen erarbeitet werden, indem die verfügbaren Quellen (aus der Literatur oder vom Vorbild anderer Unternehmungen) zusammengestellt und analysiert werden und versucht wird, daraus einen für die eigene Unternehmung geeigneten Vorschlag zu erarbeiten. Vordringliche Tätigkeit ist die Formulierung einer Informationssicherheitspolitik (ISiPol) mit dem Ziel des ISiM in der Unternehmung. Um dies vornehmen zu können, muss allerdings auch ein Vorschlag für Strukturen, Funktionen und Prozesse erstellt werden. Alle Mitglieder des Projektteams sind hier gefordert, denn sie wurden ausgewählt, um jeweils repräsentative Inhalte beizutragen.

Hier werden die in Tabelle C-2 enthaltenen Grundlagen als Elemente der Informationssicherheitspolitik vorgeschlagen.

Element	*Inhalt*
Ziel	Ziel des Informationssicherheitsmanagement (ISiM) in der Unternehmung ist die Erreichung eines angemessenen Sicherheitsniveaus der Informationsverarbeitung, um so das Auftreten von Störungen zu minimieren, ohne zuviel Flexibilität und Effizienz einzubüssen. Darüber hinaus muss jede einzelne Stelle die Verantwortung für die Sicherheit der ihr anvertrauten Informationen tragen und dazu die von der Stabsstelle für Informationssicherheit angebotenen Dienstleistungen beziehen.

Motivation	Information ist der zentrale Inhalt jeder unternehmerischen Tätigkeit. Sie muss deshalb anforderungsgerecht verwendet und verarbeitet werden.
Vorgehen (Prozess)	Zur Erreichung des Ziels müssen die Anforderungen an die Sicherheit der Informationen erhoben, bestehende Diskrepanzen erkannt und durch Massnahmen beseitigt werden. Dazu ist ein Dialog aller beteiligten Parteien notwendig, welcher mit Hilfe des Vorgehens *ISIWAY* durchgeführt werden soll.
Institutionen	Für die Informationssicherheit bestehen folgende Institutionen innerhalb der Unternehmung: Informationssicherheitsbeauftragter (ISiBe): oberster Koordinator der Informationssicherheit in der Unternehmung, erstattet der Geschäftsleitung Bericht Stabsstelle für Informationssicherheit (SSISi): Beratende und koordinierende Stelle unter Leitung des ISiBe, berät auf Anfrage oder bei bestehendem übergeordnetem Interesse und erstellt handlungs- und entscheidungsrelevante Unterlagen zur Unterstützung der Informationssicherheit innerhalb der Unternehmung Linienstellen als Verantwortliche für die Informationssicherheit in ihren Bereichen Gremium oder Forum für Informationssicherheit (ISi-Forum): Interdisziplinäres Forum unter Leitung des ISiBe, welches alle Abteilungsleiter der Unternehmung und den Sicherheitsbeauftragten der Unternehmung umfasst und übergreifende sicherheitsrelevante Fragestellungen behandelt.
Verantwortung	Jede Linienstelle ist für die Sicherheit der ihr zugeteilten Information verantwortlich. Die Durchführung von *ISIWAY* verlangt die Zuordnung jeder vorhandenen Information zu genau einer Linienstelle oder deren Vernichtung. Die Linienstellen sind für die Durchführung von *ISIWAY* verantwortlich. Der ISiBe unterstützt die Linienstellen beratend.

Tabelle C-2: Elemente der Informationssicherheitspolitik

Ergebnis dieser Aktivität ist ein Vorschlag für Ziel, Institutionen, Aufgaben und Prozesse, der in der folgenden Aktivität weiter diskutiert werden kann.

Aktivität 2.30: Diskussion

Nachdem der Vorschlag zusammengestellt wurde, muss er modifiziert werden, bis ein Konsens gefunden wird. Dabei muss einerseits die später notwendige Zustimmung der Geschäftsleitung berücksichtigt werden, andererseits müssen aber alle Gremien und Funktionen innerhalb der Unternehmung berücksichtigt (d.h. gefragt) werden, welche diese Informationssicherheit später umzusetzen haben. Die Entwicklung einer nicht akzeptierten Basis kann nicht zu einer konsequenten Umsetzung des ISiM führen. Umgekehrt kann der Einbezug der Betroffenen zur besseren Motivation führen, da diese schon früh über die entstehenden Entscheidungen informiert werden und selbst Einfluss nehmen können.

Auch hier sind wieder alle Projektteammitglieder gefragt, korrigierende und ergänzende Beiträge selbst zu formulieren oder in den betroffenen Bereichen einzuholen. Ergebnis ist ein konsensfähiger Vorschlag.

Aktivität 2.40: Verabschiedung

Ziel dieser Aktivität ist es, den Vorschlag für die Grundlagen der Informationssicherheit in der Unternehmung von der Geschäftsleitung verabschieden zu lassen. Dazu werden die Grundlagen nach Konsultation der Projektteammitglieder und Einholen deren Einverständnis der Geschäftsleitung in knapper Form präsentiert. Bei positivem Ausgang kann die Existenz und Gültigkeit dieser Grundlagen kommuniziert werden. Ergebnis ist also die Gültigkeit der erarbeiteten Grundlagen.

Aktivität 2.50: Unterlagen vorbereiten

Nachdem die Gültigkeit erklärt wurde, müssen die entsprechenden erarbeiteten Unterlagen gesamthaft ausgestaltet und dargestellt werden, um sie anschliessend zu publizieren. Dazu müssen Kommunikationskanäle ausgewählt und benutzt werden.

Aktivität 2.51: Bewertungskriterienkatalog

Die Grundanforderungen an die Informationssicherheit, welche in der Unternehmung zu betrachten sind, müssen zusammenstellt werden (vgl. Abschnitt 2.3). Darauf aufbauend muss eine einheitliche Wertezuteilung festgelegt werden, um Vergleichbarkeit der später auf dieser Basis vorgenommenen Bewertungen zu erreichen. Im Anhang zur Dokumentation von *ISIWAY 1.5* (in Anhang C.2) ist ein solcher Katalog aufgeführt.

Aktivität 2.52: Objektklassifikation

Die Aufteilung des Bezugsobjektes in verschiedene Teilobjekte wurde in Kapitel 3 vorgestellt und beschrieben. Für die konkrete Umsetzung ist eine stärkere Detaillierung empfehlenswert, um einerseits den Ein- oder Ausschluss einzelner Objektkategorien zu erlauben und um andererseits auch hier Vergleichbarkeit der erhobenen (betrachteten) Objektklassen zu erreichen.

Aktivität 2.53: Allgemeiner Massnahmenkatalog

Falls in der Grundlagenerarbeitung beschlossen wurde, dass ein minimales Sicherheitsniveau der Unternehmung durch die Festlegung eines allgemeinen Massnahmenkataloges erreicht werden soll, muss dieser hier erarbeitet werden. Er kann aufgrund der zu diesem Zeitpunkt von *ISIWAY* noch nicht bekannten Objektstrukturen jedoch nicht sehr konkret festgelegt werden; es werden also abstrakte allgemeine Massnahmen festgelegt. Deshalb kann es vorteilhaft sein, auf einen extern verfügbaren Massnahmenkatalog zu verweisen.

Aktivität 2.54: Referenzmaterialien erfassen

Falls möglich sollte ein Verzeichnis der für die Bearbeitung notwendigen Referenzmaterialien und Ressourcen erstellt und publiziert werden. Dies kann beispielsweise Adressenverzeichnisse von Personen, internen und externen Anlaufstellen und Organisationen, Verzeichnisse verfügbarer Systeme, allgemeine Bedrohungskataloge und Literaturangaben umfassen.

Aktivität 2.55: Publikationsmedium wählen

Die zusammengestellten Unterlagen sollten über mehrere Kanäle verbreitet werden. Es bieten sich insbesondere interne bestehende oder speziell eingerichtete Verteillisten, Intra- und Extranets an.

3: Einführung

In der Einführung werden die erarbeiteten Grundlagen präsentiert und die betroffenen Personen erstmals involviert. Damit findet eine erste Bewusstseinsbildung für die Probleme der Informationssicherheit statt.

Aktivität 3.10: Aufteilung des Untersuchungsobjekts

Zu Beginn des Informationssicherheitsmanagements muss bestimmt werden, welche Teile der Unternehmung von Anfang an zu involvieren sind. Das kann die gesamte Unternehmung sein. Es ist jedoch sinnvoll, mit einzelnen Bereichen zu beginnen, um Erfahrungen zu sammeln. Ausserdem ist ein Beginn in der Zentrale, dem Hauptsitz oder bei der Geschäftsleitung der Unternehmung zu empfehlen, um als Vorbild die Umsetzung in den weiteren Bereichen zu stimulieren. Ergebnis ist eine Selektion der zu involvierenden Bereiche.

Aktivität 3.20: Schulung der Koordinatoren

In den ausgewählten Bereichen werden Koordinatoren für Informationssicherheit (ISiKos) bestimmt. Dies geschieht möglicherweise direkt durch den ISiBe, aber sinnvollerweise durch die jeweiligen direkten Vorgesetzten (Rolle: übergeordnetes Management), welche gemäss Informationssicherheitspolitik die Verantwortung tragen. Das übergeordnete Management und die von ihnen bezeichneten Koordinatoren werden für eine Einführung in das Verfahren eingeladen. Diese Einführung stellt die gesamte Konzeption und das Vorgehen von *ISIWAY* vor. Ergebnis ist die ein erster Kenntnisstand der Koordinatoren.

4: Durchführung

In der vierten Phase von DG0 wird das Informationssicherheitsmanagement innerhalb der Unternehmung erstmals in denjenigen Teilbereichen ausgelöst, in welchen zuvor die Einführung stattgefunden hat. Die Durchführung besteht für die jeweiligen Koordinatoren aus einem der vier *ISIWAY*-Zyklen DG1 bis DG4; ihre

jeweiligen Tätigkeiten beginnen mit der ersten Aktivität der ersten Phase des DG1 und durchlaufen nach und nach alle Phasen bis zur Kontrollphase von DG4. Der Informationssicherheitsbeauftragte, der als oberster Koordinator agiert, verharrt mit seiner Ausführung jedoch in der Durchführungsphase von DG0; DG0 kann also auch als Durchführung der durch ihn mitgetragenen Planung, Entscheidung und Anordnung des Informationssicherheitsmanagements in der Unternehmung betrachtet werden. DG0 stellt für ihn also einen eigenen speziellen Zyklus dar, in dessen Wiederholung es auch die Grundlagen zu überarbeiten gilt. In den Phasen 4 und 5 von DG0 geht es für ihn darum, die Durchführung der weiteren *ISIWAY*-Teilprojekte in den beteiligten Bereichen auszulösen, zu betreuen und zu kontrollieren.

Aktivität 4.10: Durchführung planen

Zunächst muss der ISiBe, um seine eigenen Ressourcen nicht zu überfordern, die Durchführung der *ISIWAY*-Teilprojekte in den Bereichen mit den jeweils zuständigen Koordinatoren terminieren, also einen gestaffelten Beginn und Beendigung vorsehen.

Aktivität 4.20: Teilprojektdurchführung planen

In dieser Aktivität wird die Planung der einzelnen Teilprojekte gemeinsam mit den jeweiligen Koordinatoren vorgenommen. Dies entspricht der Phase 1 des jeweiligen Detaillierungsgrades der Teilprojekte (bei der ersten Durchführung also der Phase 1 von DG1 des untergeordneten Teilprojektes). Ergebnis ist die Planung des jeweiligen Teilprojektes.

Aktivität 4.40: Teilprojektdurchführung begleiten

Diese Aktivität umfasst die Begleitung und Unterstützung des Ablaufs der Phasen 2 bis 4 der jeweiligen Teilprojekte. Die Federführung für diese Durchführung liegt beim jeweiligen Koordinator des Teilprojektes; der ISiBe leistet auf Anfrage Unterstützung. Dabei kann es sich um übergeordnete Koordinationsaufgaben handeln, beispielsweise wenn ein direkter Dialog scheitert oder der Dialog aufgrund übergreifender Ressourcen auf übergeordneter Ebene stattfinden muss. Es kann auch die Vermittlung von Beratern, die Motivation der Betroffenen, die direkte fachliche Beratung oder die Konsolidierung[110] von erhobenen Inhalten umfassen.

Aktivität 4.50: Teilprojekt kontrollieren

Hier werden die Kontrollphasen der einzelnen Teilprojekte kontrolliert, indem beim Durchlaufen der jeweiligen Kontrollaktivitäten unterstützt und koordiniert wird. Ergebnis dieser Phase ist ein abgeschlossenes Teilprojekt.

---

110 Unter Konsolidierung wird hier das Zusammenführen von Erhebungsdaten verschiedener Bereiche verstanden, welche dasselbe Objekt beschreiben.

5: Kontrolle

Die fünfte und letzte Phase der Vorbereitung umfasst die Kontrolle und Berichterstattung über die geleisteten Arbeiten durch den ISiBe an die Geschäftsleitung. Im Gegensatz zu den einzelnen Teilprojekten, welche dem beschriebenen Muster der DGs 1 bis 4 folgen, finden im DG0 nur Review, Respawn und Report statt.

Phase 5 des DG0 kann nie erreicht werden, denn die Phase 4 mit der Unterstützung der Teilprojekte *endet nie*. Alle Teilprojekte sind zyklisch aufgebaut, und bei mehreren parallel laufenden Projekten wird immer eines darunter sein, welches Phase 5 des jeweiligen DGs nicht abgeschlossen hat. Es bestehen deshalb zwei Möglichkeiten:

- Der ISiBe durchläuft die Phase 5 von DG0 periodisch, also beispielsweise einmal jährlich und fasst aus diesem Anlass den aktuellen Zustand aller abgeschlossenen und noch laufenden Teilprojekte zusammen, oder
- der ISiBe verlangt von allen Teilprojekten den Abschluss auf einen bestimmten Termin, um aufbauend auf den Ergebnissen die Kontrollphase von DG0 einzuleiten.

Letztere Variante scheint aufgrund der (normalerweise) fehlenden Weisungsbefugnis schwer durchsetzbar und könnte auch bei der Verpflichtung auf einen termingerechten Abschluss durch einzelne verzögerte Teilprojekte verunmöglicht werden. Ausserdem würde das Informationssicherheitsmanagement während dieser Aktivitäten ruhen und es würde eine Belastungsspitze des ISiBe entstehen, denn er müsste gleichzeitig die Ergebnisse verarbeiten und die einzelnen Teilprojekte neu starten.

Es liegt also nahe, die Phase 5 des DG0 periodisch zu durchlaufen, z.B. einmal jährlich oder auf Anfrage des übergeordneten Managements bzw. der Geschäftsleitung oder der Revision.

Aktivität 5.10: Review

In der rückblickenden Betrachtung der Tätigkeiten des ISiBe geht es vor allem darum, die Qualität der erarbeiteten Grundlagen und der Organisation zu bewerten sowie den Status der bisher durchgeführten und noch laufenden Teilprojekte mit Kennzahlen zu beschreiben. Daraus kann die Notwendigkeit von Anpassungen hergeleitet werden, welche einen erneuten Start des DG0 auslösen können.

Ausserdem muss die Involvierung weiterer Teilbereiche der Unternehmung vorgesehen werden (falls nicht von Beginn an die gesamte Unternehmung involviert wurde).

Aktivität 5.50: Report

Aufgrund der Ergebnisse des Reviews kann ein Bericht an das übergeordnete Management bzw. die Geschäftsleitung zusammengestellt werden, in welchem über

die Durchführung der Teilprojekte berichtet werden kann sowie über die anstehenden weiteren Arbeiten. Dabei werden v.a. die quantitativen und qualitativen Ergebnisse verwendet, welche von den Koordinatoren zur Verfügung gestellt wurden.

Aktivität 5.70: Audit

Im Audit wird festgestellt, ob die von den Koordinatoren gemachten Angaben mit der Realität übereinstimmen. Dies stellt die nachträgliche, prozessunabhängige Kontrolle dar, in welcher der ISiBe (aber möglicherweise auch andere Rollen) sich Kenntnis über den tatsächlichen Zustand der Informationssicherheit in einem Bereich verschaffen. Diese Kontrolle kann einmalig stattfinden, sollte aber, um auch als Kontrolle wahrgenommen zu werden, periodisch stattfinden (z.B. jährlich).

C.1.3 Minimale Informationssicherheit (Detaillierungsgrad 1)

Ziel von DG1 ist es, möglichst schnell einen Überblick über die aktuelle Sicherheit des Untersuchungsobjektes zu bekommen, Sofortmassnahmen auszulösen, falls notwendig, und danach grundsätzliche Massnahmen ohne besondere Berücksichtigung einzelner Werte oder höherer Bedürfnisse zu veranlassen. DG1 folgt damit mehrheitlich dem in Abschnitt 6.4 beschriebenen Grundschutzansatz. DG1 ist in Abbildung C-2 detailliert dargestellt.

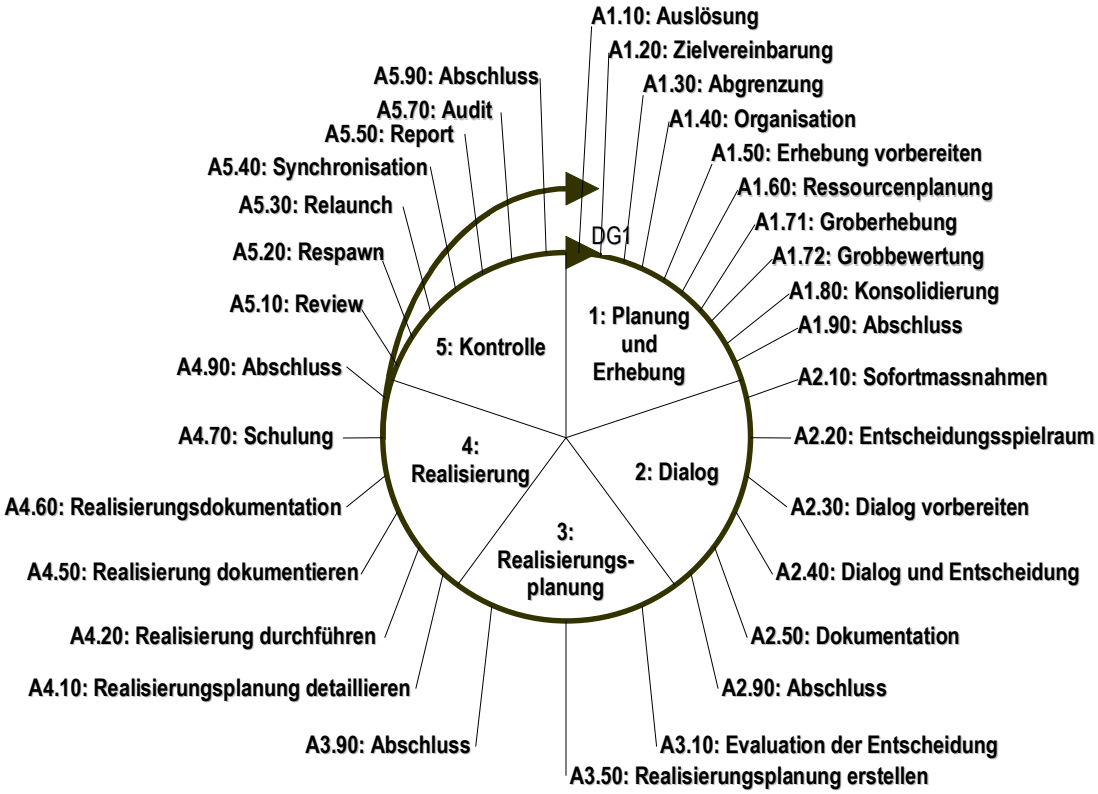


Abbildung C-2: Detaillierungsgrad 1

1: Planung und Erhebung

In Phase 1 muss das Teilprojekt initialisiert werden.

Aktivität 1.10: Auslösung

Aktivität 1.10 startet das Teilprojekt. Üblicherweise geschieht dies durch den Auftrag einer übergeordneten Stelle, also beispielsweise durch den übergeordneten Manager, welcher die Verantwortung für diesen Teilbereich der Unternehmung trägt oder direkt durch den Informationssicherheitsbeauftragten (dann allerdings ohne Weisungsbefugnis). Bei der Auslösung geht es vorerst darum, das übergeordnete Ziel des Beauftragenden zu erfüllen und dessen Richtlinien und Rahmenbedingungen einzuhalten. Darunter fallen die geplante Dauer für die Durchführung des Teilprojektes, das Budget, die Möglichkeit, Grundlagen-dokumente anzupassen und weitere Vereinbarungen. Die Verantwortung für die

Durchführung des aktuellen Teilprojekts liegt dann beim jeweiligen Informationssicherheitskoordinator (ISiKo). Ergebnis dieser Aktivität ist also der Start eines Teilprojektes. Es muss sich dabei nicht um die *erste* Auslösung dieses Teilprojektes handeln; vielmehr kann dasselbe Betrachtungsobjekt schon vorgängig betrachtet worden sein (vgl. Aktivität 5.30).

Aktivität 1.20: Zielvereinbarung

Nach dem Start müssen die Ziele für das aktuelle Projekt konkretisiert und in Absprache mit dem übergeordneten Management und evtl. mit dem ISiBe festgelegt werden. Dabei müssen auch konkrete Anforderungen an einzelne im Teilprojekt identifizierbare Informationssammlungen und Informationen bestimmt werden. Ergebnis ist eine konkrete Zielvereinbarung sowie eine Einigung auf Budgets und Termine.

Aktivität 1.30: Abgrenzung

Ausgehend von der Zielvereinbarung muss bestimmt werden, welche Teile des aktuellen Bereichs im Projekt betrachtet werden sollen. Die allgemeinen Vorgaben des ISiBe aus der Auslösung (Aktivität 1.10) bestimmt die Auswahl einzelner Objektklassen für die Betrachtung, wobei die Objektklassifikation (vgl. DG0, Aktivität 2.20) berücksichtigt werden muss. Für jede Objektklasse kann zusätzlich bestimmt werden, wie detailliert die entsprechenden Objekte erhoben werden, indem die Erhebung bestimmter Attribute verlangt oder ausgelassen wird (z.B. Standort eines Objektes, Grösse (in MByte), Alter etc. je nach Objektklasse). Darüber hinaus kann es auch innerhalb des Teilprojektes sinnvoll sein, einzelne Teilbereiche zunächst auszuklammern. Die Betrachtungs*tiefe* anzupassen, ist in DG0 nicht möglich, da in DG0 ohnehin nur minimaler Schutz betrachtet wird.

Aktivität 1.40: Organisation

In Abhängigkeit der berücksichtigten Objektklassen und der zu berücksichtigenden Teilbereiche der Unternehmung ergibt sich, welche Personen und Institutionen im Teilprojekt involviert werden müssen. Die Verantwortung für die Durchführung liegt beim ISiKo, die Verantwortung für das Endresultat beim übergeordneten Management, die Verantwortung für die Sicherheit der einzelnen Informationssammlungen muss konkret einzelnen Personen zugeordnet werden. Ebenso müssen die wichtigen Verwalter identifiziert und angesprochen werden. Ergebnis ist eine Zusammenstellung der zu involvierenden Personen.

Aktivität 1.50: Vorbereitung der Erhebung

In dieser Phase geht es um die konkrete Planung der Erhebung. Dazu gehören die Auswahl und Bereitstellung von Werkzeugen (Formulare, computergestütztes Erfassungssystem etc.) und Arbeitsunterlagen (Grundlagendokumente und -informationen aus DG0, bereichs- und technologieabhängige Dokumente).

Falls dies zulässig ist (dies wird in der Aktivität 1.10 festgelegt), so kann auch der vorgegebene Grundschutzmassnahmenkatalog angepasst werden, indem Massnahmen ausgeklammert oder hinzugefügt werden. Dies erschwert jedoch die spätere Vergleichbarkeit der Ergebnisse.

Aktivität 1.60: Ressourcenplanung

Die Ressourcenplanung muss Zeitaufwand, Termine und Budget umfassen. Gesamthaft sollten die zeitlichen Rahmenbedingungen aus der Auslösung berücksichtigt werden. Wie der Zeitaufwand sich über die einzelnen Phasen verteilt, kann nicht allgemein bestimmt werden, da dies stark bereichs- und technologieabhängig ist. Der ISiKo muss jedoch eine Planung erstellen. Daraus müssen die Anzahl und Dauer der Termine hervorgehen, welche er für die Erhebung, den Dialog, den Massnahmenbeschluss, die Massnahmenumsetzung und die Kontrolle benötigt. Dies ist wiederum abhängig von der Art der notwendigen Betreuung, welche vom Vorwissen der beteiligten Personen abhängt. Das Budget wird vor allem in der Massnahmenplanung verteilt und in der Massnahmen-umsetzung bezogen.

Aktivität 1.71: Groberhebung

Die Erhebung der schützenswerten Objekte muss durchgeführt werden. Dies umfasst in erster Linie eine Inventarisierung derjenigen Objekte, welche den in Aktivität 1.30 ausgewählten Objektklassen angehören. Zentral ist in jedem Fall die Erhebung der *Informationssammlungen*. Diese geschieht durch die Ansprechpartner für die Informationssammlungen (die *Info Owner*) mit Hilfe der in Aktivität 1.50 zur Verfügung gestellten Arbeitsunterlagen und Hilfsmittel. Ebenfalls essentiell ist die Erhebung der wichtigsten *technischen Informationssysteme (IT-Systeme)* durch die Ansprechpartner für die IT-Systeme (*Verwalter*). Das Format und die Attribute der Erhebung wurden ebenfalls in Aktivität 1.30 festgelegt. Beim erneuten Durchlaufen wird die beim vorherigen Durchlaufen vorgenommene Erhebung dem aktuellen Status angepasst, also *nachgeführt*. Die Resultate werden dem ISiKo übergeben.

Aktivität 1.72: Grobbewertung

Während der Erhebung der Objekte kann durch die Info Owner oder Verwalter auf besondere bestehende Schwachstellen der Systeme oder auf besondere Bedrohungen hingewiesen werden. Diese Angaben müssen erhoben und festgehalten werden, um so schnell wie möglich Sofortmassnahmen auslösen zu können. Die Resultate werden dem ISiKo übergeben.

Aktivität 1.80: Konsolidierung

In dieser Phase muss der ISiKo die Erhebung der Objekte sichten und konsolidieren. Es ist möglich, dass einzelne Objekte mehrfach (durch verschiedene Personen) erhoben werden und sich diese Erhebungen unterschieden oder sogar

widersprechen. Der Koordinator muss in Zusammenarbeit mit den Erhebenden und dem ISiBe diese Konflikte beheben. Allenfalls kann er aufgrund eigenen Wissens die Vervollständigung oder stärkere Detaillierung von unberücksichtigten Objekten verlangen. Gesamthaft muss er den Ansprechpartnern beider Gruppen eine Rückmeldung über die von ihm akzeptierten Informationen geben, um von diesen wiederum ein Visum für die Richtigkeit dieser Erhebung zu erhalten. Resultat ist ein konsolidiertes Inventar der ausgewählten Objektklassen des gesamten Betrachtungsobjekts des Teilprojekts.

Aktivität 1.90: Abschluss

Am Ende der Planungsphase stellt der ISiKo die Erhebung zusammen und generiert erste Kennzahlen zum Inventar. Er kann die konkretisierten Zielvorgaben und die vorgenommenen Planungen anpassen und dem übergeordneten Management und dem ISiBe eine erste Rückmeldung über den Zustand des Systems liefern.

2: Dialog

In Phase 2 werden die Massnahmen aufgrund der Grundlagen des DG0 sowie der Ergebnisse von Phase 1 ausgewählt. Dies geschieht im Dialog der Betroffenen.

Aktivität 2.10: Sofortmassnahmen

Bevor die eigentliche Massnahmenauswahl angegangen wird, gilt es, die in Aktivität 1.72 identifizierten besonderen Schwachstellen und Risiken zu bewerten und bei dringendem Handlungsbedarf Sofortmassnahmen auszuwählen oder zu formulieren und in Zusammenarbeit mit den Betroffenen sofort umzusetzen. So soll die Entstehung von Schäden mindestens bis zum Zeitpunkt der Umsetzung sorgfältig ausgewählter Massnahmen verzögert werden.

Aktivität 2.20: Entscheidungsspielraum festlegen

Der ISiKo kann aufgrund des ihm vorliegenden Inventars, der erhobenen Schwachstellen und des verfügbaren Budgets Prioritäten für die Umsetzung zusammenstellen und vorschlagen.

Aktivität 2.30: Dialog vorbereiten

Die entscheidungsrelevanten Unterlagen müssen den Ansprechpartnern der jeweils betroffenen Parteien übersichtlich formatiert vorgelegt werden. Irrelevante Informationen müssen ausgefiltert werden.

Aktivität 2.40: Dialog und Entscheidung

Im Dialog geht es vor allem darum, die Entscheidung für die Umsetzungsplanung von Massnahmen vorzubereiten. Jede Massnahme betrifft Info Owner, Verwalter

oder beide und jeweils einen oder mehrere beider Gruppen. Neben den üblicherweise bereichsexternen Verwaltern kann auch die Beteiligung weiterer externer Personen notwendig sein, z.B. bei ausgelagerter Dienstleistungserbringung (Outsourcing). Der Dialog muss so geführt und aufgeteilt werden, dass jeweils nur die von einer Massnahme betroffenen Parteien anwesend sind. Dies bedingt hohen Planungsaufwand beim ISiKo, welcher allerdings zu Zeitersparnissen bei den Beteiligten führt.

Im Dialog werden die Vor- und Nachteile der Umsetzung einzelner Massnahmen aus dem in den Grundlagen in DG0 erarbeiteten Massnahmenkatalog diskutiert. Es kann festgestellt werden, dass einzelne Massnahmen schon umgesetzt wurden, einzelne sich in der Umsetzung befinden, andere schon beschlossen, die Umsetzung geplant, sie aber noch nicht umgesetzt sind und weitere beschlossen, ihre Umsetzung aber noch nicht konkret geplant wurde. Dies ist v.a. nach dem erstmaligen Durchlaufen des DGs wahrscheinlich. Ebenfalls kann festgestellt werden, dass einzelne der schon behandelten Massnahmen aktuell diskutierte Massnahmen ganz oder teilweise ersetzen können.

Die Info Owner und Verwalter sind prinzipiell an Sicherheit interessiert, welche die Flexibilität und Effizienz der unternehmerischen Prozesse nicht beeinträchtigt. Info Owner sind besonders an der Umsetzung von Massnahmen interessiert, von denen sie erhöhte und von ihnen nachgefragte Sicherheit erwarten und sind dann allenfalls auch bereit, einen Teil ihres eigenen Budgets (bzw. desjenigen des übergeordneten Managers) zur Verfügung zu stellen. Für andere Massnahmen muss unter Umständen das Budget derjenigen Stellen bemüht werden, welche den Grundschutzmassnahmenkatalog zusammengestellt haben. Allerdings sollte der Grundschutzmassnahmenkatalog so zusammengestellt werden, dass die Erreichung einer minimalen Sicherheit ohne die Umsetzung jeder einzelnen Massnahme schwierig ist.

Es ist aber auch möglich, dass die Umsetzung einer Massnahme als unangemessen oder unwirksam zurückgewiesen wird. Gegen Ende des Dialogs, der auf mehrere Diskussionstermine verteilt werden kann, wird eine Entscheidung gefällt, für welche Massnahmen die Umsetzung konkret betrachtet werden soll. Einzelne Massnahmen können also übergeordnet an den ISiBe zur Erarbeitung einer übergeordneten Lösung weiterverwiesen werden. Für die Ausarbeitung konkreter Umsetzungspläne müssen Termine festgelegt werden. Die gefällte Entscheidung muss zusammengefasst und den entscheidenden Institutionen nochmals informativ zur Verfügung gestellt werden.

Der ISiKo leitet diesen Dialog. Es entsteht eine Liste der umzusetzenden Massnahmen sowie ein Terminplan für die Ausarbeitung der Umsetzungsplanung.

Aktivität 2.50: Dokumentation

Die Entscheidung und die Entscheidungsfindung muss dokumentiert werden. Aus dieser Dokumentation muss hervorgehen, warum die Umsetzung einzelner Massnahmen aus dem vorgegebenen Massnahmenkatalog nicht geschehen soll,

warum Massnahmen umgesetzt werden sollen, welche nicht im Massnahmenkatalog enthalten sind und welche Budget und Termine für die Umsetzungsplanung festgelegt wurden.

Aktivität 2.90: Abschluss

Der Abschluss der Phase 2 geschieht durch die Zusammenstellung der umgesetzten und umzusetzenden Massnahmen, die Erstellung von Kennzahlen und die Abgabe eines Zwischenberichtes an die beauftragende Stelle und den ISiBe.

3: Realisierungsplanung

In Phase 3 wird die Massnahmenplanung konkretisiert, d.h. für jede der im Dialog diskutierten und beschlossenen Massnahmen wird die Umsetzung der Massnahme im Detail geplant. Dabei werden Termine, Kosten und Beeinflussung des Betrachtungsobjekts berücksichtigt.

Aktivität 3.10: Evaluation der Entscheidung

In Aktivität 3.10 wird die Entscheidung evaluiert, indem grob die Schwierigkeit der Umsetzung und die entstehenden Nebenwirkungen von den jeweils betroffenen Ansprechpartnern begutachtet werden. Dann geschieht eine Priorisierung der Umsetzungsplanung und allenfalls eine Aufteilung und Zuweisung zu einzelnen Personen.

Aktivität 3.50: Realisierungsplanung erstellen

Für jede der beschlossenen Massnahmen wird die Realisierung möglichst konkret geplant, wobei Termine und die konkrete Umsetzung diskutiert und festgelegt werden.

Aktivität 3.90: Abschluss

Der Abschluss der Phase 3 geschieht durch die Zusammenstellung der konkreten Realisierungsplanung, die Erstellung von Kennzahlen und die Abgabe eines Zwischenberichtes an die beauftragende Stelle und den ISiBe.

4: Realisierung

In Phase 4 werden die beschlossenen und konkret geplanten Massnahmen umgesetzt.

Aktivität 4.10: Realisierungsplanung detaillieren

Für die Implementation der Massnahme ist in jedem Fall die Beurteilung der aktuellen Situation am IT-System (technische Massnahme) bzw. in der Organisation (organisatorische Massnahme), in den Institutionen (personelle

Massnahme) und der Infrastruktur (bauliche Massnahme) nochmals zu betrachten. Dies geschieht in der Regel durch einen Fachmann des jeweiligen Bereichs im Auftrag des jeweiligen Ansprechpartners. Es entstehen konkretere Aussagen über die Umsetzung.

Aktivität 4.20: Realisierung durchführen

Die detailliert geplanten Massnahmen können nun umgesetzt werden. Die Dauer und Komplexität dieser Umsetzung variiert stark von der Art und dem konkreten Bezugsobjekt der jeweiligen Massnahme. Die Durchführung der Realisierung kann deshalb einen grossen Anteil an der Gesamtdauer des Projektes haben.

Aktivität 4.50: Realisierung dokumentieren

Die Veränderungen an den betroffenen Systemen und ihre Auswirkungen müssen dokumentiert werden. Dabei entsteht ein Sicherheitshandbuch, welches das Sicherheitskonzept enthält.

Aktivität 4.60: Realisierungsdokumentation publizieren

Die Dokumentation muss allen davon betroffenen Personen zugänglich gemacht werden, indem sie darauf hingewiesen werden und sie ihnen zur Verfügung gestellt wird.

Aktivität 4.70: Schulung

Bei hohem Einfluss auf die Durchführung der unternehmerischen Prozesse müssen die durch die Realisierung entstehenden Veränderungen in die allgemeine Benutzerschulung aufgenommen oder in einer speziellen Sicherheitsschulung den Betroffenen mitgeteilt werden.

Aktivität 4.90: Abschluss

Der Abschluss der Phase 3 geschieht durch die Zusammenstellung der umgesetzten Massnahmen bzw. den Stand der Umsetzung, die Erstellung von Kennzahlen und die Abgabe eines Zwischenberichtes an die beauftragende Stelle und den ISiBe.

5: Kontrolle

Phase 5 umfasst die Kontrolle von DG1 in den Aktivitäten *Review, Respawn, Relaunch, Synchronisation, Report* und *Audit*.

Aktivität 5.10: Review

Der Review umfasst die rückblickende Betrachtung des gesamten Detaillierungsgrades. Es wird begutachtet, ob die in der Zielerreichung festgelegten Ziele im Rahmen der bei der Auslösung vereinbarten Bedingungen erreicht werden konnten, ob die Erhebung, Bewertung und Sofortmassnahmen erfolgreich waren,

wie die Entscheidungsfindung der Massnahmenumsetzung und die konkrete Planung und Realisierung abgelaufen sind. Dies dient einerseits dazu, erneut Kennzahlen über die einzelnen Phasen zu generieren, so den Fortschritt des Teilprojektes zu dokumentieren und einen Vergleich dieses Teilprojektes mit anderen Teilprojekten zu ermöglichen. Darüber hinaus erlaubt es die Zusammenstellung von Inhalten und Zielsetzungen eines allfällig notwendigen erneuten Durchlaufens dieses Detaillierungsgrades. Die gesammelten Informationen können zu einem Bericht über das Teilprojekt zusammengefasst werden.

Aktivität 5.20: Respawn

Im Respawn wird untersucht, inwieweit das Auslösen weiterer Teilprojekte notwendig ist, welche diesem Teilprojekt untergeordnet sind. Dies kann v.a. dann notwendig sein, wenn einzelne Teilbereiche im aktuellen Projekt nicht berücksichtigt wurden. Im Gegensatz dazu führt der Ausschluss einzelner Objektklassen lediglich zu einem Relaunch.

Der Respawn, also die Auslösung untergeordneter Teilprojekte, bedingt ebenfalls einen Relaunch des aktuellen Teilprojektes, um die Unter- / Überordnung zu gewährleisten. Falls jedoch im aktuellen Teilprojekt kein Handlungsbedarf mehr besteht, weil die Ziele erreicht wurden und die Rahmenbedingungen sich nicht verändert haben, kann seine Durchführung sehr schnell und ohne grossen Aufwand geschehen.

Aktivität 5.30: Relaunch

Der Relaunch bedeutet die Neuauslösung desselben Teilprojektes mit veränderten (oder auch gleich gebliebenen) Rahmenbedingungen. Falls die Ziele des aktuellen Teilprojektes erreicht wurden, kann in den übergeordneten Detaillierungsgrad gewechselt werden. Dort werden höhere Anforderungen an die Durchführung gestellt, was jedoch auch zu besser angepasster Sicherheit führt. Da der Aufbau der verschiedenen Detaillierungsgrade sich ähnelt, kann ein Teilprojekt untergeordnete Teilprojekte in anderen Detaillierungsgraden haben.

Aktivität 5.40: Synchronisation

Unter Synchronisation wird die Mitteilung der Ergebnisse an das direkt übergeordnete Teilprojekt und / oder den ISiBe beschrieben. Grundsätzlich muss entschieden werden, wieviele der im Teilprojekt angefallenen Informationen an die übergeordnete Stelle weitergegeben werden.

Für eine Weitergabe spricht, dass sie der übergeordneten Stelle (sei dies ein Teilprojekt oder der ISiBe) eine Koordination des Teilprojektes mit anderen Teilprojekten erlaubt, beispielsweise durch die Konsolidierung der erhobenen Daten oder durch die Vereinbarung von Massnahmen für Objekte, welche von mehreren Teilbereichen der Unternehmung verwendet werden. Darüber hinaus erlaubt es die

detaillierte Analyse der Erhebungen zur selbständigen Generierung von Kennzahlen.

Gegen eine detaillierte Weitergabe spricht, dass die Analyse von Details auf dem übergeordneten Niveau oft nicht wünschenswert erscheint und die Befürchtung besteht, diese Details würden für Kontrollen oder Audits verwendet. Ebenfalls gegen eine detaillierte Weitergabe spricht, dass die Erhebungen selbst vertraulich behandelt werden sollten, da sie potentiellen Angreifern Informationen über Schwachstellen der unternehmerischen Informationsverarbeitung liefern können. Die Möglichkeit der unbeabsichtigten Weitergabe stiegt mit jeder angefertigten Kopie, also auch durch eine detaillierte Synchronisation.

Es wird hier vorgeschlagen, eine Synchronisation nur für diejenigen Objekte detailliert vorzunehmen, welche bereichsübergreifend verwendet werden oder übergeordneten Risiken unterliegen oder durch übergeordnete Massnahmen beeinflusst werden. Die restlichen Erhebungen sollten summarisch (d.h. über die generierten Kennzahlen) synchronisiert werden, so dass die übergeordnete Stelle die Möglichkeit zur Generierung eigener Kennzahlen und für Vergleich bekommt.

Aktivität 5.50: Report

Der Report umfasst die Berichterstattung des ISiKos über das Teilprojekt an die übergeordnete Stelle. Dazu werden die Informationen aus dem Review übergeben, die Synchronisation durchgeführt und interpretierte Aussagen zum Erfolg des Teilprojektes abgegeben. Es werden konkrete Vorschläge für Respawn und Relaunch abgegeben.

Aktivität 5.70: Audit

Der Audit umfasst die Prüfung des Teilprojektes durch verschiedene Institutionen (Rollen).

- Im ISiKo Audit prüft der Koordinator, ob die ihm mitgeteilten Informationen über Umsetzungen, Kosten etc. korrekt sind. Zwar geschieht diese Kontrolle über das Controlling, welches der ISiKo im Laufe der Umsetzung durchführt, jedoch sollte er sich in Stichproben über die Richtigkeit der ihm angegebenen Informationen überzeugen.
- Im Client Audit prüfen die Info Owner, ob die Anforderungen, welche sie an die Informationen stellen (ab DG2), durch die umgesetzten Massnahmen erreicht werden.
- Im Sponsor Audit prüfen die Sponsoren, ob die von ihnen zur Verfügung gestellten Mittel und Unterstützungsleistungen sinnvoll eingesetzt wurden.
- Im Management Audit überprüft das übergeordnete Management, ob die Ziele des Teilprojektes erreicht wurden, und wie die Durchführung der Geschäftsprozesse davon beeinflusst wird.

- Im General Audit werden Dritte über die Auswirkungen des Teilprojektes informiert, beispielsweise weil sie indirekt von den Veränderungen betroffen sind, weil ein allgemeines Interesse besteht oder als Motivation für die Durchführung ähnlicher Teilprojekte in anderen Bereichen der Unternehmung.

Aktivität 5.90: Abschluss

Der Abschluss besteht aus der Terminierung des Teilprojektes und der Übergabe der gesammelten Unterlagen an den ISiKo des übergeordneten Projektes oder den ISiBe, wenn das Projekt nicht sofort mit demselben ISiKo neu gestartet wird (Relaunch).

C.1.4 Angepasste Informationssicherheit (Detaillierungsgrad 2)

Detaillierungsgrad 2 behandelt *angepasste Informationssicherheit*. Dazu werden *Werte* der einzelnen Objekte des Betrachtungsbereiches bestimmt und im Dialog *angemessene* Massnahmen bestimmt und umgesetzt. DG2 folgt damit mehrheitlich dem in Abschnitt 6.2.3 im Zusammenhang beschriebenen Werteansatz. DG2 ist in Abbildung C-3 detailliert dargestellt.

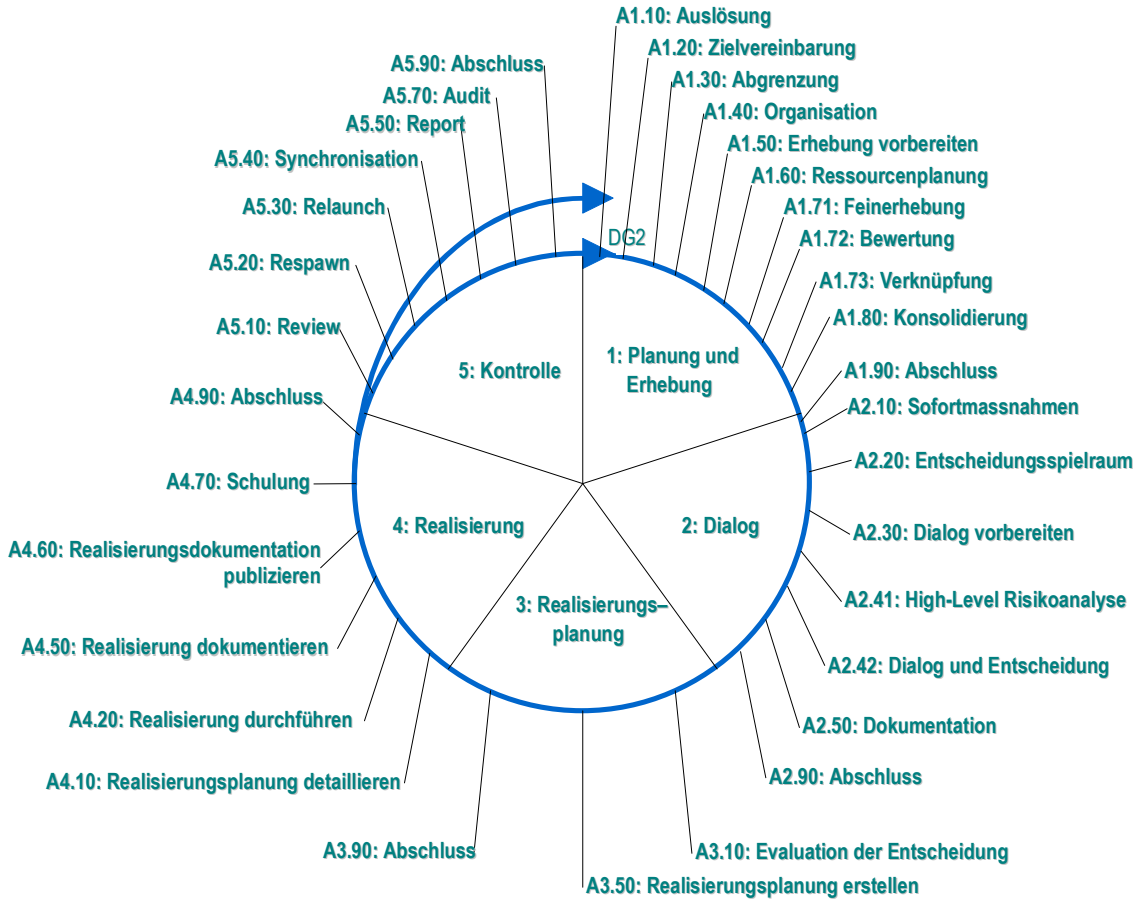


Abbildung C-3: Detaillierungsgrad 2

1: Planung und Erhebung

Aktivität 1.10: Auslösung

Ablauf: Sinngemäss entsprechend Aktivität 1.10 von DG1. Darüber hinaus muss festgelegt werden, ob auch die Ziele des vorherigen DGs erreicht werden müssen. Dies sollte vereinbart werden, denn ohne Grundschutz kann eine umfassende Informationssicherheit nicht gewährleistet werden. Dies führt dazu, dass in jeder Aktivität dieses DGs alle Anforderungen und Inhalte des entsprechenden tieferliegenden DGs berücksichtigt und bei Bedarf nachgeführt werden müssen.

