University of Zurich^UZH

BACHELOR THESIS – Communication Systems Group, Prof. Dr. Burkhard Stiller

Design and Implementation of a Comparison Tool for Selecting an Information Security Risk Assessment Method

Maximilian Huwyler
Zürich, Switzerland
Student ID: 13-925-557

Supervisor: Jan von der Assen, Christian Killer
Date of Submission: March 1, 2023

University of Zurich
Department of Informatics (IFI)
Binzmühlestrasse 14, CH-8050 Zürich, Switzerland

ifi

Bachelor Thesis
Communication Systems Group (CSG)
Department of Informatics (IFI)
University of Zurich
Binzmühlestrasse 14, CH-8050 Zürich, Switzerland
URL: http://www.csg.uzh.ch/

Zusammenfassung

Mit zunehmender Bedeutung des Risikokonzepts im Bereich der Informationssicherheit wurden zahlreiche neue Risikobewertungsmethoden entwickelt. Die Auswahl einer geeigneten Risikobewertungsmethode kann sich als erste Hürde für Organisationen erweisen, die nicht über die finanziellen Ressourcen verfügen, um Beratungsfirmen einzustellen, die sie bei dem Risikobewertungsprozess unterstützen. Um diese Herausforderung zu bewältigen, wurden Vergleichsmethoden und -tools in der akademischen Welt und im privaten Sektor entwickelt. Diese Arbeit bietet eine umfassendes Review über diese Methoden und Tools. Auf Basis dieses Reviews und einer gründlichen Analyse mehrerer gängiger Methoden zur Bewertung von Informationsrisiken wird eine verbesserte Vergleichsmethode entwickelt. Diese Methode wird dann genutzt, um neun Methoden zur Bewertung von Informationssicherheitsrisiken zu evaluieren. Ein navigierbarer Prototyp für eine Wissensdatenbank zur Bewertung von Informationssicherheitsrisiken wurde entworfen und entwickelt, um den Vergleich zwischen den Methoden zu erleichtern und den Nutzern bei der Auswahl der am besten geeigneten Bewertungsmethode zu helfen. Es wird gezeigt, dass die verbesserte Vergleichsmethode bisherigen überlegen ist, da entscheidende Kriterien übernommen werden und neuartige Kriterien den Auswahlprozess verbessern. Abschließend wird anhand eines Anwendungsfalls die Effizienz des Prototyps veranschaulicht.

Abstract

With the increasing relevance of the risk concept in the field of information security, numerous new risk assessment methods have emerged. The selection of a suitable risk assessment method can prove itself to be a first obstacle for organizations that do not have the financial resources to employ consulting firms that assist with the risk assessment process. To address this challenge, comparison methods and tools have been developed in academia and the private sector. This thesis provides a comprehensive review of these methods and tools. An improved comparison method is designed based on this review and an in-depth analysis of several common information risk assessment methods. This method is then used to evaluate nine information security risk assessment methods. A navigable prototype for an information security risk assessment knowledge base has been designed and implemented, with the aim of facilitating comparison between methods and helping users select the most suitable assessment method. The improved comparison method is shown to be superior to predecessors by demonstrating that crucial criteria are adopted and novel criteria improve the selection process. Finally, a use case illustrates the efficiency of the prototype.

Acknowledgments

I would like to express my deepest gratitude to my supervisor, Jan von der Assen, for his exceptional guidance, encouragement, and support throughout my Bachelor thesis. Jan's insightful feedback and constructive criticism have been instrumental in shaping the final outcome. Without his expert guidance, this work would not have been possible.

I am also grateful to the Communications Systems Group (CSG) at the University of Zürich and Prof. Dr. Burkhard Stiller for providing me the chance to work on a topic that sparked my interest from the beginning and let me explore the field of information security risk management.

Lastly, I would like to thank my father and my girlfriend for proofreading my work.

Contents

Chapter 1

Introduction

FINMA's annual report of 2021 [1] stated that cyber risks are one of the primary risks in the Swiss financial market. It also reported that many companies do not have a clear definition of the scope of their critical information security (InfoSec) assets. As a result, the implementation of extensive security controls and safeguards becomes more challenging [1]. The adoption of an information security risk management (ISRM) framework can solve this problem. An essential part of the ISRM is the information security risk assessment (ISRA) process, which identifies, analyzes, and evaluates risk such that a suitable treatment can be applied [2]. Because there are numerous different approaches to conducting an ISRA [3], it is in the best interest of an organization to choose the most suitable method. In the course of this thesis, an improved comparison approach for ISRA methods is developed and used to implement a knowledge base prototype to facilitate the comparison and selection of ISRA methods. Below the motivation for comprehensively studying ISRA methods and the development of such a tool is demonstrated. The chapter ends with an outline of this thesis.

1.1 Motivation

Regarding ISRM, Wheeler [4] states, ”there is no single out-of-the-box security approach, implementation, or standard that will work for every organization”. This statement can as well be applied to ISRA methods. Organizations are left to choose from a vast amount of different ISRA methods that are growing every year. Just recently, the Center for Information Security released their new CIS-RAM [5] method.

Research by the author indicated that there are not many tools in the private or government sector to support the selection of a suitable ISRA method. The author of this paper assumes that this is because most consulting firms or governmental bodies are interested in providing their own custom-designed solution. Either to be able to sell a product or to guarantee compliance with their standards. The identified tools either depend too much on expert knowledge [6] or were mainly focused on ISRM selection [7] [8]. One tool in academia [9] was discovered but turned out to use the same method as [6]. Other selection support methods discovered in academic papers included comparison frameworks like the ones of Shukla and Kumar [10] or Agrawal [11]. In this thesis, comparison frameworks are defined as a set of criteria, like tool support or target audience, that can be used to evaluate ISRA methods with respect to numerous different aspects. These comparison frameworks were seen as insufficient because either the criteria were not expressive [10] enough or clearly enough defined [11]. The approach developed by Wangen, Hallstensen, and Snekkenes [3] only focused on completeness, which seemed not enough to select a suitable ISRA method. This inspired the author of this work to develop an improved comparison framework.

Because of the lack of proper summarizing of ISRA methods in related work, the author of this thesis needed to dedicate a substantial amount of time to research each ISRA method. This had two implications: First, for each evaluated method a summary and discussion should be provided in this thesis. And second, an efficient, easily navigable prototype for a knowledge base containing the output of evaluation of ISRA methods should be implemented. This knowledge base prototype aims to facilitate the ISRA method selection process.

1.2 Description of Work

The goal of this thesis is to develop a navigable ISRA method knowledge base prototype that facilitates comparing methods and therefore assists with the selection of a suitable ISRA method. The prototype is based on an enhanced comparison framework that is developed in the course of this thesis. It is complemented by a collection of comprehensive summaries of each ISRA method that should help assure the user that an appropriate method is chosen.

To get familiar with the topic of information security risk Wheeler's [4] book about building an ISRM was studied. To deepen the knowledge about ISRA methods, two standard methods were analyzed. The acquired background knowledge was the basis for a thorough review of the academic literature and material found in the private sector, which treated the comparison of ISRA methods and tools that support selection or comparison. After realizing that there was not enough material concerning comparison and selection tools, the focus was shifted to the ISRA method comparison literature. The review of existing comparison frameworks inspired the idea to develop an improved framework that was going to be implemented using a knowledge base.

Nine common ISRA methods were chosen to be studied further, which required the review of each primary source. Based on this review and the related academic work, the methods were summarized and discussed. The information gathered this way would later assist a user of the prototype in case no unambiguous choice could be made or if the user needs extra assurance that his selection choice was indeed suitable.

The improved comparison framework was developed by defining each evaluation criterion based on the previous frameworks, the related work, and the study of the ISRA methods.

It was then used to evaluate the different ISRA approaches. The output of the evaluation through the improved comparison framework was compiled into a knowledge base prototype using an existing, free, open-source software.

At last, the framework developed in this thesis was compared to its predecessors and its superiority was demonstrated. Additionally, a use case proves the efficiency of the prototype and demonstrates how it can be used together with this thesis to facilitate ISRA method selection in a real-world situation.