Aktivität 1.20: Zielvereinbarung

Sinngemäss entsprechend Aktivität 1.20 von DG1.

Aktivität 1.30: Abgrenzung

Sinngemäss entsprechend Aktivität 1.30 von DG1. Darüber hinaus können möglicherweise einzelne der in DG0 Aktivität 2.51 festgelegten Bewertungskriterien ausgeschlossen oder zusätzlich aufgenommen werden, falls dies im aktuellen Teilprojekt angebracht erscheint und diese Möglichkeit in Aktivität 1.10 vereinbart wurde. Zusätzlich können einzelne Objektkategorien wieder eingeschlossen werden, welche in der Betrachtung in DG1 nicht berücksichtigt wurden. Mindestens sollten jedoch im DG2 Prozesse, Informationssammlungen und IT-Systeme erhoben werden. Ausserdem sollten mehr Attribute für jedes Objekt festgelegt werden, um auf diese Weise genauere Angaben für die später vorzunehmende Bewertung zu erhalten.

Aktivität 1.40: Organisation

Sinngemäss entsprechend Aktivität 1.40 von DG1.

Aktivität 1.50: Vorbereitung der Erhebung

Sinngemäss entsprechend Aktivität 1.50 von DG1. Es ist aufgrund der grösseren Komplexität der Erhebung empfehlenswert, ein datenbankbasiertes Erhebungswerkzeug einzusetzen, um den Verwaltungsaufwand möglichst tief zu halten. Der Grundschutzmassnahmenkatalog ist zwar auch in diesem DG relevant, auf den Ausschluss einzelner Massnahmen kann aber verzichtet werden, da keine Pflicht zur Umsetzung dieser Massnahmen besteht.

Aktivität 1.60: Ressourcenplanung

Sinngemäss entsprechend Aktivität 1.60 von DG1.

Aktivität 1.71: Feinerhebung

Die Feinerhebung geschieht entsprechend der Groberhebung in Aktivität 1.71 von DG0. Sie berücksichtigt jedoch die zusätzlichen Objektklassen und Attribute, so dass der Umfang des entstehenden Inventars grösser ist. Besonders beachtenswert ist, dass die Verantwortung für jedes erhobene Objekt genau einer Person zugeteilt werden muss, diese Person wird dann als Objektverantwortlicher bezeichnet. Das führt dazu, dass einzelne Objekte nicht eindeutig sind und deshalb nicht sofort einzelnen Personen zugeordnet werden können. Der ISiKo (und im Zweifelsfall der ISiBe) müssen die Zuordnungsprobleme im Einvernehmen mit den betroffenen Personen lösen. Indirekt bedeutet das, dass nicht unbedingt die erhebende Person auch die Verantwortung für das erhobene Objekt trägt. Die Objektverantwortlichen müssen jedoch in jedem Fall über alle Objekte informiert werden, deren

Verantwortung sie tragen sollen, und sich gegenüber dem ISiKo damit einverstanden erklären.

Aktivität 1.72: Bewertung

Über die in Aktivität 1.72 von DG1 durchgeführte Identifikation von Schwachstellen und besonderen Risiken hinaus werden die einzelnen erhobenen Objekte nun von den jeweils Verantwortlichen bewertet. Dies geschieht anhand des Bewertungskriterienkatalogs. Jedes Objekt erhält in jedem Kriterium einen Wert zugeteilt. Dieser Wert bezeichnet im Falle von Informationssammlungen die *Anforderung*, welche die jeweils bewertende Person an die Sicherheit dieser Information stellt. Für die anderen Objekte, welche die Informationsverarbeitung unterstützen, wird mit dem Wert die höchste Anforderung bezeichnet, welche dieses Objekt zu erfüllen vermag. Dies wird als *Sicherheitsleistung* bezeichnet. Über die Bewertung hinaus bietet sich auch die Erfassung von zurückliegenden Sicherheitsvorfällen (Störungen der Informationsverarbeitung) an, um eine breitere Basis für die Bewertung zu schaffen.

Aktivität 1.73: Verknüpfung

Um die angepasste Sicherheit gewährleisten zu können, muss bekannt sein, welche Informationssammlung mit welchen IT-Systemen verarbeitet wird. Diese Verknüpfung muss ebenfalls erhoben und festgehalten werden. Dies kann wahlweise bei der Erhebung der Informationssammlungen geschehen, indem die jeweils verarbeitenden IT-Systeme gekennzeichnet werden oder bei den IT-Systemen, indem die jeweils verarbeiteten Informationssammlungen bezeichnet werden. Die erste Variante ist sinnvoller, da sie eine aus Sicht der Informationen vollständige Erhebung erlaubt. Ebenfalls sollte bei den IT-Systemen jeweils festgehalten werden, von welchen weiteren Systemen sie abhängig sind.

Aktivität 1.80: Konsolidierung

Die Konsolidierung findet sinngemäss zu Aktivität 1.80 von DG1 statt. Zusätzlich muss der ISiKo die Bewertungen konsolidieren, indem er (aus seiner Sicht oder im Vergleich) über- oder untertriebene Bewertungen in Rücksprache mit den Bewertenden korrigiert.

Aktivität 1.90: Abschluss

Sinngemäss entsprechend Aktivität 1.90 von DG1.

2: Dialog

Phase 2 von DG1 entspricht weitgehend Phase 2 von DG1. Im besonderen wird jedoch eine werteabhängige Diskussion über die umzusetzenden Massnahmen geführt.

Aktivität 2.10: Sofortmassnahmen

Sinngemäss entsprechend Aktivität 2.10 von DG1.

Aktivität 2.20: Entscheidungsspielraum festlegen

Sinngemäss entsprechend Aktivität 2.20 von DG1. Basis des Vorschlages sind die Ergebnisse von Phase 1 des DG2.

Aktivität 2.30: Dialog vorbereiten

Sinngemäss entsprechend Aktivität 2.30 von DG1. Darüber hinaus muss bei der Planung des Dialogs die Verknüpfung der Objekte berücksichtigt werden. Dazu wird zunächst in Diskussion mit allen Beteiligten eine Risikoanalyse auf hohem Niveau durchgeführt (vgl. Aktivität 2.41). Daran anschliessend werden Dialoge jeweils mit den Betroffenen einzelner Teilsysteme durchgeführt.

Aktivität 2.41: High-Level-Risikoanalyse

In dieser Risikoanalyse auf hohem Niveau werden aufgrund der Erkenntnisse der Erhebung und Verknüpfung Bereiche mit besonders hohen Risiken erkannt und zusammengestellt. Diese Zusammenstellung beeinflusst einerseits die Prioritäten der in Aktivitäten 2.42, 3.50, 4.10 und 4.20 zur Umsetzung entschiedenen und umgesetzten Massnahmen. Andererseits kann entschieden werden, sofort nach Abschluss des DG2 dasselbe Teilprojekt sofort im DG3 neu zu starten (Relaunch), um für die identifizierten Risiken eine detaillierte Risikoanalyse durchzuführen. Ergebnis ist eine Zusammenstellung besonders hoher Risiken und eine prinzipielle Entscheidung über den Umgang mit ihnen.

Aktivität 2.42: Dialog und Entscheidung

Sinngemäss entsprechend Aktivität 2.40 von DG1. Es ist essentiell, dass bei jeder Diskussion die Info Owner anwesend sind, welche die Anforderungen an die Sicherheit ihrer Informationen stellen, sowie die Verwalter aller IT-Systeme, auf welchen diese Informationen bearbeitet werden, welche diese Anforderungen erfüllen müssen. Durch den Dialog entsteht ein "Sicherheitsmarkt", in welchem die von den Info Ownern nachgefragte Sicherheit mit der Zuweisung von Mitteln bezahlt werden muss, welche mehrheitlich aus dem Budget der Info Owner stammen. Es ist deshalb möglich, dass die Info Owner ihre Anforderungen senken, dass die Verwalter ihre Leistungen unter Forderung von finanziellen Mitteln erhöhen oder dass beide Seiten in Einzelfällen auf die weitere Verarbeitung von Informationen verzichten. Ebenfalls möglich ist eine Gruppierung der Informationssammlungen nach Anforderungen, so dass die Sicherheitsleistung gruppenweise erhöht werden kann. Gesamthaft kann der Diskussionsbedarf der Massnahmen weitaus höher sein als der entsprechende Aufwand in DG1, da die Massnahmen an die individuellen Anforderungen angepasst werden müssen. Der Zeitaufwand wird durch Einsparungen bei der Umsetzung ausgeglichen, denn die

Massnahmen des Grundschutzkatalogs müssen nicht mehr prinzipiell umgesetzt werden.

Aktivität 2.50: Dokumentation

Sinngemäss entsprechend Aktivität 2.50 von DG1. Die Dokumentation muss sich allerdings weniger auf den vorgegebenen Massnahmenkatalog beziehen als auf die Dokumentation der Entscheidungsfindung des Dialogs zwischen den beteiligten Parteien.

Aktivität 2.90: Abschluss

Sinngemäss entsprechend Aktivität 2.90 von DG1.

3: Realisierungsplanung

Phase 3 umfasst die Konkretisierung der Massnahmenplanung durch detaillierte Betrachtung der Umsetzung. Die einzelnen Aktivitäten entsprechen genau denjenigen von DG1.

4: Realisierung

In Phase 4 werden die beschlossenen und konkret geplanten Massnahmen umgesetzt. Die einzelnen Aktivitäten entsprechen genau denjenigen von DG1.

5: Kontrolle

Phase 5 umfasst die Kontrolle von DG2. Die einzelnen Aktivitäten entsprechen genau denjenigen von DG1.

C.1.5 Risikogerechte Informationssicherheit (Detaillierungsgrad 3)

Ziel von DG3 ist die Erreichung risikogerechter Sicherheit. Dazu werden die einzelnen Bedrohungen und Risiken bestimmt, welchen die Objekte unterliegen. Das kann für alle Objekte durchgeführt werden, idealerweise aber nur für diejenigen, die hohen Risiken unterliegen, was in DG2 (Aktivität 2.41) festgestellt werden konnte. DG3 folgt damit mehrheitlich dem in Abschnitt 6.2.3 im Zusammenhang beschriebenen Bedrohungs- und Risikoansatz. DG3 ist in Abbildung C-4 detailliert dargestellt.

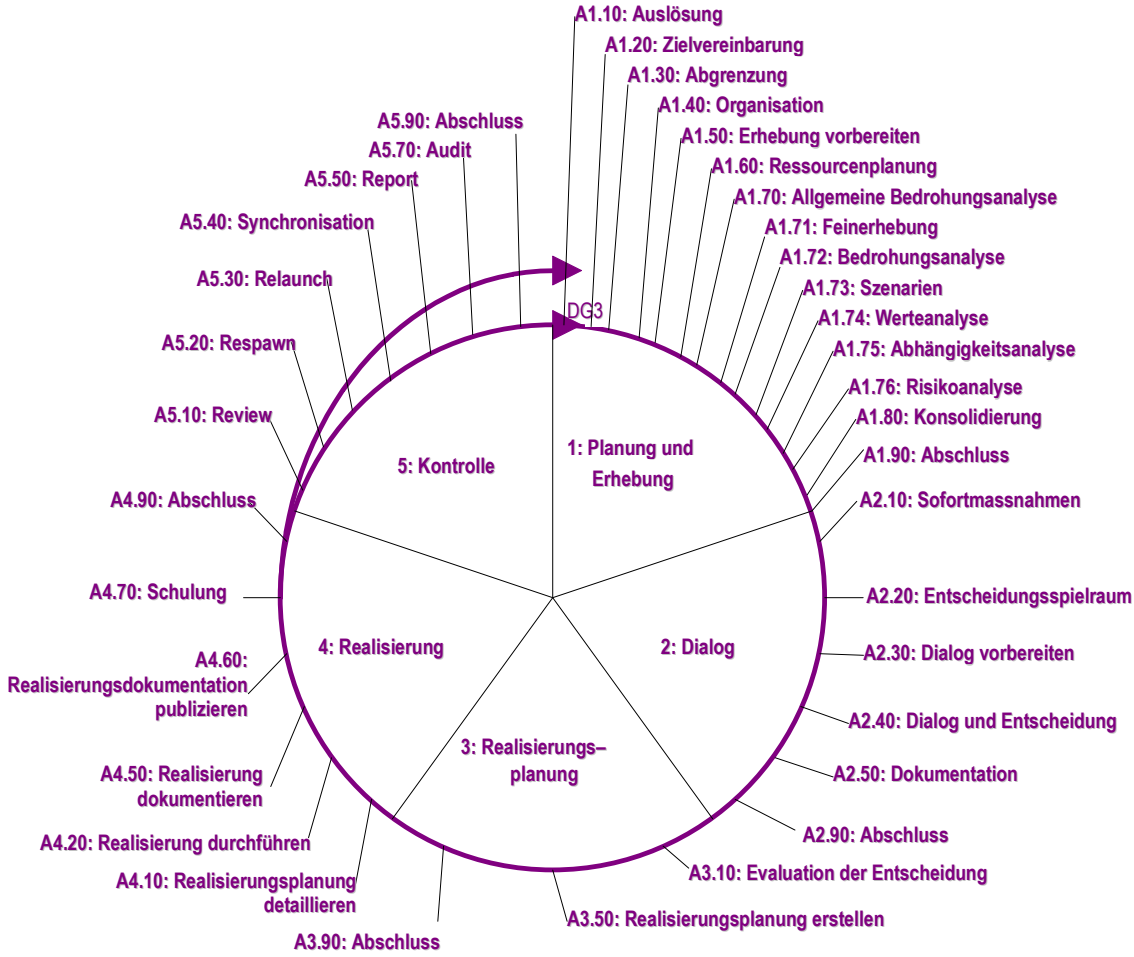


Abbildung C-4: Detaillierungsgrad 3

1: Planung und Erhebung

In Phase 1 wird das Teilprojekt im DG3 initialisiert. Die einzelnen Aktivitäten entsprechen denjenigen von DG2.

Aktivität 1.10: Auslösung

Sinngemäss entsprechend Aktivität 1.10 von DG2.

Aktivität 1.20: Zielvereinbarung

Sinngemäss entsprechend Aktivität 1.20 von DG2.

Aktivität 1.30: Abgrenzung

Sinngemäss entsprechend Aktivität 1.30 von DG2. Der Einschluss weiterer Objektklassen und Attribute ist sinnvoll, um eine genauere Einschätzung der Risiken zu erlauben. Die Einengung der Betrachtung auf einzelne Objekte oder die in DG2 identifizierten besonders hohen Risiken ist sinnvoll, um den Aufwand möglichst gering zu halten.

Aktivität 1.40: Organisation

Sinngemäss entsprechend Aktivität 1.40 von DG2. Bei der Risikoanalyse ist besonders das Wissen unternehmensexterner Berater gefragt, welche ihre eigenen Erfahrungen in ähnlichen Projekten anderer Unternehmungen einfliessen lassen können und auf diese Weise die Bestimmung der Höhe einzelner Risiken zusätzlich abstützen.

Aktivität 1.50: Vorbereitung der Erhebung

Sinngemäss entsprechend Aktivität 1.50 von DG2. Zusätzlich müssen Unterlagen für die Evaluation von Risiken bereitgestellt werden. Diese können aus den dokumentierten Vorfällen innerhalb der Unternehmung entstehen, als Teil eines einzusetzenden Werkzeugs oder von externen Stellen (idealerweise von Versicherungsgesellschaften) bezogen werden. Auch ist die Vorbereitung spezieller Risikoerfassungs- und Bewertungsbögen oder entsprechender computergestützer Hilfsmittel angebracht.

Aktivität 1.60: Ressourcenplanung

Sinngemäss entsprechend Aktivität 1.60 von DG2.

Aktivität 1.70: Allgemeine Bedrohungsanalyse

In dieser Aktivität werden die allgemeinen Bedrohungen in Diskussion mit allen Beteiligten erhoben. Dabei werden beispielsweise Umweltfaktoren, Verhalten von Mitarbeitern, die allgemeine Bedrohungssituation der Unternehmung (geographisches Krisengebiet, Branche mit sozialer Unruhe etc.) berücksichtigt. Die Typisierung in Abschnitt 2.4 kann Anhaltspunkte bieten. Es entsteht eine Beschreibung der Bedrohungen, noch ohne detaillierte Betrachtung, aber mit provisorischer Bewertung. Diese kann in einem Dokument als *Beschreibung der Bedrohungslage* festgehalten werden und kann als Basis für detailliertere Diskussionen verwendet werden.

Aktivität 1.71: Feinerhebung

Sinngemäss entsprechend Aktivität 1.70 von DG2. Die Erfassung derjenigen Objekte, welche mit den zu betrachtenden Risiken und identifizierten allgemeinen Bedrohungen in Zusammenhang stehen, ist besonders zu detaillieren.

Aktivität 1.72: Bedrohungsanalyse

In der Bedrohungsanalyse wird die Erhebung aus Aktivität 1.70 für die erhobenen Objekte konkretisiert. Es wird im Detail betrachtet, welche der einzelnen Objekte von den allgemeinen Bedrohungen betroffen wären. Allenfalls kann es notwendig sein, die Erhebung zu vervollständigen. Es entsteht ein konkreter Bedrohungskatalog.

Aktivität 1.73: Szenarien

Die Bedrohungen werden in dieser Aktivität zur weiteren Betrachtung zu *Szenarien* zusammengestellt. Ein Szenario beschreibt ein Ereignis, durch welches verschiedene der diskutierten Bedrohungen entstehen. Um eine handhabbare Anzahl von Szenarien zu erhalten, sind Verallgemeinerungen der Bedrohungen notwendig. Alternativ können Szenarien auch konkretisiert werden, indem detailliert festgelegt wird, wie das Eintreten eines Szenarios auf die einzelnen Informationssammlungen und Systeme wirken würde. Die Konkretisierung ist jedoch immer beispielhaft, muss sich immer auf konkrete, sich schnell ändernde Objekte beziehen und würde nur zufällig so eintreffen. Deshalb ist eine Verallgemeinerung der Bedrohungen zur Szenarienbildung besser für die Bedrohungsanalyse geeignet. Jedes der Szenarien kann mit einer Eintretenswahrscheinlichkeit bewertet werden. In Einzelfällen können auch den einzelnen Bedrohungen Eintrittswahrscheinlichkeiten zugeordnet werden. Es entstehen Beschreibungen von Szenarien, welche die wichtigsten Bedrohungen abdecken.

Aktivität 1.74: Werteanalyse

In der Werteanalyse wird untersucht, welche Schäden durch das Eintreten von Szenarien oder allenfalls von einzelnen Bedrohungen entstehen würden. Dazu muss die Erhebung der Objekte betrachtet werden. Die Bestimmung des Schadens ersten Grades (vgl. Abschnitt 2.2) kann möglicherweise durch die Betrachtung des Objektwertes geschehen, wenn dieser als Attribut der Erfassung erhoben wurde. Die Bestimmung von G2- und G3-Schäden ist nur durch Diskussion möglich und kann möglicherweise durch die Abhängigkeitsanalyse vervollständigt werden. Ergebnis ist die Zusammenstellung von Schäden und Schadenssummen für die verschiedenen Szenarien.

Aktivität 1.75: Abhängigkeitsanalyse

In der Abhängigkeitsanalyse wird versucht, die Auswirkungen eines Szenarios auf diejenigen Systeme und Bereiche nachzuvollziehen, welche indirekt betroffen sind, weil sie von den bedrohten Objekten abhängig sind. Dies kann der genaueren Bestimmung des G2-Schadens und der Identifikation grosser möglicher Schäden dienen. In Ansätzen kann eine Simulation auf Basis der erfassten Erhebungsdaten Anhaltspunkte für die Abhängigkeiten liefern. Ergebnis ist eine Zusammenstellung möglicher unternehmerischer Schäden.

Aktivität 1.76: Risikoanalyse

In der Risikoanalyse werden die Wahrscheinlichkeiten und Schäden zu Risiken kombiniert. Diese können mit Hilfe einer Matrix dargestellt werden. Ein Sicherheitsziel kann definiert werden und es entstehen Prioritäten für die Senkung der jeweiligen Risiken (vgl. Abschnitt 6.2.3).

Aktivität 1.80: Konsolidierung

Die Konsolidierung umfasst die erneute gesamtheitliche Betrachtung der Risiken, die Evaluation von Verhältnismässigkeit in Bezug auf die gesamte Unternehmung, die Identifikation wichtiger, nicht betrachteter Bedrohungen und die daraus möglicherweise entstehende Anpassung der Ergebnisse. Vergleiche dazu auch Aktivität 1.80 von DG 2.

Aktivität 1.90: Abschluss

Sinngemäss entsprechend Aktivität 1.90 von DG2.

2 Dialog

Phase 2 von DG3 entspricht weitgehend Phase 2 von DG2. Im besonderen wird jedoch anstatt einer werteabhängigen Diskussion eine Diskussion über die risikosenkende Wirkung der umzusetzenden Massnahmen geführt.

Aktivität 2.10: Sofortmassnahmen

Sinngemäss entsprechend Aktivität 2.10 von DG2 mit vordringlicher Berücksichtigung der hohen identifizierten Risiken.

Aktivität 2.20: Entscheidungsspielraum festlegen

Sinngemäss entsprechend Aktivität 2.20 von DG2.

Aktivität 2.30: Dialog vorbereiten

Sinngemäss entsprechend Aktivität 2.30 von DG2. Die Verknüpfung der Objekte muss in Bezug auf die Abhängigkeiten, welche in Aktivität 1.75 identifiziert wurden, besonders betrachtet werden.

Aktivität 2.40: Dialog und Entscheidung

Sinngemäss entsprechend Aktivität 2.42 von DG2. Jede der Massnahmen kann eine oder mehrere der Wirkungen gemäss Sicherheitsdispositiv in Abbildung 6-3 (Seite 182) entfalten (vgl. Abschnitt 6.5).

Aktivität 2.50: Dokumentation

Sinngemäss entsprechend Aktivität 2.50 von DG2.

Aktivität 2.90: Abschluss

Sinngemäss entsprechend Aktivität 2.90 von DG2.

3: Realisierungsplanung

Phase 3 umfasst die Konkretisierung der Massnahmenplanung durch detaillierte Betrachtung der Umsetzung. Die einzelnen Aktivitäten entsprechen denjenigen von DG2.

4: Realisierung

In Phase 4 werden die beschlossenen und konkret geplanten Massnahmen umgesetzt. Die einzelnen Aktivitäten entsprechen denjenigen von DG2.

5: Kontrolle

Phase 5 umfasst die Kontrolle von DG2. Die einzelnen Aktivitäten entsprechen denjenigen von DG2.

C.1.6 Umfassende Informationssicherheit (Detaillierungsgrad 4)

DG4 unterscheidet sich von den anderen DGs, da nicht ein relativ schmales Untersuchungsobjekt tief betrachtet wird, sondern umgekehrt Themengebiete, welche die gesamte Unternehmung betreffen einzeln, aber im Detail betrachtet werden. Dabei werden die meisten der in Kapitel 5 identifizierten Themengebiete behandelt. Die Reihenfolge der Behandlung ist nicht vorgegeben, jedoch wird die hier verwendete Abfolge vorgeschlagen. Unabhängig vom Inhalt folgt auch DG4 einem einheitlichen Ablauf, welcher sich allerdings von den Abläufen der anderen DGs unterscheidet. Da DG4 der letzte DG ist, wird er ständig wiederholt durchlaufen. Es ist allerdings auch vom DG4 aus möglich, mit dem Respawn von Teilprojekten auf verschiedenen DGs die Informationssicherheit mit geringerer Detaillierung ständig zu gewährleisten. Ziel des Detaillierungsgrades 4 ist die Erreichung umfassender (nicht vollständiger)[111] Informationssicherheit.

Der Zyklus selbst ist hier generisch definiert und in Abbildung C-5 dargestellt. Die Themenbereiche sind in Kapitel 5 definiert.

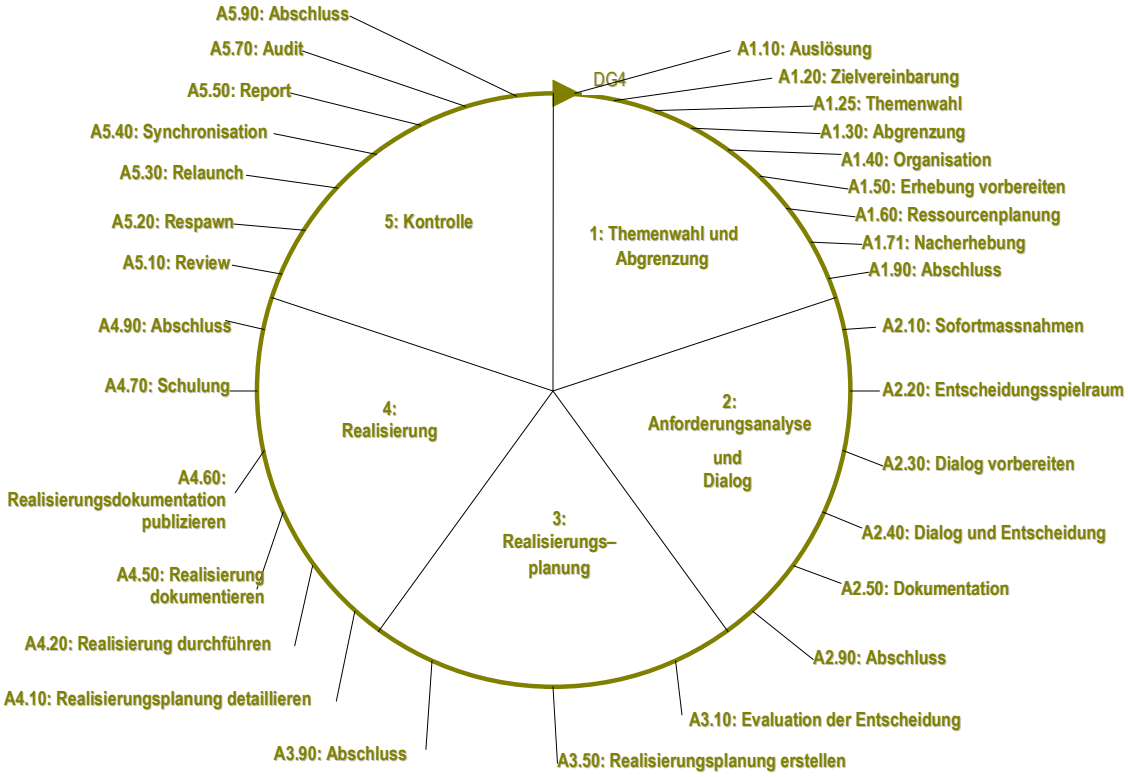


Abbildung C-5: Detaillierungsgrad 4

111 Es wurde in Abschnitt 2.2 argumentiert, dass *vollständige* Informationssicherheit nicht erreicht werden kann. Mit *umfassender* Informationssicherheit ist gemeint, dass alle inhaltlichen Teilgebiete der Informationssicherheit berücksichtigt wurden. Dies kann in der Praxis nie erreicht werden, da aufgrund der technologischen Entwicklung ständig neue Sicherheitsfachgebiete entstehen.

1: Themenwahl und Abgrenzung

In Phase 1 wird das zu betrachtende inhaltliche Themengebiet identifiziert, das Betrachtungsobjekt abgegrenzt und der bestehende Zustand erhoben.

Aktivität 1.10: Auslösung

Sinngemäss entsprechend Aktivität 1.10 von DG3.

Aktivität 1.20: Zielvereinbarung

Sinngemäss entsprechend Aktivität 1.20 von DG3, jedoch mit der Randbedingung, dass DG4 oft in einem sehr hoch angesiedelten Teilprojekt ausgeführt wird oder durch den ISiBe selbst.

Aktivität 1.25: Themenwahl

Die Wahl eines inhaltlichen Themas der Betrachtung geschieht in dieser Aktivität. Dabei ist darauf zu achten, dass das Thema eng genug gewählt wird, um handhabbar und in nützlicher Zeit behandelbar zu sein. Einige Themengebiete werden in Abschnitt 5.4 vorgeschlagen. Diese Liste ist jedoch nicht abschliessend; auch Kombinationen von Themengebieten (d.h. die gleichzeitige Behandlung mehrerer Themen) sind möglich.

Aktivität 1.30: Abgrenzung

Sinngemäss entsprechend Aktivität 1.30 von DG3. Die Abgrenzung erfolgt sehr breit, d.h. das Bezugsobjekt sollte möglichst viele einzelne Objekte enthalten, um eine ganzheitliche Aussage im gewählten Themengebiet für das Objekt formulieren zu können. Dabei wird extensiv auf die vorgenommenen Erhebungen aufgebaut.

Aktivität 1.40: Organisation

Sinngemäss entsprechend Aktivität 1.40 von DG3. Es ist zu beachten, dass hier noch weitere interne und externe Berater hinzugezogen werden sollten, welche sich mit dem betroffenen Fachgebiet besonders auskennen.

Aktivität 1.50: Vorbereitung der Erhebung

Sinngemäss entsprechend Aktivität 1.50 von DG3. Für die Erhebung der speziellen Inhalte sind spezifische, dem jeweiligen Themengebiet angepasste Hilfsmittel zur Verfügung zu stellen.

Aktivität 1.60: Ressourcenplanung

Sinngemäss entsprechend Aktivität 1.60 von DG3.

Aktivität 1.70: Nacherhebung

Sinngemäss entsprechend Aktivität 1.71 von DG3, jedoch besonders der Verfeinerung derjenigen Attribute der Objekte verpflichtet, welche beim gewählten Themengebiet eine besondere Rolle spielen.

Aktivität 1.90: Abschluss

Sinngemäss entsprechend Aktivität 1.90 von DG3.

2: Anforderungsanalyse und Dialog

In Phase 2 werden die Anforderungen an das Bezugsobjekt hinsichtlich des gewählten Themengebiets analysiert und priorisiert. Im Dialog wird festgelegt, welche Anforderungen zu erfüllen sind.

Aktivität 2.10: Sofortmassnahmen

Sinngemäss entsprechend Aktivität 2.10 von DG3 und DG2. Auch in DG4 kann festgestellt werden, dass im gewählten Themenbereich grosse Schwachstellen und Risiken bestehen, denen sofort durch Massnahmen begegnet werden muss.

Aktivität 2.20: Entscheidungsspielraum festlegen

Sinngemäss entsprechend Aktivität 2.20 von DG3.

Aktivität 2.30: Dialog vorbereiten

Sinngemäss entsprechend Aktivität 2.30 von DG3. Bei der Priorisierung spielt weniger die erhobene Verknüpfung der Objekte eine Rolle als die von ISiKo und den Beratern aufgrund ihrer Erfahrung angenommene Verknüpfung.

Aktivität 2.40: Dialog und Entscheidung

Sinngemäss entsprechend Aktivität 2.40 von DG3.

Aktivität 2.50: Dokumentation

Sinngemäss entsprechend Aktivität 2.50 von DG3.

Aktivität 2.90: Abschluss

Sinngemäss entsprechend Aktivität 2.90 von DG3.

3:Realisierungsplanung

In Phase 3 wird konkretisiert, mit welchen Massnahmen die Anforderungen zu erfüllen sind. Die einzelnen Aktivitäten entsprechen genau denjenigen von DG3.

4: Realisierung

In Phase 4 werden die Massnahmen aus Phase 3 umgesetzt. Die einzelnen Aktivitäten entsprechen genau denjenigen von DG3.

5: Kontrolle

In Phase 5 wird die Umsetzung der Massnahmen und die allgemeine Zielerreichung kontrolliert. Phase 5 umfasst die Kontrolle von DG3. Die einzelnen Aktivitäten entsprechen denjenigen von DG3 mit der offensichtlichen Ausnahme, dass ein Wechsel in einen übergeordneten DG hier nicht möglich ist.

C.1.7Krisenmanagement (Detaillierungsgrad 3.5)

Das Krisenmanagement ist ein spezieller Zyklus, welcher nur im Krisenfall (oder allenfalls bei der Simulation einer Krise) durchlaufen wird. Dazu muss dieser Zyklus im Rahmen einer detaillierten Betrachtung in DG4 mit konkreten Inhalten gefüllt und so „für den Ernstfall“ vorbereitet werden. Hier wird die generische Struktur vorgegeben, wobei die einzelnen Phasen Anhaltspunkte für die inhaltliche Planung geben. DG4 unterscheidet sich von den anderen DGs dadurch, dass keine Planungsphase (Phase 1) vorgesehen ist. Die Planung des Krisenmanagements findet als spezielle inhaltliche Betrachtung in DG4 statt (vgl. Inhalte in Abschnitt 5.2). DG3.5 ist in Abbildung C-6 detailliert dargestellt.

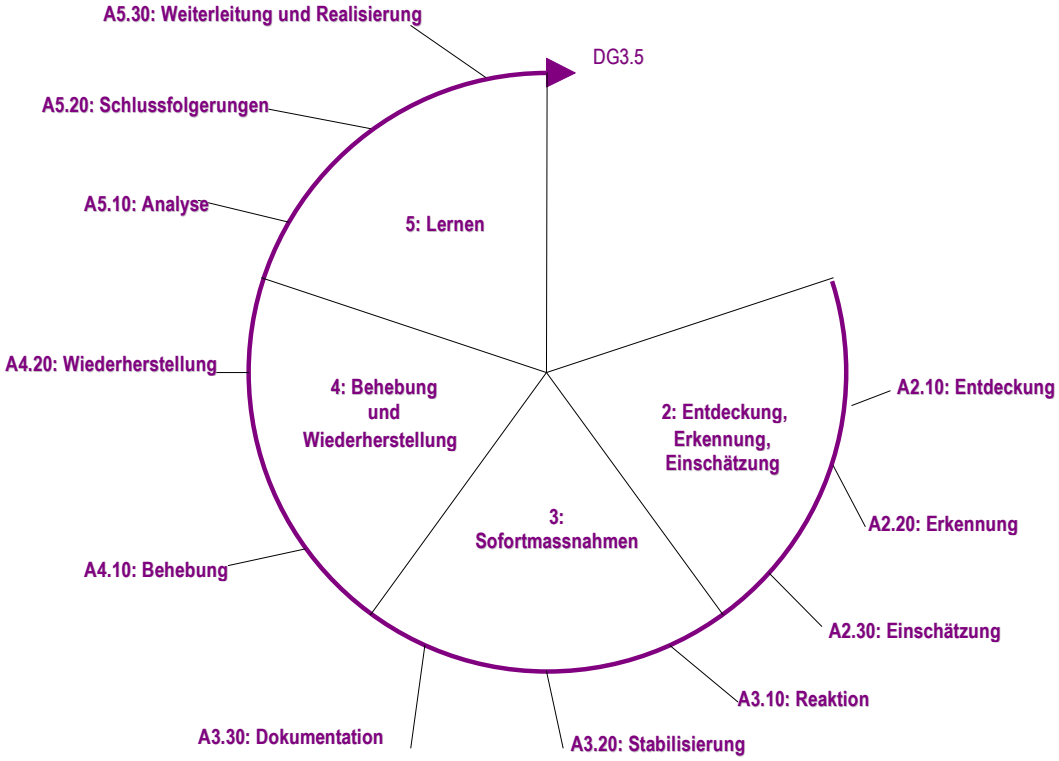


Abbildung C-6: Detaillierungsgrad 3.5

2: Entdeckung, Erkennung, Einschätzung

Sobald eine Störfall eintritt, muss in Phase 2 zunächst entschieden werden, ob dieser zu einer Krise führt.

Aktivität 2.10: Entdeckung

Diese Aktivität umfasst die Entdeckung des Störfalls. Dieser kann an jedem Ort des unternehmerischen Informationssystems entstehen. Seine Entdeckung ist Vorraussetzung für eine Behandlung.

Die Entdeckung kann proaktiv (durch Suchen), reaktiv (durch auftretendes Fehlverhalten), automatisiert (durch Einsatz von überwachenden Hilfsmitteln) oder zufällig geschehen.

Der Störfall muss dokumentiert werden und allen direkt davon betroffenen Institutionen bekannt gemacht werden.

Aktivität 2.20: Erkennung

Ist der Störfall erkannt, muss er sofort behandelt werden, indem die Störung beseitigt wird oder ihre bisherigen und angenommenen zukünftigen Auswirkungen an eine zentrale Störfallmeldestelle (z.B. den ISiBe) weitergeleitet werden. Der ISiBe muss das Potential des Störfalles selbst erkennen.

Aktivität 2.30: Einschätzung

Die Einschätzung umfasst die Bestimmung des bisher eingetretenen Schadens und des noch bestehenden Risikos (also des Schadenpotentials und dessen Wahrscheinlichkeit) durch den ISiBe und / oder durch ihn beauftragte Experten. Die konkrete Lage muss beurteilt werden, indem das Verhalten des Störfalles bzw. des davon betroffenen Systems beobachtet wird.

In Abhängigkeit von der Einschätzung kann wie folgt vorgegangen werden:

- Der Vorfall löst keine Krise aus und hat auch nicht das Potential dazu. Er wird also als normaler Störfall der Behandlung durch die ordentlichen unternehmerischen Prozesse übergeben. Das Krisenmanagement wird abgebrochen.
- Der Vorfall löst noch keine Krise aus, hat jedoch das Potential dazu. Das Krisenmanagement wird fortgesetzt, agiert jedoch nur präventiv.
- Der Vorfall löst eine Krise aus. Das Krisenmanagement wird fortgesetzt, reagiert und agiert und übernimmt dabei Aktivitäten der ordentlichen Geschäftsprozesse.

3: Sofortmassnahmen

In Phase 3 muss versucht werden, die weitere Ausbreitung des Störfalles zu vermeiden, sein Potential also möglichst zu vernichten. Dies geschieht durch Sofortmassnahmen, welche ein ad-hoc einberufenes Team aus Betroffenen, Experten und übergeordnetem Management zur Umsetzung bestimmen kann.

Aktivität 3.10: Reagieren

Es werden Sofortmassnahmen getroffen, um die weitere Ausbreitung des Störfalles zu vermeiden (Begrenzen).

Aktivität 3.20: Stabilisieren

Es werden Sofortmassnahmen getroffen, um das Eintreten direkter und indirekter Folgeschäden zu vermeiden. Dies kann beispielsweise durch Abschottung des betroffenen Teilbereichs oder Teilsystems der Unternehmung geschehen.

Aktivität 3.30: Dokumentation

Das Auftreten des Störfalls sowie der geschehenen Reaktionen und weiteren Aktivitäten müssen aufgezeichnet werden, um späteres Lernen zu ermöglichen.

4: Behebung und Wiederherstellung

Ziel von Phase 4 ist es, den Störfall komplett zu beseitigen und die normalen Arbeitsabläufe wieder herzustellen.

Aktivität 4.10: Behebung

In Diskussion von ISiBe, Verwaltern und betroffenen InfoOwnern und Beratern müssen Massnahmen geplant, zusammengestellt und umgesetzt werden, um den Störfall komplett zu beseitigen und ein störungsfreies Grundsystem wiederherzustellen.

Aktivität 4.20: Wiederherstellung

Danach muss das System soweit wiederhergestellt werden, dass die normalen unternehmerischen Prozesse wie zuvor ablaufen können. Dabei können erheblicher zeitlicher Aufwand und Verzögerungen entstehen.

5: Lernen

In Phase 5 werden Lehren aus dem Auftreten des Störfalls gezogen, um ein erneutes Auftreten zu verhindern und das Auftreten ähnlicher Fälle zu vermeiden.

Aktivität 5.10: Analyse

Es muss betrachtet werden, welche Faktoren zum Auftreten des Störfalles geführt haben und welche Zusammenhänge dabei eine Rolle gespielt haben. Dies kann anhand von Risikobäumen verdeutlicht werden.

Aktivität 5.20: Schlussfolgerungen

Aus der Analyse müssen Schlussfolgerungen formuliert werden, welche als konkrete Massnahmen oder als allgemeine Verhaltensmassregeln formuliert werden können und zur Verhinderung eines erneuten Auftretens des Störfalles eingesetzt werden können.

Aktivität 5.30: Weiterleitung und Realisierung

Die Schlussfolgerungen müssen Konsequenzen auf die Unternehmung haben, indem sie an die ISiKos der laufenden und zukünftigen Teilprojekte weitergeleitet werden und in die in der Unternehmung bestehenden Verhaltensregeln integriert werden.

C.2 Vollständige Beschreibung von ISIWAY 1.5

Auf den nachfolgenden Seiten ist die vollständige Dokumentation zu *ISIWAY 1.5* eingefügt. Diese Dokumentation kann unabhängig von dieser Dissertation verwendet werden. Das Dokument kann beim Autor im HTML-Format bezogen werden.

Management der Informations-sicherheit mit *ISiWay 1.5*

Kurzbeschreibung

ISiWay 1.5 ist ein Verfahren zum Management der Informationssicherheit in Unternehmungen. Es umfasst eine einfache Vorgehensweise und beruht auf dem Dialog zwischen den informationsverarbeitenden Personen innerhalb der Unternehmung. Es stellt dabei die *Inhalte* der Informationsverarbeitung ins Zentrum.

Dieser Text beschreibt *ISiWay 1.5* vollständig. Er ist damit gleichzeitig die Dokumentation des Verfahrens wie auch konkrete Handlungsanleitung für diejenigen Personen, welche *ISiWay 1.5* anwenden möchten.

Dazu wird in einem ersten Teil ein Überblick über das Verfahren und die notwendige Motivation abgegeben. Der zweite Teil beschreibt die einzelnen Aktivitäten und geht auf die Verwendung des Hilfsmittels *ISiGo 1.5* ein. Danach folgen Abschlussbemerkungen und Beispiele.

Inhalt

- 1 *ISiWay 1.5* im Überblick
  - 1.1 Information und Informatik
  - 1.2 Phasen, Ablauf und Durchführung
  - 1.3 Aufwand und Dauer
  - 1.4 Rollen
  - 1.5 *ISiWay 1.5* und weitere ISiWay-Verfahren
  - 1.6 Werkzeug *ISiGo 1.5*
- 2 ISiWay 1.5 im Detail
  - 2.1 Erhebung
    - A1.1 Auslösung / Projektform
    - A1.2 Vorbereitung
    - A1.3 Erhebung Inhalte
    - A1.4 Erhebung Systeme
    - A1.5 Abschluss
  - 2.2 Bewertung
    - A2.1 Bewertungskriterienkatalog
    - A2.2 Bewertung Inhalte
    - A2.3 Bewertung Systeme (optional)
    - A2.4 Abschluss
  - 2.3 Dialog
    - A3.1 Filterung (optional)
    - A3.2 Vorbereitung
    - A3.3 Durchführung
    - A3.4 Abschluss
  - 2.4 Realisierungsplanung
    - A4.1 Erarbeitung konkreter Lösungen
    - A4.2 Beschluss
    - A4.3 Abschluss
  - 2.5 Massnahmenumsetzung
    - A5.1 Massnahmenumsetzung
    - A5.2 Abschluss
  - 2.6 Kontrolle
    - A6.1 Client Audit
    - A6.2 Sponsor Audit (optional)
    - A6.3 Coordinator Audit
    - A6.4 General Audit
    - A6.5 Management Audit
    - A6.6 Internal Audit
  - 2.7 Abschlussbemerkungen
- 3 Anhang / Beispiele
  - zu 1.1: Schriftlicher Projektauftrag
  - zu 1.2: Projektbeschreibung
  - zu 2.2: Bewertungskriterienkatalog

1 *ISiWay 1.5* im Überblick

ISiWay 1.5 umfasst ein einfaches Verfahren zum Management der Informationssicherheit in Unternehmungen. Ziel dieses Managements ist es, den Zustand der Informationssicherheit in der Unternehmung zu erheben und durch gemeinsame Arbeit mit *allen* Beteiligten *langfristig* zu verbessern.

1.1 Information und Informatik

Im Zentrum der Betrachtung steht die unternehmerische Ressource Information, die es zu schützen gilt. Der Begriff *Information* bezeichnet dabei nicht nur dasjenige Wissen, welches mit Informationstechnik (Informatik) verarbeitet wird, sondern umfasst das *gesamte* unternehmerische Wissen, unabhängig von Aufzeichnungs- und Kommunikationsmedien. Schliesslich ist es aus unternehmerischer Sicht irrelevant, ob Informationen durch Eindringen in Computernetze, durch Kopieren von Papierdokumenten oder durch Ablauschen eines vertraulichen Gesprächs ungewollt verbreitet werden. Ebenso ist es unwichtig, ob Informationen durch Ausfall einer Festplatte oder durch Wassereinbruch in einem Papierarchiv verloren gehen. Technik (nicht nur Informationstechnik) wird hier als wichtiges und unabdingbares Mittel zum Zweck betrachtet, steht aber nicht im Zentrum. Deshalb wird hier auch konsequent von *Informationssicherheit* und nicht von *Informatik-Sicherheit* gesprochen.

1.2 Phasen, Ablauf und Durchführung

Zur Erreichung des eingangs genannten Ziels wird hier ein Vorgehen mit den sechs Phasen *Erhebung*, *Bewertung*, *Dialog*, *Realisierungsplanung*, *Massnahmenumsetzung* und *Kontrolle* gemäss Abbildung 1-1 vorgeschlagen. Für jede Phase werden verschiedene Aktivitäten vorgeschlagen, welche in Kapitel 2 genauer beschrieben werden. Unter anderem wird für jede Aktivität definiert, welches *Teilziel* damit verfolgt wird, *wer* sie ausführen soll und welche *Ergebnisse* erarbeitet werden.

ISiWay beginnt in der ersten Phase mit der Zusammenstellung der schützenswerten Informationen und der bestehenden Infrastruktur. In der zweiten Phase werden die Anforderungen an diese schützenswerten Informationen gesammelt. In der dritten Phase wird geprüft, ob die bestehende Infrastruktur diese Anforderungen erfüllen kann. Kann sie es, sind keine weiteren Tätigkeiten notwendig. Falls sie es nicht kann, müssen Massnahmen geplant und beschlossen werden, um diese Anforderungen zu erfüllen. Dies geschieht in der vierten Phase. Die Massnahmen können einerseits Veränderungen der Infrastruktur bedingen, andererseits aber auch Anpassungen der Anforderungen zur Folge haben. Da diese Anpassungen Zeit und Geld erfordern, müssen alle beteiligten Parteien mit einbezogen werden. Sind die Anpassungen beschlossen, müssen sie in der fünften Phase umgesetzt werden. Schliesslich erfolgt in der sechsten Phase die Kontrolle durch Berichterstattung über die Erfüllung der Anforderungen an diejenigen Parteien, welche die Ressourcen zur Verfügung gestellt haben.

Diese Betrachtungen sind natürlich nicht einmalig, sondern müssen in regelmässigen Abständen wiederholt werden, da sich Abläufe, Informationen und Anforderungen in den Fachabteilungen ändern und die Infrastruktur sich verändert. Die Phasen sind daher zyklisch angeordnet, um die Notwendigkeit kontinuierlicher Betrachtung zu betonen.

Abbildung 1-1: ISiWay 1.5

1.3 Aufwand und Dauer

Um den Aufwand für die Betrachtung der Informationssicherheit in "vernünftigem" Rahmen zu halten, verfolgt ISiWay folgende Konzepte:

- ISiWay verlangt keine vollständige oder umfassende Erhebung aller vorhandenen Objekte. Im Gegenteil soll ISiWay genau dort punktuell eingesetzt werden, wo konkret Bedarf und Willen zur Detaillierung besteht. Diese einzelnen punktuellen Anstrengungen lassen sich durch die immer gleiche Verwendung von ISiWay in verschiedenen Bereichen später zu einem Ganzen integrieren.
- ISiWay erlaubt es, auf den vorhandenen Unterlagen über dokumentierte Prozesse (z.B. bei Qualitätsprojekten) oder Unterlagen über Informationssysteme aufzubauen und sie um sicherheitsrelevante Elemente zu ergänzen.
- ISiWay bietet durch die Benutzung von *ISiGo 1.5* als Hilfsmittel eine Unterstützung bei der Verwaltung und Kommunikation an und hilft so, den Aufwand zu senken.
- ISiWay beschränkt den Aufwand auf das von den jeweiligen Betroffenen gewünschte Mass und wird durch das Feedback der Betroffenen angetrieben. Es werden also weder unangemessene Massnahmen vorgeschlagen noch "Papiertiger" erstellt.
- Für allgemeine Fragestellungen wird die Schaffung einer übergeordneten, nicht weisungsbefugten Stelle vorgeschlagen, welche sich mit übergreifenden Thematiken

beschäftigen kann, generische Lösungen vorbereitet und zur Verfügung stellt und, wo notwendig, auf übergeordneter Stufe koordiniert.

Da der Aufwand einer konkreten Durchführung von ISiWay von verschiedenen Voraussetzungen abhängt, die stark von der individuellen Unternehmung abhängen, wird hier nur vorgeschlagen, den Projektleiterposten mit einem genügenden Zeitbudget für die Durchführung von ISiWay auszustatten, so dass der gesamte Zyklus innerhalb eines Jahres einmal durchlaufen werden kann. Der Projektleiter ist jedoch nur ein Koordinator, der die entstehenden Arbeiten verteilt und die Ergebnisse integriert. Er hat also Controller-Funktion.

Der Aufwand für den Koordinator liegt in der Steuerung der gemeinsamen Problemlösung. Dieser Aufwand fällt vor allem in den ersten drei Phasen an, während der - absolut gesehen - grössere Aufwand durch die Ansprechpartner der Fachbereiche und der Informationssysteme getragen werden muss.

1.4 Rollen

Über die Unternehmung, in welcher ISiWay angewendet werden soll, werden nur minimale Annahmen getroffen. ISiWay baut auf der Kooperation der verschiedenen Fachbereiche auf, welche an der Informationsverarbeitung beteiligt sind. Dabei lassen sich in jeder Unternehmung grob zwei Parteien unterscheiden: die *Informatikabteilung* als Verwalterin der weitaus meisten technischen Informationssysteme und die *Fachabteilungen*, welche diese Informationssysteme für ihre inhaltliche Informationsverarbeitung nutzen.

In vielen Unternehmungen beauftragt die Geschäftsleitung die Informatikabteilung, Informatik-Sicherheit zu betrachten und zu erreichen, also ein sicheres technisches Informationssystem aufzubauen bzw. das bestehende System zu sichern. Es ist für die Informatikabteilung jedoch *unmöglich*, Informationssicherheit in *eigener* Regie zu erreichen, da oft nicht formuliert wird, was unter Sicherheit zu verstehen ist und wie die Sicherheitsanforderungen sich genau zusammensetzen. Schliesslich betreibt die Informatikabteilung ihre Systeme nicht für sich selbst, sondern für die Fachabteilungen. Rein technische Betrachtungen können dazu führen, dass aus technischer Sicht sinnvolle Einschränkungen vorgenommen werden -- z.B. Verhinderung oder Einschränkung eines direkten Internet-Zugangs, Beschränkung von Zugriffszeiten etc. -- welche in den Fachabteilungen auf Unverständnis stossen und nicht akzeptiert werden. Ebenso ist es möglich, dass inhaltlich notwendige Sicherungen nicht geschehen -- z.B. der spezielle Schutz von Personaldaten -- weil die Informatikabteilung diese Notwendigkeit nicht selbständig erkennt. Es ist also wichtig, dass der Wunsch zur Untersuchung der Informationssicherheit von den Fachabteilungen ausgeht.

Es ist in jedem Fall unumgänglich, dass Fachabteilungen und Informatikabteilung miteinander reden und ihre Anforderungen und Möglichkeiten austauschen. Dazu bestimmen sie jeweils *Ansprechpartner*. Es ist prinzipiell offen, ob die Fachabteilungen gesamthaft *einen* Ansprechpartner bestimmen, der dann seinerseits die Aufteilung der entstehenden Arbeiten innerhalb der Fachabteilungen organisiert, oder ob *jede* Abteilung einen eigenen Ansprechpartner ernennt. Dasselbe gilt für die Betreiber der Informationssysteme.

Damit die notwendigen Gespräche nicht an unterschiedlichem Verständnis scheitern -- schliesslich sind die Fachabteilungen nicht an technischen Details interessiert und die Informatiker oft nicht an der geschäftlichen Bedeutung der Informationen -- ist es Aufgabe des *Koordinators,* den Dialog vorzubereiten und zwischen beiden Parteien zu vermitteln. Es ist vorteilhaft, wenn dieser Koordinator sowohl die geschäftlichen Tätigkeiten beurteilen kann

wie auch grundlegendes Wissen im Informatikbereich mitbringt. Dies hilft ihm, von allen Ansprechpartnern als kompetenter Gesprächspartner akzeptiert zu werden. Im Zweifelsfalle sollte der Koordinator näher bei den Fachbereichen als bei der Informatik stehen. Es ist auch möglich, dass der Koordinator einer der Ansprechpartner der Fachbereiche ist (Personalunion). Von einer Personalunion von Koordinator und Verwalter wird jedoch dringend abgeraten, da dann ein technikzentrierter Blickwinkel entstehen kann, der vermieden werden sollte.

Der Koordinator ist dafür *verantwortlich*, dass das Verfahren *durchgeführt* wird und die einzelnen Aktivitäten stattfinden. Es ist jedoch *nicht für das Resultat* des Verfahrens verantwortlich.

Um das Projekt zum Erfolg zu führen, ist es ausserdem sinnvoll, *Sponsoren* zu finden. Dies sind Personen, welche ein besonderes Interesse an den Zielen der Informationssicherheit in der Unternehmung haben, beispielsweise ein unternehmerischer Datenschutzbeauftragter, ein IT-Sicherheitsverantwortlicher, oder Personen mit Qualitätsmanagement-Aufgaben. Die Unterstützung dieser Personen kann auch deshalb sinnvoll sein, weil sie über Hintergrund-Informationen über die Unternehmung verfügen. Sponsoren sind jedoch am Projektablauf nicht direkt beteiligt, es sei denn, dass sie zusätzlich noch eine der anderen Rollen einnehmen.

In Einzelfällen ist es darüber hinaus sinnvoll, weitere, unabhängige Ansprechpartner zur Verfügung zu haben, welche Stellungnahmen zu einzelnen Sicherheitsfragen abgeben können, unabhängig beobachten können und den Koordinator bei der Vorbereitung der Berichterstattung an die Geschäftsleitung unterstützen (*unabhängige Berater)*.

Im nachstehenden Text werden deshalb folgende Rollenbezeichnungen verwendet:

- Der oder die *Ansprechpartner der Fachbereiche* vertreten die Fachbereiche der Unternehmung, welche die Informationen *inhaltlich* verarbeiten und für welche die Technik lediglich ein Mittel zum Zweck darstellt.
- Der oder die Ansprechpartner derjenigen Abteilungen, welche die technischen Systeme betreiben, werden als *Verwalter* bezeichnet, weil sie die mit diesen Systemen bearbeiteten und darin gespeicherten Informationen treuhänderisch verwalten. Im Vordergrund stehen die Informatiksysteme, aber es sind alle informationsspeichernden und -verarbeitenden Medien zu betrachten, also auch Telefon, Fax, Briefpost, Ablagesysteme, Papierarchive, Schreibmaschinen, Diktiergeräte etc., letztendlich aber auch Bleistift und Papier, die oft auch für vertrauliche Notizen verwendet werden. Die Prioritäten dieser Betrachtungen werden von den Fachbereichen festgelegt. Alle diese Medien und Werkzeuge sollen hier gesamthaft als Informationstechnische Systeme (IT-Systeme) bezeichnet werden.
- Der *Koordinator* leitet die Durchführung des Verfahrens, indem er den Dialog der Ansprechpartner der Fachbereiche mit den Verwaltern fördert.
- Das *übergeordnete Management* wacht über die Mittelverwendung innerhalb der Unternehmung und fordert deshalb Berichterstattung über Zustand und Fortschritt der Informationssicherheit.
- Die *Sponsoren* sind an der Zielerreichung des Projekts interessierte Personen und unterstützen das Projekt, ohne direkt involviert zu sein.
- Die *Unabhängigen Berater* stehen für übergreifende Fragestellungen zur Verfügung und können ihrerseits koordinierende Funktionen auf übergeordneter Ebene wahrnehmen.

Diese Rollen sind in Abbildung 1-2 dargestellt.

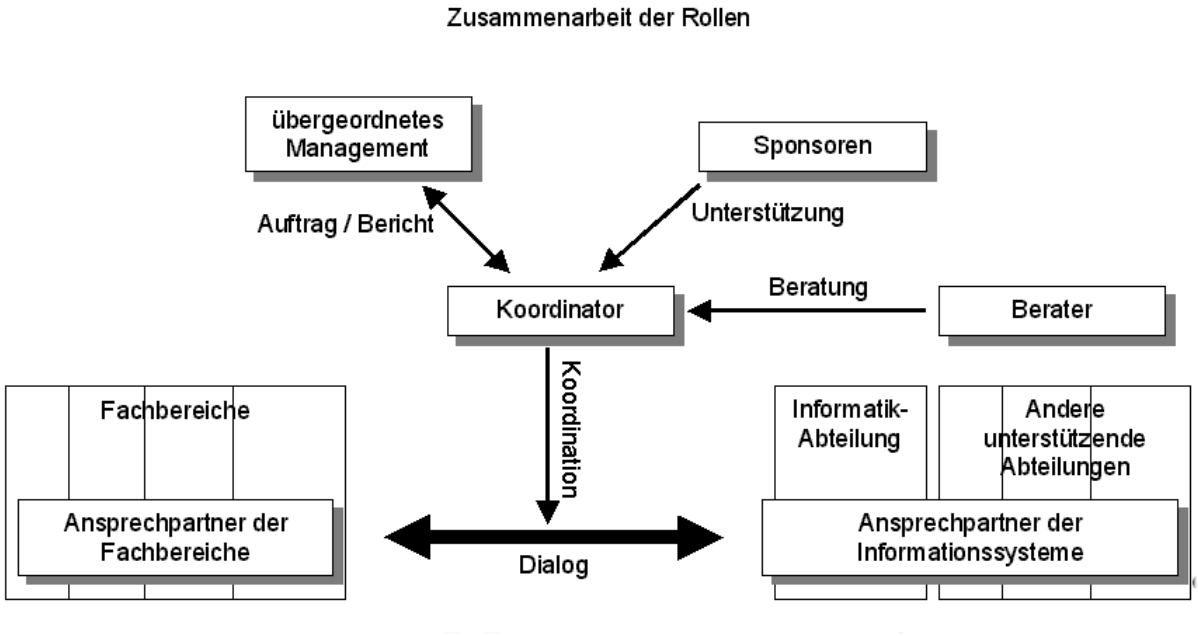


Abbildung 1-2: Zusammenarbeit der Rollen

1.5 *ISiWay 1.5* und weitere ISiWay-Verfahren

ISiWay 1.5 ist ein Teilverfahren aus dem ISiWay-Zyklus, welcher spiralförmig aufgebaut ist und vier verschiedene Detaillierungsgrade enthält (ISiWay 1 bis 4). Das hier beschriebene Verfahren *ISiWay 1.5* integriert Elemente aus den Detaillierungsgraden 1 und 2 des vollen Zyklus und ist dementsprechend eine Mischung aus Grundschutz- und Bewertungsansatz.

Ein Wechsel zu anderen ISiWay-Detaillierungsgraden ist jeweils zum Abschluss eines Zyklus möglich. Die vollständige Dokumentation von ISiWay ist beim Autor erhältlich.

1.6 Werkzeug *ISiGo 1.5*

ISiGo 1.5 ist ein einfaches Werkzeug zur Durchführung von ISiWay 1.5. Es besteht aus einer *Excel*-Datei mit Kurzanleitung, welche die Abfolge und die Inhalte der einzelnen ISiWay-Aktivitäten enthalten und Tabellen, welche mit den Ergebnissen der einzelnen Projektphasen und Aktivitäten gefüllt werden. Es wurden möglichst viele Voraussetzungen einer effizienten Durchführung schon vorbereitet, z.B. Formatierung für den Ausdruck und die Auswertung von Daten (Anzahl, Summen, etc.).

In der dieser Dokumentation beiliegenden Version von *ISiGo 1.5* sind Beipieldaten enthalten, welche durch die im Projekt erhobenen Daten ersetzt werden sollten. Falls Sie *ISiGo 1.5* in einer für Sie angepassten Version erhalten haben, sind möglicherweise schon Projektdaten vorerfasst.

Die in *ISiGo 1.5* erfassten Informationen sind alle als strikte Tabellen aufgebaut. Das ist Voraussetzung für die automatische Erzeugung von Summen, Durchschnittswerten etc. Die Tabellenstruktur sollte deshalb nicht verändert werden und ist weiss auf schwarz gefärbt.

Falls in einzelnen Ausdrucken zu viele Informationen enthalten sind, empfiehlt es sich, den Druckbereich manuell anders zu setzen (`Datei | Seite einrichten...`). Nach dem erneuten Formatieren umfasst der Druckbereich wieder die gesamte Tabelle.

2 *ISiWay 1.5* im Detail

In diesem Abschnitt werden die Phasen von *ISiWay 1.5* und die einzelnen darin durchzuführenden Tätigkeiten genauer beschrieben. In Abbildung 2-1 sind die Aktivitäten den Phasen zugeordnet.

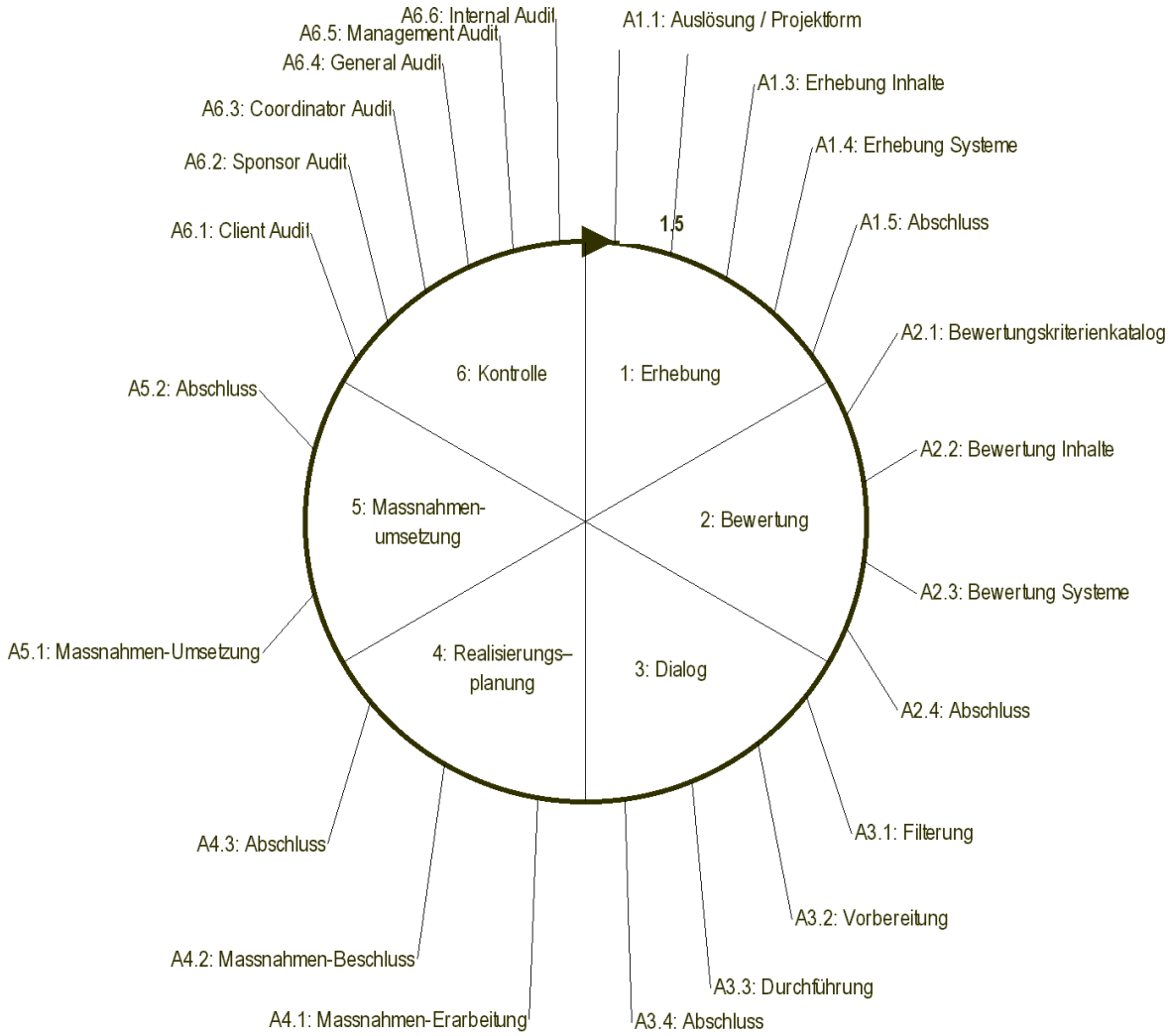


Abbildung 2-1: Phasen von *ISiWay 1.5* mit Aktivitäten

2.1 Erhebung

In der ersten Phase werden die notwendigen Vorbereitungen für das Projekt getroffen und dann die schützenswerten Objekte erhoben, um einen Überblick über Anzahl, Verteilung und Verknüpfung der Objekte untereinander zu erhalten.

A1.1 Auslösung / Projektform

Ziel dieser Aktivität:	*Beginn der Betrachtung der Informationssicherheit auslösen und notwendige Rahmenbedingungen schaffen*

Auslösung

Es bestehen verschiedene Möglichkeiten, wie die Betrachtung der Informationssicherheit ausgelöst werden kann: Eine (neue oder bestehende) verbindliche Richtlinie der Unternehmungsleitung fordert die Betrachtung der Informationssicherheit, oder ein mündlicher oder schriftlicher Auftrag der Geschäftsleitung fordert sichere Informatik, oder die Eigeninitiative des Informatik-Leiters führt zur Initiierung eines Sicherheitsprojekts, oder eine Anfrage aus den Fachbereichen führt zur genaueren Betrachtung der Sicherheit der Informationsverarbeitung eines Bereichs. Weitere Fälle sind möglich.

Die Art der Auslösung beeinflusst Betrachtungsbreite und -tiefe. Die Betrachtungs*breite* bestimmt, welche Objekte in die Untersuchung mit einzubeziehen sind und wird in Aktivität 1.2 genauer bestimmt. Es wurde schon erklärt, warum in jedem Fall eine Ausdehnung der Betrachtungs*tiefe* von der *Informatik* auf die gesamte *Information* angestrebt werden sollte. Nachfolgend wird die Argumentation erläutert, welche zu dieser Beauftragung führen kann.

Projektform

Es wird hier vorgeschlagen, die Betrachtung der Informationssicherheit als Projekt zu organisieren. Es ist sofort zu klären, wer Projektleiter ist (dies ergibt sich direkt oder indirekt aus dem Auslöser) und welcher Bereich zu betrachten ist (Abgrenzung). Der Projektleiter nimmt dabei die Rolle des *Koordinators* ein.

Zum Projektteam gehört immer *mindestens ein Ansprechpartner* der betroffenen Fachabteilungen. Dies sind idealerweise die jeweiligen Leiter, denn sie haben den besten Überblick über die in ihrem Bereich verarbeiteten Informationen. Ausserdem gehört mindestens ein Verwalter (also *ein Ansprechpartner der IT-System-Betreiber*) zum Projektteam. Der Koordinator kann selbst einer der Ansprechpartner der Fachabteilungen sein. Wenn allerdings Konflikte zu erwarten sind -- beispielsweise aufgrund vergangener Erfahrungen -- ist es sinnvoll, einen Koordinator zu wählen, der nicht zugleich Ansprechpartner ist. So kann die Unabhängigkeit des Projektleiters gewährleistet werden.

Die im Projekt anfallenden Arbeiten werden durch die beiden Ansprechpartner selbst durchgeführt oder weiterdelegiert, der Koordinator hat nur steuernde und kontrollierende Funktion. Dies bedingt ein vorheriges Einverständnis der Abteilungen, die notwendigen Aufwände für die einzelnen Phasen zu tragen und in dieser Konstellation mitzuarbeiten. Die Ansprechpartner und ihre jeweiligen Abteilungen werden dadurch gleichzeitig zu Sponsoren des Projekts. Dies ist eine der Voraussetzungen zum Gelingen eines Informationssicherheitsprojekts. Es ist ohnehin unmöglich für den Koordinator oder die Ansprechpartner, die Aufgaben des jeweils anderen Ansprechpartners durchzuführen, weil die dazu notwendigen Kenntnisse i.d.R. nicht vorhanden sind.

Insbesondere wenn der Auslöser innerhalb der Informatikabteilung liegt, ist es schwierig, die Einwilligung der betroffenen Fachabteilungen über das Tragen der Aufwände zu erhalten. In diesem Fall hilft dem Projektleiter eine objektive Analyse der Sicherheitssituation, welche er in Zusammenarbeit mit dem Informatik-Leiter erstellt. Sie muss Aussagen über die bisherigen Sicherheitsanstrengungen, die angenommenen Sicherheitsanforderungen und die wichtigsten bestehenden Bedrohungen enthalten, muss eine Empfehlung für ein Projekt enthalten und mit der Frage enden, ob mehr Sicherheit gefordert wird. Dieser Bericht wird den Fachabteilungen zur Begutachtung vorlegt. Aus den Reaktionen lässt sich entweder ein Auftrag zur genaueren Betrachtung der Informationssicherheit herleiten (die Auftraggeber sind dann zugleich Sponsoren des Projekts) oder die Bestätigung ableiten, dass der Sicherheit genüge getan ist.

Der Auftrag zur Betrachtung der Informationssicherheit sollte schriftlich festgehalten werden und die Unterschriften der Initianten und Sponsoren tragen. Die anderen Betroffenen müssen zumindest mündlich informiert werden, idealerweise an der Erstellung des Projektauftrags beteiligt werden. Ausserdem ist es anzustreben, den Projektteilnehmern den Start des Projekts durch einen "Kick-Off" anzuzeigen.

Es sei hier nochmals betont, dass nur die Fachabteilungen die Anforderungen an die Sicherheit ihrer eigenen Informationen beurteilen können und ihre Mitarbeit deshalb unabdingbar für ein erfolgreiches Sicherheitsprojekt ist.

Ergebnisse: Allgemeine Projektangaben	• *Schriftlicher Projektauftrag zur Betrachtung der Informationssicherheit mit Benennung des Projekts (optional)* • *Zusagen der Betroffenen über das Tragen der notwendigen Aufwände* • *Projektteam aus mindestens zwei, besser drei Personen mit dem Koordinator als Leiter*
Akteure:	*Koordinator, z.T. Projektteam-Mitglieder, evtl. Informatik-Leiter*

ISiGo 1.5

Aufgaben:	*Halten Sie den Projektauftrag schriftlich fest (Beispiel im Anhang der Beschreibung). Füllen Sie in Tabelle "Allgemeine Projektangaben" die Felder mit Aktivität A1.1 aus. Tragen Sie die Adressen der Teilnehmer in die Tabelle "Adressen" ein.*

In dieser und den folgenden Aktivitäten wird gleichzeitig auch die Verwendung von *ISiGo 1.5* beschrieben. Gehen Sie wie folgt vor:

- Starten Sie *ISiGo 1.5* durch Doppelklick auf das entsprechende Icon. Microsoft Excel (ab Version 5) wird aufgestartet.
- Falls Sie nicht oben den Titel "Willkommen zu *ISiGo 1.5*" sehen, wechseln Sie auf das Arbeitsblatt "Willkommen".
- Folgen Sie den Anweisungen, um das *ISiGo 1.5*-Menu zu erstellen, falls es noch nicht existiert.
- Wählen Sie `ISiGo 1.5 | ISiWay | Aktuellen Zyklus neu zeichnen`, um eine Darstellung des Verfahrens zu erhalten. Anmerkung: Durch diesen Befehl wird die Darstellung neu gezeichnet und an Ihre Bildschirmeinstellungen angepasst. Später können Sie einfach zur Darstellung wechseln, indem sie das entsprechende Arbeitsblatt wählen oder indem Sie `ISiGo 1.5 | ISiWay | Zeigen` wählen.
- *ISiGo 1.5* startet bei der ersten Benutzung immer mit der ersten Aktivität (A1.1). Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Aufgabe`, um eine Beschreibung der aktuellen Aufgabe zu erhalten.
- Halten Sie den Projektauftrag schriftlich fest. Verwenden Sie das Beispiel im Anhang als Vorlage, um mit Ihrer Textverarbeitung eine Version für Ihr Projekt zu erstellen. Füllen Sie den Dateinamen dieser Textdatei in die entsprechende Zeile in Tabelle "Allgemeine Projektangaben" ein. Überschreiben Sie dabei jetzt wie in den weiteren Schritten diejenigen Einträgen, welche als Beispiele vorhanden sind.
- Füllen Sie dann die weiteren Felder der Tabelle "Allgemeine Projektangaben" aus. Achtung: Füllen Sie jetzt und bei allen folgenden Tabellen immer nur die weissen Felder aus. Die schwarzen Felder werden für die Struktur von *ISiGo 1.5* benötigt.

Ausserdem ist bei vielen Feldern angegeben, bei welcher Aktivität sie gefüllt werden sollen (z.B. "ab A2.1").
- Tragen Sie die Adressen der Teilnehmer in der Tabelle "Adressen" ein.
- Sie können jede Tabelle mit `Datei | Drucken` ausdrucken.

A1.2 Vorbereitung

Ziel dieser Aktivität:	*Erarbeitung der Grundlagen zur Projektdurchführung*

Die Vorbereitungen werden vom Projektleiter (= Koordinator) geleitet. Sie umfassen die üblichen Projektarbeiten, insbesondere

- Abgrenzung des Betrachtungsobjektes:
  Zu Beginn des Projektes ist zu klären, welche Abteilungen, welche Informationen und welche Informationssysteme zu betrachten sind. Daraus lässt sich direkt folgern, welche Personen am Projekt zu beteiligen sind.
- Abklärung spezieller Anforderungskriterien:
  Um die Anforderungen an die Informationssicherheit einheitlich erheben zu können, muss ein einheitlicher Kriterienkatalog vorbereitet werden. Dieser wird in Aktivität 2.2 genauer beschrieben. Falls Sie in Ihrem Bereich besondere Voraussetzungen für Anforderungskriterien haben oder später die Befragungen der Erhebung und Bewertung zusammenlegen möchten, sollten Sie jetzt den Bewertungskriterienkatalog erstellen. Falls Sie ISiWay erstmals durchführen, können Sie den in Anhang angegebenen Vorschlag benutzen, und es entstehen jetzt keine weiteren Arbeiten.
- Massnahmenkatalog:
  ISiWay 1.5 enthält selbst keinen Massnahmenkatalog. Dies ist aufgrund der sich schnell verändernden Technologien und der individuellen Bedürfnisse der Anwendungsbereiche von ISiWay auch nicht sinnvoll. Es ist deshalb Aufgabe dieser Aktivität,
  - Bestehende unternehmensrelevante Massnahmenkataloge (beispielsweise aus übergeordneten Vorschriften oder Richtlinien) zu beschaffen und zur Verfügung zu stellen,
  - Öffentlich verfügbare Grundschutzmassnahmenkataloge zu identifizieren und wo notwendig anzupassen, oder
  - Individuelle Massnahmenkataloge zusammenzustellen.

  Der Massnahmenkatalog kann Massnahmen enthalten, welche bei verschiedenen Anforderungsstufen zur Anwendung kommen müssen.

- Aufstellung von Terminplan und Budget:
  Es ist eine grobe Schätzung über Anzahl und Umfang der Erhebung (Rest von Phase 1) abzugeben. Dies dient einerseits als Richtlinie für die interaktive Anpassung der Projektgrösse, andererseits zur ersten Mitteilung der notwendigen Aufwände an die beteiligten Parteien. Ausserdem muss die Erhebungsphase grob geplant werden (Vorgehen und Erhebungsform, Anzahl der Interviews, etc.)

Es ist empfehlenswert, zu Beginn nur einige wenige Personen und Abteilungen in das Projekt zu integrieren.

Ergebnisse: Projektplanung	*Projektbeschreibung (Beispiel im Anhang) mit Ziel des Projekts, Abgrenzung des Betrachtungsobjekts, Terminplan & Zeitbudget der Erhebung.*

	Massnahmenkatalog und (optional) Bewertungkriterienkatalog
Akteure:	*Koordinator*

ISiGo 1.5

Aufgaben:	*Erstellen Sie eine Projektbeschreibung mit Abgrenzung (Beispiel im Anhang der Beschreibung), die "Projektplanung" mit "Termine", stellen Sie einen Massnahmenkatalog und (optional) den Bewertungskriterienkatalog (Beispiel im Anhang) bereit.*

- Wählen Sie `ISiGo 1.5 | Aktuelle Aktivität | Zur naechsten`, um die Arbeit an der nächsten Aktivität zu beginnen. Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Aufgabe`, um eine Beschreibung der aktuellen Aufgabe zu erhalten.
- Halten Sie die Projektbeschreibung schriftlich fest. Verwenden Sie das Beispiel im Anhang als Vorlage. Tragen Sie den Ablageort in Tabelle "Projektplanung" ein.
- Füllen Sie dann die weiteren Felder der Tabelle "Projektplanung" aus.
- Tragen Sie die vereinbarten Termine in die Tabelle "Termine" ein. Erfassen Sie auch Vorbereitungs- und Nachbearbeitungszeiten im Total des Aufwandes! Auch Spesen können erfasst werden.
- Optional: Erstellen Sie den Bewertungskriterienkatalog (vgl. Aktivität 2.2).
- Optional: Erstellen Sie den allgemeinen Massnahmenkatalog. Tragen Sie ansonsten die einzelnen Massnahmen in die Tabelle "Massnahmenkatalog" ein. Referenzieren Sie die Quelle, falls vorhanden. Erfassen Sie auch, ab welcher Anforderungshöhe die einzelnen Massnahmen zum Tragen kommen sollen. Bei Grundschutzmassnahmen (Massnahmen des minimalen Schutzes) ist dies nicht spezifiziert: Tragen Sie dann 0 ein.
  Falls Sie keinen Massnahmenkatalog erstellen möchten, sondern nur auf extern verfügbare Massnahmenkataloge verweisen möchten, können Sie als Massnahme "Umsetzung des Massnahmenkatalogs xy" eintragen.

A1.3 Erhebung Inhalte

Ziel dieser Aktivität:	*Erhebung der schützenswerten Objekte*

Die Erhebung geschieht in *strukturierten Befragungen*, welche der Koordinator mit den *Ansprechpartnern der Fachabteilungen* durchführt. Ziel dieser Befragungen ist es zunächst, die schützenswerten Informationen der Fachabteilung zusammenzustellen.

Erhebungsform

Zur Erhebung und Strukturierung der notwendigen Daten eignet sich eine *strukturierte Befragung*. Dabei wird anhand eines zugestellten Fragebogens eine vorgegebene Struktur (Tabelle) mit den Werten gefüllt, die der Interviewpartner angibt. Ebenfalls gut geeignet, aber zeitaufwendig ist ein *persönliches Interview*, in welchem sich Koordinator und Ansprechpartner persönlich treffen. Möglich ist auch die schriftliche Befragung durch Zustellung und selbständiges Ausfüllen der Tabellen durch den Ansprechpartner. Als Mischform bietet sich die *telefonische Befragung* an, bei welcher der Ansprechpartner angeleitet wird, die ihm vorliegende Tabelle auszufüllen, oder bei dem der Koordinator versucht, aufgrund der Aussagen des Ansprechpartners die Tabelle auszufüllen.

Für ein persönliches Interview sollten ein bis zwei Stunden veranschlagt werden, je nach Vorkenntnis des Interviewpartners und Komplexität seines Bereichs. Telefonische Befragungen können in dreissig bis sechzig Minuten durchgeführt werden. In jedem Fall sollten jeweils dreissig bis sechzig Minuten Nachbearbeitungszeit zur Zusammenfassung und Übergabe der Ergebnisse eingeplant werden.

Es wird empfohlen, bei erstmaliger Durchführung in jedem Fall persönliche Interviews durchzuführen und erst bei späteren Wiederholungen mit dem telefonischen oder selbständigen Ausfüllen zu beginnen.

Prozesse (optional)

Zur Strukturierung der Erhebung kann von den in der Abteilung ablaufenden Prozessen (bei Prozessorientierung) oder von den funktionellen Bereichen (bei Funktionsteilung) ausgegangen werden. Anhand dieser Prozesse können dann die verarbeiteten Informationen identifiziert werden. Die Erfassung der Prozesse hat mehrere Vorteile: Sie unterstützen er die Vollständigkeit der Erhebung, weil die Führung der Abteilungen üblicherweise über Ablauf- und Aufbauorganisation geschieht und nicht über die Inhalte der Geschäftstätigkeit. Ausserdem erlauben sie die Identifikation und Zuordnung der jeweiligen Verantwortlichen für die untergeordneten Bereiche (Gruppenleiter oder Prozess-Owner als weitere Ansprechpartner). Dennoch ist die Erhebung der Prozesse nicht unbedingt notwendig.

Informationssammlungen

Die Erhebung der schützenswerten Informationen kann anschliessend beginnen. Zentral ist die Wahl einer geeigneten Grössenordnung für die Erfassung. Weder ist es sinnvoll, einzelne Dateien oder Dokumente zu erfassen, noch die Informationen für einen Prozess als eine einzige Einheit zu betrachten. Die Unterteilung sollte anhand der Arbeitsinhalte fallen. Erscheinungsformen von Informationen können als Anhaltspunkte genommen werden: So kann eine Informationssammlung einen Ordner, eine Ordnergruppe oder ein ganzes Archiv umfassen, oder die Daten in einem bestimmten Unterverzeichnis der gemeinsamen Dateiablage. Erfahrungsgemäss können die Informationen für jeden Prozess in *Bearbeitete Informationen*, *Grundlageninformationen, Steuerinformationen* und *administrative Informationen* unterteilt werden.

- *Bearbeitete Informationen (B)* enthalten die Beschreibungen von Personen oder Gegenständen, auf welche sich die geschäftliche Tätigkeit bezieht. Bei einer Abteilung einer Versicherung, welche Schadensfälle bearbeitet, wären dies beispielsweise die Schadensmeldungen selbst (Protokolle, Notizen, Gesprächsaufzeichnungen etc.) oder die Dokumente für die Abklärung von Zuständigkeit oder Eintreten. Die bearbeiteten Informationen sind in der Regel abteilungsspezifisch, werden also in erster Linie in dieser Abteilung erstellt und benutzt.
- Bei dieser Bearbeitung wird auf *Grundlageninformationen (G)* zurückgegriffen. Bei der Versicherung wären das Informationen über die versicherten Personen und Sachen sowie die Versicherungspolicen etc. Grundlageninformationen werden üblicherweise von mehreren Abteilungen gemeinsam benutzt.
- *Steuerinformationen (S)* beeinflussen die Abläufe in der Abteilung und ihr Zusammenwirken mit anderen Abteilungen. Dazu gehören z.B. Sitzungen (und ihre Protokolle) der Abteilung und mit anderen Abteilungen, Aufträge und Anweisungen an die bzw. von der Abteilung etc.
- Die *administrativen* Informationen (A) dienen der Steuerung und Verwaltung der Abteilung selbst. Dies umfasst beispielsweise Informationen über Mitarbeiter, Raumbelegung, interne Adressverzeichnisse etc.

Nicht immer sind diese Arten verschiedener Informationen genau voneinander zu trennen. Als Anhaltspunkt sollten für jede Abteilung ein bis etwa drei Informationssammlungen jeder Art unterschieden werden können. Es ist später immer noch möglich, die auf übergeordneter Ebene identifizierten Informationssammlungen durch weitere Gespräche mit den Gruppenleitern etc. zu detaillieren, falls das notwendig erscheint, oder umgekehrt, *zu* detailliert erfasste Informationssammlungen zusammenzufassen.

Ebenfalls wichtig ist bei der Erfassung, dass medienunabhängig erhoben wird. Das bedeutet, dass Papierdokumente, Dateien im Computer, Sprachaufzeichnungen, Telefongespräche und selbst ganze Sitzungen als Informationssammlungen identifiziert werden können. Die Erfassung hat sich am *Inhalt* zu orientieren. Dies ist deshalb wichtig, weil nur so später die Anforderungen sinnvoll formuliert werden können. Der Verlust von Vertraulichkeit kann beispielsweise ebenso durch Kopieren eines Papierdokuments wie durch Abhören eines Gesprächs entstehen.

Wiederum ist es wichtig, für jede Informationssammlung festzuhalten, wer der Ansprechpartner für ihre genauere Betrachtung bzw. ihren Schutz ist. Weitere administrative Angaben zu jeder Informationssammlung (Umfang, Standort, Medien etc.) runden diese Erfassung ab, sind aber nicht zentral für den Schutz und in der Erhebung deshalb optional.

Lassen Sie sich in jedem Fall die Gesamterhebung *visieren*.

Informationssysteme

Wenn die Informationssammlungen erfasst wurden, können auch die Informationssysteme erfasst werden, mit deren Hilfe die Informationen verarbeitet werden. Auch diese Erhebung findet mit den Ansprechpartnern der *Fachbereiche* statt und nicht mit denen der IT-Systeme, denn das erfolgt erst später in Aktivität 1.4. Wie bei den Informationssammlungen soll medienneutral erhoben werden, d.h. alle verwendeten Medien sind zu berücksichtigen. So stellen Telefon und Fax, Briefpost, Besprechungsraum und Aktenablage ebenso Informationssysteme dar wie Computer, Netzwerk, Inter- und Intranet oder Office-Anwendungen. Nur so kann später der Schutz der Informations*inhalte* gewährleistet werden. Auch hier wird mit Beschreibung von Technologie und Standort abgerundet.

Die in diesen Interviews entstehenden Listen mit Informationssystemen entsprechen der Benutzersicht dieser Systeme und können völlig anders strukturiert sein als die für ihre Bereitstellung notwendigen technischen Elemente. *Hier interessiert die Sicht der Benutzer.* Es wird später Aufgabe des Koordinators und der Verwalter sein, von der Benutzersicht auf die technische Sicht zu schliessen.

Lassen Sie sich in jedem Fall die Gesamterhebung *visieren*.

Verknüpfung

Jede Informationssammlung ist nur so sicher wie das System, mit welchem sie bearbeitet wird. Umgekehrt formuliert: Alle Informationssysteme, mit denen eine Informationssammlung bearbeitet wird, müssen die Sicherheitsanforderungen an diese Informationssammlung erfüllen.

Es muss also vorher festgehalten werden, welche Informationssammlungen mit welchen Informationssystemen bearbeitet werden. Dazu besteht in der Tabelle der Informationssammlungen eine zusätzliche Spalte, in welcher dies festgehalten wird.

Ansprechpartner und Verantwortlicher

Es wurde bisher mit Absicht immer von einem *Ansprechpartner* und nicht vom *Verantwortlichen* für eine Abteilung, einen Prozess, eine Informationssammlung oder ein System gesprochen. Das hat mehrere Gründe:

- Der Ansprechpartner kann beispielsweise ein Mitarbeiter des jeweils Verantwortlichen sein, welcher den konkreten Bereich ebenfalls gut kennt und Auskunft geben kann, aber selbst nicht die Verantwortung wahrnehmen kann, weil er nicht selbst über die notwendigen Kompetenzen verfügt.
- Die Bezeichnung eines Verantwortlichen muss stets in Absprache mit dieser Person selbst erfolgen, auch wenn ein direkter Vorgesetzter diese Zuweisung vornimmt.
- Einzelne Objekte (Informationssammlungen, Informationssysteme) werden von mehreren Personen gemeinsam benutzt und gepflegt. Dies betrifft insbesondere Grundlageninformationen und unternehmensweite, abteilungsübergreifende Informationssammlungen. Die Bestimmung eines *Verantwortlichen* ist hier schwierig, doch die verschiedenen Beteiligten können sich untereinander wahrscheinlich auf einen gemeinsamen *Ansprechpartner* einigen.

Bedrohungen, Vorfälle und Massnahmen (optional)

Als Ergänzung (und insbesondere, wenn die beteiligten Personen dies wünschen) können die von den Interviewpartnern angenommenen Bedrohungen festgehalten werden. Ebenso können die bisherigen Sicherheitsvorfälle aufgenommen werden und die Massnahmen festgehalten werden, welche gegen die Bedrohungen schon umgesetzt wurden.

Konsolidierung

Die Erfassungsphase endet, wenn sich Koordinator und die jeweils interviewten Ansprechpartner auf eine einheitliche Erfassung der schützenswerten Informationen und der damit verbundenen erfassten weiteren Objekte (Informationssysteme, Prozesse, etc.) geeinigt haben. Dieses Einverständnis kann nur durch ein- oder mehrmaligen Austausch der formell und inhaltlich bereinigten Tabellen erzielt werden, deren Erstellung Aufgabe des Koordinators ist. Eine Vorbereitung der Tabellen durch den interviewten Ansprechpartner ist zwar möglich, die Bereinigung durch den Koordinator ist jedoch notwendig. Diese Bereinigung umfasst

- Konsolidierung der Erfassung. Dies bedeutet, dass der Koordinator nachträglich verschiedene erhobene Einzelteile zusammenfassen darf, wo die Detaillierung nicht notwendig ist, oder dass er eine Aufteilung komplexer Objekte in zwei oder mehr getrennte vornehmen kann. Er muss dabei jedoch darauf achten, dass die ebenfalls erhobenen Verknüpfungen bestehen bleiben,
- Konsolidierung der Erfassung der Interviews untereinander. Wenn mehrere Interviewpartner dieselben Angaben machen, gerade beispielsweise bei Grundlageninformationen, kann der Koordinator diese Mehrfachnennungen vereinheitlichen. Er darf sie jedoch nicht zusammenfassen! Dies dient nur der Erreichung von Vergleichbarkeit,

· einheitliche Darstellung und Formatierung.