1.3 Thesis Outline

This thesis is structured as follows: Chapter 2 describes the necessary background knowledge to follow the rest of the thesis. In chapter 3, a review of the related work is demonstrated and at the end, it is exemplified how the related work has shaped the remainder of this thesis. Chapter 4 provides summaries and discussions of nine common ISRA methods, based on the in-depth analysis of the primary sources. Chapter 5 presents the criteria that form the improved comparison framework, which is used to evaluate ISRA methods, and the results of the evaluation of nine assessment methods. Afterward, the prototype for the ISRA method knowledge base and the software used to implement it is introduced. In chapter 6, it shows how the improved comparison framework is superior to the other alternatives. Additionally, a case study is utilized to demonstrate the efficiency of the knowledge base prototype. The final chapter summarizes the thesis and discusses possible future work.

Chapter 2

Background

This chapter intends to give the reader an understanding of what is generally understood by the term information security risk assessment. It starts with explaining the fundamental attributes of information security. Then the focus is shifted to the risk management part of information security. After the groundwork is laid, the term information security risk assessment is explained in detail, and it is shown how an assessment is integrated into the encasing information security risk management process. Throughout the remainder of this thesis, the terms risk, risk assessment, and risk management will be used to refer to concepts relating to information security risk.

2.1 Information Security

Based on the definition of [4], we define that in information security an organization or a group of people must guarantee the confidentiality, integrity, and availability of assets that lay in their purview. In this context, assets are resources of value [12] like information or services that provide access to such. Wheeler also defines accountability as part of those responsibilities. This makes sense for a more technical view of information security but is not necessary for the context of risk assessments. Based on the meanings of the terms by Peltier [12], we define ensuring the confidentiality of information as prohibiting unauthorized access. Preserving the integrity of information as guaranteeing that no unplanned modifications take place. And lastly, maintaining the availability of resources can be defined as securing access to them for authorized entities at required times. From now on, confidentially, integrity, and accountability are referred to as the attributes of the CIA-triad.

2.2 Information Security Risk

Building on the definition of information security, the corresponding risk term is defined here as a measure of compromise of one of the CIA-triad attributes [13]. Using this definition and the threat term of Peltier [12] we define a threat in the context of this work as a potential circumstance or event that could have a negative impact on either of the CIA attributes. NIST [13] characterizes the term threat through event and source or actor. The event is the realization of the threat, and the source or actor is the origin or responsible entity. Threats can be adversarial as well as non-adversarial. Non-adversarial threats are typically potential errors and accidents, whereas adversarial threats are typically potential attacks [13]. An example threat could be the crafting of a phishing attack by a hacker group conducting industrial espionage. The opening of a phishing email could be a corresponding threat event. Threat actors exploit vulnerabilities, which can affect controls, procedures, and even implementation. Not only software resources but also personnel can be vulnerable. An employee that has not received training in the field of social engineering attacks might be especially vulnerable to phishing.

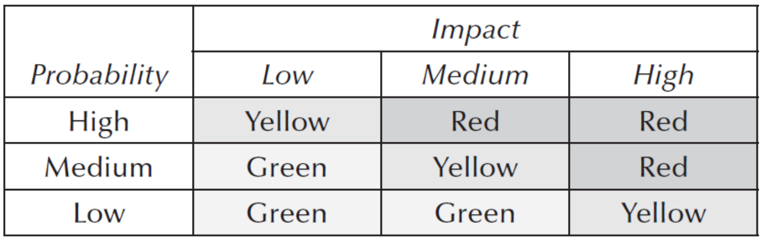
Talking about vulnerabilities, it is worth mentioning that NIST [13] makes use of the term predisposing condition. These conditions either increase or decrease the chance that a threat event negatively impacts one of the CIA-triad attributes, given it occurs. Typical examples are pre-existing security controls and safeguards. Those terms simply represent risk-altering measures [14]. As an example, the CIS controls [15] include email and web browser protection. Safeguards that make up the controls are more specific measures like email server anti-malware protection.

2.3 Information Security Risk Assessment

Risk is assessed through different risk factors depending on the risk model used [13]. In the example of NIST [13] risk is a combination of likelihood and impact. Wheeler [4] treats the likelihood as the probable frequency of CIA-compromise, NIST [13] on the other hand as the likelihood of vulnerability exploitation by a threat. Peltier [12] uses the term probability instead of likelihood, simply describing the probability of a threat event. In this work, the terms likelihood and probability are used interchangeably in the context of risk factors. Generally, the definition of Wheeler [4] is used. However, when discussing risk assessment methods, one should think of likelihood as an abstract concept that has different exact meanings depending on the method context. In the same way, impact and consequence are used interchangeably. Again, we use the terminology of Wheeler [4] and define impact as the probable extent of CIA compromise. The risk model defines risk factors and how these are connected to assess risks [13]. Most of the models that are discussed in this thesis use the relationship:

$$likelihood \times impact = risk \qquad \text{resp.} \qquad probability \times consequence = risk \quad [3]$$

Using the NIST [13] terminology, a risk model along with a risk assessment process, an assessment approach, and an analysis approach form a risk assessment methodology (see Figure 2.2). The assessment approach refers to how the risk factors of the risk model are measured and how risk is determined using the measurement of the risk factors. In this work, it is differentiated between quantitative, qualitative, and hybrid approaches as in [16]. Quantitative approaches make use of numbers for the measurement of risk factors and risk can be determined through a mathematical formula. Qualitative approaches on the other hand use scales that divide a range into categories or levels. Hybrid approaches are semi-quantitative, meaning that an integer range is used to represent different qualitative levels [13]. An example of qualitative levels for the impact risk factor could be low, medium, and high in a simple case. In qualitative and semi-qualitative approaches, risks are determined using matrices that map different risk factor levels onto an overall risk level [13]. In fig. 2.1 we see the overall risk level expressed in a traffic light rating system.



Probability	*Impact*		
	Low	*Medium*	*High*
High	Yellow	Red	Red
Medium	Green	Yellow	Red
Low	Green	Green	Yellow

Figure 2.1: Simple Risk Calculation Matrix [12]

The analysis approach as defined by NIST [13] describes the axis along which the problem gets initially split into smaller sub-problems. An asset-driven analysis approach, for example, identifies all the critical assets that are relevant to the situation and continues the assessment process for each of the assets. The assessment process describes each step that must be undertaken to yield the desired assessment output.

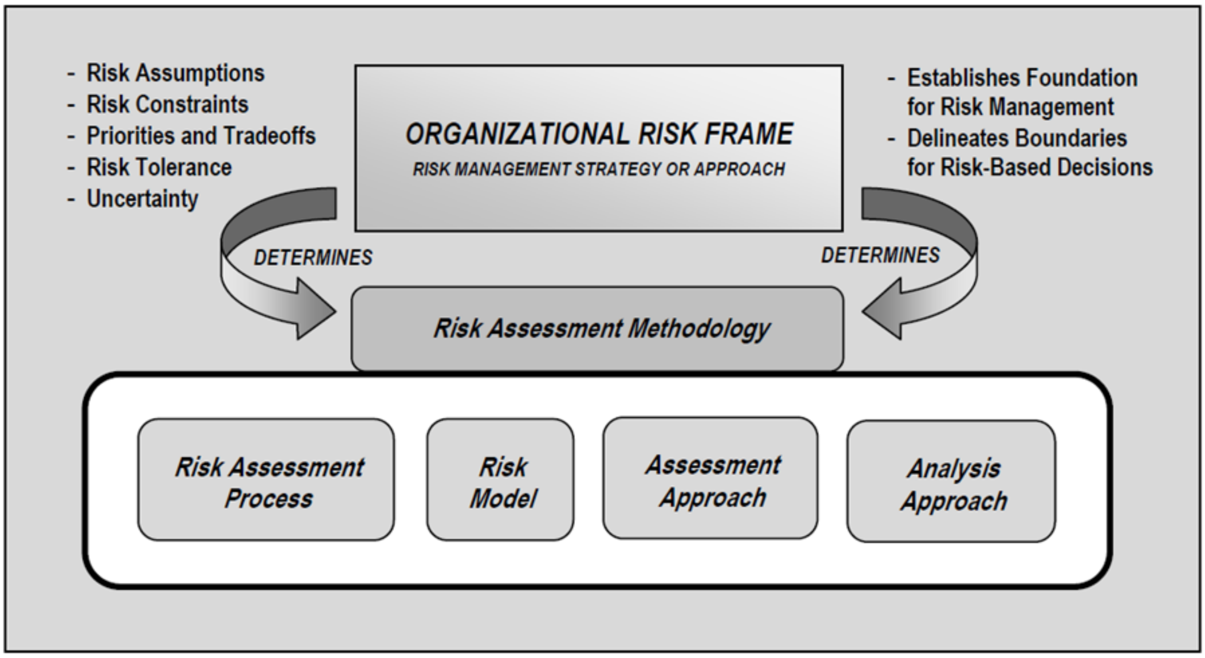

- Risk Assumptions
- Risk Constraints
- Priorities and Tradeoffs
- Risk Tolerance
- Uncertainty
ORGANIZATIONAL RISK FRAME
RISK MANAGEMENT STRATEGY OR APPROACH
- Establishes Foundation for Risk Management
- Delineates Boundaries for Risk-Based Decisions
DETERMINES
DETERMINES
Risk Assessment Methodology
Risk Assessment Process
Risk Model
Assessment Approach
Analysis Approach