Falls dies notwendig erscheint, kann der Koordinator einzelne der erhobenen Objekte genauer betrachten, indem er mit den entsprechenden angegebenen Ansprechpartnern

vertiefte Gespräche durchführt. Dies kann in der Tabellenspalte "Vertiefung notwendig" festgehalten werden und ist dann notwendig, wenn der Interviewpartner nur ungenügende Kenntnis über das entsprechende Objekt hat oder besonderen Wert auf dessen Sicherheit legt, aber nicht detaillierter Auskunft geben kann.

Ergebnisse:	*Listen der Informationssammlungen und Informationssysteme, optional Listen der Prozesse, Bedrohungen, Vorfälle und Massnahmen*
Akteure:	*Koordinator, Ansprechpartner der Fachbereiche*

ISiGo 1.5

Aufgaben:	*Führen Sie die Interviews durch. Halten Sie jeweils die erhobenen Prozesse (optional), Informationssammlungen und Informationssysteme (und optional Bedrohungen, Vorfälle und schon getroffene Massnahmen) in den gleichnamigen Tabellen fest.*

- Wählen Sie *ISiGo 1.5* | Aktuelle Aktivität | Zur naechsten, um die Arbeit an der nächsten Aktivität zu beginnen. Wählen Sie *ISiGo 1.5* | Aktuelle Aktivitaet | Aufgabe, um eine Beschreibung der aktuellen Aufgabe zu erhalten.
- Allgemeine Funktionen von *ISiGo 1.5*:
  - Sie können jede Tabelle löschen, indem Sie ISiGo 1.5 | Format | Tabelleninhalt löschen wählen. Dabei werden nur die Inhalte entfernt, nicht jedoch die Struktur der Tabelle und die summarischen Informationen. Alternativ können Sie auch die Zellen ab Zeile 7 markieren und mit der Taste "Delete" / "Löschen" löschen.
  - Die Formatierung (Darstellung) jeder Tabelle können Sie jederzeit mit ISiGo 1.5 | Format | Aktuelle Tabelle neu formatieren wiederherstellen. Dabei werden die in der Tabelle "Systemdaten" eingestellten Schriftarten verwendet.
  - Die Formatierung (Darstellung) aller Tabellen können Sie jederzeit mit ISiGo 1.5 | Format | Alle Tabellen neu formatieren wiederherstellen.
  - Mit Data | Sort bzw. Daten | Sortieren kann jede Tabelle sortiert werden. Markieren Sie zuvor die zu sortierenden Zeilen. Voreingestellt ist die Sortierung nach der ersten Spalte.
- Sie können die Tabellen "Prozesse", "Infosammlungen" und "Infosysteme" (und optional "Bedrohungen", "Vorfälle" und "Massnahmen") selbst ausfüllen (vgl. nächste drei Punkte) oder sie exportieren (vgl. fünftnächsten Punkt).
- Optional: Füllen Sie die Tabelle "Prozesse" mit den erhobenen Prozessen. Vergeben Sie jede Nummer nur einmal; Kombinationen aus Buchstaben und Zahlen sind erlaubt (beginnen Sie jede Nummer mit einem P). Halten Sie jeweils fest, wer diesen Prozess angegeben hat, benennen und beschreiben Sie den Prozess kurz. Tragen Sie bei "Ansprechpartner" ein, wer für eine weitere Detaillierung befragt werden müsste und bei "Verfeinerung notwendig", ob dies notwendig ist. Sobald Sie die Verfeinerung in einem erneuten Interview vorgenommen haben, können Sie das "ja" in dieser Spalte durch ein "nein" ersetzen. Neue Adressen können in der Tabelle "Adressen" erfasst werden. "Erfassung" sollte mit dem aktuellen Datum gefüllt werden.
- Füllen Sie in der Tabelle "Infosammlungen" die mit "Ab A1.3" gekennzeichneten Spalten. Vergeben Sie jede Nummer nur einmal; Kombinationen aus Buchstaben und Zahlen sind erlaubt (beginnen Sie jede Nummer mit einem I). Halten Sie jeweils fest, wer diese Informationssammlung angegeben hat, benennen und beschreiben Sie sie kurz. Tragen Sie bei "Ansprechpartner" ein, wer für eine weitere Detaillierung befragt

werden müsste und bei "Verfeinerung notwendig", ob dies notwendig ist. Sobald Sie die Verfeinerung in einem erneuten Interview vorgenommen haben, können Sie das "ja" in dieser Spalte durch ein "nein" ersetzen.

Neue Adressen können in der Tabelle "Adressen" erfasst werden. In die Spalte "gehört zu Prozess Nr." sollte die Nummer des Prozesses eingetragen werden, zu welchem diese Informationssammlung gehört. "Erfassung" sollte mit dem aktuellen Datum gefüllt werden.

Ausserdem ist es sinnvoll, den Umfang der Informationssammlung festzuhalten. Als Mass für die Informationsmenge werden MByte verwendet. Für digital gespeicherte Informationen lässt sich dies im Betriebssystem ablesen. Für papierbasierte Dokumente können folgende Richtwerte verwendet werden: 1000 Seiten Text umfassen ca. 2 bis 5 MByte, eine ganzseitige grafische Darstellung ca. 0.1 bis 0.5 MByte und ein ganzseitiges Farbfoto ca. 1 bis 5 MByte. Tragen Sie in jedem Fall einen Wert ein, da Informationssammlungen ohne Grössenangabe als nicht-existent gewertet werden können.

Lassen Sie die Spalte "Verwendete Informationssysteme" noch leer.

Drucken Sie nach der Erfassung die Tabelle aus und lassen Sie die jeweiligen Zeilen in der Spalte "Visum Erhebung" vom Interviewpartner visieren. Wenn Sie sie visiert zurückerhalten, können Sie in der Spalte "Visum Erhebung" ein "ja" eintragen, die Originale aufbewahren und mit der erfassten Tabelle weiterarbeiten.

Es ist auch möglich, den Ausdruck auf genau einen Namen zu beschränken. Exportieren Sie dazu die entsprechende Tabelle, geben Sie den gewünschten Namen ein und drucken Sie sie aus (vgl. unten "Exportieren").

- Füllen Sie in der Tabelle "Informationssysteme" die mit "Ab A1.3" gekennzeichneten Spalten mit den jeweiligen Ergebnissen der Interviews. Vergeben Sie jede Nummer nur einmal; Kombinationen aus Buchstaben und Zahlen sind erlaubt (beginnen Sie jede Nummer mit einem T). Halten Sie jeweils fest, wer dieses Informationssystem angegeben hat, benennen und beschreiben Sie es kurz. Beachten Sie auch papiergebundene (Fax, Briefpost, Kurier, Archiv, Ablage), tongebundene (Telefon, Beantworter, etc.) und mobile Systeme (Notebooks). Tragen Sie bei "Ansprechpartner Benutzer" ein, wer für eine weitere fachliche Detaillierung befragt werden müsste und bei "Verfeinerung notwendig", ob dies notwendig ist. Sobald Sie die Verfeinerung in einem erneuten Interview vorgenommen haben, können Sie das "ja" in dieser Spalte durch ein "nein" ersetzen.

  Tragen Sie bei "Ansprechpartner Systembetreuung" den Namen derjenigen Person ein, welche bei technischen Fragen zu diesem System konsultiert würde. Neue Adressen können in der Tabelle "Adressen" erfasst werden. "Erfassung" sollte mit dem aktuellen Datum gefüllt werden.

  Es ist nicht notwendig, jedes Gerät einzeln zu erfassen. Wenn Sie beispielsweise mehrere PCs in demselben Büro betreiben, erfassen Sie nur eine Zeile, in welcher Sie bei "Standort" die Bürobezechnung und bei "Anzahl gleichartige" die Anzahl eingeben. "Technologie" dient der genaueren Beschreibung des verwendeten Systems. Diese Spalte ist optional.

Drucken Sie nach der Erfassung die Tabelle aus und lassen Sie die jeweiligen Zeilen in der Spalte "Visum Erhebung" vom Interviewpartner visieren. Wenn Sie sie visiert zurückerhalten, können Sie in der Spalte "Visum Erhebung" ein "ja" eintragen, die Originale aufbewahren und mit der erfassten Tabelle weiterarbeiten.

Es ist auch hier möglich, den Ausdruck auf genau einen Namen zu beschränken. Exportieren Sie dazu die entsprechende Tabelle, geben Sie den gewünschten Namen ein und drucken Sie sie aus (vgl. unten "Exportieren").

- Füllen Sie nun die Spalte "Verwendete Informationssysteme" der Tabelle "Informationssammlungen" und halten Sie dort fest, welche Informationssysteme für die Verarbeitung der jeweiligen Informationen verwendet werden. Geben Sie jeweils die gesamte Nummer des Informationssystems an und trennen sie die verschiedenen Informationssysteme mit Kommata. Beispiel: Wenn für die Verarbeitung von Informationssammlung "I-GR1" die Informationssysteme "T-GR1", "T-GR3" und "T-GR4" verwendet werden, so tragen Sie in der Spalte "Verwendete Informationssysteme" der Zeile "I-GR1" in der Tabelle "Infosammlungen" ein: "T-GR1, T-GR3, T-GR4". Diese Zuordnung wird später vom System für die Feststellung von Diskrepanzen benötigt.
- Optional: Falls der Interview-Partner dies wünscht, können Sie in der Tabelle "Bedrohungen" die von ihm wahrgenommenen Bedrohungen eintragen.
- Optional: Falls der Interview-Partner dies wünscht, können Sie in der Tabelle "Vorfälle" die von ihm festgestellten Vorfälle dokumentieren.
- Optional: Falls der Interview-Partner dies wünscht, können Sie in der Tabelle "Massnahmen" die schon ergriffenen Massnahmen eintragen.
- In der Tabelle "Termine" können Sie den Zeitaufwand nachführen.

Tabellen exportieren

Es ist auch möglich, eine Tabelle gesamthaft zu exportieren und so dem Ansprechpartner selbständiges Einfüllen zu ermöglichen. Wählen Sie dazu die Tabellen, welche Sie exportieren möchten, also z.B. "Prozesse", "Infosammlungen" und "Infosysteme". Mit `ISiGo 1.5 | Exportieren | Für Interview-Partner` können sie diese gerade angewählten Tabellen als einzelne Excel-Datei speichern. Es ist dabei sowohl möglich, alle Daten zu exportieren als auch nur bestimmte (z.B. diejenigen eines Interviewpartners) zu exportieren. Die ausgefüllte Tabelle kann dann, wenn sie vom Interviewparter zurückgegeben wird, durch Kopieren der ausgefüllten Zeilen jeweils an das Ende der bestehenden Tabellen integriert werden.

A1.4 Erhebung Systeme

Ziel dieser Aktivität:	*Zuweisung der benutzten Systeme zu technischen Systemen*

Die von den Benutzern angegebenen Informationssysteme müssen nicht unbedingt denjenigen Systemen entsprechen, welche von den Verwaltern der technischen Informationssysteme angegeben wurden. Ziel dieses Schrittes ist es, einen Abgleich zwischen beiden Sichtweisen zu schaffen.

Dazu stellt der Koordinator die von den Benutzern angegebenen Informationssysteme zusammen und versucht, Ansprechpartner für diese Systeme zu finden. Dabei wird von denjenigen Personen ausgegangen, welche der Ansprechpartner der Fachbereiche als technische Kontakte angegeben hat. Darüberhinaus kann der Ansprechpartner der

Informatikabteilung in der Regel viele dieser einzelnen Technik-Ansprechpartner bezeichnen. Im Falle von Telefon- und Faxsystem, Briefpost und anderer Infrastruktur sind die Ansprechpartner über die Infrastrukturdienste (Objektschutz etc.) zu finden oder können sich sogar ausserhalb der Unternehmung befinden.

In Zusammenarbeit mit diesen Ansprechpartnern versucht der Koordinator nun, für jedes der von den Benutzern wahrgenommene System diejenigen Systeme zu finden, die technisch dahinterstecken. Die Zuweisung erfolgt durch die Vergabe einer "technischen Bezeichnung" in der schon bestehenden Liste der Informationssysteme. Diese Bezeichnung kann den Namen verschiedener technischer Systeme enthalten. Beispielsweise kann das System "E-Mail" mehrere Client-, Server- und Netzwerkdienste umfassen.

Um die Konsistenz der Erfassung zu gewährleisten, dürfen bei dieser Systemerhebung nur Umbenennungen und Umgruppierungen stattfinden, keinesfalls jedoch dürfen Informationssysteme aufgeteilt oder zusammengefasst werden. Dies deshalb, weil die Sicht des Benutzers in jedem Fall gewahrt bleiben muss.

Auch hier muss der Koordinator versuchen, die Aussagen der Interviewpartner möglichst korrekt (d.h. in deren Sinne) wiederzugeben.

Ergebnisse:	*Technische Bezeichnungen der von den Benutzern angegebenen Informationssysteme*
Akteure:	*Koordinator, Verwalter*

ISiGo 1.5

Aufgaben:	*Stellen Sie mit den Verwaltern zusammen, wie die von den Benutzern bezeichneten Systeme technisch genannt werden müssen. Tragen Sie diese Bezeichnungen in der Spalte "Technische Bezeichnung" der Tabelle "Informationssysteme" ein.*

- Wählen Sie `ISiGo 1.5 | Aktuelle Aktivität | Zur naechsten`, um die Arbeit an der nächsten Aktivität zu beginnen. Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Aufgabe`, um eine Beschreibung der aktuellen Aufgabe zu erhalten.
- Tragen Sie in der Tabelle "Infosysteme" jeweils technische Bezeichnungen für alle Informationssysteme ein. Führen Sie dazu Telefongespräche oder Interviews mit den entsprechenden Verwaltern, welche von den Benutzern als technische Ansprechpartner angegeben wurden. Halten Sie unter "Interview-Partner Verwalter" zusätzlich fest, mit wem Sie gesprochen haben. In die Spalte "Bemerkungen des Verwalters" können Sie weitere technische Angaben über das Informationssystem eintragen.

A1.5 Abschluss

Ziel dieser Aktivität:	*Erhebung abschliessen*

Nach der Erhebung ist Phase 1 abgeschlossen.

Nun muss der Koordinator entscheiden, ob er allenfalls die Betrachtungstiefe beschränkt. Aufgrund der gesammelten Daten kann er die Komplexität des untersuchten Systems und den Aufwand für weitere Erfassungen (insbesondere in der Vertiefung) abschätzen.

Ausserdem sollte ein erster Bericht an die Sponsoren abgegeben werden, welcher die wichtigsten Projektergebnisse (v.a. Erhebungsdauer, Anzahl und Grösse der erhobenen Objekte sowie weitere quantitative Werte) umfasst.

Ergebnisse:	*Neufestlegung der Tiefe, Bericht an Sponsoren*
Akteure:	*Koordinator*

ISiGo 1.5

Aufgaben:	*Schätzen Sie aufgrund der Erfahrungen und des bisherigen Aufwands ab, welchen Bereich Sie tiefer betrachten möchten. Stellen Sie mit Hilfe der summarischen Kopfzeileninformationen oder mit Hilfe der Tabelle "Statistik" einen Bericht an die Sponsoren zusammen.*

- Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Zur naechsten`, um die Arbeit an der nächsten Aktivität zu beginnen. Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Aufgabe`, um eine Beschreibung der aktuellen Aufgabe zu erhalten.
- Die Erstellung eines Berichts kann durch Ausdruck der Tabelle "Statistik" oder durch Sammlung der einzelnen summarischen Informationen geschehen, welche jeweils in den obersten Zeilen der Tabellen angegeben sind.

2.2 Bewertung

In der zweiten Phase werden die erhobenen Objekte durch die Ansprechpartner der Fachbereiche bewertet, um quantitative Angaben über die Anforderungen an die Sicherheit zu erhalten.

A2.1 Bewertungskriterienkatalog

Ziel dieser Aktivität:	*Erstellung eines Bewertungskriterienkatalogs*

Bevor Bewertungen durchgeführt werden können, müssen Kriterien der Bewertung festgelegt und die Bedeutungen der Werte bestimmt werden. Alle Bewertungen beziehen sich auf Informationen (und auf Informationssammlungen).

Bewertungskriterien

Als Bewertungskriterien bieten sich an:

- **Verfügbarkeit**: Information muss zu demjenigen Zeitpunkt an demjenigen Ort verfügbar sein, an welchem sie benötigt wird.
- **Interne Integrität (Konsistenz)**: Information darf durch Abbildungs- und Verarbeitungsvorgänge nicht verändert werden, bzw. durch diese Vorgänge dürfen keine Widersprüche und Unvollständigkeiten entstehen.
- **Vertraulichkeit**: Information darf nur denjenigen Personen zur Verfügung stehen, welche darüber aufgrund ihrer Aufgabenstellung verfügen sollen.
- **Externe Integrität (Kongruenz)**: Informationen müssen den Teil der Realität, welchen sie abbilden sollen, auch derart abbilden, dass keine Widersprüche zwischen der erkennbaren Realität und ihrer Abbildung entstehen.
- **Verbindlichkeit**: Die Verpflichtungen, welche aus einer Informationsübermittlung entstehen, müssen von Sender und Empfänger gegenseitig anerkannt werden, bzw. die gewählte Form der Informationsübermittlung muss eine derartige Verpflichtung nachweisbar machen.
- **Beabsichtigte Verwendung**: Information soll nur für diejenigen Zwecke verwendet werden, welche bei ihrer Erhebung angegeben oder beabsichtigt wurden oder welche einem anderweitig festgelegten Verwendungszweck entsprechen. Die Forderungen des Datenschutzes sind Forderungen der beabsichtigten Verwendung.
- **Effizienz**: Die Information soll so aufgebaut sein, dass sie sich mit minimalem Ressourceneinsatz nutzen lässt.

Es bleibt dem Koordinator überlassen, welche der Bewertungskriterien er verwenden möchte. Es wird jedoch empfohlen, zumindest die ersten drei zu verwenden. Die weiteren können beispielsweise für die erneute Durchführung des Verfahrens zurückgestellt werden. Auch die Definition eigener, weiterer Kriterien ist möglich, allerdings sollte der Koordinator darauf achten, dass die einzelnen Kriterien voneinander unabhängig sind und genügend genau spezifiziert sind. Der Koordinator muss die Tabellen zur Erfassung der Informationssysteme anschliessend entsprechend anpassen (Einfügen von Spalten, vgl. unten).

Werte

Sobald für alle ausgewählten Kriterien die notwendigen Angaben vorgenommen wurden oder festgelegt wurde, wie diese erhoben werden, muss eine Skala aufgestellt werden, welche die Zuteilung quantitativer Werte erlaubt. Dabei sollten diskrete Werte verwendet werden. Es sollten nicht weniger als drei und nicht mehr als fünf Werte gewählt werden, z.B.

- 0 (keine), 1 (mittel), 2 (hoch) oder
- 0 (keine), 1 (wenig), 2 (mittel), 3 (viel), 4 (hoch).

Diesen Werten müssen für jedes Kriterium dann jeweils Bedeutungen zugewiesen werden, z.B. *"Wert 0 bei der Vertraulichkeitsanforderung bedeutet, dass es sich um öffentliche Information handelt, von welcher jedermann Kenntnis haben darf."* Im Anhang ist ein Vorschlag für diese Zuordnung angegeben.

Es ist essentiell, dass sich die Anzahl der verfügbaren Werte (also die Spanne zwischen Minimal- und Maximalwert) sowie die Bedeutungen der Werte zwischen zwei Bewertungen (also zwischen zwei Durchläufen des Zyklus) *nicht verändert*. Deshalb muss *vor der ersten Bewertung* ein Kriterienkatalog aufgestellt werden, welcher alle Bedürfnisse der interviewten Parteien langfristig abdeckt. Dieser Kriterienkatalog muss breit gestreut werden und seine Bedeutungen müssen den beteiligten Parteien bewusst sein.

Da es schwierig ist, schon zu Anfang langfristig geltende Kriterien zu formulieren, müssen nachträgliche Änderungen, falls sie unumgänglich sind, sofort eine Anpassung und Umrechnung der bisherigen Werte umfassen. Dies sollte nur in Extremfällen notwendig sein und nur dann vorgenommen werden, wenn Minimal- oder Maximalwert sehr häufig von den Betroffenen verwendet werden.

Ergebnisse:	*Bewertungskriterienkatalog und entsprechende Spalten in den Tabellen "Informationssammlungen" und "Informationssysteme"*
Akteure:	*Koordinator*

ISiGo 1.5

Aufgaben:	*Stellen Sie einen Bewertungskriterienkatalog zusammen (Beispiel im Anhang). Tragen Sie dessen Ablageort in der Tabelle "Allgemeine Projektangaben" ein. Tragen Sie für jedes Kriterium eine Spalte in den Tabellen "Infosammlungen" und "Infosysteme" ein.*

- Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Zur naechsten`, um die Arbeit an der nächsten Aktivität zu beginnen. Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Aufgabe`, um eine Beschreibung der aktuellen Aufgabe zu erhalten.
- Erfassen Sie für die von Ihnen ausgewählten Bewertungskriterien jeweils eine Zeile in der Tabelle "Bewertungskriterien", indem Sie das entsprechende Kriterium (z.B. "Verfügbarkeit") in Spalte 2 in der nächsten leeren Zeile einfügen. In Spalte 1 erscheint automatisch eine Nummer. Vergeben Sie ausserdem eine Abkürzung.
- Erfassen Sie in den Spalten Minimal- und Maximalwert jeweils den kleinst- und grösstmöglichen Wert pro Kriterium.
- Wählen Sie `ISiGo 1.5 | Bewertung | Bewertungskriterien einfügen`, um die Kriterien in die Tabellen "Informationssammlungen" und "Informationssysteme" einzufügen. Pro Bewertungskriterium entsteht eine Spalte, in deren zweitoberster Zeile der aktuelle Mittelwert der Bewertung angezeigt wird,

darunter wird angezeigt, wieviele der Informationssammlungen mit einem Wert höher als 2 bzw. als 2.5 bewertet wurden.

- Falls später weitere Bewertungskriterien hinzugefügt werden, indem neue Zeilen in der Tabelle "Bewertungskriterien" eingefügt werden, so trägt die Funktion `ISiGo 1.5 | Bewertung | Bewertungskriterien einfügen` nur die zusätzlichen Bewertungskriterien ein. Die bestehenden Kriterien und die eingetragenen Werte bleiben erhalten! Die neuen Spalten können problemlos neben die alten verschoben werden (ganze Spalte markieren, `Bearbeiten | Ausschneiden` wählen, Spalte direkt nach dem zuvor letzten Bewertungskriterium markieren und `Einfügen | Ausgeschnittene Zellen` wählen.
- Erfassen Sie in einem Textverarbeitungsprogramm einen Bewertungskriterienkatalog entsprechend Anhang. Tragen Sie den Ablageort dieses Katalogs in die Tabelle "Allgemeine Projektangaben" ein.

A2.2 Bewertung Inhalte

Ziel dieser Aktivität:	*Die Inhalte mit den Bewertungskriterien bewerten, um so die Anforderungen an die Sicherheit zu erfahren*

Interview

Die Durchführung der Bewertung geschieht wiederum durch Interviewen der jeweiligen Ansprechpartner in den Fachbereichen. Für jedes Bewertungskriterium wird der Ansprechpartner um Zuordnung eines Wertes gebeten. Dabei werden die *Anforderungen* erhoben, also der vom Interviewten gewünschte Zustand. Es spielt dabei noch keine Rolle, ob diese Anforderungen realistisch sind und erfüllt werden können. Allenfalls kann der Koordinator auf die Unangemessenheit einer Anforderung hinweisen, jedoch nur, wenn er dadurch seine neutrale Rolle nicht verliert.

Wenn also beispielsweise festgelegt wurde, dass beim Kriterium Verfügbarkeit der Wert 2 bedeutet, dass die Information *innerhalb eines Arbeitstages wieder verfügbar sein muss*, und der Ansprechpartner hat an eine konkrete Informationssammlung genau diese Anforderung, dann sollte in der Spalte Verfügbarkeit in der Zeile dieser Informationssammlung eine 2 eingetragen werden.

Erfahrungsgemäss fällt einigen Personen die Wahl eines konkreten Wertes aus dem vorbereiteten Kriterienkatalog schwer. Ihnen sollte erlaubt werden, einen Zwischenwert (z.B. 1.5, 2.5) zu wählen.

Auf diese Art sollten alle neu hinzugefügten Spalten der Tabelle "Informationssammlungen" gefüllt werden.

Abgleich

Wenn der Koordinator in der Nachbearbeitung des Interviews diese Bewertungen mit anderen Bewertungen vergleicht, kann er in Absprache mit dem Interviewpartner folgende Korrekturen vornehmen:

- Falls die Anforderungen an ein Objekt von verschiedenen Ansprechpartnern beurteilt wurden (z.B. Grundlageninformationen), kann er einen Mittelwert vorschlagen. Es

kann allerdings durchaus vorkommen, dass verschiedene Personen verschiedene Anforderungen haben! In diesem Fall gilt der höchste der angegebenen Werte.
- Falls die Anforderungen gesamthaft zu hoch oder zu tief scheinen, kann er eine gesamthafte Korrektur vorschlagen.

Keinesfalls darf er ohne Rücksprache eine Veränderung des Wertes vornehmen.

Abschluss

Auch bei der Bewertung ist es wichtig, dass der Koordinator die Meinung des Interviewten korrekt wiedergibt, und auch hier ist dies nur durch allenfalls wiederholtes Austauschen der formatierten überarbeiteten Erfassungstabellen möglich. Lassen Sie sich deshalb auch die Bewertung visieren.

Zusammenfassung von Interviews

Um den Prozess zu beschleunigen, können die Interviews zur Bewertung mit denen der Erfassung (Phase 1) zusammengenommen werden.

Ergebnisse:	*Bewertungen der Anforderungen an die Informationssammlungen*
Akteure:	*Koordinator, Ansprechpartner der Fachbereiche*

ISiGo 1.5

Aufgaben:	*Verlangen Sie von jedem Ansprechpartner die Bewertung der Anforderungen an seine Informationssammlungen in jedem Bewertungskriterium. Tragen Sie diese Anforderungen in die Spalten "BK..." in der Tabelle "Infosammlungen" ein.*

- Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Zur naechsten`, um die Arbeit an der nächsten Aktivität zu beginnen. Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Aufgabe`, um eine Beschreibung der aktuellen Aufgabe zu erhalten.
- Erfassen Sie die Angaben des Ansprechpartners in der Tabelle "Infosammlungen" in den zuvor hinzugefügten Spalten. Diese Namen dieser Spalten beginnen mit "BK..." (für "Bewertungskriterium").
- Der Mittelwert und die Anzahl der Eintragungen mit 2 bzw. 2.5 oder mehr am Anfang der Spalte wird automatisch nachgetragen.

A2.3 Bewertung Systeme (optional)

Ziel dieser Aktivität:	*Die bestehende Sicherheit der Systeme bewerten*

Wie kann sichergestellt werden, dass die in der vorhergehenden Aktivität gestellten Anforderungen erfüllt werden? Dazu müssen alle Systeme, welche eine Informationssammlung verarbeiten, diese Anforderung erfüllen. Umgekehrt muss deshalb jedes Informationssystem die höchste Anforderung erfüllen, welche an eine durch sie verarbeitete Informationssammlung gestellt wird.

In einer späteren Aktivität muss abgeklärt werden, ob die Anforderungen von den Systemen erfüllt werden können. Das kann direkt geschehen, indem die Verwalter der Systeme direkt

mit den Anforderungen an die Informationssammlungen konfrontiert werden. Dann ist diese Aktivität A2.3 nicht notwendig.

Der Koordinator kann jedoch diesen Dialog vorbereiten, indem er zum Voraus abklärt, welche Anforderungen die Systeme zu erfüllen vermögen. Dazu legt er den Ansprechpartnern für die einzelnen Informationssysteme den Bewertungskriterienkatalog vor und verlangt von ihnen Angaben darüber, welche Anforderungen ihre Systeme *zu erfüllen* vermögen. Anders formuliert: Es wird bewertet, wie hoch die höchste Anforderung ist, welche das System noch erfüllen kann. Dies wird als Sicherheitsleistung des Systems bezeichnet. Beispielsweise kann eine 3 (hoch) im Kriterium *Verfügbarkeit* bedeuten, dass das System *zu jeder Tages- und Nachtzeit innerhalb einer Stunde wieder verfügbar ist*. Dies kann beispielsweise bedeuten, dass als Massnahmen Notstromversorgungen und Pikettdienst eingerichtet wurden.

Auch hier können Interviews zur Erhebung verwendet werden. Wie bei den Informationssammlungen können die Interviews mit denjenigen der Erhebung zusammengefasst werden.

Es sollte den Verwaltern bewusst sein, dass die von ihnen gemachten Angaben *verbindlich* behandelt werden. Falls Zweifel an der Gewährleistung bestehen, sollte eher tiefer eingestuft werden. Die Einhaltung der hier angegebenen Anforderungen wird später von den Ansprechpartnern der Fachbereiche verlangt werden!

Ergebnisse:	*Bewertungen der Sicherheit der Informationssysteme*
Akteure:	*Koordinator, Verwalter*

ISiGo 1.5

Aufgaben:	*Erfragen Sie bei den Verwaltern (den Betreibern der IT-Systeme), welche Anforderungen ihre Systeme jeweils maximal erfüllen können. Tragen Sie dies in die "BK..."-Spalten der Tabelle "Infosysteme" ein.*

- Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Zur naechsten`, um die Arbeit an der nächsten Aktivität zu beginnen. Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Aufgabe`, um eine Beschreibung der aktuellen Aufgabe zu erhalten.
- Erfassen Sie die Angaben der Verwalter in der Tabelle "Infosysteme" in den in A2.1 hinzugefügten Spalten. Diese Namen dieser Spalten beginnen mit "BK..."
- Der Mittelwert und die Anzahl der Eintragungen mit 2 bzw. 2.5 oder mehr am Anfang der Spalte wird automatisch nachgetragen.

A2.4 Abschluss

Ziel dieser Aktivität:	*Bewertung abschliessen*

Nach der Bewertung ist Phase 2 abgeschlossen.

Nun muss der Koordinator entscheiden, welche Prioritäten er für die weitere Betrachtung setzt. Er kann

- die Informationssammlungen und Informationssysteme mit den höchsten Bewertungen vorziehen, und die folgenden Phasen zuerst auf diese Objekte anwenden, oder
- falls die Systeme bewertet wurden, versuchen, die grössten Diskrepanzen zuerst zu bereinigen, oder
- Vollständigkeit anstreben und deshalb weiterhin dieselbe Breite behalten, jedoch allenfalls die Betrachtungstiefe beschränken, indem er zuerst nur eines der Kriterien betrachtet.

Wiederum sollte ein Bericht an die Sponsoren abgegeben werden, welcher die wichtigsten Projektergebnisse (v.a. Erhebungsdauer, mittlere Werte der Beurteilung, Identifikation der besonders schützenswerten Bereiche, wichtigste Diskrepanzen) umfasst.

Aus den Mittelwerten der Beurteilungen von Informationssammlungen und Informationssystemen lassen sich erste Aussagen ableiten:

- Sind sie etwa gleich, so bedeutet dies, dass der Aufwand für die Informationssicherheit in jener Kategorie gesamthaft genügend ist. Dennoch ist es natürlich möglich, dass in einzelnen Bereichen extreme Diskrepanzen zwischen Anforderung und Erfüllung bestehen.
- Die Unterschiede in einzelnen Anforderungen (z.B. Vertraulichkeit) erlauben es, Prioritäten zu setzen.

Ergebnisse:	*Setzen von Prioritäten, Bericht an Sponsoren*
Akteure:	*Koordinator*

ISiGo 1.5

Aufgaben:	*Fassen Sie die Ergebnisse der Bewertung zusammen und erstellen Sie mit Hilfe der summarischen Kopfzeileninformationen oder mit Hilfe der Tabelle "Statistik" einen Bericht an die Sponsoren. Legen Sie Prioritäten für die weitere Betrachtung fest.*

- Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Zur naechsten`, um die Arbeit an der nächsten Aktivität zu beginnen. Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Aufgabe`, um eine Beschreibung der aktuellen Aufgabe zu erhalten.
- Die Erstellung eines Berichts kann durch Ausdruck der Tabelle "Statistik" oder durch Sammlung der einzelnen summarischen Informationen geschehen, welche jeweils in den obersten Zeilen der Tabellen angegeben sind.

2.3 Dialog

In der dritten Phase werden die Anforderungen an die Informationen und die Möglichkeit der Informationssysteme, diese Anforderungen zu erfüllen (die Sicherheitsleistung), gegenübergestellt. Dabei tritt für jede Kombination von Informationssammlung und Informationssystem einer von zwei Fällen ein:

- Das Informationssystem erfüllt die Anforderungen an die Informationssammlung. In diesem Fall sind keine weiteren Aktivitäten notwendig, und die Betrachtung der Informationssicherheit kann mit dieser Aussage für diese eine Kombination beendet werden. Es kann jedoch sein, dass Massnahmenkataloge festgelegt wurden, welche unbedingt zur Anwendung gelangen müssen -- diese müssen dann in den Phasen 3 und 4 noch betrachtet werden.
- Das Informationssystem erfüllt die Anforderungen an die Informationssammlung nicht.

A3.1 Filterung (optional)

Ziel dieser Aktivität:	*Bereiche mit Handlungsbedarf identifizieren*

Diese Aktivität kann nur durchgeführt werden, falls die Systeme von den Verwaltern bewertet wurden (Aktivität 2.3).

In einem ersten Schritt muss der Koordinator diejenigen Bereiche identifizieren, in welchen Diskrepanzen zwischen den Anforderungen und der Erfüllung dieser Anforderungen durch die Systeme bestehen. Eine solche Diskrepanz entsteht, wenn ein Informationssystem eine Anforderung nicht erfüllen kann, welche an eine damit verarbeitete Informationssammlung gestellt wird. Die Kombination geschieht mit Hilfe der Spalte "Verwendete Informationssysteme" in Tabelle "Infosammlungen", welche in A1.3 ausgefüllt wurde.

Es wird nun wie folgt vorgegangen:

- Man nehme bei der ersten Informationssammlung die erste Bewertung der Anforderungen (z.B. Verfügbarkeit).
- Nun vergleiche man für jedes Informationssystem, mit welchem diese Informationssammlung bearbeitet wird, ob dieses Informationssystem die Anforderung erfüllen kann, also in demselben Kriterium einen gleichen oder grösseren Wert aufweist. Falls nicht, wird dies als Diskrepanz festgehalten, und zwar
  - einerseits bei der Informationssammlung, deren Anfoderungen nicht erfüllt werden, und
  - andererseits beim Informationssystem, welche diese Anforderung nicht erfüllt.
- Ebenso verfahren man mit den weiteren Bewertungskriterien und danach mit den weiteren Informationssystemen.

Das Ziel der Dialogphase ist die Entfernung dieser Diskrepanzen.

Ergebnisse:	*Zusammenstellung der Diskrepanzen, d.h. der Informationssammlungen und Systeme mit Unterschieden zwischen Anforderungen und Erfüllung*

Akteure:	*Koordinator*

ISiGo 1.5

Aufgaben:	*Vergleichen Sie bei jeder Informationssammlung die Anforderungen mit den Bewertungen derjenigen Informationssysteme, auf welche sie bearbeitet werden. Halten Sie Diskrepanzen fest.*

- Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Zur naechsten`, um die Arbeit an der nächsten Aktivität zu beginnen. Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Aufgabe`, um eine Beschreibung der aktuellen Aufgabe zu erhalten.
- Wählen Sie `ISiGo 1.5 | Bewertung | Diskrepanzen eintragen`, um die bestehenden Diskrepanzen automatisch in beide Tabellen eintragen zu lassen. Dabei entstehen in den Tabellen "Infosammlungen" und "Infosysteme" je zwei neue Spalten (bzw. falls sie bestanden, werden sie neu gefüllt).
- In der Tabelle "Infosammlungen" werden in der Spalte "Diskrepanzen von mehr als 1" diejenigen Informationssysteme eingetragen, welche die Anforderungen um mehr als 1 verfehlen. Jeweils wird dazu das Kriterium angegeben, welches verfehlt wird. In der Spalte "Diskrepanz von bis zu 1" werden die darunterliegenden Diskrepanzen eingetragen. Jede einzelne Diskrepanz wird eingetragen als Kombination von Systemnummer und Abkürzung des Bewertungskriteriums, in welchem die Diskrepanz besteht. Ein Eintrag "T-GR5: Vfg" bedeutet also, dass das System "T-GR5" die Anforderungen an die Verfügbarkeit nicht erfüllt.
- In der Tabelle "Infosysteme" werden gleichermassen die Informationssammlungen eingetragen, welche höhere Anforderungen stellen als diese Informationssystem erfüllen kann.
- Ziel ist die Entfernung *aller* Diskrepanzen in den folgenden Aktivitäten! Die Unterteilung in solche mit mehr als 1 und solche mit weniger dient der Festlegung der Prioritäten.

A3.2 Vorbereitung

Ziel dieser Aktivität:	*Effizienten Dialog zwischen Ansprechpartnern der Fachbereiche und Verwaltern vorbereiten*

Zweck

Die Koordinationssitzungen der Dialogphase dienen dazu, die Diskrepanzen zwischen den Anforderung an die Informationssammlungen und die Möglichkeiten der Informationssysteme, diese Anforderungen zu erfüllen (Sicherheitsleistung), zu erörtern und über Lösungen nachzudenken, wie diese Diskrepanzen beseitigt werden können.

Prinzipiell bestehen drei Möglichkeiten für derartige Lösungen:

- Das Informationssystem wird so verändert, dass es die Anforderungen erfüllen kann,
- die Anforderungen an die Informationssammlung werden gesenkt, d.h. der Ansprechpartner für die entsprechende Informationssammlung senkt seine Anforderungen,
- die Verarbeitung der Informationssammlung mit diesem System wird eingestellt, d.h. die Verarbeitung wird auf ein anderes System übertragen, welche die Anforderungen erfüllen kann, oder ganz eingestellt.

Ziel einer Koordinationssitzung ist es, für jede der Diskrepanzen eine der drei Lösungsmöglichkeiten zu finden. Dies führt zu Diskussionen über die Notwendigkeiten und die Höhe der Anforderungen, zu Diskussionen über die voraussichtlichen Kosten, welche die Erfüllung der Anforderungen mit sich bringt, und darüber, ob die vorgeschlagenen Lösungen die Erfüllung der Anforderungen überhaupt erlauben. Der Koordinator leitet diese Diskussionen, bleibt jedoch in jedem Fall neutral! Allenfalls kann er als unabhängige Stelle argumentieren, ob die vorgeschlagenen Massnahmen die Erfüllung der Anforderungen zulassen würde.

Teilnehmer und Vorbereitung

Wenn Diskrepanzen bestehen, sind grundsätzlich alle an den betroffenen Informationssammlungen und Systemen beteiligten Personen zu involvieren, um diese Diskrepanzen zu beheben. Für die Entfernung jeder Diskrepanz muss ein Dialog zwischen Ansprechpartner der Informationssammlung und dem Ansprechpartner für das Informationssystem initiiert werden. Wird eine Informationssammlung mit mehreren Systemen bearbeitet, können auch mehrere Diskrepanzen für dieses eine Informationssystem bestehen, und entsprechend sind mehrere Ansprechpartner der betroffenen Systeme zu involvieren.

Im einfachsten Fall bestehen keine Diskrepanzen. Dann können alle Betroffenen über diesen Status informiert werden und es geht dann lediglich um die Umsetzung der Allgemeinen Massnahmen (vgl. A5.1).

Das andere Extrem wäre, wenn keines der Systeme die daran gestellten Anfoderungen erfüllen würde. Dann müssen alle Ansprechpartner aller Informationssammlungen und aller Systeme miteinander diskutieren. Schon bei kleinen Untersuchungsbereichen (z.B. 10 Informationssammlungen mit zusammen 3 verschiedenen Anprechpartnern, 5 Informationssysteme mit 4 verschiedenen Ansprechpartnern) führt dies zu einer Diskussion von 8 Personen (inkl. Koordinator) über potentiell bis zu 50 Diskrepanzen. Bei grösseren Untersuchungsbereichen steigt diese Anzahl entsprechend. Es kann also hoher Aufwand entstehen.

In der Regel liegt die Anzahl und Verteilung der Diskrepanzen zwischen beiden Extremen: Nur einzelne Systeme oder nur einzelne Informationssammlungen sind betroffen. Deshalb kann der Koordinator diese Objekte gruppieren. Beispielsweise könnte er erst Gespräche mit den Ansprechpartnern von zwei oder drei Informationssystemen führen und sie mit den Anforderungen an diese Systeme konfrontieren.

Wenn der Koordinator also über die Bewertungen der Systeme verfügt (aus A2.3), kann er alle notwendigen Daten zur Diskussion der Diskrepanzen vorbereiten, zusammenfassen und gruppieren, um so die Voraussetzungen für die Durchführung von effizienten Koordinationssitzung zu schaffen, welche jeweils nur wenige Personen umfassen. Er kann sogar die wichtigsten Diskrepanzen herausheben und als wichtige Traktanden der Koordinationssitzung benennen.

So kann der Koordinator aufgrund der ihm vorliegenden Informationen

- einzelne der Informationssammlungen oder Informationssysteme mit Diskrepanzen auswählen und eine Besprechung mit den Betroffenen vereinbaren, oder
- die höchsten Anforderungen an ein Informationssystem zusammenstellen, und nur die Vertreter mit den höchsten Anforderungen mit dem Ansprechpartner für das

Informationssystem zusammenbringen. Traktandum sind dann die Anforderungen an dieses eine Informationssystem, oder
- mit den Koordinatoren parallel laufender Informationssicherheitsprojekte oder mit einem übergeordneten Koordinator (vgl. Hierarchie unten) Kontakt aufnehmen, falls dieser schon Lösungen in ähnlichen Fällen oder im Idealfall schon für dasselbe übergeordnete Informationssystem erarbeitet hat, oder
- schriftliche und mündliche Vorabklärungen vornehmen, in denen er versucht, eine der drei Lösungen herzuleiten oder zumindest die wichtigsten Argumente sammelt und einen Lösungsvorschlag für die Sitzung erarbeitet,

Hier wird vorerst vorgeschlagen, Besprechungen mit einzelnen Parteien vorzubereiten. Dazu ist es sinnvoll, eine oder mehrere Informationssammlungen auszuwählen und die jeweils Betroffenen einzuladen. Diesen Personen sind die jeweils relevanten Daten zur Verfügung zu stellen (Zuschicken).

Sinnvoll ist die Durchführung von Koordinationssitzungen mit Gruppen von jeweils an einem oder wenigen Informationssystemen beteiligten oder von einer oder wenigen Informationssammlungen betroffenen Personen.

Ergebnisse:	*Zusammenstellung der Diskrepanzen, d.h. der Informationssammlungen und Systeme mit Unterschieden zwischen Anforderungen und Erfüllung*
Akteure:	*Koordinator*

ISiGo 1.5

Aufgaben:	*Bereiten Sie effiziente Sitzungen zur Diskussion der Diskrepanzen vor, indem Sie analysieren, wer zu beteiligen ist und jede Diskussion auf einzelne Informationssammlungen und Informationssysteme beschränken.*

- Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Zur naechsten`, um die Arbeit an der nächsten Aktivität zu beginnen. Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Aufgabe`, um eine Beschreibung der aktuellen Aufgabe zu erhalten.
- Analysieren Sie die Diskrepanzen und gruppieren Sie die Sitzungen. Tragen Sie für jede Sitzung einen Termin in der Tabelle "Termine" ein. Tragen Sie jeweils in der Spalte "Interview-Partner" die Namen aller teilnehmenden Personen ein.
- Es ist nun möglich, alle Daten aus *ISiGo 1.5* zu exportieren, welche an einem bestimmten Termin relevant sind. Gehen Sie dazu auf den Termin, dessen Daten sie exportieren möchten, und wählen Sie `ISiGo 1.5 | Exportieren | Für Termin`. *ISiGo 1.5* erstellt nun eine Datei, in welcher alle Systeme aller Teilnehmer der Diskussion enthalten sind. Gerade wegen dieser Sammlung ist es sinnvoll, nur jeweils wenige Personen zu beteiligen.

A3.3 Durchführung

Ziel dieser Aktivität:	*Diskrepanzen ausräumen*

Führen Sie die Sitzung durch, indem Sie die erhobenen Daten als Diskussionsgrundlage verwenden. Versuchen Sie nun, für jede Diskrepanz eine der drei vorher genannten Lösungen zu erreichen.

- Falls die Lösung vorsieht, die Anwendung von Massnahmen abzuklären, erfassen Sie diese Abklärung in der Tabelle "Massnahmen" mit dem Status "Abklärung" und tragen Sie ihre Nummer in der Tabelle "Informationssystem" in der Spalte "Massnahmen" ein. Es können auch mehrere Massnahmen eingetragen werden.
- Falls der Ansprechpartner der Informationssammlung seine Anforderung senkt, korrigieren Sie diese in der Tabelle "Infosammlungen".
- Falls auf die weitere Verwendung des Systems für diese Informationssammlung verzichtet wird, streichen Sie es in der Tabelle "Informationssammlungen" aus der Liste der "verwendeten Informationssysteme".

In Einzelfällen kann es auch vorkommen, dass der Verwalter ohne weitere Massnahmen eine höhere Bewertung für sein System abgibt. Dies kann durch Erhöhung des entsprechenden Wertes in der Tabelle "Informationssysteme" behandelt werden.

Der Koordinator muss in diesen Diskussionen allen Beteiligten deutlich machen, dass sie ihre Angaben selbst verantworten müssen. Insbesondere Aussagen wie "Wenn wir unsere Anforderungen senken müssen, sind die Verwalter dafür verantwortlich." oder ähnlich, mit denen die Parteien versuchen, sich die Verantwortung gegenseitig zuzuschieben, müssen als unsachgemäss zurückgewiesen werden.

Als Ergebnis der Sitzung reduziert sich die Liste der Diskrepanzen, da die erste und die dritte Lösung die Diskrepanz entfernen. Die zweite Lösung (Abklärung) soll schliesslich auch dazu führen, die Diskrepanz zu entfernen. Vorerst muss jedoch festgehalten werden, bis wann eine Lösung vorgestellt wird. Halten Sie die vorgeschlagenen Massnahmen schriftlich fest. Vereinbaren Sie jeweils den Termin für die Übergabe eines Konzeptes und einen Termin für die nächste Sitzung.

Führen Sie alle Besprechungen durch und versuchen Sie, möglichst viele Diskrepanzen durch eine der drei Lösungen zu behandeln. Halten Sie alle Beschlüsse schriftlich fest und teilen Sie den Teilnehmern diese Ergebnisse abschliessend schriftlich mit. Im Idealfall können *alle* Diskrepanzen behandelt werden, wichtig ist aber, dass die grossen Diskrepanzen entfernt werden. Bei Streitfällen kann nur die Weisung der übergeordneten Stelle Klarheit schaffen.

Alternativ ist es für den Koordinator auch möglich, abwechslungsweise mit den Ansprechpartnern der Fachbereiche und mit den Verwaltern zu reden, und dann jeweils nur mit einzelnen davon. Das ist in jedem Fall aber als Vorbereitung zu sehen. Um zu einem Lösungsvorschlag zu kommen, müssen in jedem Fall Verwalter und Ansprechpartner der Fachbereiche an derselben Diskussion teilnehmen (deshalb auch *Dialog* genannt).

Jede der hier erarbeiteten Massnahmen ist vorerst nicht mehr als ein *Ansatz zu einer Lösung*. Es sollte vermieden werden, schon hier detailliert zu diskutieren, da dies vor allem Zeit benötigt und die konkreten Vorschläge erst noch erarbeitet werden müssen (Phase 4).

Weisen Sie zusätzlich darauf hin, dass auch die Massnahmen aus dem allgemeinen Massnahmenkatalog umgesetzt werden müssen (falls ein solcher besteht) und stellen Sie diesen Massnahmenkatalog zur Verfügung.

Ergebnisse:	*Zusammenstellung von Lösungen für die Entfernung der Diskrepanzen (Lösungsansätze)*
Akteure:	*Koordinator, Ansprechpartner der Fachbereiche, Verwalter,*

Aufgaben:	*Führen Sie die Sitzung durch, indem Sie die erhobenen Daten als Diskussionsgrundlage verwenden. Versuchen Sie nun, für jede Diskrepanz eine der drei vorher genannten Lösungen zu erreichen.*

- Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Zur naechsten`, um die Arbeit an der nächsten Aktivität zu beginnen. Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Aufgabe`, um eine Beschreibung der aktuellen Aufgabe zu erhalten.
- Tragen Sie die Lösungen in die entsprechenden Spalten der Tabelle "Massnahmen" ein.
- Tragen Sie die Termine für die nächste Sitzung in die Tabelle "Termine" (diese gehören zu Aktivität 4.3) ein.

A3.4 Abschluss

Ziel dieser Aktivität:	*Dialog über Diskrepanzen abschliessen*

Der Koordinator sollte auch am Ende dieser Phase wieder die Ergebnisse der jeweiligen Sitzungen allen Betroffenen zur Verfügung stellen und die noch bestehenden Missverständnisse direkt mit den Betroffenen klären.

Ein Zwischenbericht an die Sponsoren wird ebenfalls empfohlen. In ihm kann das Verhalten der Parteien zur Sprache gebracht werden (hartes oder nachgiebiges Verhalten). Ausserdem sollte unbedingt über Streitfälle informiert werden, bei denen sich die Parteien nicht auf einen Lösungsansatz einigen konnten. Handlungsbedarf der Sponsoren ist allerdings in dieser Aktivität noch nicht gegeben; dies erfolgt später.

Ausserdem können die quantitativen summarischen Werte den obersten Zeilen jeder Tabelle entnommen werden.

Ergebnisse:	*Lösungsansätze, Bericht an Sponsoren*
Akteure:	*Koordinator*

ISiGo 1.5

Aufgaben:	*Fassen Sie die Ergebnisse des Dialogs zusammen und erstellen Sie mit Hilfe der summarischen Kopfzeileninformationen oder mit Hilfe der Tabelle "Statistik" einen Bericht an die Sponsoren. Legen Sie Prioritäten für die weitere Betrachtung fest.*

- Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Zur naechsten`, um die Arbeit an der nächsten Aktivität zu beginnen. Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Aufgabe`, um eine Beschreibung der aktuellen Aufgabe zu erhalten.

2.4 Realisierungsplanung

Ziel der vierten Phase ist es, aufgrund der noch sehr allgemeinen Lösungsvorschläge der dritten Phase konkrete Massnahmen zu erarbeiten, und einen Konsens bezüglich Kosten und Terminen zu erhalten.

A4.1 Erarbeitung konkreter Lösungen

Ziel dieser Aktivität:	*Massnahmenvorschläge erarbeiten*

Die Erarbeitung von Lösungen ist in erster Linie Aufgabe der Betreiber der Informationssysteme (bzw. der Verwalter, welche die Ansprechpartner der Betreiber sind). Aus den Koordinationssitzungen der Dialogphase kennen sie die zu erfüllenden Anforderungen. Sie kennen die Technologien der verwendeten Informationssysteme jeweils viel besser als die Ansprechpartner der Fachbereiche oder der Koordinator, sodass sie ihre Lösungsvorschläge selbständig erarbeiten können.

Sie tauschen ihre Vorschläge mit dem Koordinator aus, der auf mögliche Synergien hinweist (z.B. bei der Evaluation verschiedener Sicherheitsprodukte), ansonsten aber keinen Einfluss auf die Massnahmenplanung nimmt.

Ergebnis dieser Aktivität ist ein konkreter Lösungsvorschlag für jede noch bestehende Diskrepanz. Dieser Vorschlag muss Auskunft über benötigte Ressourcen, Umsetzungstermine (Start und Inbetriebnahme) sowie über allfällige Nebenwirkungen geben.

Ebenso müssen die Betreiber der Informationssysteme sich mit dem allgemeinen Massnahmenkatalog beschäftigen (sofern ein solcher besteht) und Vorschläge zu dessen Umsetzung erarbeiten. Falls er umfangreich ist, können hier beträchtliche Aufwände entstehen.

In einzelnen Fällen ist es den Systembetreibern nicht möglich, die konkrete Lösung alleine zu erarbeiten, gerade wenn auch Änderungen in Organisation und Ablauf notwendig sind. Der Einbezug der betroffenen Ansprechpartner der Fachabteilungen ist ihnen selbstverständlich freigestellt. Der Koordinator kann die Erarbeitung der Lösung auf Wunsch der Parteien begleiten, hat dabei jedoch keine Führungsfunktion.

Ergebnisse:	*Konkrete Lösungsvorschläge*
Akteure:	*Verwalter (evtl. Koordinator)*

ISiGo 1.5

Aufgaben:	*Fordern Sie die Verwalter (die Betreiber der Informationssysteme) auf, konkrete Lösungsvorschläge zur Ausgestaltung der Lösungsansätze auszuarbeiten und vorzulegen. Setzen Sie Termine.*

- Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Zur naechsten`, um die Arbeit an der nächsten Aktivität zu beginnen. Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Aufgabe`, um eine Beschreibung der aktuellen Aufgabe zu erhalten.
- Sie können die in der Dialogphase festgehaltenen Lösungsansätze exportieren, indem Sie die entsprechende Tabelle markieren und `ISiGo 1.5 | Selektierte Tabellen exportieren` wählen. Die Verwalter können ihre Informationen in diese Tabellen eintragen und wieder elektronisch zur Verfügung stellen. Sie werden dann mit Kopieren / Einfügen (Cut and Paste) wieder in *ISiGo 1.5* eingefügt. Die Verwalter müssen lediglich darauf achten, dass sie die Struktur der Tabelle nicht verändern.

A4.2 Beschluss

Ziel dieser Aktivität:	*Lösung beschliessen*

Sobald für eine Diskrepanz eine konkrete Lösung vorliegt, kann diese vom Ersteller oder vom Koordinator den jeweils Betroffenen zur Verfügung gestellt werden. Ersteller und Betroffene müssen sich dann über die Umsetzung dieser Lösung einigen. Das bedeutet einerseits, dass alle Betroffenen die Nützlichkeit dieser Massnahme zur Entfernung der Diskrepanz anerkennen, andererseits die notwendigen Mittel zur Umsetzung zur Verfügung gestellt werden. Dabei kann über die konkreten Vorschläge durchaus diskutiert werden, Anpassungen sind möglich.

Ebenso muss über die Umsetzung der Massnahmen gemäss allgemeinem Massnahmenkatalog (sofern dieser besteht) diskutiert werden. Hier muss insbesondere der Koordinator argumentieren, warum er diese allgemeine Massnahme vorgeschlagen hat. Der Beschluss über die Umsetzung obliegt jedoch den anderen beiden Parteien, da diese sich über die Verteilung der Aufwände einigen müssen.

Der Koordinator löst die Beschlussfassung durch Einberufung eines Termins mit den jeweiligen Beteiligten aus und lässt sich die zustande gekommenen Beschlüsse jeweils durch Visum bestätigen. Solange die Massnahmen nicht umgesetzt sind, verändert sich die Bewertung des Informationssystems in der Tabelle nicht.

Falls kein Beschluss zustande kommt, muss er eine erneute Erarbeitung einer Lösung veranlassen.

Ergebnisse:	*Beschluss zur Lösungsumsetzung*
Akteure:	*Koordinator, Ansprechpartner der Fachbereiche, Verwalter*

ISiGo 1.5

Aufgaben:	*Lösen Sie die Umsetzung der Lösungsvorschläge aus, indem Sie eine Sitzung einberufen und eine Entscheidung über die vorgeschlagenen Lösungen herbeiführen. Legen Sie Termine fest.*

- Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Zur naechsten`, um die Arbeit an der nächsten Aktivität zu beginnen. Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Aufgabe`, um eine Beschreibung der aktuellen Aufgabe zu erhalten.

- Tragen Sie die vorgeschlagenen und beschlossenen Massnahmen in die gleichnamige Tabelle ein. Veranlassen Sie die Festlegung von Terminen für die Umsetzung und Inbetriebnahme der Massnahmen.

A4.3 Abschluss

Ziel dieser Aktivität:	*Massnahmenplanung abschliessen*

Auch am Ende dieser Phase sollte der Koordinator wieder die Ergebnisse der jeweiligen Sitzungen allen Betroffenen zur Verfügung stellen und die noch bestehenden Missverständnisse direkt mit den Betroffenen klären.

Ein Zwischenbericht an die Sponsoren wird ebenfalls wieder empfohlen. In ihm kann rein quantitativ die Anzahl der beschlossenen und schon umgesetzten Massnahmen erwähnt werden. Interessanter sind jedoch die noch immer offenen Diskrepanzen und mögliche Streitfälle, in welchen sich die Parteien nicht über die Erarbeitung eines Lösungsvorschlags, über die Wirksamkeit einer Massnahme oder über die notwendigen Ressourcen einigen können. Hier muss der Koordinator eine Empfehlung zuhanden der Sponsoren abgeben, nachdem er die betroffenen Parteien darüber informiert hat. Bis zum Entscheid der Sponsoren und der Erarbeitung einer Lösung bleibt die Diskrepanz bestehen.

Ausserdem können die quantitativen summarischen Werte den obersten Zeilen jeder Tabelle entnommen werden.

Ergebnisse:	*Bericht an Sponsoren mit Empfehlungen*
Akteure:	*Koordinator*

ISiGo 1.5

Aufgaben:	*Fassen Sie die Ergebnisse der Massnahmenplanung zusammen und erstellen Sie mit Hilfe der summarischen Kopfzeileninformationen oder mit Hilfe der Tabelle "Statistik" einen Bericht an die Sponsoren.*

- Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Zur naechsten`, um die Arbeit an der nächsten Aktivität zu beginnen. Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Aufgabe`, um eine Beschreibung der aktuellen Aufgabe zu erhalten.

2.5 Massnahmenumsetzung

Die fünfte Phase dient der Umsetzung der beschlossenen Massnahmen.

A5.1 Massnahmenumsetzung

Ziel dieser Aktivität:	*Massnahmen umsetzen*

Diese Phase wird von den Betroffenen der einzelnen Umsetzungsprojekte selbständig gestaltet. Es ist Aufgabe des Koordinators, sich zu dem von den Parteien vereinbarten Inbetriebnahmetermin (d.h. vereinbarter Wirkungsbeginn der Massnahme) erneut über den Fortschritt der Umsetzung zu informieren. Er hat jedoch keine kontrollierende Funktion, sondern kann nur Empfehlungen abgeben. Über die Angemessenheit der Massnahmen müssen später die Ansprechpartner der Fachbereiche entscheiden.

Ergebnisse:	*Umgesetzte Massnahmen*
Akteure:	*Verwalter*

ISiGo 1.5

Aufgaben:	*Informieren Sie sich zu den von den Parteien vereinbarten Umsetzungsterminen über den Stand der Umsetzung. Geben Sie Empfehlungen ab wenn notwendig.*

- Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Zur naechsten`, um die Arbeit an der nächsten Aktivität zu beginnen. Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Aufgabe`, um eine Beschreibung der aktuellen Aufgabe zu erhalten.

A5.2 Abschluss

Ziel dieser Aktivität:	*Umsetzung abschliessen*

Da der Koordinator an der Umsetzung selbst nicht aktiv teilnimmt, sollte er nur einen Bericht über Fortschritt und Erfolg der Umsetzung abgeben.

Ergebnisse:	*Kurzbericht an Sponsoren mit Empfehlungen*
Akteure:	*Koordinator*

ISiGo 1.5

Aufgaben:	*Stellen Sie mit Hilfe der "Statistik" einen Zwischenbericht über den Zustand der Informationssicherheit.*

- Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Zur naechsten`, um die Arbeit an der nächsten Aktivität zu beginnen. Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Aufgabe`, um eine Beschreibung der aktuellen Aufgabe zu erhalten.

2.6 Kontrolle

Phase 6 dient dazu, die Erfüllung der Anforderungen durch die umgesetzten Massnahmen zu überprüfen. Diese Kontrolle des Verfahrens erfolgt auf bis zu sechs Arten:

- Durch die Ansprechpartner der Informationssammlungen (*Client Audit*). Da es Ziel des Verfahrens ist, die Informationssysteme so zu gestalten, dass die Anforderungen an die Informationssammlungen erfüllt werden, müssen abschliessend die Ansprechpartner der Fachbereiche über die erfolgte Umsetzung der Massnahmen informiert werden (Bringschuld der Lösungserbringer) und ihr Einverständnis mit der Lösung erklären. Da sie in der Regel nicht über das notwendige Fachwissen verfügen, können sie jedoch oft nicht wirklich über Inbetriebnahme und Effektivität der Massnahme entscheiden. Sie können jedoch unabhängigen Rat beim Koordinator oder Beratern einholen.
- Durch die Sponsoren (*Sponsor Audit*), da sie informiert werden möchten, wie die von ihnen zur Verfügung gestellten Mittel verwendet wurden.
- Durch den Koordinator (*Coordinator Audit*). Er informiert sich bei jedem der Umsetzungsprojekte zu einem vorher festgesetzten Termin (üblicherweise dem der Inbetriebnahme) über den Stand der Umsetzung.
- Durch das interne Kontrollsystem und die Linienorganisation der Unternehmung (*General Audit*), indem der Koordinator jedem Betroffenen auf Wunsch Bericht erstattet über seine Kenntnis des Umsetzungszustandes des jeweiligen Bereichs und die von ihm angenommene Sicherheit.
- Durch die Leitungsorganisation der Unternehmung (*Management Audit*), da der Koordinator beim Abschluss jeder Phase einen Bericht über Zustand und Umsetzungsfortschritt abgibt.
- Durch die interne Revision der Unternehmung (*Internal Audit*), wo diese vorhanden ist und die entsprechenden Aufgaben umfasst.

A6.1 Client Audit

Ziel dieser Aktivität:	*Client OK*

Ziel des Client Audit ist es, dass die Betroffenen, d.h. die Ansprechpartner der Fachbereiche sich mit den Wirkungen der Umsetzung der Massnahmen zufrieden erklären. Z.B. In einer weiteren Koordinationssitzung können Verwalter über die Umsetzung der Massnahmen informieren.

Da die Clients in der Regel nicht selbst beurteilen können, ob die Massnahmen effizient und effektiv sind, müssen mitunter weitere Experten hinzugezogen werden, welche das Vertrauen der Ansprechpartner geniessen. Der Koordinator kann hier Vorschläge unterbreiten.

Ziel ist es, vom Ansprechpartner der Informationssysteme (und in jedem Fall von ihm) das *Client OK* zu erhalten. Dieses wird wieder durch Visum festgehalten. Wo dies nicht erfolgt, muss die Massnahmenumsetzung nachgebessert werden (Phase 5) oder neue Vorschläge erarbeitet werden (Phase 4). Allenfalls sind aufgrund der inzwischen verstrichenen Zeit auch andere Lösungsansätze möglich (Phase 3).

Wo das Client OK erfolgt ist, kann die Beurteilung des entsprechenden Systems heraufgesetzt werden. Damit entfällt die Diskrepanz.

Ergebnisse:	*Client OKs*
Akteure:	*Koordinator, Ansprechpartner der Fachbereiche*

ISiGo 1.5

Aufgaben:	*Holen Sie die Bestätigung der Ansprechpartner jeder Informationssammlung ein, dass sie mit den umgesetzten Lösungen zufrieden sind und einverstanden sind, dass diese Lösungen die gestellten Anforderungen erfüllen. Vermitteln Sie Experten wenn notwendig.*

- Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Zur naechsten`, um die Arbeit an der nächsten Aktivität zu beginnen. Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Aufgabe`, um eine Beschreibung der aktuellen Aufgabe zu erhalten.
- Lassen Sie bei jeder der von den Ansprechpartnern abgenommenen Massnahmen das "Client OK Visum" mit "Datum" auf einem Ausdruck handschriftlich eintragen und führen sie es in der Tabelle "Massnahmen" durch Eintragen von "ja" nach.

A6.2 Sponsor Audit (optional)

Ziel dieser Aktivität:	*Sponsor OK*

Ziel des Sponsor Audit ist die Aussage der Sponsoren, dass die von ihnen zur Verfügung gestellten Mittel in ihrem Sinne eingesetzt wurden. Das ist nur in einigen besonderen Fällen notwendig, wenn beispielsweise Mittel aus speziellen Kostenstellen verwendet wurden, wenn vertragliche Verpflichtungen erfüllt werden müssen oder wenn es sich um anderweitig gebundene Mittel handelt.

Auch hier koordiniert der Projektleiter die Einholung dieser OKs. Dazu genügt meist schriftlicher Verkehr. Das Sponsor OK hat keinen Einfluss auf die Diskrepanzen, sondern dient der Rechtfertigung der Mittelverwendung.

Ergebnisse:	*Sponsor OKs*
Akteure:	*Koordinator, Sponsoren*

ISiGo 1.5

Aufgaben:	*Unterstützen Sie die Rechtfertigung der Mittelverwendung, indem Sie von den Sponsoren Bestätigungen einholen, dass die verwendenten Mittel im gewünschten Sinne verwendet wurden.*

- Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Zur naechsten`, um die Arbeit an der nächsten Aktivität zu beginnen. Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Aufgabe`, um eine Beschreibung der aktuellen Aufgabe zu erhalten.
- Lassen Sie bei jeder der von den Sponsoren abgenommenen Massnahmen das "Sponsor OK Visum" mit "Datum" auf einem Ausdruck handschriftlich eintragen, und führen sie es in der Tabelle "Massnahmen" durch Eintragen von "ja" nach.

A6.3 Coordinator Audit

Ziel dieser Aktivität:	*Coordinator OK*

Ziel des Coordinator Audit ist die Aussage des Koordinators, dass das Durchlaufen des Zyklus nun abgeschlossen ist und ein neuer Zyklus beginnen kann. Idealerweise ist dies nach Abschluss aller Aktivitäten. Es kann sich jedoch auch um einen zeitpunktorientierten Zwischenbericht handeln (also z.B. einen Jahresbericht), welcher nicht direkt Einfluss auf den Stand des Projekts hat. Dies sei hier deshalb erwähnt, weil ein derartiger umfassender Zwischenbericht ebenfalls *gesamthaft* über das Projekt und seine Ergebnisse berichten soll.

Der Coordinator Audit umfasst die Erstellung eines abschliessenden Berichts über den Zyklus, in welchem die wichtigsten Kenndaten (aufgewendete Zeit und andere Ressourcen, Anzahl der festgestellten und entfernten Diskrepanzen, etc.) enthalten sind. Der Bericht kann mit einer Empfehlung zur Fortführung des Projekts enden.

Falls weitere ISiWay-Detaillierungsgrade betrachtet werden sollen, ist nun die Gelegenheit für einen Wechsel günstig.

Ergebnisse:	*Coordinator OK*
Akteure:	*Koordinator*

ISiGo 1.5

Aufgaben:	*Schliessen Sie die Aktivitäten dieses Zyklus ab. Stellen Sie die Ergebnisse des Projekts zusammen und verfassen Sie einen abschliessenden Bericht über die Ergebnisse dieses Zyklus. Legen Sie diesen Bericht den Auftraggebern und Sponsoren vor.*

- Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Zur naechsten`, um die Arbeit an der nächsten Aktivität zu beginnen. Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Aufgabe`, um eine Beschreibung der aktuellen Aufgabe zu erhalten.

A6.4 General Audit

Ziel dieser Aktivität:	*Information von Dritten*

Ziel des General Audit ist es, Dritte über den Projektzustand zu informieren. Auch dies muss nicht unbedingt am Ende eines Zyklus geschehen, ist jedoch von Vorteil (z.B. in einer internen Projektdokumentation oder bei allgemein spürbaren Auswirkungen des Projektes).

Prinzipiell können alle im Projekt erhobenen Daten Gegenstand eines solchen General Audit sein. Es ist jedoch auf die Vertraulichkeit der Daten zu achten.

Ergebnisse:	*keine*
Akteure:	*Koordinator, Dritte*

ISiGo 1.5

Aufgaben:	*Informieren Sie Dritte, nicht am Projekt beteiligte Personen über Ihre Tätigkeiten, die Ergebnisse und die Erfahrungen aus dem abgeschlossenen Zyklus. Dies ist informativ und kann beispielsweise zur weiteren Motivation genutzt werden.*

- Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Zur naechsten`, um die Arbeit an der nächsten Aktivität zu beginnen. Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Aufgabe`, um eine Beschreibung der aktuellen Aufgabe zu erhalten.

A6.5 Management Audit

Ziel dieser Aktivität:	*Information des übergeordneten Managements und evtl. der Geschäftsleitung*

Das Management Audit ist die vom übergeordneten Management (bzw. von der Geschäftsleitung) durchgeführte Kontrolle der Zielerreichung. Dies geschieht im Rahmen der normalen oder spezifischen Berichterstattung.

Ergebnisse:	*keine*
Akteure:	*Koordinator, übergeordnetes Management (Geschäftsleitung)*

ISiGo 1.5

Aufgaben:	*Erstatten Sie Bericht an das übergeordnete Management über die Ergebnisse des Zyklus und die dadurch erreichten Verbesserungen der Informationssicherheit.*

- Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Zur naechsten`, um die Arbeit an der nächsten Aktivität zu beginnen. Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Aufgabe`, um eine Beschreibung der aktuellen Aufgabe zu erhalten.

A6.6 Internal Audit

Ziel dieser Aktivität:	*Information der Eigentümer*

Das Internal Audit prüft, ob die getroffenen Massnahmen für die Einhaltung der gesetzlichen Rahmenbedingungen und die Erreichung der Ziele der Eigentümer genügen oder ob diese Massnahmen eingeschränkt oder erweitert werden müssen.

Der Koordinator ist der internen Revisionsstelle in der Regel vorbehaltlos zur Auskunft verpflichtet, wobei er sich zwar auf die von ihm abgegebene Vertraulichkeitsverpflichtung berufen muss, aber die Weiterleitung der Anfragen an die jeweils Betroffenen vornehmen kann.

Die Ergebnisse des Internal Audit werden von der internen Revisionsstelle in der Regel wieder dem Koordinator als Kopie zugesandt und enthalten Anregungen und Anweisungen, welche für das nächste Durchlaufen des Zyklus verwendet werden können.

Ergebnisse:	*keine*
Akteure:	*Koordinator, interne Kontrollstelle*

ISiGo 1.5

Aufgaben:	*Geben Sie der internen Revisionsstelle vorbehaltlos Auskunft über den abgeschlossenen Zyklus und verwenden Sie den Revisionsbericht zur Auslösung eines neuen Zyklus.*

- Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Zur naechsten`, um die Arbeit an der nächsten Aktivität zu beginnen. Wählen Sie `ISiGo 1.5 | Aktuelle Aktivitaet | Aufgabe`, um eine Beschreibung der aktuellen Aufgabe zu erhalten.

2.7 Abschlussbemerkungen

Erneutes Durchlaufen

Mit der sechsten Phase endet der ISiWay-Zyklus -- um sofort neu zu beginnen. Selbstverständlich kann beim Neubeginn auf den vorher erhobenen Daten aufgebaut werden. Dies erlaubt sinkenden Aufwand -- oder bei gleichbleibendem Aufwand eine Erhöhung der Betrachtungstiefe und / oder -breite.

Bei einer Zyklusdauer von einem Jahr -- dies ist ein Richtwert, der in Abhängigkeit der Umgebung stark variieren kann -- müssen die Voraussetzungen für die Projektdurchführung neu geprüft und die Beschreibungen allenfalls angepasst werden. Um die Kontinuität zu wahren, wird eine Neubesetzung des Projektteams nicht empfohlen.

Vertraulichkeit

Die vom Koordinator im Laufe seiner Arbeit erhobenen Informationen über Informationssammlungen, Informationssystem etc. stellen ein erhebliches Gefahrenpotential für die untersuchten Bereiche dar. In falschen Händen können sie zur gezielten Spionage oder Sabotage genutzt werden. Diese Informationen sind deshalb vom Koordinator (und vom jeweiligen Ansprechpartner im eigenen Interesse) vertraulich zu handhaben und dürfen Dritten (also auch anderen Ansprechpartnern) nur mit beidseitigem Einverständnis und unter Hinweis auf die damit verbundenen Gefahren weitergegeben werden. Ist der Bereich des Koordinators selbst im Untersuchungsbereich, so ist die Vertraulichkeit dieser erhobenen Daten hoch zu bewerten.

Effizienz

Es wird dringend empfohlen, für alle Schritte des Verfahrens digitale Erfassungsmedien zu verwenden -- idealerweise das darauf angepasste *ISiGo 1.5*, ansonsten aber ein Datenbankmanagementsystem oder ein Tabellenkalkulationsprogramm. Dieser Text sowie alle Vorlagen liegen in digitaler Form vor und werden idealerweise direkt so weitergegeben.

Form der Interviews und Besprechungen

Jedes der Interviews ist als strukturierte Befragung ausgelegt, d.h. der Koordinator befragt den Interviewten anhand einer Erhebungstabelle, welche er vorbereitet hat oder mitnimmt. Dabei wird das persönliche Interview als Idealform vorgeschlagen, wenn sich die beiden Personen nicht oder nur wenig kennen. Bei besserer gegenseitiger Kenntnis können einzelne der Interviews auch telefonisch oder schriftlich durchgeführt werden. Allerdings dient es der Motivation der Befragten, wenn der Koordinator persönlich anwesend ist. Ausserdem muss der Koordinator als motivierender Moderator wirken und bei Fragen zur Bearbeitung der Tabellen sofort kompetent Auskunft geben können.

Aufteilung, Prioritäten und Parallelität

Im Laufe des Projekts kann es mehrfach vorkommen, dass entstehende Fragestellungen mit einzelnen Personen nicht sofort geklärt werden können, andererseits aber die Projektarbeit mit anderen Personen fortschreitet. Dadurch entsteht eine gewisse Parallelität: Während einzelne Personen noch voll in einer Aktivität involviert sind, sind andere schon weiter,

vielleicht schon in der nächsten Phase. Das ist nur möglich, wenn die beiden Bereiche unabhängig voneinander sind. Sind sie es nicht, muss auf die Fertigstellung der vorherigen Aktivitäten gewartet werden, und die Parallelität verschwindet.

Ausserdem kann Parallelität auftauchen, wenn einzelne Bereiche mit hoher Priorität betrachtet werden: auch hier werden einzelne Bereiche schon in späteren Aktivitäten betrachtet, während andere in früheren Aktivitäten verharren.

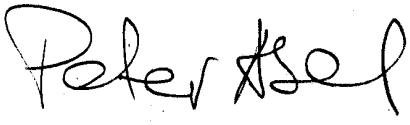
Beides ist eine Frage der Aufteilung. Anfangs und mitten im Text wurde unter dem Stichwort der *Betrachtungsbreite* beschrieben, wie die Aufteilung in verschiedene Objekte geschehen kann, um so voneinander unabhängige Projekte entstehen zu lassen, welche möglicherweise unter derselben Führung (Koordinator in Personalunion) laufen. Auch wenn beispielsweise die Betrachtungstiefe variiert wird, indem eine weniger tiefe Objektaufteilung gewählt wird, oder indem die Betrachtung einzelner Beurteilungskriterien vorgezogen wird, können daraus voneinander unabhängige Projekte entstehen.

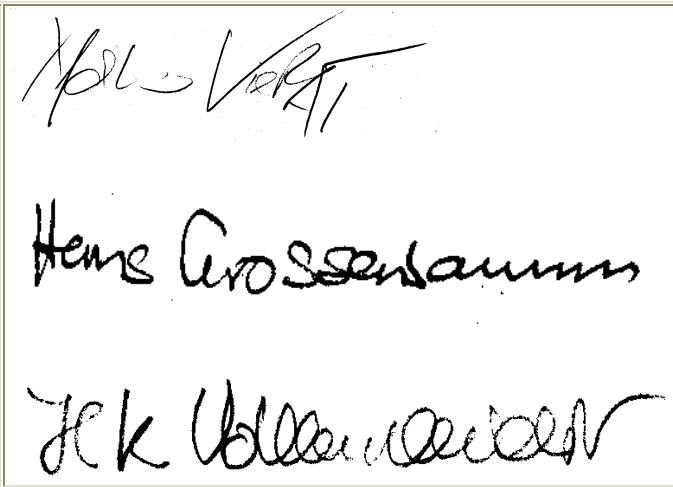
Falls diese parallelen Projekte ebenfalls mit ISiWay weiterbearbeitet werden, sind diese Effekte unproblematisch. Sie können sogar als Mittel der Verteilung des Informationssicherheitsprozesses verwendet werden (föderalistisches Prinzip) und helfen so einerseits, den Aufwand in Grenzen zu halten, führen andererseits dazu, dass Vergleichbarkeit über die verschiedenen Teilprojekte erreicht wird. Auch eine Integration mit anderen Darstellungsgraden von *ISiGo 1.5* ist möglich. Dies wird zur Vertiefung einzelner inhaltlicher Bereiche (Bedrohungen, Vorfallbehandlung, etc.) empfohlen.

3 Anhang / Beispiele

zu 1.1: Schriftlicher Projektauftrag

Projektauftrag ISIWUS

Projektauftrag	**ISiWUS**
Beschreibung	Das Projekt ISiWUS soll die Informationssicherheit in den Produktionswerken I und II sowie der Lagerstation der FirstLight AG untersuchen (Anforderungen und Zustand), Diskrepanzen zwischen Anforderungen und Zustand aufdecken und diese nachhaltig beseitigen.
Projektleiter	Peter Abel, Tel 01 635 45 80, abel@firstlight.ch, Leiter Logistik Werk I
Begründung	Die FirstLight AG wird zunehmend abhängig von der zuverlässigen Verarbeitung ihrer Informationen. Die Komplexität der benötigten Informationssysteme hat schon mehrmals zu Betriebsunterbrüchen geführt, die bisher glücklicherweise ohne schwere Folgen blieben, aber in Zukunft verhindert werden müssen. Die Zusammenarbeit zwischen Informatik und Logistik und Werksleitungen ist sehr gut, allerdings werden zunehmend technische Einschränkungen zur Erhöhung der Sicherheit umgesetzt, welche von Werksleitung und Logistik nicht goutiert werden. Ausserdem befürchtet die Werksleitung, dass auf Informationen über die Produktionsverfahren von ausserhalb der Unternehmung zugegriffen werden kann. Das Projekt ISiWUS soll diese Fragestellungen behandeln und Lösungsvorschläge machen.
Projektstart	15. 8. 1998
Verwendetes Verfahren	*ISiWay 1.5*
Projektdauer (1 Zyklus)	1 Jahr (grobe Planung)
Projektaufwand (Personentage)	30
Auftragsvergabe durch:	
Projektleiter	Peter Abel
Projektinitiatoren	Hans Grossenbaum Markus Vierat
Projektsponsoren	Hans-Karl Vollenweider
Unterschriften	

zu 1.2: Projektbeschreibung

Projektbeschreibung ISIWUS

Projektbeschreibung	**ISIWUS**
Ziel	Ziel des Projektes ISIWUS ist es, Informationssicherheit in den genannten Abteilungen (vgl. unten: Betrachtungsobjekt) herzuleiten. Darunter ist derjenige Zustand der Informationsverarbeitung zu verstehen, in welchem die Fachbereiche mit der Sicherheit der Informationsverarbeitung zufrieden sind.
Vorgehen	Zur Erreichung des Ziels wird das Verfahren ISiWay verwendet.
Betrachtungsobjekt	ISiWUS soll folgende Bereiche betrachten: • Werk I: Gesamte Informationsverarbeitung, insbesondere Administration und Produktionsplanung in der Werksleitung, Verfahrens- und Mitarbeiterplanung; vor allem Informationstechnologie, aber auch papierbasierte Informationsverarbeitung (Pläne, Aufträge, Berichte) und Kommunikation mit Aussen (Fax, Telefon) • Werk II: dito • Lagerstation: Gesamte Informationsverarbeitung, insbesondere Lagerbewirtschaftungssystem, ansonsten wie bei Werk I • Zentrale Informatik: Alle Informationssysteme, welche von den Werken und der Station benötigt werden und in ihrem Auftrag / zu ihrem direkten Nutzen betrieben werden
Projekttiefe	Es soll ein **Überblick** geschaffen werden. Die verarbeiteten Informationen sollen summarisch erhoben und zusammengestellt werden.
Terminplan Erhebung	Start: 15. 8. 98 Ende: 1. 1. 2000 zu involvierende Personen: ca. 10 (vgl. separater Terminplan)

zu 2.2: Bewertungskriterienkatalog

Bewertungskriterium	**Verfügbarkeit**
Fragestellung	Wenn auf die Information zugegriffen werden muss, und dies ist nicht möglich, innert welcher Zeitspanne muss sie dann wieder verfügbar sein?
3 (hohe Verfügbarkeit)	• Zu jedem Zeitpunkt innerhalb einer Stunde
2 (mittlere Verfügbarkeit)	• Spätestens am nächsten Arbeitstag
1 (tiefe Verfügbarkeit)	• Spätestens innerhalb einer Woche
0 (keine Verfügbarkeit)	• Nicht mehr (wird nicht mehr benötigt)
Bewertungskriterium	**Vertraulichkeit**
3 (vertraulich)	• Diese Informationen dürfen nur von einem persönlich bezeichneten und namentlich bekannten Personenkreis verwendet werden, oder • Es kann ein *hoher* Schaden entstehen, wenn diese Informationen ausserhalb dieses Personenkreises bekannt werden, oder • Diese Informationen enthalten besonders schützenswerte Personendaten (Geburtsdatum, Honorar oder Lohn, etc.)
2 (intern prozessgebunden)	• Diese Informationen dürfen nur von Personen verwendet werden, welche im Prozess direkt involviert sind und sie für ihre Arbeit benötigen, oder • Es kann ein Schaden entstehen, wenn diese Informationen ausserhalb dieses Personenkreises bekannt werden.
1 (intern allgemein)	• Diese Informationssammlung darf nur innerhalb der Unternehmung verwendet werden, aber • Es entsteht kein Schaden, wenn diese Informationen ausserhalb der Unternehmung bekannt werden.
0 (öffentlich)	• Keine Vertraulichkeitsanforderungen.

Bewertungskriterium	**Integrität**
3 (hohe Anforderung)	• Inkonsistenzen sind schwer zu entdecken oder verursachen potentiell hohe Schäden und Folgeschäden sind wahrscheinlich.
2 (mittlere Anforderung)	• Inkonsistenzen können mit Aufwand entdeckt werden, es können begrenzbare Schäden und gelegentlich Folgeschäden entstehen.
1 (tiefe Anforderung)	• Inkonsistenzen sind leicht zu erkennen, es können einmalige geringe Schäden entstehen, aber kaum Folgeschäden.
0 (keine Anforderung)	• Inkonsistenzen werden immer entdeckt und es kann kein Schaden oder Folgeschaden entstehen.

Marcus Holthaus, Dersbachstrasse 312a, Hünenberg, CH 6330 Cham, +41 (41) 780 0011, marcus@holthaus.ch,

D Dokumentation zu *ISIGO*

Anhang D enthält zusätzliche Dokumentation zum Werkzeug *ISIGO*. Zunächst wird in Abschnitt D.1 die konkret vorgenommene Implementation von *ISIGO* auf Basis von *MICROSOFT EXCEL* beschrieben. Dabei wird detailliert auf das definierte Datenmodell eingegangen. Selektionsbefehle zur Verknüpfung von *ISIGO* 1.5 und *ISIGO CENTRAL* werden wiedergegeben. Die Funktionen zur Erbringung der Funktionalität von *ISIGO* 1.5 werden summarisch erklärt.

In Anhang D.2 befinden sich zwei Beispiele für Tabellen aus *ISIGO* 1.5, welche Daten eines imaginären Projektes enthalten.

D.1 Implementation

D.1.1 Priorität der Implementation

Wie am Ende von Kapitel 8 ausgeführt wurde, eignet sich *ISIWAY* in der vollen Version (mit vier Detaillierungsgraden) nur bedingt für die Einführung in einem Unternehmen. Da die Erlernbarkeit aber als wichtige Anforderung formuliert wurde, und da angenommen wird, dass pro Unternehmung nur *ein* ISiBe existiert, hängt die Erlernbarkeit sehr stark von dieser einen Person ab. Eine Implementation von *ISIGO CENTRAL* ist deshalb zwar möglich, dient aber nicht unbedingt dem Erkenntnisgewinn, da eine breit abgestützte Betrachtung nicht möglich wäre.

Eine aussagekräftige Untersuchung der Erlernbarkeit von *ISIWAY* und *ISIGO CENTRAL* würde bedingen, dass sich die ISiBes verschiedener Unternehmungen eingehend mit *ISIWAY* und *ISIGO CENTRAL* befassen würden. Dies ist in der zur Verfügung stehenden Zeit nicht zu erreichen. Ausserdem ist nicht nur die Akzeptanz an oberster Position der Unternehmung wichtig, sondern v.a. die Anwendung des Verfahrens und des Werkzeugs "an der Basis", also dort, wo die einzelnen schützenswerten Informationen verarbeitet werden. Entsprechend ist eine Implementation eines Werkzeugs für Informationssicherheitskoordinatoren (ISiKos) derjenigen eines für Informationssicherheitsbeauftragte (ISiBes) vorzuziehen.

Aus diesem Grund wurde die Implementation von *ISIGO 1.5* vorgenommen. Dieses Werkzeug bezieht sich auf die reduzierte Variante *ISIWAY 1.5*. Seine Verteilung und Anwendung wird in der Projektion in Kapitel 10 beschrieben. Für die Verwendung von *ISIGO 1.5* wird auf das separat dokumentierte Verfahren *ISIWAY 1.5* verwiesen (in Anhang C.2 enthalten), in welchem konkrete Bedienungsvorgänge detailliert beschrieben sind.

Technologie

MICROSOFT EXCEL bildet die Basis für *ISIGO 1.5*[112] Es umfasst mehrere Arbeitsblätter, welche als Speicher für die verschiedenen Informationen und Daten dienen und implementiert die Funktionalität in mehr als 1000 Codezeilen Visual Basic. In der Lieferversion enthält es fiktive Daten, welche ein Erlernen und Testen des Produktes ermöglichen und hier zur Dokumentation verwendet werden. Einige Inhalte von *ISIGO* sind in Anhang D.2 beispielhaft wiedergegeben.

Ebenfalls wurde derjenige Teil von *ISIGO CENTRAL* entwickelt, welcher das Datenmodell und die darauf aufbauenden Auswertungen umfasst. Dazu wurde *MICROSOFT ACCESS* als Basis verwendet.

D.1.2 Datenmodell

Das Datenmodell von *ISIGO 1.5* wurde mit Hilfe von *ISIGO CENTRAL* als relationales Modell aufgebaut. Es umfasst eine Teilmenge der gesamten, für *ISIGO CENTRAL* benötigten Daten. Es ist sehr komplex, so dass hier auf eine gesamthafte Darstellung verzichtet wird und wichtige einzelne Entitäten separat vorgestellt werden.

Entitäten

Personen als zentrales Element

Im Zentrum des Datenmodells steht die Entität *Personen* (`B_PER`[113]). Jeder Person können eine oder mehrere Adressen (`B_ADR`) und eine oder mehrere

---

112 Systemvoraussetzungen sind Microsoft Excel 5 bzw. Excel 95 für Macintosh oder Windows 95 / 98 / NT. Auf Excel 98 für Macintosh und Excel 97 für Windows 95 und Windows 98 ist *ISIGO 1.5* ebenfalls lauffähig. Der Start von *ISIGO 1.5* auf einem 200MHz-Pentium-System mit 32 MByte RAM mit Excel 95 unter Windows 98 benötigt ca. 15 Sekunden. Alle Bildschirm-Abbildungen dieses Kapitels sind auf diesem System erstellt worden.

113 Das Datenmodell folgt einigen Konventionen:

- Die Namen aller Entitäten sind dreistellig mit zwei führenden Buchstaben.
- Die Namen der Entitäten mit Ergebnisdaten beginnen mit `D_`
- Die Namen der Entitäten mit Steuerungsdaten beginnen mit `C_`
- Die Namen der Entitäten mit Stammdaten beginnen mit `B_`
- Die Namen aller Attribute der Entitäten beginnen mit dem dreistelligen Namen der Entität (z.B. `PRJ`). Ausnahme: Fremdschlüssel beginnen mit dem dreistelligen Namen der Entität, welche sie referenzieren (z.B. `ADRID`).
- Alle Entitäten enthalten folgende Attribute:
  - `ID` Primärschlüssel
  - `Desc` Beschreibung des Tupels
  - `EntryDat` Datum der Erfassung dieses Tupels
  - `UpdateDat` Datum der letzten Veränderung an diesem Tupel
- Viele Entitäten enthalten zusätzlich folgende Attribute:

Telefonnummern und E-Mail-Adressen (B_PHM) zugewiesen werden (vgl. Abbildung D-1).

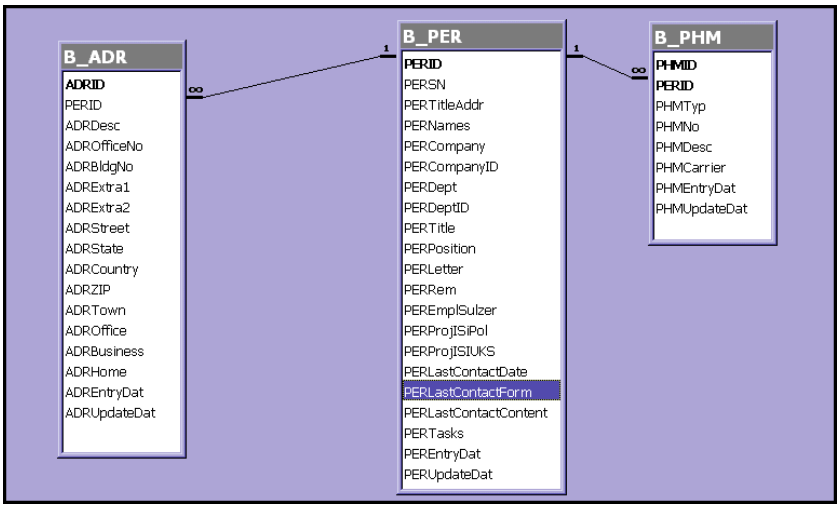


Abbildung D-1: Personen, Adressen, Telefonnummern und E-Mail-Adressen

Projektbezogene Erarbeitung

Die Erfassungsarbeit geschieht projektorientiert, wobei die *Projekte* (C_PRJ) die einzelnen Teilprojekte einer *ISIWAY*-Umsetzung enthalten; deshalb besteht auch ein Selbstbezug zur Unterordnung eines Projektes unter ein anderes (C_PRJ_1[114]). Jedes Projekt wird von einer Person geleitet (Beziehung zu B_PER). Jedes Projekt bezieht sich auf ein Untersuchungsobjekt (D_EXT), welches in der Regel eine Abteilung einer Unternehmung oder ein Produkterstellungsprojekt ist; in D_EXT können noch einige Details dazu festgehalten werden wie z.B. der Verantwortliche des Untersuchungsbereichs (wieder aus B_PER) sowie Anzahl Mitarbeiter und Abgrenzung (vgl. Abbildung D-2).