Figure 2.2: Overview Risk Assessment Methodology [13]

The ISO 27005:2018 [2] document is used to give an overview of a general risk assessment process. It identifies three stages of the general information security risk assessment process: Risk identification, risk analysis, and risk evaluation. Risk identification entails identifying and documenting information security risks. In the risk analysis phase risk factors like likelihood and impact are assessed and based on these factors the overall risks for the situation are calculated. Finally, during risk evaluation, it is decided whether the risks calculated during the analysis are acceptable and are ranked by priority. This is done by checking them against risk evaluation criteria, which were defined while establishing the context before the start of the risk assessment process. This is part of the general risk management process after ISO 27005:2018 [2] and includes besides defining the risk evaluation criteria, which reflect the risk acceptance position of an organization, the setting of the assessment scope.

After the assessment process, based on the risk evaluation, a risk treatment plan is compiled. Treatment actions are accepting, avoiding business processes leading to the risk, transferring the risk by outsourcing or insurance, or mitigating using controls [4]. Next to context establishment and risk treatment, the risk management process includes communication and monitoring, which are both continuous functions that run in parallel to all the before-mentioned phases. The communication makes sure that relevant information concerning the risks and assessment results are passed to management and affected stakeholder, possibly in the form of a risk assessment report (RAR). The duty of monitoring entails the review and improvement of the ISRM process itself. Figure 2.3 shows an overview of the ISRA and ISRM process after ISO 27005:2018 [2].

The processes described in the last paragraph should be an example of general ISRA and ISRM to give the reader an initial understanding. In reality, there are different assessment and management approaches that employ a variety of sub-processes and functions. Context establishment and risk treatment for example are seen as part of the risk assessment process in many methods [3].

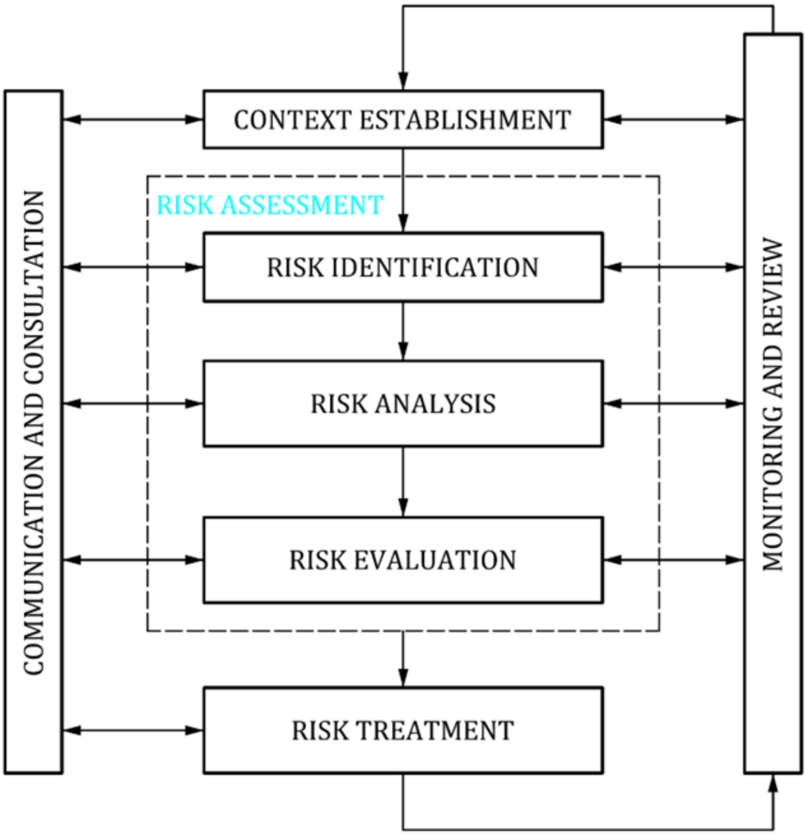


Figure 2.3: ISO 27005 Within the ISO 31000 Process [2]

Chapter 3

Related Work

3.1 Related Academic Work

To search for related academic work the two web search engines Google Scholar and IEEE XPLORE were employed. At first, a combination of the search terms ”cyber”, ”information”, ”risk”, ”assessment”, ”management”, ”method”, ”framework”, ”choose”, ”selection”, ”software”, and ”tool” were used to search for mentions of ISRA selection frameworks, software or tools. One conference proceeding was found introducing a selection framework that uses a multi-criteria model [9]. A decision was made to loosen the criteria for related academic work and the additional search terms ”comparison” and ”review” were used to search for comparison frameworks. Eight papers were found on the topic of comparing and classifying ISRA and risk analysis methods. Since risk analysis is a crucial part of the risk assessment process [2] works with the said subject were included. Academic papers older than a decade of comparison frameworks and taxonomies were studied but aren’t explicitly listed below as these concepts are referenced in recent works. In the following, the related academic works are summarized and an overview table (see Table 3.1) is provided.

3.1.1 Multi-Criteria Selection Framework

In this conference proceeding Sajko, Hadjina, and Pešut [9] create a selection framework supported by a multi-criteria model which uses an analytical hierarchy process (AHP) [17]. The AHP helps an assessor choose from risk assessment methods depending on the importance of predefined criteria and sub-criteria. The authors first define a set of basic characteristics of risk assessment methods. Based on an analysis of methods, tools, scientific papers, and surveys on the importance of these characteristics in business organizations a hierarchy of criteria and sub-criteria is established. A group of IT directors of business organizations function as assessors and compare the relative importance of the criteria. This yields a model, which is then subjected to sensitivity analysis. The researchers conclude that the model implies that smaller businesses with fewer financial resources, knowledge, and historical data should use simple qualitative methods. Larger companies on the other hand are recommended to utilize methods and frameworks that are able to both do a quantitative and qualitative analysis. The paper ends with the most important findings, namely that the multi-criteria model is suitable for choosing an appropriate risk assessment method and that the quantification of the importance of criteria enables a method type (qualitative, quantitative) independent comparison [9].

3.1.2 Taxonomy of security risk assessment approaches for researchers

Paintsil [18] proposes a taxonomy for security risk assessment method. The primary use of this taxonomy is to help researchers determine their exact research area within the realm of risk assessment approaches. The author first differs between bottom-up/IT-centric (asset-oriented) and top-down/info-centric approaches. Additionally, the taxonomy distinguishes between traditional and contemporary methods. Traditional approaches are prone to be subjective since the assessment depends on the opinion of a subject matter expert. These are further categorized as list- or model-based either with or without formal support (estimation techniques to reduce uncertainty). Contemporary approaches on the other hand, are not subjective since they depend on formal processes, defined models, and tests. There are three kinds of contemporary approaches: Formal model-based, executable (informal) model-based, and system-based. The latter does not use a model but works with a prototype or the real-world implementation [18]. The work presented here focuses on traditional, bottom-up/IT-centric approaches since most prominent examples that are treated in research papers belong to these two categories.

3.1.3 A comparative study on information security risk analysis practices

In the study Shukla and Kumar [10] compare six risk analysis methods and tools. A brief overview of each risk analysis practice is given where the calculation method is explained and a rating for simplicity and accuracy is proposed. They further provide a table where the different methods and tools are categorized into qualitative and quantitative and various properties like price, compliance to standards, skill level, availability, and tool support are listed [10]. As mentioned by Agrawal [11] one does not get information on the advantages and disadvantages of different methods but a rather simple comparison of attributes like price or vendor name.

3.1.4 A conceptual framework of info structure for information security risk assessment (ISRA)

The paper commences by arguing that at the time of its writing, no standardized comparative framework for ISRA methods exist. Shamala, Ahmad, and Yusoff [19] then introduce definitions for the ISRA term and list six methodologies they compare to come up with a desired ISRA info-structure to standardize comparison. The six methodologies are summarized within a table that includes the risk model/phases of the approaches. It is then documented how they developed their info-structure: A first comparative study yielded one category of information and three activities to gather information to be able to properly conduct a risk assessment: Management requirements, establishing organizational context, identifying assets, threats, and, vulnerability, and risk management improvements. These were labeled main features. Using a second comparative study those main features were divided into sub-features. Main and sub-features were then temporally arranged into the desired info-structure. A graphic of this info-structure is presented in the article. Further, a table with the main and sub-features and an indicator of whether each of the ISRA methodologies fulfills the criteria or not is given as well [19].

3.1.5 Taxonomy of information security risk assessment (ISRA)

Based on 125 published papers, Shameli-Sendi, Aghababaei-Barzegar, and Cheriet [16] aim to provide a thorough taxonomy of ISRA methods. Three new characteristics are proposed to classify ISRA methods: Perspective, resource valuation, and risk measurement. The perspective category relates to the risk identification phase and divides into asset-, service-, and business-driven approaches depending on whether risks to assets, services, or business processes are identified. Resource valuation corresponds to risk analysis and looks at the connections between different types of resources. From a vertical view an asset can be connected to services, services connected to business processes, both of the before mentioned connections can be present, or all levels can be independent. Additionally, those resources are dependent on or independent of resources on the same level. The newly proposed category risk measurement looks at the measurement model and differs between propagated and non-propagated risk scores. The researchers classify nine approaches developed by professional organizations and 22 approaches from research papers using their newly proposed and well-known categories qualitative, quantitative, and hybrid. The results are presented in a table where additionally used techniques, input/output, and risk phases are mentioned. In the end, the paper lists each category's advantages and disadvantages of approaches depending on how they were classified within this category. Even though the proposed taxonomy is suitable for classifying newer and lesser-known risk assessment approaches, it has limited use for this thesis since the majority of the approaches considered here do not differ in terms of perspective, resource valuation, or propagation [16].

3.1.6 A comparative study on information security risk analysis methods

In this work Agrawal [11] compares two qualitative and two quantitative methods using a previously known classification Scheme. Each method is characterized as having a type of approach and level of expertise. Types of approaches include temporal, functional, and comparative, whereas levels of expertise include expert-, collaborative-, and owner-level [20]. After the methods are summarised and their corresponding ontology is shown, each is classified using the mentioned scheme. In the end, a table is presented in which the different methods are compared in respect of methodology, purpose, input, effort, outcome, scalability, and advantages, respectively disadvantages [11]. Even though only four different risk analysis methods are compared the paper still provides useful information in a compact format since important properties are discussed.

3.1.7 Information Security Risk Assessment: A Method Comparison

In this study, Wangen [21] compares three different ISRA methods. At the beginning of the paper the reader is provided a short overview of the ISRA approaches and the CURF [3] framework. The result of applying the CURF framework to the three methods is shown in tabular form. Afterward, the method of the study is explained: For each method, a risk assessment report was produced and then compared to the findings of applying CURF. Several different groups of students had to perform an assessment using one of the ISRA approaches in the setting of a Norwegian academic institution with the support of supervisors. To collect the data for the risk assessment report interviews and questionnaires were utilized. It is important to note that all of the students were given a six-week basic ISRA training before working on the assessments. The paper summarizes the experiences of the students for each of the ISRA approaches. A table of the findings is given which includes advantages, disadvantages, and an overview of supplementing literature that was used to conduct the assessments. In the end, the Wangen conclude that the comparison of applying CURF and the practical experiences of the students show a direct connection between the completeness and further a causation between which ISRA tasks are covered and outcomes of the assessments [21].

3.1.8 A framework for estimating information security risk assessment method completeness

In this article Wangen, Hallstensen, and Snekkenes [3] present the Core Unified Risk Framework (CURF), whose application is to assess the completeness of ISRA approaches. To build this framework the three core activities risk identification, estimation, and evaluation of eleven different ISRA methods were compared. Complementary software was ignored and didn't influence the framework. After giving a short summary of all of the ISRA approaches the authors go on to explain how they build the framework. Instead of comparing different methods to predetermined criteria, the covered tasks of all of the methods compared are gathered in a collective task inventory. Now a method used in building the framework can be assessed by evaluating how many and which kind of tasks it addresses compared to the collective inventory. Tasks are either addressed, partially addressed, or not addressed. Applying the framework to a method that was not used to build it includes gathering all the tasks covered by the approach, adding them to the collective task inventory, and evaluating it like in the procedure explained before. For each core activity, all tasks are summarized and a table is provided that shows which of the eleven compared methods addresses which task of said activity [3]. An additional table is provided that summarizes the overall outcomes. The results for each of the compared ISRA approaches are then discussed in more detail. Moreover, it is classified using an older scheme developed by Sandia Labs [20] and a formula for the risk estimation is given using previous work of Aven [22]. After discussing the completeness of ISRA approaches the authors then present their general findings on the scope and limitations of current ISRA methods, and discuss the limitations of their own work [3].

3.2 Related Work in the Private or Government Sector

The search for related work in the private sector started with using the general Google search engine. Unfortunately, no selection frameworks were found this way. Searching in the references of academic works yielded three results. One of them is part of a book written by Wheeler [4] and short and high-level that it is not summarised here. Nevertheless, its implications will be mentioned later in this work. The lack of selection frameworks coming from the private sector can be explained by companies and governmental bodies wanting to offer their own ISRA solution instead of helping to select an existing method. Another possible reason is that customers want certifiable methods that are smaller in number and standardized. Therefore eliminating the need for an elaborate selection framework. In the following, the related works from the private and government sector are summarized.

3.2.1 Determining Your Organization's Information Risk Assessment and Management Requirements and Selecting Appropriate Methodologies

ENISA's tech report [7] describes a questionnaire that organizations can use to roughly estimate their risk profile, a combination of risk exposure and impact. Based on this profile risk assessment and management methods are recommended to fit the organization's needs. A tool is mentioned called the Self Assessed Risk Profiler (SARP) and was later developed to automate the process described in this report [8]. The questionnaire consists of 15 high-level questions of which nine are related to risk exposure and six to risk impact. Each answer corresponds to a numerical score and the total is used to determine the place in a four-quadrant matrix with axis exposure and impact both being divided into low and high. This can be used to give a first estimate of the risk assessment and management needs of the organization. The granularity of both axes of the matrix is then refined to be divided into low, some, high, and critical. From the resulting 16 quadrants, two are left out leaving 14 exposure-impact segments. Further 15 risk management processes are defined. For each segment general information, level of concern, requirements, and recommendations are given. Depending on the exposure-impact segment of an organization, it is either able to ignore an objective or has to use a simple, formal, or detailed process to accomplish said objective. This gives a risk profile for an organization which can be compared to a profile of a risk management method that has been assessed in previous work to determine whether it is a fitting solution for the organization. This process was tested in an ENISA-sponsored conference and is according to the authors a feasible method for organizations to select an appropriate methodology [7]. When trying to use this method to choose a fitting risk assessment approach a major problem emerges: Only three of the 15 defined risk management processes used to create the risk profile are part of a typical risk assessment [23]. This reduces the expressiveness of the risk profile by approximately four-fifths when choosing a risk assessment instead of a general risk management method. Therefore this approach does not provide a proper solution for the issue discussed in this work.