- CustOrd Eineindeutiger Schlüssel, der vom Benutzer vergeben werden kann und so spezifische Sortierungen erlaubt
- VA Verantwortliche Person
- Rem Bemerkungen
- DetaillationReq Detaillierung dieser Daten ist notwendig

- Verknüpfende Entitäten (Entitäten, welche M:N-Verknüpfungen abbilden) werden mit den beiden dreistelligen Namen der verknüpften Entitäten bezeichnet (z.B. B_REQVAL)

114 Entitäten mit Laufnummern (_1, _2 etc.) sind zusätzliche Darstellungen derselben Entität ohne Laufnummer, um eine mehrfache Beziehung zu verdeutlichen. Wenn also zwischen Entität A und Entität B zwei Beziehungen bestehen wobei jeweils in Entität B der Fremdschlüssel enthalten ist, so wird Entität A doppelt dargestellt (A und A_1). Im hier verwendeten Datenmodell betrifft dies insbesondere B_PER. Die doppelte Darstellung wird auch verwendet, wenn eine Selbstreferenz besteht (z.B. bei sich selbst über- bzw. untergeordneten Entitäten).

Zu jedem Projekt können festgehalten werden: Name, Beschreibung, Pfadangaben[115] für weitere gespeicherte Beschreibungen, Ziel des Projektes, Abgrenzung, Pfad des Projektauftrages, die Art der Unterstützung von Initianten, Sponsoren und Betroffenen, Pfad des Organigramms, Starttermin des Projektes, vorgesehener und tatsächlicher Endtermin sowie Bemerkungen.

Jedes Projekt befindet sich ausserdem in einem Zustand, welcher durch einen Verweis auf die aktuelle Aktivität (C_ACT) festgehalten wird (vgl. unten). In jedem Projekt werden verschiedene Personen in verschiedenen Rollen involviert. Diese dreifache Beziehung wird in C_PRJPERROL abgebildet, indem eine Beziehung zwischen Projekten (C_PRJ), Personen (B_PER) und Rollen (B_ROL) hergestellt wird. Die Rollen entsprechen dem in Abschnitt 4.2.3 (Seite 116) vorgestellten und in Abbildung 8-3 (Seite 228) abgebildeten Rollenmodell.

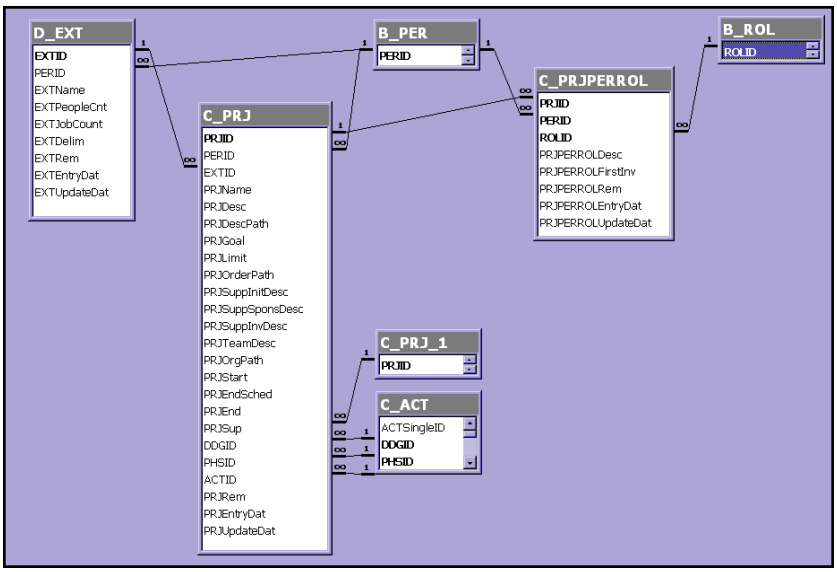


Abbildung D-2: Projekte, Untersuchungsobjekte und Teilnahme

Ergebnisdaten: Vorgehen bei der Erfassung

Die Erhebung der Ergebnisdaten (Prozesse, Informationssammlungen, Informationssysteme etc.) geschieht immer durch Auskunft einer befragten Person, deren Identität sowie Zeitpunkt der Auskunft im jeweiligen Datensatz festgehalten werden. Diese Person muss nicht selbst der Ansprechpartner sein, kann jedoch einen Ansprechpartner angeben. Die Erhebung ist jedoch nicht gültig, bevor dieser Ansprechpartner sie nicht visiert hat und so zu erkennen gegeben hat, dass er diese Rolle wahrnimmt. Darüber hinaus kann bei jeder Erhebung immer noch eine Vertiefung (Detaillierung) notwendig sein, wozu ein entsprechendes Attribut vorgesehen ist.

---

115 Mit "Pfad" ist die Spezifikation eines Dateinamens mit Verzeichnis in einem Dateisystem eines Computers gemeint.

Bei den Bewertungen und Zuordnungen erlaubt es *ISIGO* gleichermassen, verschiedene Auskünfte festzuhalten. Verbindlich sind jedoch nur die Auskünfte des jeweiligen Ansprechpartners des Objekts. Wenn also beispielsweise der erste Interviewpartner angibt, dass er an ein Objekt eine hohe Vertraulichkeits-anforderung stellt, kann dies in *ISIGO* festgehalten werden. Wenn er jedoch gleichzeitig eine andere Person als Ansprechpartner für dieses Objekt angibt, ist diese Bewertung irrelevant.

Ergebnisdaten: Prozesse

Die Erhebung der Elemente des Untersuchungsobjekts beginnt mit den Prozessen (D_PRC). Jeder Prozess gehört zu einem Untersuchungsobjekt (D_EXT). Die Erhebung geschieht durch Auskunft einer Person (eines Interviewpartners aus B_PER). Prozessname und -beschreibung sowie eine eindeutige Bezeichnung werden festgehalten. Eine Unterordnung dieses Prozesses unter einen anderen ist möglich (D_PRC_1). Der Prozess-Owner ist wieder eine Person aus B_PER. Weitere Details wie Kostenstelle, Anteil am Gesamtvolumen sowie Bemerkungen werden festgehalten (vgl. Abbildung D-3).

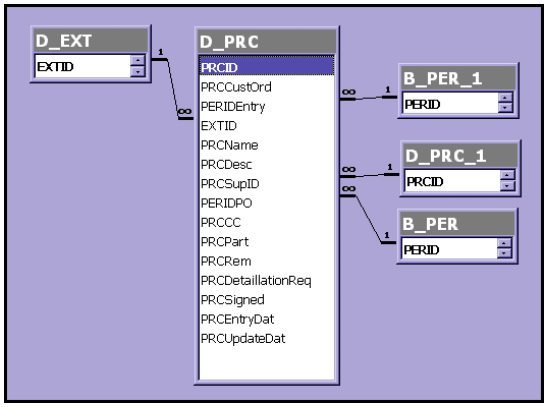


Abbildung D-3: Prozesse

Ergebnisdaten: Informationssammlungen

Die Erhebung der Informationssammlungen (D_ICL) geschieht sinngemäss (vgl. Abbildung D-4). Auch hier werden allgemeine Eigenschaften wie Name, Beschreibung, Typ, Datenvolumen und spezifische Bezeichnung festgehalten. Die Zuweisung des Interviewpartners geschieht aus B_PER, ebenso die des Ansprechpartners (Info Owner). Zusätzlich wird festgehalten, zu welchem Prozess die Informationssammlung gehört (D_PRC). Der Standort wird als Verweis auf eine Adresse (B_ADR) festgehalten. Auch die hierarchische Anordnung von Informationssammlungen ist möglich (Beziehung zu D_ICL_1).

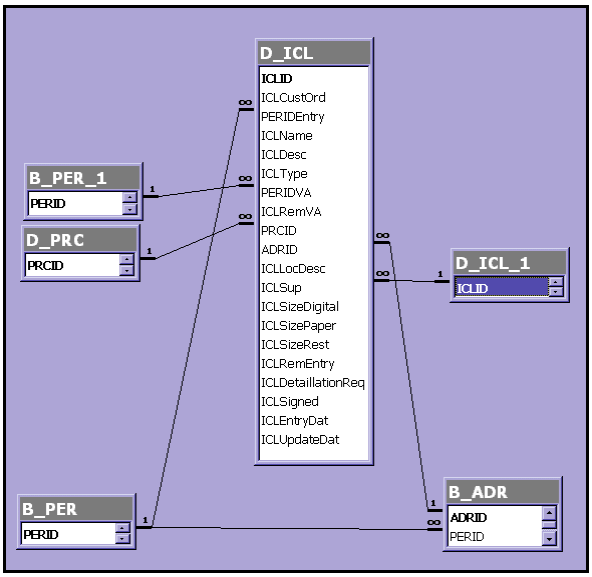


Abbildung D-4: Informationssammlungen

Ergebnisdaten: Bewertung

Die Informationssammlungen werden bewertet. Dazu wird auf die Bewertungskriterien zurückgegriffen, die in B_REQ erfasst wurden (meist sind dies die drei grundlegenden "Verfügbarkeit", "Vertraulichkeit" und "Integrität"). Sie sind in B_REQ mit Name, Beschreibung, Minimal- und Maximalwerten und Bemerkungen erfasst. Zusätzlich ist erfasst, ob eine kontinuierliche Wertzuweisung erlaubt ist (z.B. Wert *2.45*) und eine Fragestellung festgehalten, anhand derer die Wertzuteilung bestimmt werden kann.

In B_REQVAL sind die Bedeutungen von üblichen Bewertungen festgehalten. Beispielsweise wird dort festgelegt, dass der Wert 3 für Vertraulichkeit "Hohe Vertraulichkeitsanforderung" bedeutet. Dazu werden die möglichen Konsequenzen einer Nichterfüllung dieser Anforderung noch zusätzlich beschrieben.

Die Bewertung der Informationssammlungen geschieht durch Zuteilung von Werten aus B_REQVAL in den Kriterien, die in B_REQ festgehalten wurden. Dies wird für die Informationssammlungen in der Bewertungstabelle D_ICLREQ festgehalten. Zusätzlich wird dort verzeichnet, wer diese Bewertung vornahm (aus B_PER), wieviel Prozent der Informationssammlung von dieser Bewertung betroffen ist sowie weitere Bemerkungen. Eine Kombination von Informationssammlungen und Bewertungen wird in der Abfrage K_ICLREQ kombiniert (vgl. Abbildung D-5, Abbildung D-6).

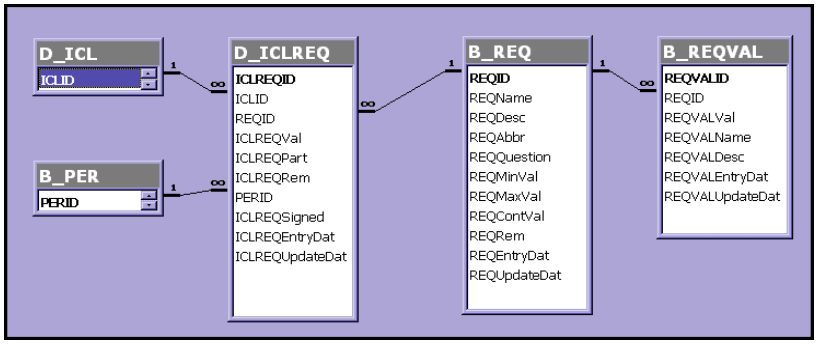


Abbildung D-5: Bewertungskriterien, Werte und Bewertung von Informationssammlungen

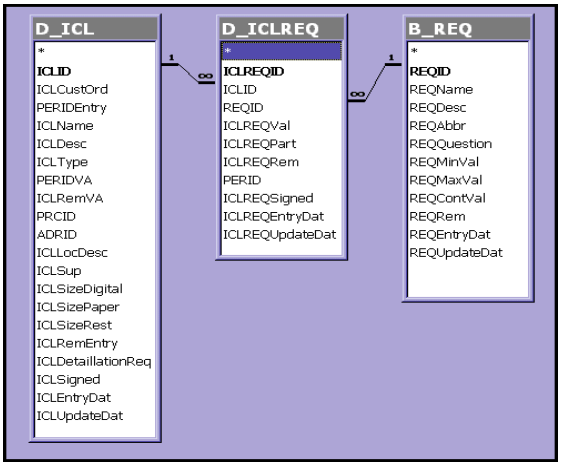


Abbildung D-6: Anforderungen der Informationssammlungen

Ergebnisdaten: Informationssysteme

Die Erhebung der Informationssysteme geschieht zweistufig: Es wird konsequent zwischen einer technischen und einer benutzerorientierten Sicht unterschieden. Beispielsweise nimmt ein Benutzer ein E-Mail-System wahr, mit welchem er seine E-Mail-Daten bearbeitet. Aus technischer Sicht besteht dieses aus einer lokalen oder zentralen Datenablage (Fileserver), einem E-Mail-Programm, einer Netzwerkverbindung, einem zentralen E-Mail-Adressenverzeichnis etc. Ziel dieser Trennung ist es also, von der Benutzersicht auszugehen und eine Verbindung zwischen technischer und benutzerorientierter Sicht herzustellen.

Die Informationssysteme werden aus Benutzersicht zunächst in D_ITU erfasst. Auch hier ist die Erfassung von benutzerspezifischer Bezeichnung, Name, Beschreibung, technischer Beschreibung, Standort (aus B_ADR) mit Detaillierung, inhaltlichen und technischen Bemerkungen vorgesehen. Zunächst wird der Interviewpartner (aus B_PER) festgehalten. Er weist auf einen Benutzer-administrator hin (meist ein sogenannter *Power-User*, ein technischer Koordinator o.a.), der ebenfalls festgehalten wird (aus B_PER). Dieser wiederum muss die Erfassung signieren und damit seine Rolle als Benutzersystemverantwortlicher anerkennen, hält aber zusätzlich die Person fest, welche über die dahinter liegenden einzelnen technischen Systeme informieren kann (Systemadmin aus B_PER).

Es ist nun Aufgabe des Systemadmins, die technischen Systeme zu erfassen (D_SYS). Neben spezifischer Bezeichnung, Name, allgemeiner und technischer Beschreibung, Standort (aus B_ADR) sowie inhaltlichen und technischen Bemerkungen ist es auch hier notwendig, dass der Systemadmin diese Erfassung signiert.

Die Bewertung geschieht in der Tabelle D_SYSREQ. Hier werden die Bewertungen in den einzelnen Bewertungskriterien (aus B_REQ) eingetragen und den bewerteten Systemen (aus D_SYS) zugeordnet. Dabei wird nicht bewertet, welche Anforderungen an die entsprechenden Systeme gestellt werden, sondern welche Anforderungen diese Systeme in den Kriterien maximal erfüllen können. Dies wird als *Sicherheitsleistung* des Systems bezeichnet. Auch hier wird wieder die Person festgehalten, welche die Bewertung vorgenommen hat (aus B_PER) und ob diese sie signiert hat.

Schliesslich müssen die Systemadministratoren sich mit dem Benutzersystem-verantwortlichen gemeinsam darauf einigen, welche technischen Systeme notwendig sind, um das vom Benutzer gesehene System bereitzustellen. Diese Abbildung wird in der Tabelle D_ITUSYS festgehalten. Der Benutzersystem-verantwortliche ist letztlich der Ansprechpartner für diese Zuteilung, so dass dies nicht extra festgehalten und signiert werden muss (vgl. Abbildung D-7).

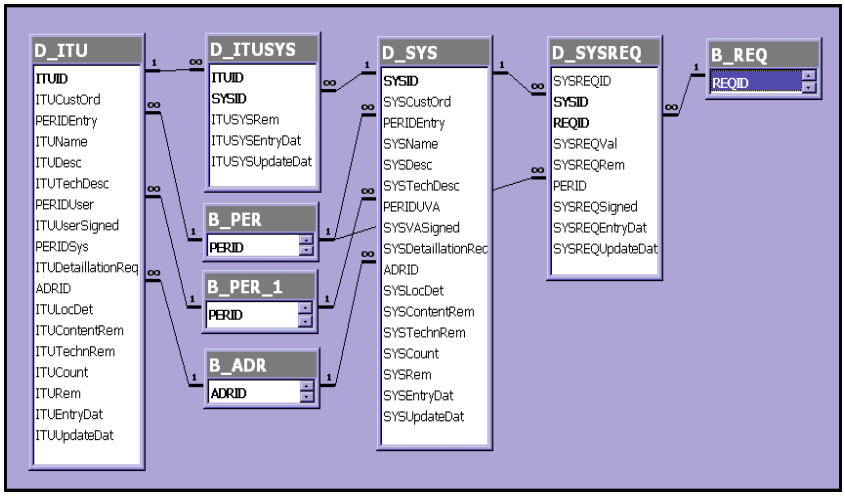


Abbildung D-7: Informationssysteme aus technischer und benutzerorientierter Sicht, deren Verknüpfung und Bewertung

Die Bewertung der einzelnen Systeme aus Benutzersicht erfolgt nun durch Vererbung aus der technischen Sicht und kann automatisiert werden. Die Zusammenfassung der Bewertungen der technischen Systeme geschieht in der Abfrage K_SYSREQ. Diese wird mit den Systemen aus Benutzersicht (D_ITU) und deren Verknüpfung (D_ITUSYS) in K_ITUREQ kombiniert, wobei jeweils der Minimalwert der Bewertungen gebildet wird. K_ITUREQ zeigt also die Sicherheitsleistung des Systems an (vgl. Abbildung D-8).

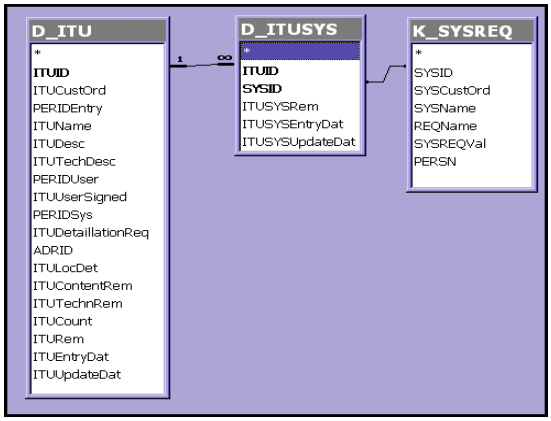


Abbildung D-8: Sicherheitsleistung der Systeme

Ergebnisdaten: Diskrepanzen

Ziel der Erfassung ist es, Unterschiede zwischen Sicherheitsanforderungen (an die erfassten Informationssammlungen) und der Sicherheitsleistung (der erfassten Informationssysteme) zu identifizieren (Diskrepanzen) – also Handlungsbedarf aufzuzeigen. Dazu muss für jede Informationssammlung festgehalten werden, mit welchem Informationssystem sie verarbeitet wird. Diese Zuordnung geschieht in `D_ICLITU` durch den jeweiligen Info Owner (vgl. Abbildung D-9).

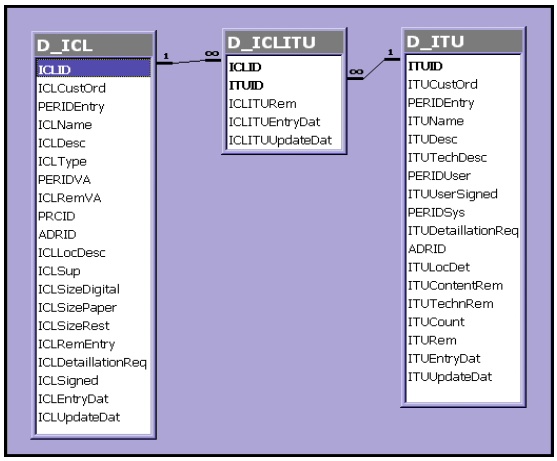


Abbildung D-9: Verknüpfung von Informationssammlungen und Informationssystemen (Bearbeitung)

Die Herleitung der Diskrepanzen kann nun wieder automatisiert werden. Dies geschieht mit der Abfrage `K_ICLREQITUREQ` (vgl. Abbildung D-10). Sie vergleicht die Anforderungen an die Informationssammlungen mit den Sicherheitsleistungen der Systeme, mit denen sie verarbeitet werden und zeigt diejenigen Kombinationen an, welche hier Diskrepanzen aufweisen (d.h. höhere Anforderungen als Leistungen). Die Diskrepanz wird als Wert ausgewiesen sowie in zwei Gruppen geteilt: Diskrepanzen grösser als 1 und Diskrepanzen darunter. Dies erlaubt eine Priorisierung der Massnahmen. Ziel des gesamten Sicherheitsprojektes ist es, diese Diskrepanzen zu eliminieren.

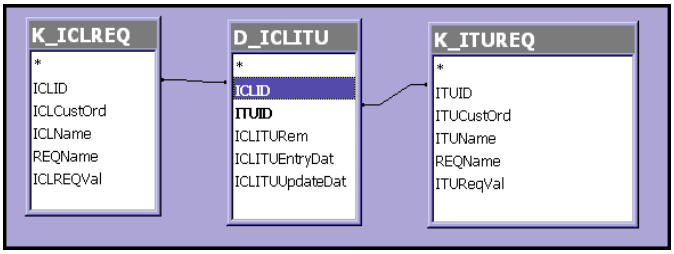


Abbildung D-10: Herleitung der Diskrepanzen

Bedrohungen

Die Erfassung der Bedrohungen erfolgt in D_THR. Hier ist es möglich, unbestimmte Bedrohungen zu erfassen (Gefahren), oder einer Bedrohung eine oder mehrere Informationssammlungen (D_THRICL) oder Informationssysteme (D_THRITU) zuzuweisen (vgl. Abbildung D-11). X_Bedrohungen[116] fasst dies zusammen.

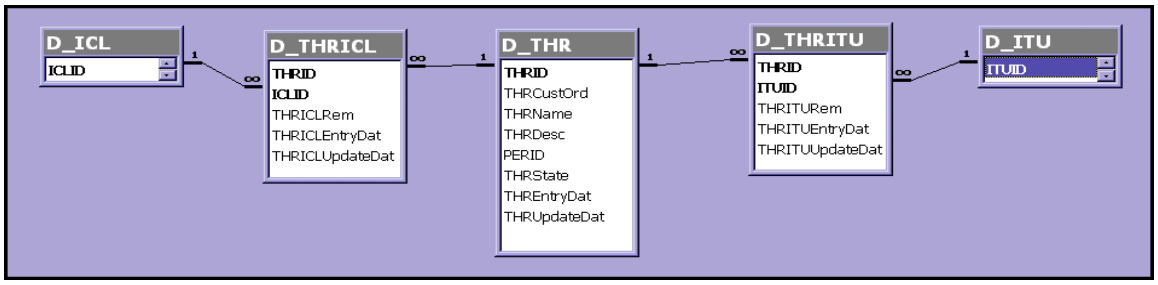


Abbildung D-11: Bedrohungen

Vorfälle

Die Erfassung der Vorfälle erfolgt in D_EVT. Neben Bezeichnung und Beschreibung können Zeitraum und Anzahl festgehalten werden. X_Vorfaelle fasst dies zusammen.

Massnahmen

Angewendete und anzuwendende Massnahmen werden in D_CTR erfasst. Dabei werden Bezeichnung, Beschreibung und Urheber der Massnahme erfasst, ausserdem ihr Status mit Terminen (geplanter und tatsächlicher Umsetzungsstart und -abschluss), Kosten, sowie die Identitäten der betroffenen Personen (Info Owner und Systemadministratoren aus B_PER) und ihre Visa. Welches System durch diese Massnahme wie beeinflusst wird (Veränderung der Sicherheitsleistung in einem Kriterium) wird in D_CTRSYSREQ (vgl. Abbildung D-12) festgehalten und in K_CTRSYSREQ (vgl. Abbildung D-13) kombiniert dargestellt. Wenn Massnahmen nachweislich wirken (dies wird im Statusfeld festgehalten) kann der entsprechende

116 Die mit X_ beginnenden Abfragen von *ISIGO CENTRAL* enthalten die Daten der gleichnamigen (ohne X_) Tabellen von *ISIGO 1.5*.

Wert des Systems verändert werden (die Sicherheitsleistung des Systems steigt also). X_Massnahmen fasst diese Informationen zusammen.

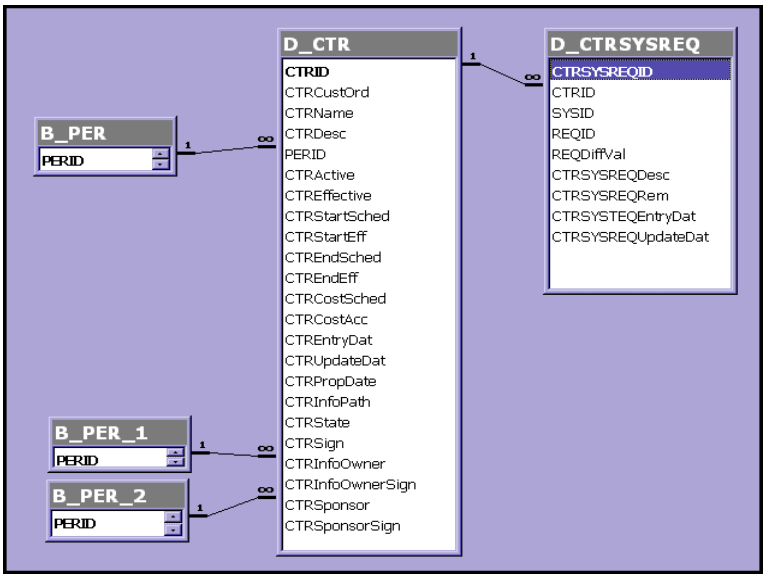


Abbildung D-12: Massnahmen und ihre Beeinflussung der Sicherheitsleistung der Systeme

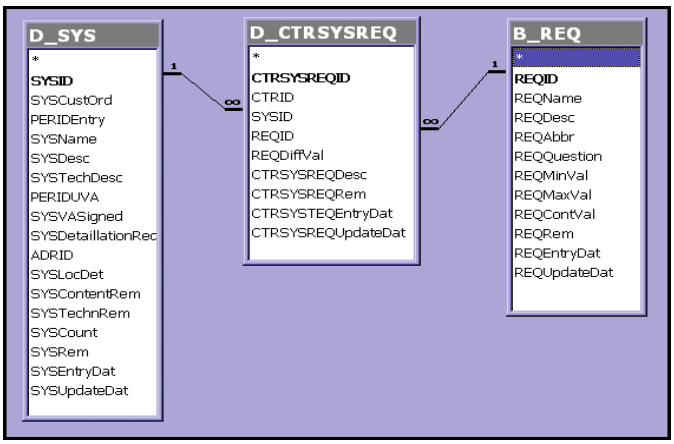


Abbildung D-13: Zusammenfassung der Beeinflussung der Sicherheitsleistung des Systems

Aktivitäten, Phasen und Detaillierungsgrade

Angaben zur Steuerung des Ablaufes von *ISIWAY* finden sich in den Tabellen *Detaillierungsgrade* (C_DDG), *Phasen* (C_PHS) und *Aktivitäten* (C_ACT) sowie deren Kombinationen. In C_DDG werden die Detaillierungsgrade gesamthaft jeweils mit Name und Ziel festgehalten. C_PHS beschreibt die fünf Phasen der Detaillierungsgrade (PEAUK) generisch (bzw. sechs bei *ISIWAY 1.5*). C_DDGPHS beschreibt dann die Phasen spezifisch für jeden Detaillierungsgrad und in C_ACT werden alle Aktivitäten einzeln mit Name, Ziel, Beschreibung, Resultat, Voraussetzungen, Rahmenbedingungen und Bemerkungen festgehalten. C_PHSROL umfasst generische Beschreibungen der Aufgaben der einzelnen Rollen in den Phasen.

Abbildung des Datenmodells in *ISIGO* 1.5

Das Datenmodell bildet mehr Elemente ab, als für *ISIGO 1.5* notwendig sind. Für *ISIGO CENTRAL* werden jedoch weitere Elemente benötigt, die hier nicht dargestellt sind.

Die Tabellen von *ISIGO 1.5* lassen sich nun einfach aus dem Datenmodell herleiten. Es entsteht die Zuordnung gemäss Tabelle D-1.

Tabelle *ISIGO 1.5*	Auswertung *ISIGO CENTRAL*
Willkommen	-[117]
Allgemeine Projektangaben	X_AllgemeineProjektangaben
Projektplanung	X_Projektplanung
Adressen	X_ Adressen
Termine	X_ Termine
Massnahmenkatalog	X_Massnahmenkatalog
Prozesse	X_Prozesse
Infosammlungen	X_ Infosammlungen
Infosysteme	X_Infosysteme
Bedrohungen	X_Bedrohungen
Vorfälle	X_Vorfaelle
Massnahmen	X_Massnahmen
Statistik	-[118]
Bewertungskriterien	X_Bewertungskriterien
Phasen	X_Phasen
Aktivitäten	X_Aktivitaeten
ISIWAY	-[119]
Systemdaten	-[120]

Tabelle D-1: Zuordnung von *ISIGO 1.5*-Tabellen und *ISIGO CENTRAL*-Abfragen

Die Tabellen von *ISIGO 1.5* sowie die auf den Abfragen basierenden Berichte von *ISIGO CENTRAL* sind nachfolgend wiedergegeben.

Wichtige Selektionen mit SQL-Befehlen

Die hier angegebenen Auswertungen stellen die Verbindung zwischen *ISIGO CENTRAL* und *ISIGO 1.5* her. Sie sind hier als SQL-Select-Befehle wiedergegeben. Ihre Ausführung in *ISIGO CENTRAL* produziert genau diejenigen Angaben, welche in den Tabellen von *ISIGO 1.5* enthalten sind und ein Subset aller relevanten

---

117 Die Tabelle "Willkommen" enthält keine Daten, sondern nur Bedienungshinweise spezifisch für *ISIGO 1.5*.

118 Die Tabelle "Statistik" enthält Zusammenfassungen von Werten, welche in *ISIGO CENTRAL* auf andere Weise in einer Maske zusammengefasst werden sollen. Diese Tabelle ist also spezifisch für *ISIGO 1.5*.

119 Die Tabelle "*ISIWAY*" enthält die Darstellung der *ISIWAY*-Spirale bzw. des aktuell bearbeiteten Detaillierungsgrads. Sie ist deshalb spezifisch für *ISIGO 1.5*.

120 Die Tabelle "Systemdaten" enthält spezifische Ablage- und Darstellungsdaten für *ISIGO 1.5*.

Informationen darstellen. Die Bezeichnung dieser SQL-Befehle folgt der Bezeichnung der Tabellen in *ISIGO 1.5* und entspricht Tabelle D-1.

X_AllgemeineProjektangaben

```
SELECT              C_PRJ.PRJName,
                    C_PRJ.PRJDesc,
                    C_PRJ.PRJOrderPath,
                    C_PRJ.PRJSuppInitDesc,
                    C_PRJ.PRJSuppSponsDesc,
                    C_PRJ.PRJSuppInvDesc,
                    C_PRJ.PRJTeamDesc,
                    C_PRJ.PRJOrgPath,
                    C_PRJ.PRJRem,
                    C_PRJ.DDGID,
                    "A"+C_PRJ.PHSID+"."+C_PRJ.ACTID AS ActNo,
                    B_PER.PERSN,
                    C_PRJ.PRJSup,
                    C_PRJ.PRJID
FROM                B_PER
INNER JOIN          C_PRJ
ON                  B_PER.PERID = C_PRJ.PERID;
```

X_Projektplanung

```
SELECT              C_PRJ.PRJDescPath,
                    C_PRJ.PRJGoal,
                    C_PRJ.PRJLimit,
                    C_PRJ.PRJStart,
                    C_PRJ.PRJEndSched,
                    C_PRJ.PRJEnd
FROM                C_PRJ;
```

X_ Adressen

```
SELECT              C_PRJ.PRJID,
                    B_PER.PERSN,
                       B_PHM.PHMTyp+" "+B_PHM.PHMNo AS TelNo,
                     B_PHM_1.PHMTyp+" "+B_PHM_1.PHMNo AS EMail,
                    [B_ROL].[ROLName]+", "+[C_PRJPERROL].[PRJPERROLDesc] AS
                    RolInProj,
                    [B_PER].[PERCompany]+", "+[B_PER].[PERDept]+",
                    "+[B_PER].[PERPosition] AS OrgAbtPos,
                    C_PRJPERROL.PRJPERROLFirstInv,
                    Format$([PERTitleAddr])+" "+Format$([PERNames])+", "+[AdrRef] AS
                    Adr,
                    B_PER.PERRem
FROM                (C_PRJ
INNER JOIN          (B_ROL
INNER JOIN          ((B_ADRRef
RIGHT JOIN          (B_PER
LEFT JOIN           B_PHM
ON                  B_PER.PERID = B_PHM.PERID)
ON                  B_ADRRef.PERID = B_PER.PERID)
INNER JOIN          C_PRJPERROL
ON                  B_PER.PERID = C_PRJPERROL.PERID)
ON                  B_ROL.ROLID = C_PRJPERROL.ROLID)
ON                  C_PRJ.PRJID = C_PRJPERROL.PRJID)
LEFT JOIN           B_PHM AS B_PHM_1
ON                  B_PER.PERID = B_PHM_1.PERID
WHERE               (((C_PRJ.PRJID)=[Welches Projekt (ID)?])
AND                 ((B_PHM.PHMTyp)<>"I")
AND                 ((B_PHM_1.PHMTyp)="I"))
ORDER BY            B_PER.PERSN;
```

X_ Termine

```
SELECT              C_MTG.ACTRef,
                    B_PER.PERSN,
                    C_MTG.MTGName,
                    C_MTG.MTGDate,
                    C_MTG.MTGDesc,
                    C_MTG.MTGState,
                    C_MTG.MTGRem,
                    C_MTG.MTGTime,
                    C_MTG.MTGExpenses,
                    C_MTG.MTGDataExportPath,
                    B_ADRRef.ADRRef,
                    C_MTGCTR.CTRID
FROM                ((B_ADRRef
RIGHT JOIN          C_MTG
ON                  B_ADRRef.ADRID = C_MTG.MTGADR)
LEFT JOIN           C_MTGCTR
ON                  C_MTG.MTGID = C_MTGCTR.MTGID)
INNER JOIN          (B_PER
INNER JOIN          C_MTGPER
ON                  B_PER.PERID = C_MTGPER.PERID)
ON                  C_MTG.MTGID = C_MTGPER.MTGID;
```

X_Massnahmenkatalog

```
SELECT              B_CTC.CTCID,
                    B_CTC.CTCName,
                    B_CTCREQ.REQID,
                    B_CTCREQ.CTCREQVal,
                    B_CTC.CTCType,
                    B_CTC.CTCDesc
FROM                B_CTCREQ
RIGHT JOIN          B_CTC
ON                  B_CTCREQ.CTCID = B_CTC.CTCID;
```

X_Prozesse

```
SELECT              D_PRC.PRCCustOrd,
                    B_PER_1.PERSN,
                    D_PRC.PRCName,
                    D_PRC.PRCDesc,
                    B_PER.PERSN,
                    D_PRC.PRCRem,
                    D_PRC.PRCDetaillationReq,
                    D_PRC.PRCSigned
FROM                (D_EXT
INNER JOIN          C_PRJ
ON                  D_EXT.EXTID = C_PRJ.EXTID)
INNER JOIN          (B_PER
INNER JOIN          (B_PER AS B_PER_1
INNER JOIN          D_PRC
ON                  B_PER_1.PERID = D_PRC.PERIDEntry)
ON                  B_PER.PERID = D_PRC.PERIDPO)
ON                  D_EXT.EXTID = D_PRC.EXTID
WHERE               (((C_PRJ.PRJID)=[Welches Projekt (ID)?]))
ORDER BY            D_PRC.PRCCustOrd;
```

X_ Infosammlungen

```
SELECT                D_ICL.ICLCustOrd,
                      B_PER_1.PERSN,
                      D_ICL.ICLName,
                      D_ICL.ICLDesc,
                      D_ICL.ICLType,
                      B_PER.PERSN,
                      D_PRC.PRCCustOrd,
                      D_ICL.ICLDetaillationReq,
                      B_ADRRef.ADRRef,
                      D_ICL.ICLLocDesc,
                      D_ICL.ICLSizeDigital,
                      D_ICL.ICLRemEntry,
                      D_ICL.ICLSigned,
                      D_ICL.ICLEntryDat,
                      B_REQ.REQName,
                      D_ICLREQ.ICLREQVal,
                      B_PER_2.PERSN,
                      D_ICLREQ.ICLREQSigned,
                      D_ICLREQ.ICLREQEntryDat,
                      K_ICLREQITUREQ.Diskrepanz,
                      K_ICLREQITUREQ.DiskBis1,
                      K_ICLREQITUREQ.DiskAb1,
                      K_ICLREQITUREQ.ITUCustOrd
FROM                  B_REQ
INNER JOIN            (D_PRC
INNER JOIN            (B_PER
INNER JOIN            (((D_ICL AS D_ICL_1
RIGHT JOIN            (B_ADRRef
RIGHT JOIN            (B_PER AS B_PER_1
INNER JOIN            D_ICL
ON                    B_PER_1.PERID = D_ICL.PERIDEntry)
ON                    B_ADRRef.ADRID = D_ICL.ADRID)
ON                    D_ICL_1.ICLID = D_ICL.ICLSup)
LEFT JOIN             K_ICLREQITUREQ
ON                    D_ICL.ICLID = K_ICLREQITUREQ.ICLID)
INNER JOIN            (B_PER AS B_PER_2
INNER JOIN            D_ICLREQ
ON                    B_PER_2.PERID = D_ICLREQ.PERID)
ON                    D_ICL.ICLID = D_ICLREQ.ICLID)
ON                    B_PER.PERID = D_ICL.PERIDVA)
ON                    D_PRC.PRCID = D_ICL.PRCID)
ON                    B_REQ.REQID = D_ICLREQ.REQID
ORDER BY              D_ICL.ICLCustOrd,
                      B_REQ.REQName;
```

X_Infosysteme

```
SELECT              D_ITU.ITUCustOrd,
                    B_PER.PERSN,
                    D_ITU.ITUName,
                    D_ITU.ITUDesc,
                    B_PER_1.PERSN,
                    D_ITU.ITUDetaillationReq,
                    D_SYS.SYSCustOrd,
                    B_PER_2.PERSN,
                    B_ADRRef.ADRRef,
                    D_ITU.ITUCount,
                    D_SYS.SYSName,
                    D_SYS.SYSDesc,
                    D_SYS.SYSTechDesc,
                    D_ITU.ITURem,
                    D_ITU.ITUEntryDat,
                    D_ITU.ITUUserSigned,
                    B_PER_4.PERSN,
                    D_SYS.SYSRem,
                    K_ITUREQ.REQName,
                    K_ITUREQ.ITUReqVal,
                    D_SYS.SYSVASigned,
                    K_ICLREQITUREQ.Diskrepanz,
                    K_ICLREQITUREQ.DiskBis1,
                    K_ICLREQITUREQ.DiskAb1,
                    K_ICLREQITUREQ.ICLCustOrd
FROM                (B_PER AS B_PER_4
RIGHT JOIN          (B_PER AS B_PER_2
RIGHT JOIN          D_SYS
ON                  B_PER_2.PERID = D_SYS.PERIDEntry)
ON                  B_PER_4.PERID = D_SYS.PERIDUVA)
INNER JOIN          ((B_PER
RIGHT JOIN          (B_ADRRef
RIGHT JOIN          (B_PER AS B_PER_1
RIGHT JOIN          ((D_ITU
LEFT JOIN           K_ITUREQ
ON                  D_ITU.ITUID = K_ITUREQ.ITUID)
LEFT JOIN           K_ICLREQITUREQ
ON                  D_ITU.ITUID = K_ICLREQITUREQ.ITUID)
ON                  B_PER_1.PERID = D_ITU.PERIDUser)
ON                  B_ADRRef.ADRID = D_ITU.ADRID)
ON                  B_PER.PERID = D_ITU.PERIDEntry)
INNER JOIN          D_ITUSYS
ON                  D_ITU.ITUID = D_ITUSYS.ITUID)
ON                  D_SYS.SYSID = D_ITUSYS.SYSID;
```

X_Bedrohungen

```
SELECT              D_THR.THRCustOrd,
                    B_PER.PERSN,
                    D_THR.THRName,
                    D_THR.THRDesc,
                    K_THRICL.ICLCustOrd,
                    K_THRICL.ICLName,
                    K_THRITU.ITUCustOrd,
                    K_THRITU.ITUName,
                    D_THR.THRState
FROM                ((D_THR
LEFT JOIN           K_THRICL
ON                  D_THR.THRID = K_THRICL.THRID)
LEFT JOIN           K_THRITU
ON                  D_THR.THRID = K_THRITU.THRID)
INNER JOIN          B_PER
ON                  D_THR.PERID = B_PER.PERID;
```

X_Vorfaelle

```
SELECT              D_EVT.EVTCustOrd,
                    B_PER.PERSN,
                    D_EVT.EVTName,
                    D_EVT.EVTDesc,
                    D_EVT.EVTFrom,
                    D_EVT.EVTTo,
                    D_EVT.EVTCount,
                    D_EVT.EVTEntryDat
FROM                B_PER
INNER JOIN          D_EVT
ON                  B_PER.PERID = D_EVT.PERID;
```

X_Massnahmen

```
SELECT              D_CTR.CTRCustOrd,
                    B_PER.PERSN,
                    D_CTR.CTRName,
                    D_CTR.CTRDesc,
                    K_CTRSYSREQ.SYSCustOrd,
                    K_CTRSYSREQ.REQName,
                    K_CTRSYSREQ.REQDiffVal,
                    D_CTR.CTREntryDat,
                    D_CTR.CTRPropDate,
                    D_CTR.CTRCostAcc,
                    D_CTR.CTRStartSched,
                    D_CTR.CTREndSched,
                    D_CTR.CTRInfoPath,
                    D_CTR.CTRState,
                    D_CTR.CTRSign,
                    B_PER_1.PERSN,
                    D_CTR.CTRInfoOwnerSign,
                    B_PER_2.PERSN,
                    D_CTR.CTRSponsorSign
FROM                B_PER
INNER JOIN          ((B_PER AS B_PER_2
RIGHT JOIN          (B_PER AS B_PER_1
RIGHT JOIN          D_CTR
ON                  B_PER_1.PERID = D_CTR.CTRInfoOwner)
ON                  B_PER_2.PERID = D_CTR.CTRSponsor)
LEFT JOIN           K_CTRSYSREQ
ON                  D_CTR.CTRID = K_CTRSYSREQ.CTRID)
ON                  B_PER.PERID = D_CTR.PERID;
```

X_Bewertungskriterien

```
SELECT              B_REQ.REQID,
                    B_REQ.REQName,
                    B_REQ.REQMinVal,
                    B_REQ.REQMaxVal,
                    B_REQ.REQAbbr,
                    B_REQ.REQRem
FROM                B_REQ;
```

X_Phasen

```
SELECT              C_DDGPHS.DDGID,
                    C_DDGPHS.PHSID,
                    C_DDGPHS.PHSName,
                    Format$([PHSGoal]) AS [Desc],
                    Count(C_ACT.ACTID) AS [Anzahl von ACTID],
                    "DG"+[C_DDGPHS].[DDGID]+"-P"+[C_DDGPHS].[PHSID] AS [DG-PHS]
FROM                C_DDGPHS
INNER JOIN          C_ACT
ON                  (C_DDGPHS.PHSID = C_ACT.PHSID)
AND                 (C_DDGPHS.DDGID = C_ACT.DDGID)
GROUP BY            C_DDGPHS.DDGID,
                    C_DDGPHS.PHSID,
                    C_DDGPHS.PHSName,
                    Format$([PHSGoal]),
                    "DG"+[C_DDGPHS].[DDGID]+"-P"+[C_DDGPHS].[PHSID];
```

X_Aktivitaeten

```
SELECT              C_ACT.DDGID,
                    C_ACT.PHSID,
                    C_ACT.ACTID,
                    C_ACT.ACTName,
                    C_ACT.ACTGoal,
                    C_ACT.ACTDesc,
                    C_ACT.ACTResult,
                    "DG"+[DDGID]+"-P"+[PHSID] AS DHPHS,
                    C_ACTROL.ROLID,
                    C_ACT.ACTPrereq,
                    C_ACT.ACTEnv,
                    C_ACT.ACTRem
FROM                C_ACTROL
INNER JOIN          C_ACT
ON                  C_ACTROL.ACTSingleID = C_ACT.ACTSingleID
WHERE               (((C_ACT.DDGID)<>"1.5"
AND                 (C_ACT.DDGID)<>"3.5"));
```

D.1.3 Funktionsbeschreibung

Informationen und Daten

ISIGO 1.5 verwaltet die Informationen und Daten in Tabellen der Tabellenkalkulation. Der Eröffnungsbildschirm ist in Abbildung D-14 (Seite 447) wiedergegeben; man beachte insbesondere die "Reiter" am unteren Tabellenrand, welche die einzelnen Tabellen identifizieren.

Ergebnisdaten

Für die Ergebnisdaten besteht je eine Tabelle für *Prozesse, Informationssammlungen u*nd *Informationssysteme*. Darüber hinaus bestehen (zur Unterstützung von *ISIWAY 1.5*) weitere Ergebnisdatentabellen für *Bedrohungen, Vorfälle* und *Massnahmen*.

Steuerungsdaten

Die Steuerungsdaten sind in den Tabellen *Willkommen*, *Allgemeine Projektangaben, Projektplanung, Termine, Statistik, Phasen, Aktivitäten* und *ISIWAY* enthalten.

Beim Start von *ISIGO 1.5* erscheint die Tabelle *Willkommen*, welche einen kurzen Begrüssungstext enthält und auf das von *ISIGO 1.5* eingerichtete neue Menu *ISIGO* hinweist. Dieses Menu implementiert die zentrale Funktionswahl (vgl. Abbildung D-15).

In den *Allgemeinen Projektangaben* werden übergreifende Informationen wie Projektname, Kurzbeschreibung und Ergebnisse der Vorbereitungsarbeiten (entspricht Phase 1 von *ISIWAY 1.5*) abgelegt.

Die *Projektplanung* enthält Angaben über Ziel, Start- und Endtermin des Projektes

Die Tabelle *Termine* erlaubt die Eingabe von Terminen zur Erhebung, Bewertung oder beliebigen anderen Besprechungen.

Die *Statistik* fasst die Resultate der automatischen Auswertungen zusammen.

Die Tabellen *Phasen* und *Aktivitäten* enthalten alle Phasen- und Aktivitätendefinitionen nicht nur von *ISIWAY 1.5*, sondern auch für die anderen *ISIWAY*-Detaillierungsgrade.

Die Tabelle *ISIWAY* enthält eine anpassbare Darstellung des aktuell durchlaufenen Detaillierungsgrades (vgl Abbildung C-1 ff.)

Stammdaten

Die Tabellen *Adressen, Massnahmenkatalog, Bewertungskriterien* und *Systemdaten* enthalten die Stammdaten von *ISIGO 1.5*.

In *Adressen* können die Adressen, Telefonnummern etc. der im aktuellen Teilprojekt anzusprechenden Personen festgehalten werden, um einerseits eine schnelle Referenz zur Verfügung zu haben und um andererseits die Erfassung von Adressen bei den Ergebnisdaten zu vermeiden. Letzteres würde schnell zu Redundanzen führen, was vermieden werden soll.

Der *Massnahmenkatalog* enthält die von der Geschäftsleitung oder dem ISiBe vorgeschlagenen Massnahmen. Die Basisversion enthält den Massnahmenkatalog aus der Umgebung der Projektion.

Die *Bewertungskriterien* werden ebenfalls in den Vorbereitungen vom ISiBe festgelegt, können aber auch im Verfahren noch angepasst werden. In der Basisversion sind hier *Verfügbarkeit*, *Vertraulichkeit* und *Integrität* definiert.

Die *Systemdaten* enthalten Daten, welche sich direkt auf die Benutzerschnittstelle von *ISIGO 1.5* beziehen, z.B. Schriftgrössen und –namen.

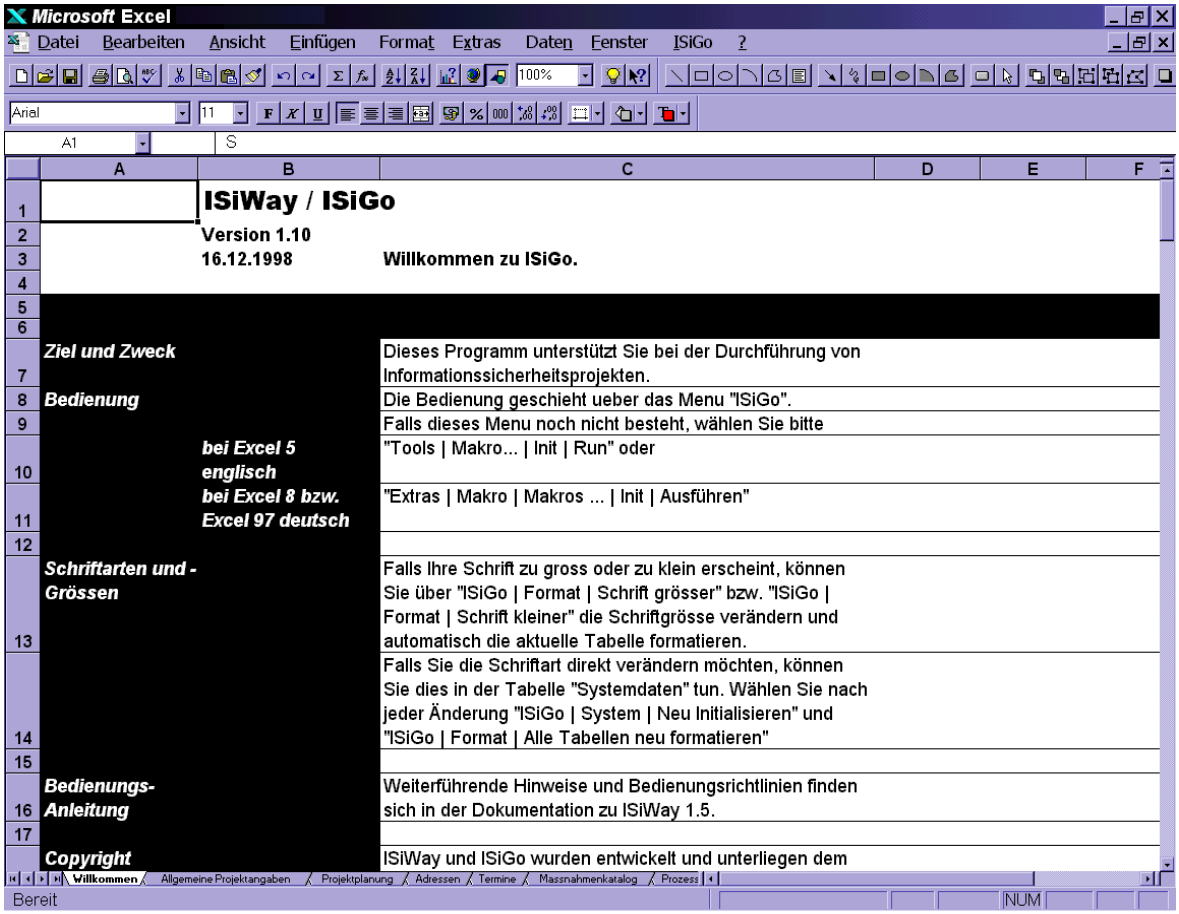


Abbildung D-14: *ISiGo* Tabelle "Willkommen"

Funktionalität

Steuerung

Die Steuerung von *ISiGo* geschieht über das gleichnamige Menu *ISiGo*, welche die *Funktionswahl* implementiert (vgl. Abbildung D-15). Die einzelnen Steuerungsfunktionen sind in Beschreibung des Verfahrens *ISiWay 1.5* [121] detailliert erklärt, so dass nur im Überblick darauf eingegangen wird.

121 Die Dokumentation von *ISiWay 1.5* ist in Anhang C.2 enthalten.

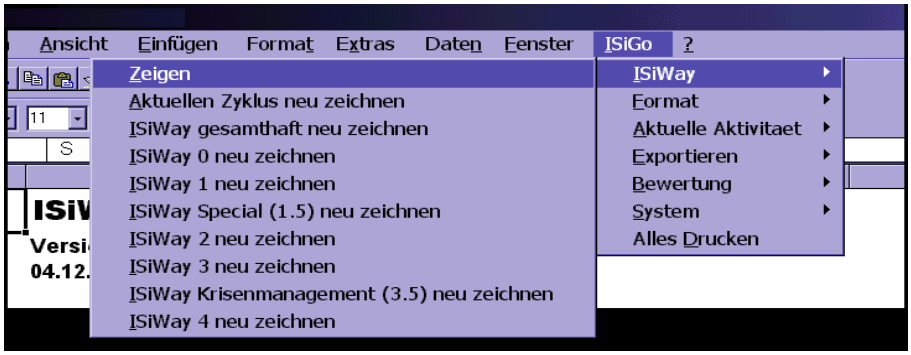


Abbildung D-15: Steuerungsfunktion von *ISIGO* (Menu)

Zentrales Element ist die Darstellung des Zyklus, welche mit der Befehlskombination `ISIGO | ISIWAY | Aktuellen Zyklus neu zeichnen` (bzw. bei späteren Starts mit `ISIGO | ISIWAY | Zeigen`) angezeigt werden kann. Es entsteht eine Bildschirmdarstellung gemäss Abbildung D-16. Die aktuelle Aktivität ist dabei rot und umrandet dargestellt.

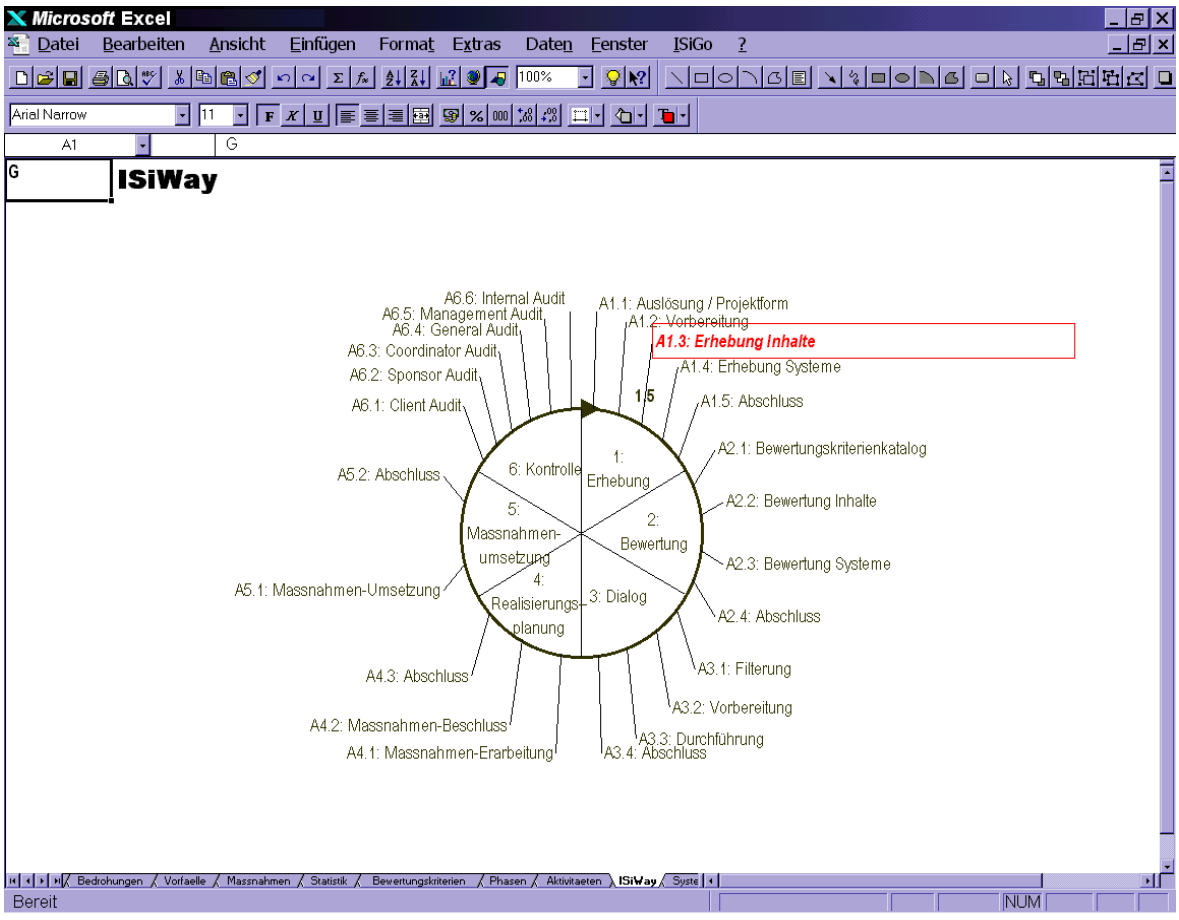


Abbildung D-16: Bildschirmdarstellung des Zyklus *ISIWAY1.5*[122]

122 Die Darstellung kann mit Bildschirmauflösung, Fenstergrösse, gewählter Betriebssystemeinstellungen und den Einstellungen aus der Tabelle "Systemdaten" variiert werden.

Durch Wahl von *ISIGO* | `Aktuelle Aktivitaet` | `Aufgabe` (oder `Ziel` oder `Resultat`) können die entsprechenden Inhalte dieser Aktivität angezeigt werden (vgl. Abbildung D-17).

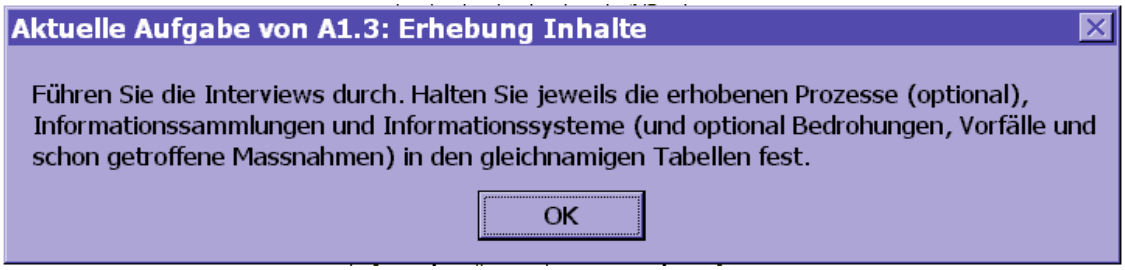


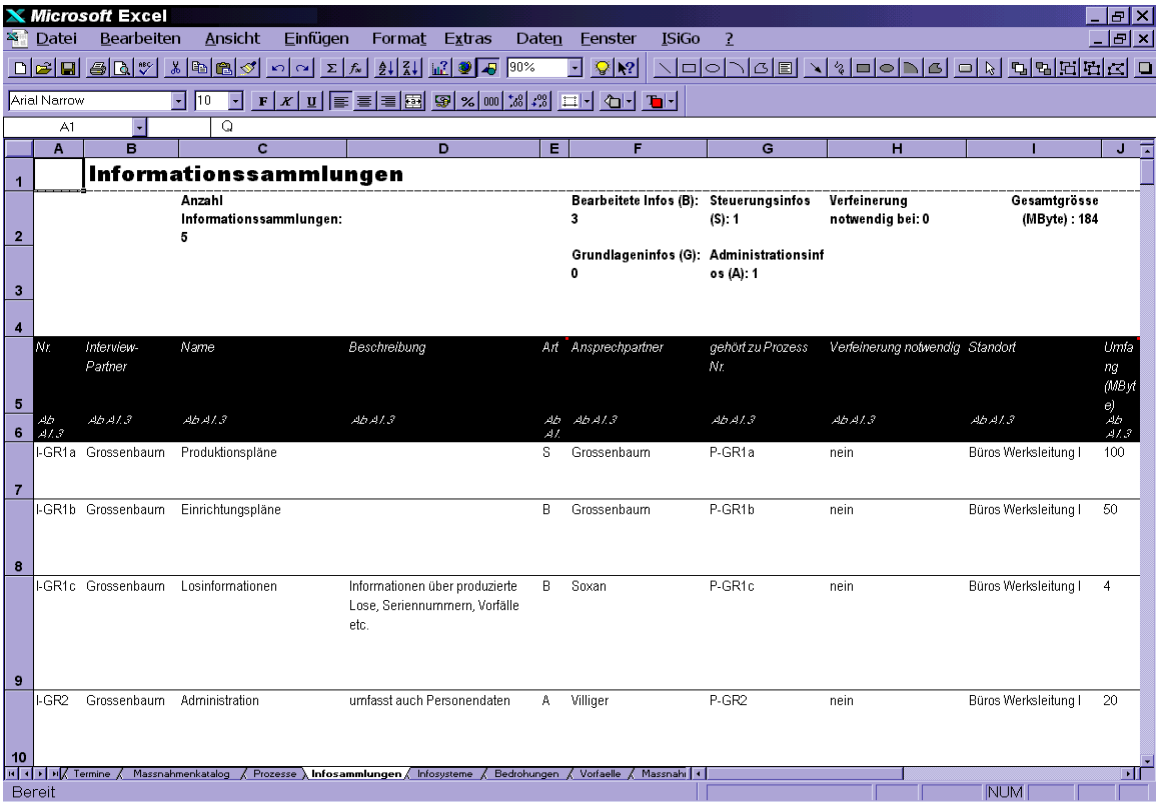
Abbildung D-17: Darstellung der Aufgabe der aktuellen Aktivität

Die Darstellung des Zyklus und die Anzeige der Aufgaben, Ziele und Resultate der einzelnen Phasen stellen zusammen die Funktion *Steuerung* dar. Sie bezieht sich auf die Daten in den Tabellen *Allgemeine Projektbeschreibung, Phasen* und *Aktivitäten.*

Die Implementation der nicht in *EXCEL* vorhandenen Funktionalitäten geschieht in acht Visual-Basic-Modulen.

Verwaltung

Die *Verwaltung* aller Daten geschieht über die direkte Eingabe der Werte in die entsprechenden Tabellen. Die Tabelle mit den Informationssammlungen ist in Abbildung D-18 und Abbildung D-19 als Beispiel abgebildet. Es bestehen keine Feldsperrungen oder andersartige Schutzmechanismen. Der Einsatz von *ISIGO 1.5* setzt Erfahrungen mit *EXCEL* und die Einarbeitung in *ISIWAY 1.5* voraus.

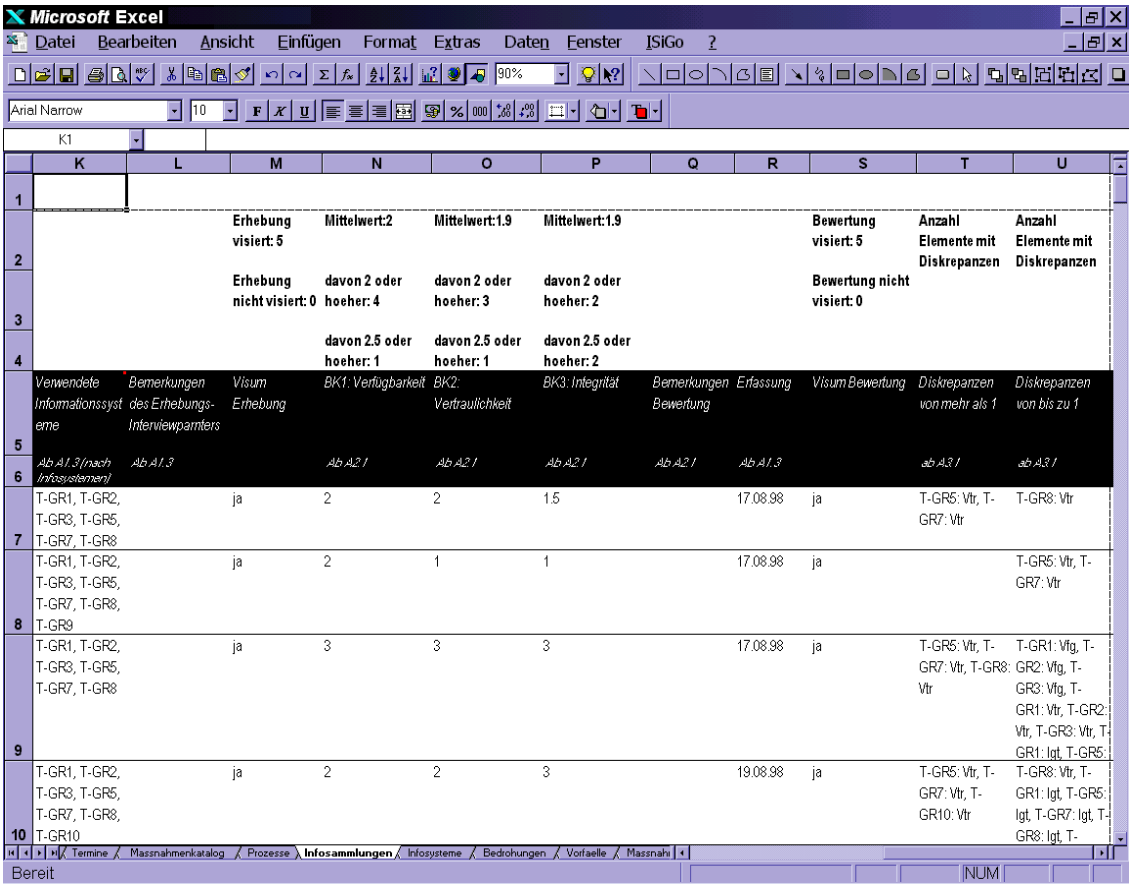


Informationssammlungen

		Anzahl Informationssammlungen: 5			Bearbeitete Infos (B): 3 Grundlageninfos (G): 0	Steuerungsinfos (S): 1 Administrationsinfos (A): 1	Verfeinerung notwendig bei: 0		Gesamtgrösse (MByte) : 184

Nr.	Interview-Partner	Name	Beschreibung	Art	Ansprechpartner	gehört zu Prozess Nr.	Verfeinerung notwendig	Standort	Umfang (MByte)
Ab A1.3	Ab A1.3	Ab A1.3	Ab A1.3	Ab A1.	Ab A1.3	Ab A1.3	Ab A1.3	Ab A1.3	Ab A1.3
I-GR1a	Grossenbaum	Produktionspläne		S	Grossenbaum	P-GR1a	nein	Büros Werksleitung I	100
I-GR1b	Grossenbaum	Einrichtungspläne		B	Grossenbaum	P-GR1b	nein	Büros Werksleitung I	50
I-GR1c	Grossenbaum	Losinformationen	Informationen über produzierte Lose, Seriennummern, Vorfälle etc.	B	Soxan	P-GR1c	nein	Büros Werksleitung I	4
I-GR2	Grossenbaum	Administration	umfasst auch Personendaten	A	Villiger	P-GR2	nein	Büros Werksleitung I	20

Abbildung D-18: Tabelle "Informationssammlungen", linker Teil



Informationssammlungen

		Erhebung visiert: 5 Erhebung nicht visiert: 0	Mittelwert:2 davon 2 oder hoeher: 4 davon 2.5 oder hoeher: 1	Mittelwert:1.9 davon 2 oder hoeher: 3 davon 2.5 oder hoeher: 1	Mittelwert:1.9 davon 2 oder hoeher: 2 davon 2.5 oder hoeher: 2			Bewertung visiert: 5 Bewertung nicht visiert: 0	Anzahl Elemente mit Diskrepanzen	Anzahl Elemente mit Diskrepanzen

Verwendete Informationssysteme	Bemerkungen des Erhebungs-Interviewpartners	Visum Erhebung	BK1: Verfügbarkeit	BK2: Vertraulichkeit	BK3: Integrität	Bemerkungen Bewertung	Erfassung	Visum Bewertung	Diskrepanzen von mehr als 1	Diskrepanzen von bis zu 1
Ab A1.3 (nach Informationssystemen)	Ab A1.3		Ab A2.1	Ab A2.1	Ab A2.1	Ab A2.1	Ab A1.3		ab A3.1	ab A3.1
T-GR1, T-GR2, T-GR3, T-GR5, T-GR7, T-GR8		ja	2	2	1.5		17.08.98	ja	T-GR5: Vtr, T-GR7: Vtr	T-GR8: Vtr
T-GR1, T-GR2, T-GR3, T-GR5, T-GR7, T-GR8, T-GR9		ja	2	1	1		17.08.98	ja		T-GR5: Vtr, T-GR7: Vtr
T-GR1, T-GR2, T-GR3, T-GR5, T-GR7, T-GR8		ja	3	3	3		17.08.98	ja	T-GR5: Vtr, T-GR7: Vtr, T-GR8: Vtr	T-GR1: Vfg, T-GR2: Vfg, T-GR3: Vfg, T-GR1: Vtr, T-GR2: Vtr, T-GR3: Vtr, T-GR1: Igt, T-GR5:
T-GR1, T-GR2, T-GR3, T-GR5, T-GR7, T-GR8, T-GR10		ja	2	2	3		19.08.98	ja	T-GR5: Vtr, T-GR7: Vtr, T-GR10: Vtr	T-GR8: Vtr, T-GR1: Igt, T-GR5: Igt, T-GR7: Igt, T-GR8: Igt, T-

Abbildung D-19: Tabelle "Informationssammlungen", rechter Teil

Auswertung

Die Auswertung der Daten geschieht über Summen- und Mittelwertfunktionen, welche schon in die obersten Zeilen jeder Tabelle eingetragen sind. In der *Statistik*-Tabelle werden alle Ergebnisse wiederholt. Jede Tabelle kann über die normalen *EXCEL*-Funktionen ausgedruckt werden. Spezielle Formatierungs- und Druckfunktionen werden in der Dokumentation zu *ISIWAY 1.5* beschrieben.

Kommunikation

Die Kommunikation mit anderen Instanzen von *ISIGO 1.5* geschieht über den Austausch von Dateien, z.B. auf Diskette. Die entsprechenden Funktionalitäten sind ebenfalls in der Dokumentation zu *ISIWAY 1.5* beschrieben und umfassen v.a. den Export von Daten.

Der Export wurde sehr flexibel gestaltet: Es können sowohl einzelne Objekte (Informationssammlungen, Informationssysteme etc.) gesamthaft oder einzeln in zusätzliche Dateien exportiert werden, als auch eine vollkommene Kopie der relevanten Daten automatisiert erzeugt werden. Die Resultate sind jeweils *EXCEL*-Tabellen (auch mehrere pro Datei), welche in Dateien gespeichert werden.

Beispiel: Eine Person, welche bei der Erhebung und Bewertung der Daten vom Interviewpartner als Ansprechpartner vorgeschlagen wurde, möchte die Erhebung telefonisch vervollständigen. Nun kann der ISiKo durch geschickte Wahl der Exporte ein *EXCEL*-Tabellen zusammenstellen, welche genau diejenigen Informationen enthalten, welche für diese Person relevant sind (also nur diejenigen Informationssammlungen etc., in denen diese Person als Ansprechpartner festgehalten wurde). Diese Tabelle wird dann automatisch gespeichert, wobei der ISiKo den Pfad angegeben kann (er kann so auch eine Speicherung auf Diskette bewirken). Das Original der Erfassung bleibt von diesem Export unbeeinflusst.

Auch ein Austausch über die Zwischenablage funktioniert wie in *EXCEL* üblich. Dies ist beispielsweise dann notwendig, wenn veränderte Daten von dem zuvor beschriebenen Ansprechpartner als *EXCEL*-Datei zurückgeschickt werden. Der ISiKo kann diese Datei parallel in *EXCEL* öffnen, alle Datenzeilen der jeweiligen Tabellen markieren, mit `Bearbeiten | Kopieren` in die Zwischenablage übertragen, mit `Fenster | ISIGO 1.5` wieder in die Hauptdatensammlung wechseln, mit `Bearbeiten | Einfügen` die Datensätze an die entsprechende Tabelle anfügen, sie mit `Daten | Sortieren` nach Ansprechpartner sortieren und die jeweils älteren Erfassungen (es besteht ein Datumsfeld der Erfassung) aus den Tabellen entfernen. So geschieht ein kontrollierter Import.

Weitere Funktionalitätsebenen

Die Funktionen der weiteren Ebenen wurden grösstenteils mit Funktionen von *EXCEL* direkt implementiert, oder durch geschickte Kombination dieser Funktionen in Visual Basic-Modulen.

D.1.4 Erklärung der implementierten Funktionen

ISIGO 1.5 enthält zahlreiche Funktionen, welche in Visual Basic implementiert wurden und im nachfolgenden Abschnitt wiedergegeben werden. Hier soll jede Funktion kurz erklärt werden.

Modul *ISIGO*Table:

- i_*ISIGO*_Table_ElCnt: Zählt die Elemente (eingetragenen Zeilen) in der angegebenen Tabelle
- i_*ISIGO*_Activate_Sheet: aktiviert und löscht (bei entsprechenden Parametern) ein bestimmtes Tabellenblatt
- *ISIGO*_Tabelle_Loeschen: löscht eine Tabelle
- i_*ISIGO*_Tabellen_Export: Steuert den Export einer oder mehrerer Tabellen in eine oder mehrere Dateien
- i_*ISIGO*_Do_Export_For: führt den konkreten Export einer Tabelle in eine Datei durch und filtert die unpassenden Zeilen heraus
- *ISIGO*_Tabellen_Export_Interviewpartner: erlaubt den Export einer Tabelle durch Selektion des Interviewpartners
- *ISIGO*_Tabellen_Export_Dialog: steuert den terminbezogenen Export von Tabellen

Modul *ISIGO*Format:

- i_*ISIGO*_Format_FontChg: trägt die Veränderung der Grösse der verwendeten Schriftart im System ein und steuert die Neuformatierung aller betroffenen Tabellen
- *ISIGO*_Format_FontBigger: erlaubt die Vergrösserung der verwendeten Schriftart
- *ISIGO*_Format_FontSmaller: erlaubt die Verkleinerung der verwendeten Schriftart
- i_*ISIGO*_Format_Basic: führt die grundlegende Formatierung von Tabellen nach einheitlichem Muster durch
- i_*ISIGO*_Format_Subtitle: formatiert den Untertitel einer Tabelle
- i_*ISIGO*_Format_SuperTitle: formatiert den Übertitel einer Tabelle
- i_*ISIGO*_Format_Seite_Einrichten: steuert die Festlegung der Druckparameter für eine einheitliche Druckausgabe
- *ISIGO*_Print_All: löst den Druck aller Tabellen aus
- i_*ISIGO*_Format_BlkOnWht: führt die Formatierung der Tabellenköpfe weiss auf schwarz vor
- i_*ISIGO*_Format_Hoch: nimmt die spezifische Formatierung von Tabellen im Hochformat vor

- i_*ISIGO*_Format_Quer: nimmt die spezifische Formatierung von Tabellen im Querformat vor
- *ISIGO*_Format_Grafik: nimmt die spezifische Formatierung der Tabellen mit der *ISIWAY*-Darstellung vor
- *ISIGO*_Format_Alle: führt die Formatierung mit den aktuellen Systemvorgaben für alle Tabellen durch
- *ISIGO*_Format_This: führt die Formatierung mit den aktuellen Systemvorgaben für die aktuelle Tabelle durch
- i_*ISIGO*_Format_Worksheet: führt die Formatierung mit den aktuellen Systemvorgaben für eine spezifische Tabelle durch

Modul *ISIGO*BKDisk:

- i_*ISIGO*_Insert_Diskr_Cols: fügt die Spalten für die Eintragung der Diskrepanzen in die Tabellen Infosammlungen und Infosysteme ein, bzw. löscht die Inhalte dieser Spalten
- *ISIGO*_Disk_Ins: fügt die Diskrepanzen in die zuvor angelegten Spalten ein
- s_*ISIGO*_Make_BK_FullName: erstellt den Namen eines Bewertungskriteriums
- *ISIGO*_BK_Ins: fügt die Spalten für die Bewertungskriterien in die Tabellen Infosammlungen und Infosysteme ein

Modul *ISIGO*Init:

- allgemeine Variablendeklarationen für die Verwendung der Variablen in den verschiedenen Modulen[123]
- *ISIGO*_Menu_Remove: Entfernt das Menu *ISIGO*
- *ISIGO*_Menu_Add: fügt das Menu *ISIGO* und seine Untermenus und Menupunkte dem Menubalken hinzu
- Init: führt allgemeine Initialisierungsaktivitäten durch, v.a. die Zuweisung von Initialwerten zu den verwendeten globalen Variablen sowie Bereitstellung systemweit gültiger Konstanten (z.B. Grösse des Ausgabefensters)
- *ISIGO*_Exit: führt De-initialisierungsaufgaben zur sauberen Beendigung von *ISIGO* durch
- Auto_Öffnen: beim Start von *ISIGO 1.5* automatisch aktiviertes Makros (falls die automatische Aktivierung nicht aus Gründen des Virenschutzes deaktiviert wurde)

---

123 Aufgrund der Sprachkonzepte von Visual Basic in Microsoft Excel Version 5 vereinfacht die Verwendung globaler Variablen die Programmentwicklung, beschleunigt die Ausführung und verhindert Inkonsistenzen. Die Verwendung lokaler Variablen wurde wo immer möglich bevorzugt.

- Auto_Schließen: bei der Beendigung von *ISIGO 1.5* automatisch aktiviertes Makro
- Auto_Open: wie Auto_Öffnen; für die englischsprachige Version von *EXCEL*
- Auto_Close: wie Auto_Schließen; für die englischsprachige Version von *EXCEL*
- *ISIGO*_ReInit: erlaubt die erneute Initialisierung von *ISIGO 1.5* über einen Menubefehl

Modul *ISIGO*Draw:

- i_*ISIGO*_Init_Draw: Initialisierung der Zeichenfunktionen
- i_*ISIGO*_Draw_DG_RelSize: Berechnen der relativen der Darstellungsgrösse eines Detaillierungsgrades
- l_*ISIGO*_Draw_Calc_fgcol: Berechnen der Vordergrundfarbe der Darstellung eines Detaillierungsgrades
- i_*ISIGO*_Draw_DGs: zeichnet alle Detaillierungsgrade (gemäss übergebenen Parametern)
- i_*ISIGO*_Draw_DG: zeichnet einen Detaillierungsgrad
- i_*ISIGO*_Draw_DGNumber: fügt die Nummer des Detaillierungsgrades der Zeichnung hinzu
- o_*ISIGO*_Draw_Add_Text_Box: zeichnet eine Beschriftungsfeld
- i_*ISIGO*_Draw_Circle: stellt einen Kreis dar
- i_*ISIGO*_Draw_Arrow: stellt einen Pfeil dar
- i_*ISIGO*_Draw_Arc: stellt ein Kreissegment dar
- i_*ISIGO*_Draw_Phs: zeichnet und beschriftet die Phasen des Detaillierungsgrades
- i_*ISIGO*_Draw_Act: zeichnet und beschriftet die Aktivitäten des Detaillierungsgrades
- *ISIGO*_Draw_*ISIWAY*_Cur: stellt den aktuell durchlaufenen Detaillierungsgrad gesamthaft dar
- *ISIGO*_Draw_*ISIWAY*0 bis *ISIGO*_Draw_*ISIWAY*4: stellt den jeweiligen Detaillierungsgrad gesamthaft dar
- *ISIGO*_Draw_*ISIWAY*_x: stellt einen oder mehrere beliebige Detaillierungsgrade gesamthaft dar
- *ISIGO*_Draw_*ISIWAY*: stellt die Detaillierungsgrade 0 bis 4 von *ISIWAY* dar
- *ISIGO*_*ISIWAY*_Select_All: wählt alle Zeichnungselemente aus
- *ISIGO*_Show_*ISIWAY*: wechselt auf die Tabelle mit der Darstellung von *ISIWAY*

- *ISIGo*_Draw_Exit: führt De-Initialisierungsfunktionen zum sauberen Abschluss von *ISIGo*Draw durch

Modul *ISIGo*PhsAct:

- i_*ISIGo*_Phs_PhsAct: extrahiert die Phasennummer aus einer kombinierten Angabe
- i_*ISIGo*_Act_PhsAct: extrahiert die Aktivitätsnummer aus einer kombinierten Angabe
- *ISIGo*_Goto_Act: wechselt die aktuell bearbeitete Aktivität zur nächsten oder vorherigen
- *ISIGo*_Goto_Next_Act: wechselt die aktuell bearbeitete Aktivität zur nächsten
- *ISIGo*_Goto_Prev_Act: wechselt die aktuell bearbeitete Aktivität zur vorherigen
- *ISIGo*_Show_Cur_Act: selektiert die Zelle, in welcher die Nummer der aktuell bearbeiteten Aktivität enthalten ist
- *ISIGo*_Show_Cur_Act_Result: Zeigt das gewünschte Resultat der aktuell bearbeiteten Aktivität an
- *ISIGo*_Show_Cur_Act_Goal: Zeigt das Ziel der aktuell bearbeiteten Aktivität an
- *ISIGo*_Show_Cur_Act_Task: Zeigt die Aufgabe der aktuell bearbeiteten Aktivität an
- i_*ISIGo*_Show_Cur_Act_x: Zeigt die Aufgabe einer beliebigen Aktivität an
- i_*ISIGo*_Phs_PhsAct_Cnt: zählt die Anzahl Aktivitäten einer Phase
- s_*ISIGo*_Phs_Name: gibt den Namen einer Phase zurück
- s_*ISIGo*_Act_Name: gibt den Namen einer Aktivität zurück
- i_*ISIGo*_Act_Line: identifiziert die Zeilennummer, auf welcher eine Aktivität in der Tabelle *Aktivitaeten* enthalten ist
- i_*ISIGo*_Phs_Line: identifiziert die Zeilennummer, auf welcher eine Phase in der Tabelle *Phasen* enthalten ist
- i_*ISIGo*_DG_Phs_Cnt: zählt die Phasen eines Detaillierungsgrades
- i_*ISIGo*_DG_Act_Cnt: zählt die Aktivitäten eines Detaillierungsgrades

Modul *ISIGo*Fld:

- v_*ISIGo*_Fld_Read: liefert den Wert einer bestimmten Zelle zurück, welche durch Angabe einer Spaltenüberschrift und einen Elementenummer identifiziert wird
- i_*ISIGO*_Fld_Write und i_*ISIGO*_Fld_Write2: ändern eine bestimmte Zelle

Modul *ISIGO*Misc:

- strstr: gibt die Position einer Zeichenkette in einer anderen zurück
- isdig: gibt zurück, ob das übergebene Zeichen eine Ziffer ist
- issep: gibt zurück, ob das übergebene Zeichen ein Separatorzeichen ist

D.2 Beispiele

Auf den folgenden Seiten sind die Inhalte der Tabellen "Infosammlungen" und "Statistik" von *ISIGO 1.5* abgebildet, um beispielhaft die Verwaltungsmöglichkeiten von *ISIGO* 1.5 zu belegen. Alle enthaltenen Daten sind fiktiv und sollen nur den Zustand eines Projektes bei der ebenfalls fiktiven Firma „First Light“ beschreiben. Der (absichtlich erscheinende) Hinweis "VERTRAULICH" kann also ignoriert werden.

Info: marcus@holthaus.ch

Anzahl Informationssammlungen: 5 | **Bearbeitete Infos (B): 3** | **Steuerungsinfos (S): 1** | **Verfeinerung notwendig bei: 0** | **Gesamtgrösse (MByte): 184**

Grundlageninfos (G): 0 | **Administrationsinfos (A): 1**

Nr.	*Interview-Partner*	*Name*	*Beschreibung*	*Art*	*Ansprechpartner*	*gehört zu Prozess Nr.*	*Verfeinerung notwendig*	*Standort*	*Umfang (MByte)*	*Verwendete Informationssysteme*
Ab A1.3	*Ab A1.3*	*Ab A1.3*	*Ab A1.3*	*Ab A1.3*	*Ab A1.3*	*Ab A1.3*	*Ab A1.3*	*Ab A1.3*	*Ab A1.3*	*Ab A1.3 (nach Infosystemen)*
I-GR1a	Grossenbaum	Produktionspläne		S	Grossenbaum	P-GR1a	nein	Büros Werksleitung I	100	T-GR1, T-GR2, T-GR3, T-GR5, T-GR7, T-GR8
I-GR1b	Grossenbaum	Einrichtungspläne		B	Grossenbaum	P-GR1b	nein	Büros Werksleitung I	50	T-GR1, T-GR2, T-GR3, T-GR5, T-GR7, T-GR8, T-GR9
I-GR1c	Grossenbaum	Losinformationen	Informationen über produzierte Lose, Seriennummern, Vorfälle etc.	B	Soxan	P-GR1c	nein	Büros Werksleitung I	4	T-GR1, T-GR2, T-GR3, T-GR5, T-GR7, T-GR8

Nr.	*Interview-Partner*	*Name*	*Beschreibung*	*Art*	*Ansprechpartner*	*gehört zu Prozess Nr.*	*Verfeinerung notwendig*	*Standort*	*Umfang (MByte)*	*Verwendete Informationssysteme*
Ab A1.3	*Ab A1.3*	*Ab A1.3*	*Ab A1.3*	*Ab A1.3*	*Ab A1.3*	*Ab A1.3*	*Ab A1.3*	*Ab A1.3*	*Ab A1.3*	*Ab A1.3 (nach Infosystemen)*
I-GR2	Grossenbaum	Administration	umfasst auch Personendaten	A	Villiger	P-GR2	nein	Büros Werksleitung I	20	T-GR1, T-GR2, T-GR3, T-GR5, T-GR7, T-GR8, T-GR10
I-GR3	Grossenbaum	Verfahrensinformationen	Beschreibungen neuer Verfahren und ihrer Erprobung im eigenen Haus	B	Grossenbaum	P-GR3	nein	Büros Werksleitung I	10	T-GR1, T-GR2, T-GR3, T-GR5, T-GR7, T-GR10

Info: marcus@holthaus.ch

		Erhebung visiert: 5	**Mittelwert:2**	**Mittelwert:1.9**	**Mittelwert:1.9**			**Bewertung visiert: 5**	**Anzahl Elemente mit Diskrepanzen von mehr als 1: 4**	**Anzahl Elemente mit Diskrepanzen von bis zu 1: 4**
		Erhebung nicht visiert: 0	**davon 2 oder hoeher: 4**	**davon 2 oder hoeher: 3**	**davon 2 oder hoeher: 2**			**Bewertung nicht visiert: 0**		
			davon 2.5 oder hoeher: 1	**davon 2.5 oder hoeher: 1**	**davon 2.5 oder hoeher: 2**					
Nr.	*Bemerkungen des Erhebungs-Interviewparnters*	*Visum Erhebung*	*BK1: Verfügbarkeit*	*BK2: Vertraulichkeit*	*BK3: Integrität*	*Bemerkungen Bewertung*	*Erfassung*	*Visum Bewertung*	*Diskrepanzen von mehr als 1*	*Diskrepanzen von bis zu 1*
Ab A1.3	*Ab A1.3*		*Ab A2.1*	*Ab A2.1*	*Ab A2.1*	*Ab A2.1*	*Ab A1.3*		*ab A3.1*	*ab A3.1*
I-GR1a		ja	2	2	1.5		17.08.98	ja	T-GR5: Vtr, T-GR7: Vtr	T-GR8: Vtr
I-GR1b		ja	2	1	1		17.08.98	ja		T-GR5: Vtr, T-GR7: Vtr
I-GR1c		ja	3	3	3		17.08.98	ja	T-GR5: Vtr, T-GR7: Vtr, T-GR8: Vtr	T-GR1: Vfg, T-GR2: Vfg, T-GR3: Vfg, T-GR1: Vtr, T-GR2: Vtr, T-GR3: Vtr, T-GR1: Igt, T-GR5: Igt, T-GR7: Igt, T-GR8: Igt

Info: marcus@holthaus.ch

Nr.	*Bemerkungen des Erhebungs-Interviewparnters*	*Visum Erhebung*	*BK1: Verfügbarkeit*	*BK2: Vertraulichkeit*	*BK3: Integrität*	*Bemerkungen Bewertung*	*Erfassung*	*Visum Bewertung*	*Diskrepanzen von mehr als 1*	*Diskrepanzen von bis zu 1*
Ab A1.3	*Ab A1.3*		*Ab A2.1*	*Ab A2.1*	*Ab A2.1*	*Ab A2.1*	*Ab A1.3*		*ab A3.1*	*ab A3.1*
I-GR2		ja	2	2	3		19.08.98	ja	T-GR5: Vtr, T-GR7: Vtr, T-GR10: Vtr	T-GR8: Vtr, T-GR1: Igt, T-GR5: Igt, T-GR7: Igt, T-GR8: Igt, T-GR10: Igt
I-GR3		ja	1	1.5	1		19.08.98	ja	T-GR5: Vtr, T-GR7: Vtr, T-GR10: Vtr	

Info: marcus@holthaus.ch

Angabe		*1*	*2*
Projektname		ISI-WUS	
Zyklus (DG)		1.5	
Aktuelle Aktivität		A1.1	
Planungsbeginn		17.08.98	
Adressen	***Anzahl***	Anzahl Adressen: 9	
Termine	***Anzahl***	Anzahl Termine: 5	Anzahl geplant: 1
			Anzahl vereinbart: 0
			Anzahl durchgeführt: 4
	Aufwand	Aufwand:	Zeit total (h): 14
			Spesen total (Fr.): 20
Massnahmenkatalog	***Quelle***	Vorschrift Informationssicherheit vom 24. März 1998	
	Anzahl	Anzahl Teil-Massnahmen:62	
		Teil-Massnahmen ab 2:	23
		Teil-Massnahmen ab 2.5:	16
	Typen	Organisatorisch (O):	O: 24
		Personell (P):	P: 4
		Technisch (T):	T: 34
Prozesse	***Erhebung***	Anzahl Prozesse: 5	
		Verfeinerung notwendig bei: 0	
		Erhebung visiert: 5	Erhebung nicht visiert: 0
Informationssammlungen	***Erhebung***	Anzahl Informationssammlungen: 5	Bearbeitete Infos (B): 3
			Grundlageninfos (G): 0
			Steuerungsinfos (S): 1
			Administrationsinfos (A): 1
		Verfeinerung notwendig bei: 0	
		Gesamtgrösse (MByte) : 184	
		Erhebung visiert: 5	Erhebung nicht visiert: 0
	Bewertung	BK1: Verfügbarkeit	Mittelwert:2
			davon 2 oder hoeher: 4
			davon 2.5 oder hoeher: 1
		BK2: Vertraulichkeit	Mittelwert:1.9
			davon 2 oder hoeher: 3
			davon 2.5 oder hoeher: 1

Angabe		*1*	*2*
		BK3: Integrität	Mittelwert:1.9
			davon 2 oder hoeher: 2
			davon 2.5 oder hoeher: 2
		Bewertung visiert: 5	Bewertung nicht visiert: 0
		Anzahl Elemente mit Diskrepanzen von mehr als 1: 4	Anzahl Elemente mit Diskrepanzen von bis zu 1: 4
Informationssysteme	***Erhebung***	Anzahl Informationssysteme: 10	Anzahl Systeme total: 90
		Verfeinerung notwendig bei: 0	
		Erhebung visiert: 10	Erhebung nicht visiert: 0
	Bewertung	BK1: Verfügbarkeit	Mittelwert: 2.4
			davon 2 oder hoeher: 10
			davon 2.5 oder hoeher: 4
		BK2: Vertraulichkeit	Mittelwert: 1
			davon 2 oder hoeher: 4
			davon 2.5 oder hoeher: 0
		BK3: Integrität	Mittelwert: 2.4
			davon 2 oder hoeher: 10
			davon 2.5 oder hoeher: 4
		Bewertung visiert: 10	Bewertung nicht visiert: 0
		Anzahl Elemente mit Diskrepanzen von mehr als 1: 4	Anzahl Elemente mit Diskrepanzen von bis zu 1: 7
		Anzahl gelöst: 3	Anzahl ungelöst: 4
Bedrohungen	***Erhebung***	Anzahl Bedrohungen: 4	
		Anzahl erledigt: 2	Anzahl offen: 2
Vorfälle	***Erhebung***	Anzahl Vorfälle: 1	
Massnahmen	***Realisierung***	Anzahl Massnahmen: 3	Anzahl vorbei: 3
			Anzahl laufend: 0
			Anzahl über Termin: 3
		Anzahl umgesetzt: 2	
	Vorschlag	Anzahl Vorschlag: 1	
	Beschluss	Anzahl Beschlossen:0	
	Visum and Audit	Umsetzung visiert: 2	Umsetzung nicht visiert: 1
		Anzahl Client OKs: 3	
		Anzahl Sponsor OKs: 3	

E Glossar

Nachfolgend findet sich eine Zusammenfassung der Schlüsselbegriffe und Konzepte der Informationssicherheit, welche Teil der Dokumentation von *ISIWAY* ist. Sie ist nicht in den Text in Kapitel 8 integriert worden, um dort Redundanzen zu vermeiden. Sie stellt jedoch eine guten Überblick dar und sollte deshalb aus didaktischen Gründen mit *ISIWAY* gemeinsam verbreitet werden.