3.2.2 Selection of information security risk management method using analytic hierarchy process (ahp)

Sajko, Hadjina, and Pešut proposed a multi-criteria model which utilized AHP [17] to determine a fit risk management approach [9]. Smojver [6] utilizes the same model but tests its applicability with information security risk specialists instead of business leaders. Assessing the model consists of a selection between five ISRA approaches. As in the previous paper [9] Smojver deems the model to facilitate choosing ISRA methods [6]. It is to be said that the author of this paper speaks of ISRM rather than ISRA methods but still compares methods that are seen as ISRA methods. Therefore we treat this work as an ISRA selection rather than an ISRM selection.

3.2.3 FINMA Guidance 05/2020

Since governmental bodies of other countries like Germany [24] or Norway [25] had come up with their own ISRA guidance, it was natural to search for a similar approach in Switzerland. By simple means of googling nothing could be found. Since one of FINMA's core tasks includes continuous cyber supervision of the finance sector with on-site supervisory reviews and monitoring of cyber attacks [1] their official website was searched. Unfortunately, no guidance concerning ISRA was found. Nevertheless, a document was found concerning the obligation to report cyber attacks to the FINMA [26]. It specifies the contents of a mandatory cyber attack report to the FINMA. Among them is an initial assessment of the attack severity, which is linked to a risk via the exploited vulnerability. This initial attack assessment is therefore closely connected to an insufficient risk assessment that has already been done and a reassessment of said risk or a risk assessment that has yet to be conducted. In the appendix, the FINMA gives the definitions and criteria for different cyber attack severity levels. This can be used to link them directly to different possible outcomes of one's risk analysis stage to facilitate the transition from risk to attack assessment or vice versa.

3.3 Implications of Related Work

An initial approach to support the selection of an appropriate ISRA method included the implementation of a multi-criteria model based on AHP [17] like in the papers of Sajko, Hadjina, and Pešut [9] or Smojver [6]. This idea was discarded based on the reason that in both papers expert practitioners with several years of experience in managing or practicing InfoSec were required to conduct the selection.

Another approach that could have been implemented was the use of a questionnaire to create a scorecard describing the needs of a user with numerical values and comparing it to the values of pre-defined ISRA method scorecards as done by ENISA [7] [23]. A downside of such an approach is that numerical values can not capture the characteristics of an ISRA method as well as text. Assigning a value for the level of tool support methods provide is not nearly as expressive as a short one-sentence description of the actual tool. It would have been possible to complement the scorecards with text documenting characteristics that were unfit to be described by numerical values.

Instead, the approach of developing a framework for comparison as done by Shukla and Kumar [10] or Agrawal [11] was chosen, where an ISRA method is evaluated by analyzing characteristics that do not need an expert practitioners knowledge to be assessed. The term framework here is not to be understood as a technical framework but as a comparison framework. As mentioned in the introduction, a comparison framework includes a set of criteria, which are used to evaluate ISRA methods and compare them against each other. The difference to methods like the CURF [3] framework, which also declares itself as a comparison framework, is that the criteria allow for a general evaluation and do not only concentrate on one aspect like completeness. Agrawal [11] criticized Shukla and Kumar harshly saying, ”the reader learns nothing about the particular benefits, performance, input, output, effort associated with these methods.” Agrawal [11] presented an improved ISRA method comparison framework, which builds the basis together with the work of Shukla and Kumar [10] for the selection-support product of this work.

Academic papers about the classification and comparison of ISRA methods were combed through in the search of possible ISRA method candidates for selection and evaluation criteria that would make up the comparison framework. Paintsil [18] created a taxonomy to classify different ISRA methods to guide research. Unfortunately, this classification does not help an organization to choose a fitting method, nor could any useful evaluation criteria for use in the improved framework be identified. Shamala, Ahmad, and Yusoff [19] developed a conceptual framework of info-structure for ISRA and studied whether six ISRA methods fulfill the criteria of the framework. These criteria inspired some of the comparison framework characteristics discussed in section 5.1. Another well-thought-out taxonomy was created by Shameli-Sendi, Aghababaei-Barzegar, and Cheriet [16]. The newly proposed characteristics perspective, resource valuation, and risk measurement seemed interesting to include in the comparison framework at first. It turned out that all of the methods considered for selection in this work fall into the same categories for each of those characteristics with minor exceptions. Therefore these characteristics lacked the expressiveness to be included as evaluation criteria.

The participants of the study conducted by Wangen [21] emphasized the importance of complementary material and examples for non-specialists. Because they argued that assessments are often conducted by non-specialists, complementary material became a crucial evaluation criterion for the comparison framework developed in the course of this thesis. Another implication of this study was that ISRA completeness as assessed by the CURF framework of Wangen, Hallstensen, and Snekkenes [3] correlates with RAR completeness, which led to including a completeness measure based on CURF. The initial selection of ISRA method candidates was also based on the methods analyzed by Wangen, Hallstensen, and Snekkenes [3]. The fact that Shukla and Kumar [10] and Agrawal [11] only covered a fraction of the ISRA methods deemed important by the author of this work led to the detailed analysis of different ISRA methods, which is covered in the next chapter.

Table 3.1: Summary of Related Academic Works

Paper	**Authors**	**Output**	**ISRA Approaches**	**Year**
Multi-criteria model for evaluation of information security risk assessment methods and tools [9]	M. Sajko, N. Hadjina, and D. Pešut	Selection framework	CRAMM, COBRA, FMEA, OCTAVE, RUSECURE	2010
Taxonomy of security risk assessment approaches for researchers [18]	E. Paintsil	Taxonomy	CRAMM, CORAS, OCTAVE, ISRAM, IS, ISO/IEC 27005:2011, Game theoretic approach, EBIOS, RiskIt, Delphi approach, Attack graph-based, Dynamic incentives method, LBRT, FTA, Goal-oriented, STRAP and 7+ ”contemporary” approaches	2012
A comparative study on information security risk analysis practices [10]	N. Shukla and S. Kumar	Comparative study	CRAMM, CORA, CORAS, OCTAVE, IS, ISRAM	2012
A conceptual framework of info structure for information security risk assessment (ISRA) [19]	P. Shamala, R. Ahmad, and M. Yusoff	Comparison framework	CRAMM, CORAS, OCTAVE, ISRAM, NIST SP 800-30	2013
A comparative study on information security risk analysis methods [11]	V. Agrawal	Comparative study	CORAS, CIRA, ISRAM, IS	2015
Taxonomy of information security risk assessment (ISRA) [16]	A. Shameli-Sendi, R. Aghababaei-Barzega, and M. Cherie	Taxonomy	CRAMM, CORAS, OCTAVE, OCTAVE Allegro, Magerit V2, Microsoft’s Risk Assessment model, Mehari, ISO/IEC 27005:2011, NIST SP 800-30 and 22 research projects	2016
Information Security Risk Assessment: A Method Comparison [21]	G. Wangen	Comparative study	OCTAVE Allegro, ISO/IEC 27005:2011, NSMROS	2017
A framework for estimating information security risk assessment method completeness [3]	G. Wangen, C. Hallstensen, and E. Snekkenes	Completeness comparison framework	CIRA, CORAS, CCTA, FAIR, NSMROS, OCTAVE Allegro, ISO/IEC 27005:2011, NIST SP 800-30, ISACA, RAIS, Microsoft’s Cloud Risk Decision Framework	2018

Chapter 4

Information Security Risk Assessment Methods

The selection of ISRA methods treated in this work was based on the approaches in the CURF development by Wangen, Hallstensen, and Snekkenes [3]. CIRA [27], CRAMM [28], NSMROS, RAIS [25] and RISK IT [29] were removed. Instead, two methods were added: The CIS RAM [5] method, because of its focus on controls [15] and the FRAAP [12] method, because of its mention by Wheeler [4]. In the following, each ISRA method is summarized or the reason for its omitting is given. In the end, a table (see Table 4.1) is presented, which lists the ISRA methods that are considered candidates for selection, their corresponding ISRM, and the publication year of the source that was used to investigate the method.

The summaries of the ISRA methods demonstrated below constitute a significant contribution of this thesis. To compile them each method was studied using the corresponding white paper or the book that introduced the ISRA approach. The summaries should be understandable by everyone who familiarized themselves with the background as presented in Section 2. Even if the reader does not intend to read the rest of the thesis, they are provided with comprehensive and succinct summaries of some commonly used ISRA method processes.

4.1 BSI-Standard 200-3

The BSI-Standard 200-3 [24] based on the IT-Grundschutz-Kompendium [30] is the only risk assessment method written in German that is considered in this work. The document starts off by explaining the problem that the German word *Risikoanalyse* translates to risk analysis, but in the context of information, security corresponds to the risk assessment and treatment process. Therefore even though titled as risk analysis, the BSI-Standard 200-3 includes risk identification, analysis, evaluation, and even treatment. The target audience of this paper is defined as organizations that are already familiar with the IT-Grundschutz and want to complement their information security management.

There are mandatory preliminary tasks which are described in the BSI-Standard 200-2 [31] that entail: Establishing scope, roles, and duties, conducting a structure analysis, determination of the need for protection, and assessment of the IT-Grundschutz elements in place. IT-Grundschutz elements can be system elements like applications, hardware, network components, or process elements like human resources, software development, or cloud usage and are all described in detail in the IT-Grundschutz-Kompendium [30]. The output of this preliminary work is a list of target assets for which a risk assessment should be done. Additionally, the management level must decide on the risk assessment method, define the risk appetite and determine the different risk owners and the time frame of the assessment. The document provides a list of fundamental threats and maps them onto a CIA attribute [24].

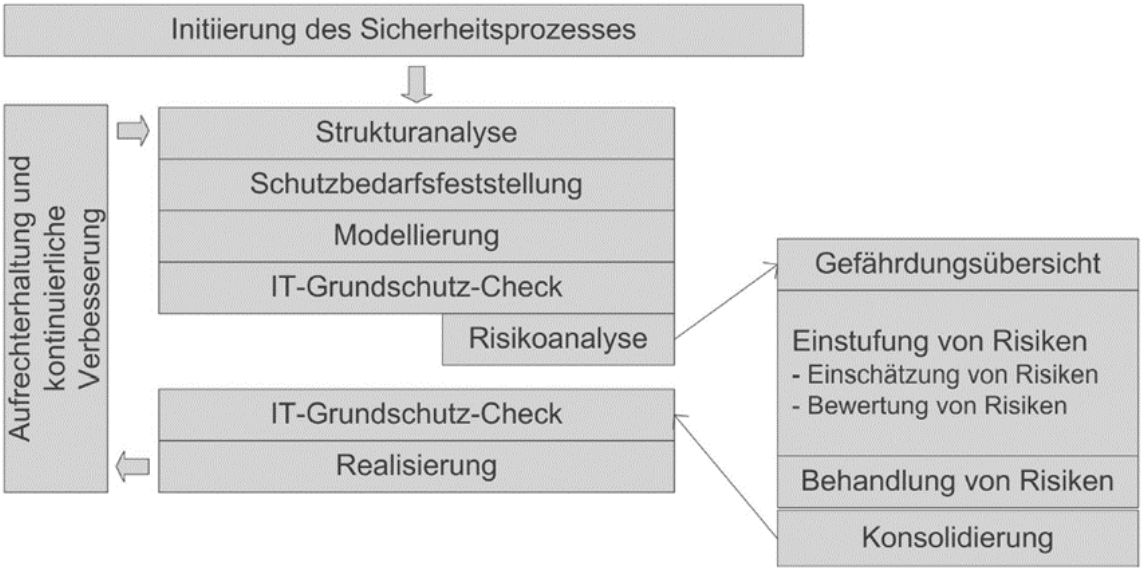


Figure 4.1: BSI Standard 200-3 within the IT-Grundschutz Security Process [24]

The actual risk assessment process starts with the identification of threats (Gefährdungsübersicht) which possibly impact the assets defined in the preliminary work. For each asset, one determines which elements of the IT-Grundschutz-Kompendium [30] make up the asset and maps the threats associated with these elements onto the asset. It is then checked whether other fundamental threats could impact the asset and if so whether they are directly or indirectly relevant. The asset should then be analyzed with respect to the CIA attributes and threats need to be identified that are not part of the fundamental threat list. It advised doing this in a dedicated brainstorming session with the different stakeholders of the asset and an information security expert. The output of the first stage is a table for each asset that lists all the possible threats with information about the CIA compromise, their relevance, and a short commentary. The document provides a short and a long extensive example for guidance[24].

In the risk analysis stage (Einstufung von Risiken), the likelihood and impact of each threat are determined. Regarding choosing a qualitative approach the standard takes a stance and discourages the use of a quantitative assessment approach except if extensive historical data is present and the knowledge to interpret it. The Standard provides two simple assessment scales for likelihood and impact. The risk can then be assessed by using a risk matrix they provide. The output from this step is a risk overview for each asset that is assessed. The examples from the last chapters are used to show how such an overview could look like, however, it is not clearly documented how to create each separate part of the overview [24].

The BSI-Standard 200-3 also contains guidance for risk treatment (Behandlung von Risiken) next to the traditional steps of a risk assessment method. The treatment options are: Avoiding, mitigating, transferring, and accepting. To guide the reader, for each of those actions the document provides a question that must be answered and reasons for this question to be answered with yes. For example, if one wants to avoid risk, it is crucial to ask whether this is feasible by restructuring a business process. Now the assessors have to repeat the risk analysis and treatment steps until an acceptable level of residual risk is reached. Subsequently, the risk treatment proposition is given to the management for approval. Regarding risk monitoring, the document advises noting down risks that could change in foreseeable future and already devising plans for their treatment. Additionally, a risk inventory should be installed to help keep an eye on all of the risks. The chapter ends with the continuation of the longer example to guide the reader [24].

The last stage of their risk assessment process is the consolidation (Konsolidierung) of one's security concept. This means that if, in the treatment stage, new security measures or controls were added, then their suitability, user-friendliness, quality, and how they act together must be assessed and possibly improved. After the successful integration of the new security measure and controls, it is possible to complement the IT-Grundschutz-Kompendium with user-defined elements for improved representation of critical assets and add newly found threats to the list of fundamental threats [24].

This risk assessment method is closely embedded into the BSI-Standard 200-2 [31], which is the ISRM based on the IT-Grundschutz-Kompendium [30]. It is hard to use as a stand-alone approach since the first step already builds on the identification of critical assets BSI-Standard 200-2 and the identification of IT-Grundschutz elements, which needs to be completed before beginning [24]. The description of the risk analysis part is lean in comparison with other methods, which decreases its usefulness to use it as a stand-alone method or integrate it into another ISRM. On the other hand, the strength of this method is exactly it's embedding into the IT-Grundschutz framework. It is one of the only risk assessment approaches available in German and its framework is certifiable on the basis of ISO 27001 [32]. Additionally, it incorporates existing knowledge about critical assets and existing security controls with the use of the assessed IT-Grundschutz elements of the organization. Supposing one is already familiar with the IT-Grundschutz framework, it is a simple method, which comes with advantages like having a sequential example, a risk treatment phase, and recommendations for determining the risk appetite of one's organization [24]. Unfortunately, no tool or documentation for automating the process in the Standard was found.

4.2 CIRA

The Conflicting Incentives Risk Analysis method [27] by Rajbhandari and Snekkenes is a risk analysis method in which stakeholders compete with the risk owners to accomplish their goals resulting in risk. Even though Rajbhandari and Snekkenes [33] demonstrated a use-case of CIRA, it is questionable whether this method is relevant, because of its rare mention in academia as well as in the private sector. At the time of writing, the initial [27] paper and the use-case article [33] had combined less than 50 citations on Google Scholar and couldn't be found on IEEE XPLORE. The Google search engine did not yield any results regarding mentions of CIRA in either the private or governmental sector. Therefore this approach was not taken into account in the further continuation of this work.

4.3 CIS RAM

The CIS Risk Assessment Method [5] is based on the CIS Controls [15] (see Figure 4.2). These are 18 controls consisting of different safeguards that need to be implemented by an organization to comply with the CIS framework. The extent of the implementation depends on the implementation group of an organization. The first implementation group corresponds to small to medium-sized organizations where limited IT and information security knowledge is present. The second implementation group characterizes bigger organizations with multiple departments, which employ information management and security personnel. The third and last group includes organizations, whose resources include a security department with specialized information security experts. [15] can be consulted for more details. The CIS RAM documentation consists of one core overview document and a CIS-RAM version with an Excel workbook for execution for each of the implementation groups [5].