Was ist Informationssicherheit?

Informationssicherheit ist der *sichere Zustand* von Information. *Sicher* ist dabei ein sehr weiter Begriff, den jede Person unterschiedlich definieren kann. Sicherheit ist deshalb in hohem Masse von den Anforderungen einer Person an die Information abhängig: Erfüllt die Information die Anforderungen, bezeichnet die Person die Information als sicher.

Was ist Information?

Information ist ein Oberbegriff für mehrere Konzepte:

- Information umfasst *Daten*: auf Medien (Papier, Disketten etc.) gespeicherte Angaben und Fakten, welche mit Hilfe von Zeichen dargestellt werden und von Personen mit oder ohne die Hilfe von Maschinen gelesen werden können. In der Aussage "Ich habe die Information notiert" wird die Speicherung von Daten auf Papier ausgedrückt.
- Information umfasst das *Wissen*, welches durch die Interpretation der Daten entsteht, also beispielsweise bei der Lektüre einer Zeitung (z.B. "Die Zeitung enthält Informationen."),
- Information beschreibt die *Kommunikation* zwischen zwei Personen, also den Vorgang, mit welchem Wissen von einer Person zur nächsten weitergegeben wird (z.B. "Er hat mich darüber informiert."),
- Information umfasst die *Verwendung* des Wissens in Handlungen, welche der handelnden Person zur Erreichung ihrer Ziele dienen (z.B. "Wir haben aufgrund der verfügbaren Information entschieden.")

Information hat verschiedene Eigenschaften:

- Information ist *medienneutral*:
  - Ein und dieselbe Information kann auf verschiedenen Trägern gespeichert werden (z.B. auf Diskette und auf Papier), ohne dass dadurch inhaltliche Unterschiede entstehen,
  - Zur Informationsweitergabe können beliebige Medien verwendet werden, z.B. Computer, Telefon oder Stift und Papier. Die Information kann auf diesen Medien Zeit und Distanz überwinden,

- Information ist *flüchtig*, wenn sie nicht aufgezeichnet wird,
- Information ist beliebig *kopierbar* oder *löschbar*, ohne dass Spuren zurückbleiben,
- Information ist beliebig *beschreibbar*, d.h. über jede Information können weitere Aussagen gemacht werden, wodurch neue Information entsteht, die wieder beschrieben werden kann, usw.

Jede Kommunikation zwischen Personen ist eine Informationsübertragung. Es kann sogar gefolgert werden, dass Informationsverarbeitung prinzipiell an Personen gebunden ist, weil nur sie die gespeicherten Daten zu Wissen interpretieren können. Letztlich ist also Informationsverarbeitung eine rein menschliche Domäne. Die Informationsverarbeitung kann durch Werkzeuge (Computer, Stift und Papier) unterstützt werden, wobei jedoch immer nur *Daten* verarbeitet werden. Der Begriff *Information* wird hier in der Folge als Oberbegriff für alle vier genannten Konzepte verwendet (Daten, Wissen, Nachrichten und Informationsverwendung).

Worauf bezieht sich Informationssicherheit?

Informationssicherheit bezieht sich auf Information, also auf die informationellen *Inhalte*. Da Information selbst aufgrund ihrer Immaterialität nicht direkt beeinflusst werden kann, bezieht sich Informationssicherheit sekundär auf alle Vorgänge, in denen Informationen verarbeitet werden (Informationsverarbeitung) und die Werkzeuge, welche dazu verwendet werden (Informationssysteme).

Was ist Informationsverarbeitung?

Informationsverarbeitung ist jeder Vorgang der Erzeugung, Speicherung, Übertragung, Veränderung, Verbreitung, Weitergabe und Löschung von Information. Es bestehen sehr viele verschiedene Begriffe für Vorgänge, welche der Informationsverarbeitung zugerechnet werden können. Informationsverarbeitung ist wie die Information medienneutral. Die computergestützte Verarbeitung eines Textes ist demnach ebenso Informationsverarbeitung wie das Führen eines Telefongesprächs, eine persönliche Besprechung oder die Anfertigung handschriftlicher Notizen.

Was ist ein Informationssystem?

Ein Informationssystem umfasst jene Objekte, welche die Informationen verarbeiten und die für die Informationsverarbeitung notwendig sind. Dies schliesst technische Systeme wie Computer, Telefon und Fax mit ein, ebenso alle einfachen Werkzeuge wie Stift und Papier, aber auch Menschen als Teile des Informationssystems, denn auch Menschen verarbeiten Information.
Oft wird der Begriff jedoch nur für das *informationstechnische* System verwendet (vgl. IT-System). Dies ist darauf zurückzuführen, dass das IT-System ein sehr gut kontrollierbares System ist und die Verarbeitung grosser Mengen von Informationen (Daten) erlaubt.

Was ist unternehmerische Informationssicherheit?

Unternehmerische Informationssicherheit ist die Sicherheit derjenigen Informationen, welche in einer Unternehmung für die Erbringung der geschäftlichen Tätigkeiten benötigt werden. Information wird von vielen Unternehmungen heute als zentrale Ressource betrachtet, vergleichbar mit Finanzen, Arbeitskraft, Immobilien und Maschinen. Das Überleben einer Unternehmung ohne Informationen ist unmöglich. Informationssicherheit wird hier immer im Zusammenhang einer Unternehmung betrachtet.

Warum ist Informationssicherheit für Unternehmungen wichtig?

Unternehmerische Informationssicherheit bedeutet, dass die für die Unternehmung unentbehrliche Ressource Information die Anforderungen erfüllt, die daran gestellt werden. Wenn Informationssicherheit nicht besteht, die Information also die Anforderungen nicht erfüllt, so hat dies Störungen der unternehmerischen Tätigkeit zur Folge.
Beispiel: Eine Unternehmung hat sich auf die schnelle und zuverlässige Lieferung von Rohstoffen spezialisiert. Dazu werden Informationen über die gewünschte Menge, den vereinbarten Preis und den Liefertermin zwischen Käufer und Verkäufer vereinbart. Geht diese Information verloren oder wird sie verfälscht, so berechnet die Unternehmung einen falschen oder keinen Preis, oder liefert nicht zum gewünschten Termin.
Informationssicherheit ist deshalb ein Ziel der Unternehmung, um derartige Störungen zu vermeiden; die Unternehmung fordert Informationssicherheit.

Was ist IT-Sicherheit?

IT-Sicherheit ist die Sicherheit der informationstechnischen Einrichtungen (des IT-Systems), mit denen die Informationen verarbeitet werden. Die IT-Sicherheit ist eine direkte Folge der Forderung nach Informationssicherheit, denn die Informationstechnik muss dazu beitragen, dass die Anforderungen an die Informationen erfüllt werden.
Der Begriff Informationstechnik ist missverständlich. Da der Begriff *Information* eine inhaltliche Interpretation voraussetzt (vgl. oben), handelt es sich eigentlich um Datentechnik. Im deutschen Sprachgebrauch wird deshalb auch (korrekt) von elektronischer Datenverarbeitung (EDV) in EDV-Systemen und von EDV-Sicherheit gesprochen. IT-Sicherheit und EDV-Sicherheit sind also Synonyme.
IT-Sicherheit ist ein wichtiger Bestandteil der Informationssicherheit, da viele Beeinträchtigungen der Sicherheit erst durch die Möglichkeit entstanden sind, grosse Mengen von Daten automatisiert zu verarbeiten. Jeder dieser Verarbeitungsvorgänge im IT-System beruht auf vorher festgelegten Abläufen (Programmen). Diese Programm können Fehler aufweisen, welche lange nicht entdeckt werden oder sogar lange nicht einmal zu Fehlverhalten führen, oder Vorgänge ermöglichen, welche vom Betreiber des IT-Systems nicht gewünscht werden. IT-Sicherheit setzt deshalb vor allem die Beherrschung der komplexen IT-

Systeme voraus, welche heute in den Unternehmungen bestehen, und welche zunehmend die verschiedenen Unternehmungen auch verbinden.

Was ist Sicherheitsmanagement?

Um Informationssicherheit in einer Unternehmung zu erreichen, muss dies nicht nur als Ziel festgelegt werden, sondern es müssen auch Vorgehensweisen (Strategien) entwickelt und verfolgt werden, welche die Erreichung dieses Ziels erst möglich machen. Dies wird gesamthaft als Sicherheitsmanagement bezeichnet. Sicherheitsmanagement bezieht sich dabei ganz allgemein auf die Sicherheit der Unternehmung, also auf den störungsfreien (oder zumindest störungsarmen) Betrieb aller unternehmerischen Systeme, z.B. der Produktion oder der Infrastruktur. In bezug auf die unternehmerische Information wird vom *Management der Informationssicherheit* oder vom Informationssicherheits-management gesprochen.
(Informations-) Sicherheitsmanagement umfasst

- die detaillierte Festlegung des Ziels der Informationssicherheit,
- die Schaffung der organisatorischen Voraussetzungen für die Verfolgung des Ziels,
- die Definition einer Strategie und eines konkreten Prozesses zur Erreichung dieses Ziels mit
  - Definition der erforderlichen Institutionen (Stellen, Kompetenzen, Verantwortlichkeiten, Qualifikationen der Stelleninhaber),
  - Definition der notwendigen Aktivitäten (Tätigkeiten, Funktionen, Aufgaben),
  - Bereitstellung der notwendigen Werkzeuge (Hilfsmittel, Instrumente),
- das Durchlaufen des Prozesses mit
  - Analyse des bestehenden Zustands der Informationssicherheit,
  - Veränderung der Unternehmung, um die Informationssicherheit zu verbessern,
  - Kontrolle der Zielerreichung und Verbesserung der Informations-sicherheit,
  - Anpassung aller vorher genannten Elemente (Ziel, Prozess etc.) um neue Anforderungen zu berücksichtigen,
- die konsequente Kommunikation der Ziele der Informationssicherheit und des Vorgehens innerhalb der Unternehmung,
- die Betrachtung aller zur Erreichung von Informationssicherheit relevanter Fachgebiete.
- Sicherheitsmanagement ist also eine umfassende Aufgabe und Tätigkeit innerhalb der Unternehmung. Sicherheitsmanagement

- ist ein eigener Prozess, der innerhalb der Unternehmung abläuft und die Erreichung von Informationssicherheit zum Ziel hat,
- in die Geschäftsprozesse der Unternehmung integriert, durch sie erneut angestossen und als Teil von ihnen durchgeführt, um Informationssicherheit als integriertes Element der Unternehmung zu etablieren,
- ein nachträglich das Vorgehen und die Ergebnisse des erstgenannten Prozesses und der Geschäftsprozesse im allgemeinen betrachtender, separater Prozess, der durch unabhängige Identifizierung von Handlungsbedarf Mängel beim Durchlaufen der Prozesse aufdeckt und so einen erneuten Anstoss zum Sicherheitsmanagement gibt.

Die ersten beiden Elemente bilden den *Controlling*-orientierten Teil des Sicherheitsmanagements, das dritte den *Revisions*-orientierten Teil.

Wer ist für Informationssicherheit verantwortlich?

Da Informationssicherheit ein unternehmerisches Ziel ist, sind die Linienverantwortlichen der Unternehmung auch für die Informationssicherheit verantwortlich.

Welche Stellen für Informationssicherheit sind üblich?

Üblich ist die Bestimmung eines *Beauftragten für Informationssicherheit*. Dieser hat i.d.R. beratende Funktion. In Einzelfällen kann die Verantwortung für einen konkreten Bereich einem *Verantwortlichen für Informationssicherheit* übertragen werden. Da Verantwortung allerdings Kompetenz voraussetzt, muss jeder Sicherheitsverantwortliche auch die Möglichkeit haben, das Verhalten des Bereichs oder des Systems zu bestimmen, für welches er die Verantwortung trägt. Er muss also mit dem für den Bereich oder das System direkt verantwortlichen Linienmanager zumindest eng zusammenarbeiten.

Wie kann Informationssicherheit erreicht werden?

Informationssicherheit wird durch das Durchlaufen eines Prozesses erreicht. Dieser Prozess kann grob in eine Analysephase, eine Beeinflussungs- und eine Kontrollphase unterteilt werden. In diesem Prozess werden verschiedene Tätigkeiten durchgeführt, welche Schritt für Schritt die Informationssicherheit verbessern.

Kann Informationssicherheit erreicht werden?

Nein. Informationssicherheit ist ein idealistisches Ziel. Die Massnahmen und Beeinflussungen, welche umgesetzt werden, um Informationssicherheit zu erreichen, schränken in der Regel die Flexibilität und die Effizienz des betroffenen Systems oder Bereichs ein. Informationssicherheit bedeutet, dass das System Erwartungen erfüllt. Diese erfüllt es um so eher als sich sein Verhalten voraussagen lässt. Um diese Verhalten voraussagen zu können, darf das System aber möglichst wenig verändert werden (verliert also an Flexibilität) und muss Kontrollen

enthalten, welche unerwünschte Zustände und Vorgänge verhindern, denn dadurch sinkt i.d.R. die Effizienz. Informationssicherheit kann deshalb für einzelne Systeme annähernd erreicht werden, für viele Systeme, deren Anpassung für die Unternehmung wichtig ist, will sie in einem sich ständig ändernden Markt bestehen, kann Informationssicherheit nur ansatzweise oder nur teilweise erreicht werden.
Die Verfolgung von Informationssicherheit ist aufgrund der notwendigen Veränderungen und Anpassungen der Unternehmung an ihre Umwelt eine ständige, kontinuierlich Aufgabe und Tätigkeit der Unternehmung.

Wer führt den Informationssicherheitsprozess durch?

Da die Verantwortung für Informationssicherheit in den Linienstellen der Unternehmung liegt, wird das Management der Informationssicherheit ebenfalls von diesen Stellen durchgeführt. Jede Stelle muss also die Sicherheit derjenigen Information, welche sie verwendet, gewährleisten.

F Literatur

Referenz	[124]	Quelle
[Abrams95]		Abrams, Marshall D. (Hrsg.); Podell, Harold J. (Hrsg.); Jajodia, Sushil (Hrsg.): Information Security, An Integrated Collection of Essays; IEEE Computer Society Press, Los Alamitos, CA; 1995
[Abrams95a]		Abrams, Marshall D.; Podell, Harold J.: Supporting Policies and Functions; in: [Abrams95]; 1995
[ACMCode92]		ACM Code of Ethics and Professional Conduct, Draft, February 12, 1992; http://www.acm.org/pubs/articles/journals/cacm/1992-35-5/p94-anderson/p94-anderson.pdf; in: [CACM]; ACM; Mai 1992
[Anderson93]		Anderson, Ronald E.; Johnson, Deborah G.; Gotterbarn, Donald; Perrolle, Judith: Using the ACM Code; in: [Ermann97]; 1993
[Atteslander92]		Atteslander, Peter: Methoden der empirischen Sozialforschung; Verlag Walter de Gruyter, Berlin; 7. Auflage 1992
[Bailer97]	*	Bailer, Brigitte: Geschäftsmodelle: Methoden und Qualität, Dissertation der wirtschaftswissenschaftlichen Fakultät der Universität Zürich; Universität Zürich; 1997
[Bailey95]		Bailey, David: A Philosophy of Security Management; in: [Abrams95]; 1995
[Barger87]		Barger, Robert N.: Can we find a single ethical code?; in: [Ermann97]; 1987
[Bauknecht98]		Bauknecht, Kurt (Hrsg.); Büllesbach, Alfred (Hrsg.); Pohl, Hartmut (Hrsg.); Teufel, Stephanie (Hrsg.): Sicherheit in Informationssystemen, Proceedings der Fachtagung SIS '98, Universität Hohenheim; vdf Hochschulverlag AG an der ETH Zürich; 26. 3. 1998
[Bea91]		Bea, Franz Xaver (Hrsg.); Dichtl, Erwin (Hrsg.); Schweitzer, Marcell (Hrsg.): Allgemeine Betriebswirtschaftslehre; Gustav Fischer Verlag, Stuttgart; 1991
[Benz93]	*	Benz, Roger: Informationsmanagement: Glossar wichtiger Begriffe mit deutschen und englischen Definitionen; Institut für Informatik, Universität Zürich; 1. Mai 1993
[BFFSiBe96.2]		Holthaus, Marcus; Teufel, Stephanie; Bauknecht, Kurt: Sicherheitsbericht BFF, VERTRAULICH; Institut für Informatik, Universität Zürich; 2. Auflage 4. Juli 1996
[BFIWS02.95.4]		Bundesamt für Informatik der Schweiz [BFI]: Weisung Informatik-Sicherheit Nr. S02, Grundschutz von Informatik-Systemen und -Anwendungen; 19. April 1995
[BFIWS02 HB1.96.6]		Bundesamt für Informatik der Schweiz [BFI]: Handbuch Nr. 1 zur Weisung Informatiksicherheit Nr. S02, Verfahren für die Checklistenbearbeitung und Gesamtmassnahmenkatalog; 1. Juni 1996
[Block97]		Block, Peter: Erfolgreiches Consulting, Das Berater-Handbuch; Campus Verlag GmbH, Frankfurt / Main; 1997
[Brandao94]		Brandao, Rui P.: Diplomarbeit in Informatik, IT-Sicherheitskultur im Unternehmen; Institut für Informatik, Universität Zürich; 15. Dezember 1994
[Britsch95]	*	Britsch, Werner: Personelle Sicherheit in Unternehmen; in: [Pohl95]; 1995

[124] Die in dieser Spalte mit einem Stern gekennzeichnete Literatur wurde nicht direkt referenziert, wurde jedoch inhaltlich konsultiert und wird hier als weiterführende Referenz angegeben.

Referenz	[124]	Quelle
[BSI-COP95]		British Standards Institution [BSI (GB)]: Code of Practice for Information Security Management; British Standards Institution, Chiswick High Road, London; 1995
[BSI-IT-GSHB97]		Deutsches Bundesamt für Sicherheit in der Informationstechnik [BSI (D)]: IT-Grundschutzhandbuch 1997, Massnahmenempfehlungen für den mittleren Schutzbedarf; Verlag Bundesanzeiger, Bonn; 3. Auflage 1997
[BSI-IT-SHB92]		Deutsches Bundesamt für Sicherheit in der Informationstechnik [BSI (D)]: IT-Sicherheitshandbuch, Handbuch für die sichere Anwendung der Informationstechnik; Bundesanzeiger Verlagsgesellschaft m.b.H., Köln; Version 1.0, 1. März 1992
[BSI-IT-SHB94]		Deutsches Bundesamt für Sicherheit in der Informationstechnik [BSI (D)]: IT-Sicherheitshandbuch, Handbuch für die sichere Anwendung der Informationstechnik; Bundesanzeiger Verlagsgesellschaft m.b.H., Köln; Version 1.1C, Juli 1994
[BSI-IT-SK89]		Zentralstelle für Sicherheit in der Informationstechnik [ZSI]: IT-Sicherheitskriterien: Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (IT); Bundesanzeiger-Verlag, Köln; 1989
[Buckland91]		Buckland, Michael Keeble: Information and Information Systems; Praeger Publishers, New York NY, USA; 1991
[CACM]		Communications of the ACM (Zeitschrift); ACM Press
[Camphausen98]		Camphausen, Ingmar: Erfahrungen beim Aufbau einer bundesweiten Zertifizierungsinfrastruktur für den Individual Network e.V.; in: [Bauknecht98]; 1998
[Cash]		CASH (Zeitschrift); Ringier AG, Zürich
[Cash98.39]		Settele, Claude: Wachsamkeit ist alles, Exklusiv: CASH präsentiert eine weltweite Studie über Sicherheitsfragen in der Informatik; in: [Cash]; 25.9.98
[COBIT96.1]		Information Systems Audit and Control Foundation [ISACF]: Control Objectives for Information and Related Technology, Software; Information Systems Audit and Control Foundation; September 1996
[COBIT96.2]		Information Systems Audit and Control Foundation [ISACF]: Control Objectives for Information and Related Technology, Control Objectives; Information Systems Audit and Control Foundation; September 1996
[COBIT96.3]		Information Systems Audit and Control Foundation [ISACF]: Control Objectives for Information and Related Technology, Framework; Information Systems Audit and Control Foundation; September 1996
[COBIT96.4]		Information Systems Audit and Control Foundation [ISACF]: Control Objectives for Information and Related Technology, Executive Summary; Information Systems Audit and Control Foundation; September 1996
[COBIT96.5]		Information Systems Audit and Control Foundation [ISACF]: Control Objectives for Information and Related Technology, Audit Guidelines; Information Systems Audit and Control Foundation; September 1996
[CompSec]		Computers and Security (Zeitschrift); Elsevier Science Ltd., London
[CompSec96]		CompSec 96, Computers and Security Conference Proceedings, 1996, London; Elsevier Science, London; 23. Oktober 1996
[ConstLib]	*	Poole, Patrick (E-Mail: ppoole@fcref.org) [FCF]: Constitutional liberties newsletter; http://www.fcref.org/; Free Congress Research and Education Foundation
[CRCL98]		ACM Computing Classification System; http://www.acm.org/class/1998; ACM, New York, USA; 3. Auflage 1998

Referenz	[124]	Quelle
[Crypto-Gram]	*	Schneier, Bruce: Crypto-Gram, A free monthly newsletter providing summaries, analyses, insights, and commentaries on cryptography and computer security, Counterpane Systems, Minneapolis MN, USA, http://www.counterpane.com/crypto-gram.html
[c't]		c't (Zeitschrift); Verlag Heinz Heise, Hannover
[Davidson97]		Davidson, James Dale; Rees-Mogg, William: The Sovereign Individual, How to survive and thrive during the collapse of the welfare state; Simon & Shuster, New York; 1997
[DBW]		Die Betriebswirtschaft (Zeitschrift); Senkel Verlag, München
[Dierstein97]		Dierstein, Rüdiger: Duale Sicherheit - IT-Sicherheit und ihre Besonderheiten; in: [Müller97a]; 1997
[Dissmann86]	*	Dissmann, S.; Zurwehn, V.: Vorschlag für ein sichtenorientiertes Qualitätsmodell, Forschungsbericht Nr. 11; Lehrstuhl Software-Technologie, Universität Dortmund; Mai 1986
[Duden85]		Drosdowski, Günther (Hrsg.): Duden Bedeutungswörterbuch (Band 10); Bibliographisches Institut und Dudenverlag Zürich, Mannheim, Wien; 2. Auflage 1985
[Duden90]		Drosdowski, Günther (Hrsg.): Duden Fremdwörterbuch (Band 5); Bibliographisches Institut und Dudenverlag Zürich, Mannheim, Wien; 5. Auflage 1990
[Earl89]		Earl, Michael J.: Management Strategies for Information Technology; Prentice Hall; 1989
[Eggmann97]		Eggmann, Irene C.; Forstmoser, Peter (Hrsg.): Schweizer Schriften zum Handels- und Wirtschaftsrecht, Band 176, Die aktienrechtliche Verantwortung der Revisionsstelle bei der Abschlussprüfung; Schulthess Polygraphischer Verlag Zürich; 1997
[Ermann97]		Ermann, M. David (Hrsg.); Williams, Mary B. (Hrsg.); Shauf, Michele S. (Hrsg.): Computers, Ethics, and Society; Oxford University Press, New York, Oxford; 2. Auflage 1997
[Friedrichs90]		Friedrichs, Jürgen: Sozialwissenschaft, Methoden der empirischen Sozialforschung; Westdeutscher Verlag GmbH, Opladen; 14. Auflage 1990
[Golder98]		Golder, Stefan M.: Ökonomische Literatur, Auf dem Weg in die Informationsgesellschaft, Tertiarisierung als Motor für die Innovationsdynamik; in: [NZZ], 13.3.98
[Hamel94]	*	Hamel, Gary; Pralahad, C. K.: Competing for the Future; Harvard Business School Press; 1994
[Heinrich93]		Heinrich, Lutz J.: Wirtschaftsinformatik: Einführung und Grundlegung; R. Oldenbourg Verlag München Wien; 1993
[Heinrich95]		Heinrich, Lutz J.: Informationsmanagement; R. Oldenbourg München Wien; 7. Auflage 1995
[Heise98.01.13]		Spionage in US-High-Tech-Firmen - auch die BRD wird beschuldigt; http://www.heise.de/newsticker/data/fr-13.01.98-000/default.html; Heinz Heise, Hannover; 13.1.98
[HillW90]		Hill, Wilhelm: Der Stellenwert der Unternehmungsberatung für die Unternehmungsführung; in: [DBW]; Nr. 2 1990, S. 171-180
[Holbein96]		Holbein, Ralph: Dissertation in Informatik, Secure Information Exchange in Organisations, An approach for solving the information misuse problem; Shaker Verlag, Ulm; 1. Juli 1996
[Horster98]		Horster, Patrick; Wohlmacher, Petra: Grundüberlegungen zur Gestaltung von Sicherheitsinfrastrukturen; in: [Bauknecht98]; 1998
[Hummelt97]	*	Hummelt, Roman: Wirtschaftsspionage auf dem Datenhighway, Strategische Risiken und Spionageabwehr; Carl Hanser Verlag, München, Wien; 1997

Referenz	[124]	Quelle
[InfoWeekD]		InformationWeek, Das zweiwöchentliche IT-Magazin; CMP-WEKA, Poing, Deutschland
[InfoWeekD98.19]		Zwischen Panik und Perfektion; in: [InfoWeekD]; 17. 9. 1997
[ISO13335-1]		International Organization for Standardization [ISO]: ISO/IEC TR 13335-1, Information Technology - Security Techniques – Guidelines for the Management of IT Security (GMITS), Part 1: Concepts and models for IT Security; ISO, Genf; 15. Dezember 1996
[ISO13335-2]		International Organization for Standardization [ISO]: ISO/IEC TR 13335-2, Information Technology - Security Techniques – Guidelines for the Management of IT Security (GMITS), Part 2: Managing and Planning IT Security; ISO, Genf; 15. Dezember 1997
[ISO13335-3]		International Organization for Standardization [ISO]: ISO/IEC TR 13335-3, Information Technology - Security Techniques - Guidelines for the Management of IT Security (GMITS), Part 3 - Techniques for the Management of IT Security; ISO, Genf; 15. Februar 1998
[ISO13335-4]		International Organization for Standardization [ISO]: ISO/IEC TR 13335-4, Information Technology - Security Techniques - Guidelines for the Management of IT Security (GMITS), Part 4 - Baseline Approach; ISO, Genf; (noch nicht veröffentlicht)
[ISO7498-2]		International Organization for Standardization [ISO]: Information Processing Systems, Open Systems Interconnection Reference Manual, Part 2: Security Architecture; ISO, Genf; 1988
[ISO7498-4]		International Organization for Standardization [ISO]: Information Processing Systems, Open Systems Interconnection Reference Manual, Part 4: Management Framework; ISO, Genf; 1991
[ISPT]		Pirow, Peter C.; Duffy, Neil M.; Ford, John C.: Information Systems in Practice and Theory (Zeitschrift); North Holland, Amsterdam
[Ives80]	*	Ives, Blake; Hamilton, Scott; Davis, Gordon Bitter: A framework for research in computer-based management information systems; in: [MgmtSc]; Vol. 26, No. 9, September 1980, S. 910ff
[Janal98]		Janal, Daniel S.: Risky Business, Protect your business from being stalked, conned, or blackmailed on the web; John Wiley and Sons, Inc., New York, Weinheim, Toronto; 1998
[Kabay93]		Kabay, Mich E.: Social Psychology & INFOSEC, Psycho-Social Factors in the Implementation of Information Security Policy; http://catless.ncl.ac.uk/Risks/15.16.html; in: [RISKS]; RISKS Digest; 19. Oktober 1993
[Kelly97]		Kelly, Kevin: Das Ende der Kontrolle, Die biologische Wende in Wirtschaft, Technik und Gesellschaft; Bollmann Verlag, Frankfurt; 1997
[Kersten95a]	*	Kersten, Heinrich: Sicherheit in der Informationstechnik, Einführung in Probleme, Konzepte und Lösungen; R. Oldenbourg, München, Wien; 2. Auflage 1995
[Klander97]		Klander, Lars: Hacker Proof, The Ultimate Guide to Network Security; Jamsa Press, Gulf Publishing Company, Houston TX, USA; 1997
[Klodt97]		Klodt, Henning; Maurer, Rainer; Schimmelpfennig, Axel: Tertiarisierung der deutschen Wirtschaft, Kieler Studien 283; Verlag J.C.B. Mohr (Paul Siebeck), Tübingen; 1997
[Korber93]		Korber, Wilfried: Interne Revision; R. Oldenbourg Verlag GmbH, München; 2. Auflage 1993
[Krcmar97]	*	Krcmar, Helmut: Informationsmanagement; Springer Verlag Hamburg und Stuttgart; 1997

Referenz	[124]	Quelle
[Kuhlen89]		Kuhlen, Rainer: Pragmatischer Mehrwert von Information, Sprachspiele mit informationswissenschaftlichen Grundbegriffen; Universität Konstanz, Fachbereich Informationswissenschaft; Oktober 1989
[Kuhlen95]		Kuhlen, Rainer: Schriften zur Informationswissenschaft Band 15, Informationsmarkt, Chancen und Risiken der Kommerzialisierung von Wissen; Verlag Hochschulverband für Informationswissenschaft (HI) e.V., Konstanz; 1995
[Kunze98]		Kunze, Michael: Lasst es leuchten, LAMP: ein datenbankgestütztes Web-Publishing-System mit Freeware; in: [c't]; 12 / 98, S. 230ff
[Lippa94]		Lippa, Richard A.: Introduction to social psychology; Brooks / Cole Publishing, Pacific Grove, California; 2. Auflage 1994
[Lockemann88]		Lockemann, P. C.: Information Systems for Designing Information Systems; in: [ISPT]; 1988
[Lutz95]		Lutz, Christian: Leben und Arbeiten in der Zukunft; Langen Müller / Herbig; 1995
[Menkus94]	*	Menkus, Belden: The new importance of "Business Continuity" in Data Processing Disaster Recovery Planning; in: [CompSec]; 1994, S. 116f
[MgmtSc]		Management Science (Zeitschrift); http://www.informs.org; Institute for Operations Research and the Management Sciences, Stanford, CA, USA
[Mresse84]	*	Mresse, Moscheh: Leitfäden der Informatik, Information Retrieval - Eine Einführung, Von der Theorie zur Praxis anhand einer Implementierung in UNIX; B.G. Teubner Stuttgart; 1984
[Müller97a]		Müller, Günter (Hrsg.); Pfitzmann, Andreas (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik, Verfahren, Komponenten, Integration; Addison-Wesley, Bonn; 1997
[Müller97b]		Rannenberg, Kai; Pfitzmann, Andreas; Müller, Günter: Sicherheit, insbesondere mehrseitige IT-Sicherheit; in: [Müller97a]; 1997
[Negroponte95]		Negroponte, Nicholas: Total Digital, Die Welt zwischen 0 und 1 oder Die Zukunft der Kommunikation; C. Bertelsmann; 1995
[Neumann95]		Neumann, Peter G.: Computer-Related Risks; ACM Press, New York; 1995
[NewScientist]		New Scientist (Zeitschrift); Reed Business Information Ltd., England
[NRC91]	*	National Research Council [NRC]: Computers at risk, Safe computing in the information age; National Academic Press, Washington, D.C.; 1991
[NZZ]		Neue Zürcher Zeitung (Zeitung); AG für die neue Zürcher Zeitung, Zürich
[NZZ98.09.29]		Aufmerksame Kühlschränke und intelligente Badewannen, Das intelligente Heim - trotz vielen Initiativen noch weitgehend eine Vision; in: [NZZOrbit98]; 29.9.98
[NZZOrbit98]		Neue Zürcher Zeitung, Orbit Messe Basel "Interdog", Ein PC ist kein PC ist ein PC; in: [NZZ] 22.9.98
[Ølnes94]		Ølnes, Jon: Development of Security Policies; in: [CompSec]; 1994, Vol. 13, No. 8, p. 628
[OR92]		Stauffacher, W.: Schweizerisches Obligationenrecht; Orell Füssli, Zürich; 30. Auflage 1992
[Page-Jones85]	*	Page-Jones, Meilir: Practical Project Management, Dorset House Publishing, New York, 1985
[Peterhans96]		Peterhans, Markus: Informationsmanagement, Theoretische Grundlagen und Führungskonzept; vdf Hochschulverlag an der ETH Zürich; 1996
[Peters96]		Peters, Glen: Beyond the next wave, Imagining the next generation of customers; in: [PW96]; 1996
[Pohl95]	*	Pohl, Hartmut (Hrsg.): Sicherheit in der Informationstechnik Handbuch 2, Managementaufgaben im Bereich der Informationssicherheit; R. Oldenbourg Verlag München Wien; 1995

Referenz	[124]	Quelle
[Pohl95a]		Pohl, Hartmut: Verantwortung und Aufgaben des IV-Sicherheitsbeauftragten; in: [Pohl95]; 1995
[PonsWirtsch90]		Pons Fachwörterbuch Wirtschaft, Englisch - Deutsch / Deutsch - Englisch; Klett, Stuttgart, München, Düsseldorf, Leipzig; 1990, Nachdruck 1997
[Popcorn96]		Popcorn, Faith: Clicking - Der neue Popcorn-Report, Trends für unsere Zukunft; Heyne; 1996
[Pordesch97]		Pordesch, Ulrich; Schneider, Michael J.: Sichere Kommunikation in der Gesundheitsversorgung; in: [Müller97a]; 1997
[Postman90]		Postman, Neil: Informing Ourselves to Death; in: [Ermann97]; 1990
[PW96]		Price Waterhouse [PW]: Riding the Next Wave, Imagining your Future; Price Waterhouse, London; 1996
[Quadbeck-Seeger98]	*	Quadbeck-Seeger, Hans-Jürgen: Faszination Innovation, Wissenswertes von A bis Z, Wiley-VCH, Weinheim, New York, 1998
[Raymond91]		Steele, Guy L.; Raymond, Eric: The New Hacker's Dictionary; MIT Press, Cambridge USA & London GB; 1991
[RISKS]		Neumann, Peter G. (Moderator): RISKS, Forum on Risks to the Public in Computers and Related Systems; http://www.CSL.sri.com/risksinfo.html; ACM Committee on Computers and Public Policy
[Robertson93]		Robertson, Jack C.: Auditing; Irwin, Homewood, IL / Boston, MA, USA; 7. Auflage 1993
[Rosenthal98]		Rosenthal, David: Beilage Medien und Informatik, Informationen als Droge der neunziger Jahre, Manager zwischen Sammelleidenschaft und Überforderung; in: [NZZ]; 13.3.98
[Rühli71]		Rühli, Edwin: Beiträge zur Unternehmungsführung und Unternehmungspolitik; Schriftenreihe des Instituts für betriebswirtschaftliche Forschung an der Universität Zürich
[Rühli85]		Rühli, Edwin: Unternehmungsführung und Unternehmungspolitik 1; Verlag Paul Haupt, Bern / Uni-Taschenbuch Nr. 260; 2. Auflage 1985
[Rühli88]		Rühli, Edwin: Unternehmungsführung und Unternehmungspolitik 2; Verlag Paul Haupt, Bern; 2. Auflage 1988
[Rühli91]		Rühli, Edwin (Hrsg.): Strategisches Management in schweizerischen Industrieunternehmungen; Verlag Paul Haupt, Bern; 2. Auflage 1991
[Rühli91a]		Rühli, Edwin: Strategische Unternehmungsführung heute; in: [Rühli91]; 1991
[Rühli92]		Rühli, Edwin: Gestaltungsmöglichkeiten der Unternehmungsführung; Verlag Paul Haupt, Bern; 1992
[Rühli93a]		Rühli, Edwin: Unternehmungsführung und Unternehmungspolitik 3; Verlag Paul Haupt, Bern; 1993
[Rühli95]		Rühli, Edwin (Hrsg.); Keller, Andrea (Hrsg.): Kulturmanagement in schweizerischen Industrieunternehmungen; Verlag Paul Haupt, Bern; 1995
[Ruhmann98]	*	Ruhmann, Ingo; Schulzki-Haddouti, Christiane: Abhör-Dschungel, Geheimdienste lesen ungeniert mit - Grundrechte werden abgebaut; in: [c't]; Heft 5/98, S. 83-93
[Russell91]	*	Gangemi Sr., G. T.; Russell, Deborah: Computer Security, Computer Security Basics; O'Reilly & Associates, Inc., Sebastopol CA 95472; 1991
[Rüttler91]		Rüttler, Martin: Technological Economics, Information als strategischer Erfolgsfaktor, Konzepte und Leitlinien für eine informationsorientierte Unternehmensführung; Dissertation; Erich Schmidt Verlag Berlin; 1991
[Salton87]	*	Salton, Gerard; McGill, Michael J.: Information Retrieval - Eine Einführung; B.G. Teubner Stuttgart; 1983 (Orig.) / 1987 (deutsch)
[Sauter92]		Sauter-Sachs, Sybille: Organisatorische Probleme einer vermehrten Umweltorientierung der Unternehmungen; in: [Sauter92a]; 1992

Referenz	[124]	Quelle
[Sauter92a]		Sauter-Sachs, Sybille (Hrsg.); Rühli, Edwin (Hrsg.): Strukturmanagement in schweizerischen Industrieunternehmungen; Verlag Paul Haupt, Bern; 1992
[Schneider86]		Schneider, Wolf: Wörter machen Leute, Magie und Macht der Sprache; R. Piper&Co., München; 5. Auflage 1989
[Shaffer94]	*	Simon, Alan R.; Shaffer, Steven L.: Network Security; AP Professional, Boston, San Diego, New York et. al.; 1994
[Sherwood96]	*	Sherwood, John: SALSA: A Method for Developing the Enterprise Security Architecture and Strategy, SALSA: Sherwood Associates Limited Security Architecture; in: [CompSec96]; 23. Oktober 1996
[Sienkiewicz95]	*	Sienkiewicz, Bodo S.: Computer-Sicherheit - Praxis und Organisation; Addison-Wesley Publishing Company; 1994
[Suter95]		Suter, Madeleine: IFI TR 95.25, Informatik-Controlling Stand der Forschung; Institut für Informatik, Universität Zürich; Sept. 1995
[Tapscott96]		Tapscott, Don: Digital Economy, Promise and peril in the age of networked intelligence; McGraw-Hill; 1996
[TCSEC85]		DoD 5200.28-STD, Trusted Computer Systems Evaluation Criteria (TCSEC), "Orange Book"; Department of Defense, Washington, USA; Dezember 1985
[Teufel95]		Teufel, Stephanie; Sauter, Christian; Mühlherr, Thomas; Bauknecht, Kurt: Computerunterstützung für die Gruppenarbeit; Bonn: Addison Wesley; 1995
[Ulich94]		Ulich, Eberhard: Arbeitspsychologie; vdf Hochschulverlag, Zürich; 3. Auflage 1994
[Ulrich90]		Ulrich, Hans: Unternehmungspolitik; Verlag Paul Haupt, Bern; 3. Auflage 1990
[Venables91]		Venables, Julian S. R.; Impey, Ken W.: Internal Audit; Butterworths London, Dublin and Edinburgh; 3. Auflage 1991
[VerwOrg]		Verwaltung und Organisation (Zeitschrift); Union Druck und Verlag, Solothurn
[VonStockar95]		von Stockar, Daniel Marc: Informationssicherheit als organisatorische Aufgabe, Dissertation der wirtschaftswissenschaftlichen Fakultät der Universität Zürich; 5. Juli 1995
[Wallmüller90]	*	Wallmüller, Ernest: Software-Qualititätssicherung in der Praxis; Hanser Verlag, München; 1990
[Wallmüller95]		Wallmüller, Ernest: Ganzheitliches Qualitätsmanagement in der Informationsverarbeitung; Hanser Verlag, München und Wien; 1995
[Wallmüller96]	*	Wallmüller, Ernest: Qualitätsmanagement in der Informationsverarbeitung, Bewusste Gestaltung von Prozessen und deren Umgebung; in: [WI]; Heft 2, 1996
[WI]		Wirtschaftsinformatik (Zeitschrift); http://www.wirtschaftsinformatik.de/; Friedrich Vieweg Verlagsgesellschaft mbH, Braunschweig/Wiesbaden
[Williams97]	*	Williams, Mary B.: The Ethical Context of Computers, Ethical Issues in Computing: Work, Privacy, and Justice; in: [Ermann97]; 1997
[Winterthur90]		Winterthur Versicherungen: Sicherheitsanalyse, Einführung und Wegleitung; 22. Mai 1990
[Winterthur97]		Winterthur Versicherungen: Winterthur Safety Engineering, Leitwörter für die Risikoidentifizierung (Sach, Produktehaftpflicht, Gesamtunternehmen); 24. Januar 1997
[Wohlgemuth86]		Wohlgemuth, Andre C.: Trends in der professionellen Unternehmungsberatung, Die sich verändernde Rolle der Unternehmungsberaters bei der Unterstützung in unternehmungs-strategischen und organisatorischen Fragen; in: [VerwOrg]; Nr. 5 / 1986, S. 142-148

Referenz	124	Quelle
[Wohlgemuth97a]		Wohlgemuth, Andre C.: Unternehmensberatung (Management Consulting), Dokumentation zur Vorlesung "Unternehmensberatung"; Universität Zürich; WS 1997/98
[Wohlgemuth97b]		Wohlgemuth, Andre C.: Unternehmensberatung (Management Consulting), Anhang zur Dokumentation zur Vorlesung "Unternehmensberatung"; Universität Zürich; WS 1997/98
[Wood95b]		Wood, Charles Cresson: Writing InfoSec Policies; in: [CompSec]; 1995, Vol. 14, No. 8, p. 667
[Wood95c]	*	Wood, Charles Cresson: Shifting Information Systems Security Responsibilities from User Organizations to Vendor / Publisher Organizations; in: [CompSec]; 1995
[Zahn91]		Zahn, Erich: Informationstechnologie und Informationsmanagement; in: [Bea91]; 1991
[Zehnder91]		Zehnder, Carl-August: Informatik-Projekt-Entwicklung; Verlag der Fachvereine, Zürich und Verlag B.G. Teubner, Stuttgart; 2. Auflage 1991

G Curriculum Vitae

Name	Holthaus
Vorname	Marcus
Adresse	Dersbachstrasse 312a Hünenberg CH 6330 Cham marcus@holthaus.ch
Geburtsjahr und -ort	1967, Mülheim a. d. Ruhr, Deutschland
Zivilstand	verheiratet
Staatsangehörigkeit	Deutschland

Ausbildung

September 1974 - Juni 1979	Grundschule und Gymnasium, Mülheim a. d. Ruhr, Deutschland
August 1979 - Juli 1980	Primarschule Hünenberg ZG
August 1980 - Juni 1987 Juni 1987	Kantonsschule Zug Matura Typ C
Oktober 1987 - Juli 1988	ETH Zürich, Abteilung Informatik (IIIC)
Oktober 1988 - Mai 1995 Mai 1995	Universität Zürich, Rechts- und Staatswissenschaftliche Fakultät lic. oec. publ., Richtung Wirtschaftsinformatik
Juni 1995 - Februar 1999	Institut für Informatik der Universität Zürich Promotion an der Abteilung für Informatik (Wirtschaftswissenschaftliche Fakultät) Leiter der Dissertation: Prof. Dr. K. Bauknecht

Beruf

August 1987 - März 1995	Informatiker bei Softinc Ltd., Baar
Januar 1995 - Februar 1999	Wissenschaftlicher Assistent am Institut für Informatik der Universität Zürich bei Prof. Dr. K. Bauknecht Dissertationsbegleitende Beratungstätigkeiten in der schweizerischen Bundesverwaltung und bei einem globalen Industriekonzern