The overview document [5] starts with a list of fundamental principles and practices based on DoCRA [34]. Afterward, the general risk assessment approach is described which begins with developing the risk criteria. Risk is defined as the combination of impact and expectancy, both of which need to be divided into different magnitude categories. If a quantitative assessment approach is used CIS RAM advises establishing a conversion from numerical values to categorical values using thresholds. Next is developing risk acceptance criteria, which is done by combining the minimal acceptable impact and expectancy one can determine the maximal level of accepted risk. After these two preparation steps, the actual modeling of the risk begins. Critical information assets and threats that endanger the confidentiality, integrity, or availability of said assets are identified. Next, all the CIS safeguards of the different controls that could defend the assets from the threats are determined and their corresponding implementation status within the organization. Possible vulnerabilities are mapped onto the safeguards and assets. Risks are then evaluated and if a risk is not within an acceptable level, CIS safeguards must be implemented or improved to mitigate the danger. In the end, the organization needs to make sure that the residual risk is in line with the fundamental principles of the CIS RAM. The target

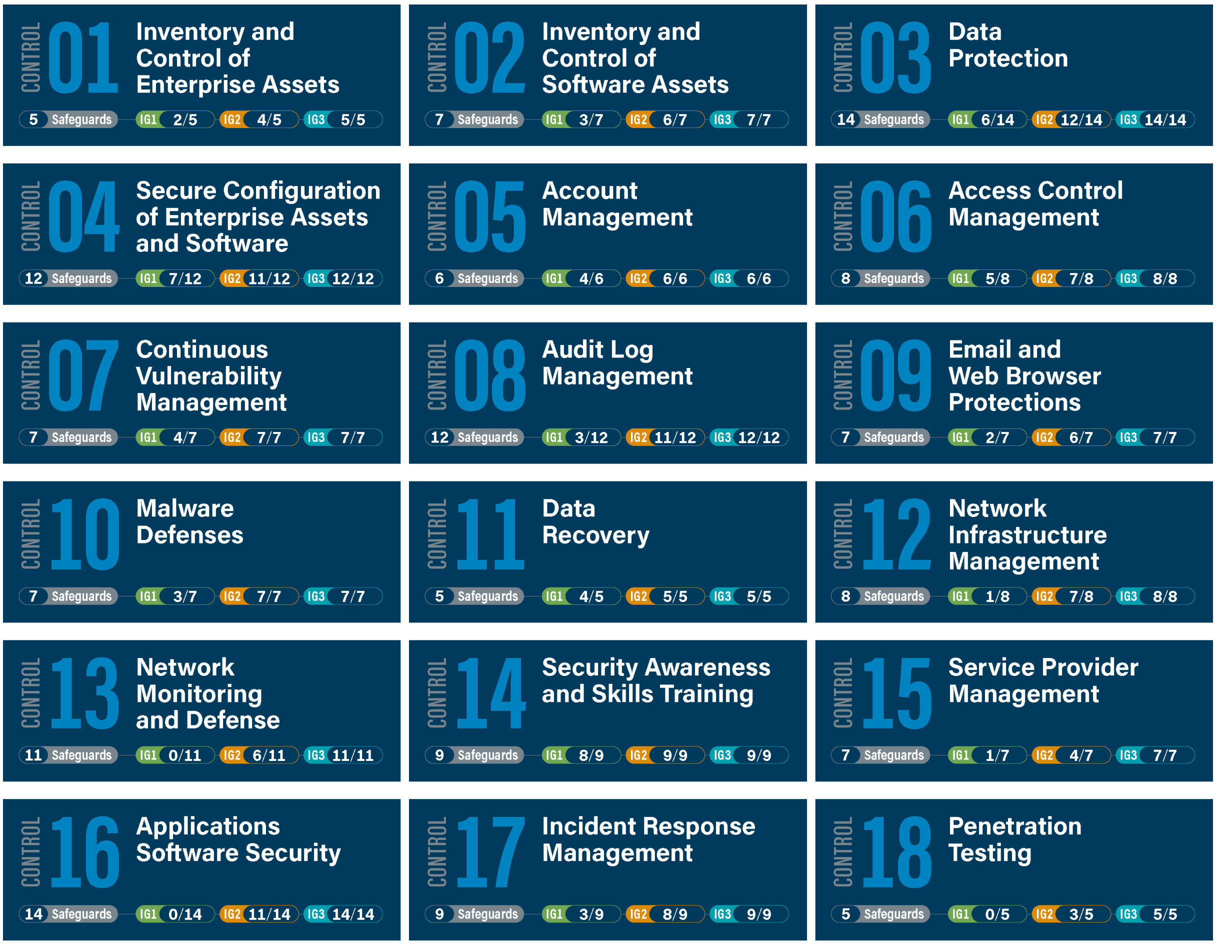

CONTROL 01 Inventory and Control of Enterprise Assets
5 Safeguards IG1 2/5 IG2 4/5 IG3 5/5
CONTROL 02 Inventory and Control of Software Assets
7 Safeguards IG1 3/7 IG2 6/7 IG3 7/7
CONTROL 03 Data Protection
14 Safeguards IG1 6/14 IG2 12/14 IG3 14/14
CONTROL 04 Secure Configuration of Enterprise Assets and Software
12 Safeguards IG1 7/12 IG2 11/12 IG3 12/12
CONTROL 05 Account Management
6 Safeguards IG1 4/6 IG2 6/6 IG3 6/6
CONTROL 06 Access Control Management
8 Safeguards IG1 5/8 IG2 7/8 IG3 8/8
CONTROL 07 Continuous Vulnerability Management
7 Safeguards IG1 4/7 IG2 7/7 IG3 7/7
CONTROL 08 Audit Log Management
12 Safeguards IG1 3/12 IG2 11/12 IG3 12/12
CONTROL 09 Email and Web Browser Protections
7 Safeguards IG1 2/7 IG2 6/7 IG3 7/7
CONTROL 10 Malware Defenses
7 Safeguards IG1 3/7 IG2 7/7 IG3 7/7
CONTROL 11 Data Recovery
5 Safeguards IG1 4/5 IG2 5/5 IG3 5/5
CONTROL 12 Network Infrastructure Management
8 Safeguards IG1 1/8 IG2 7/8 IG3 8/8
CONTROL 13 Network Monitoring and Defense
11 Safeguards IG1 0/11 IG2 6/11 IG3 11/11
CONTROL 14 Security Awareness and Skills Training
9 Safeguards IG1 8/9 IG2 9/9 IG3 9/9
CONTROL 15 Service Provider Management
7 Safeguards IG1 1/7 IG2 4/7 IG3 7/7
CONTROL 16 Applications Software Security
14 Safeguards IG1 0/14 IG2 11/14 IG3 14/14
CONTROL 17 Incident Response Management
9 Safeguards IG1 3/9 IG2 8/9 IG3 9/9
CONTROL 18 Penetration Testing
5 Safeguards IG1 0/5 IG2 3/5 IG3 5/5

Figure 4.2: Overview of the CIS Controls v8 [15]

implementation group of the CIS RAM version and its workbook determine, which tasks are necessary to assess the risk of an organization adequately [5].

The CIS RAM for the first implementation group [35] has three impact categories: Acceptable, unacceptable, and catastrophic. For each, the user needs to define the implications for the mission, operational objectives, and obligations. Additionally, it is possible to set financial objectives to check the reasonability of the annual cost in the end. Different asset classes are given and one needs to determine the highest possible impact on the mission, operational objectives, and obligations using the defined categories from before for each class. Now each safeguard is connected to a risk that needs to be assessed. Using a legend the maturity of a safeguard must be assigned and based on this the expectancy score, risk scores, and corresponding acceptance levels are automatically calculated. Now the risk is either chosen to be accepted or reduced. The safeguard maturity is then to be reevaluated after realizing the treatment option. Finally, it is shown whether the treatment option was sufficient or not and if the safeguard still needs improvement. Optionally, treatment cost and time frame can be entered such that the reasonability of annual cost can be automatically calculated [35].

Defining the impact categories for the second implementation group [36] differs in having five categories instead of three. As for the first implementation group implications for the mission, operational objectives and obligations need to be given. Additionally, an impact criteria survey needs to be filled out where each impact magnitude can be described in more detail if the default answers do not fit the organization. After having identified the maximal acceptable risk as mentioned in the core document, the asset classes are assessed the same way as for group one. During the risk assessment, more details need to be provided concerning the implementation of the safeguards and the vulnerabilities that affect them. Besides that, the process stays the same [36].

The method for the third implementation group [37] only deviates from the other versions in assessing the risk of each safeguard compared to the method for the second group. For each safeguard, threats have to be identified before assessing the maturity of the safeguard. Moreover, the impact on the mission, operational objectives, finances, and obligations must be scored before and after the risk treatment [37].

The CIS RAM [5] is embedded into a framework like the BSI-Standard 200-3 [24]. However, this connection is much weaker since the CIS Controls [15] are much more accessible compared to the elements of the IT-Grundschutz Kompendium [30], because of their sheer number and level of detail. In addition, no preliminary work needs to be done to be able to use the method. The different versions for each implementation group make CIS RAM accessible to the laymen and also useful to the expert. Using a version, whose need for expertise exceeds the level available is not advisable. The methods for the second and third implementation group require familiarity with the CIS Controls and information security risk concepts. The CIS RAM methods are completely dependent on their corresponding excel workbooks. If Excel is available, then the workbook automates much of the workflow and do many of the tedious calculation for the user. Each workbook comes with a legend and a lookup table, that summarizes the necessary terms and explains the default scoring. Guidance on how to fill these workbooks is given in the document as a short manual and in the workbooks as detailed pre-filled examples. If the CIS Controls [15] framework has been implemented the assessment of the controls can also be supported by a tool [38], which is provided as free or a pro-version with cost. In the core document, it is mentioned that the principles of the CIS RAM can be used in combination with FAIR [39], but there is no explanation provided for how this can be achieved.

4.4 CORAS

The CORAS [40] method is an option for conducting risk assessments that comes with its own UML-like risk modeling language and free online [41] and desktop tools [42] to draw threat diagrams. The CORAS method defines clear roles that need to perform their respective duties during several workshops and meetings. The analysis team consists of an analysis leader, which is responsible for the execution of the CORAS process, and an analysis secretary that assists the leader and documents the process. Optionally, more analysis members can be added. Its counterpart is the target team, which is made of at least one decision-maker and a contact person. Additionally, the team can be filled with technical experts, consultants, or even users. The entity requesting the risk assessment is known as the customer. Both decision-makers and the contact person are representatives of the customer [40]. The method consists of eight steps that are summarized in the following.

The first step known as the preparation for the analysis is a meeting between the customer and the analysis team. The analysis team gets briefly given ideas by the customer about the target, scope, and level of detail of the assessment. The customer's deliverables are then communicated by the analysis leader and a representative from the customer side is chosen to maintain communication with the analysis team. In the end, customer and analysis team must agree upon a schedule for the assessment [40].

Next is a meeting where the customer team gives a more detailed presentation on the target. Outputs of this meeting are a fixed agreement about the scope of the assessment and the planning of further meetings and workshops. Before the presentation, the analysis leader makes representatives of the customers familiar with the CORAS method and terms. The target team then gives detailed information about the target and pitches the goals of the assessment. Because of the nature of the output, it is important that decision-makers from the customer's side are present[40].

Refining the target description through the use of the CORAS language is the third step of the process. The goal of this stage is for the analysis team to conduct a high-level analysis of the target. This consists of creating UML class diagrams of the target, activity diagrams for services, and the identification of assets which are then modeled through asset diagrams using the CORAS language. The identification of critical assets itself is done in a plenary discussion using provided material by the analysis team. In the same discussion, a first brainstorming session takes place where vulnerabilities and threats are taken into account [40].

The fourth step is called approval of the target description but also includes the ranking of the critical assets and determining the risk model. The approval solely consists of the target team green-lighting the documentation of the target complied by the analysis team based on the last step. In a plenary discussion, assets are ranked by their importance. The CORAS method uses the term consequence instead of impact, which is interpreted as a negative impact. CORAS uses a qualitative assessment approach, where risk is a combination of consequence and likelihood. Again in plenary discussions, the scales for consequence and likelihood are defined. The analysis together with the target team then develops a risk function, which maps a consequence and a likelihood level to a corresponding risk level. Finally, it is the customers' responsibility to determine what risk level is acceptable and what should be considered for further treatment [40].

Risk identification using CORAS threat diagrams is the fifth step of the process. The analysis team proposes a set of types of threat diagrams that suffice to describe the risk to critical assets. For each type, a set of critical assets (rep. by bags in Figure 4.3) is placed on the very right of a virtual or physical whiteboard. The target team then comes up with a threat actor (rep. by a manikin in Figure 4.3) that could impact those critical assets. The threat actors are listed on the very left and connected to the assets via unwanted incidents (rep. by rectangles in Figure 4.3). Afterward, the connections between threats and unwanted incidents are refined by adding possible initiation scenarios (rep. by circulars in Figure 4.3) between the two. In the end, threat actors and initiating threat scenarios are linked by vulnerabilities (rep. by locks in Figure 4.3) [40].

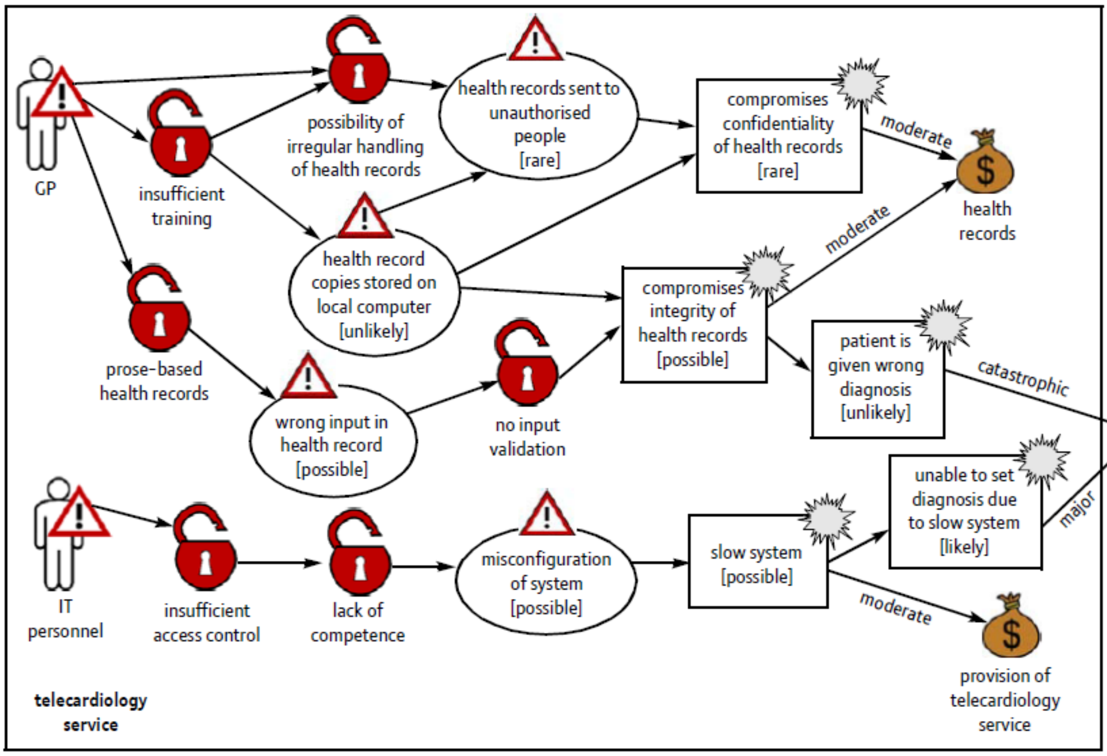

GP
insufficient training
possibility of irregular handling of health records
health records sent to unauthorised people [rare]
compromises confidentiality of health records [rare]
moderate
health records
health record copies stored on local computer [unlikely]
moderate
compromises integrity of health records [possible]
prose-based health records
wrong input in health record [possible]
no input validation
patient is given wrong diagnosis [unlikely]
catastrophic
patient's health
unable to set diagnosis due to slow system [likely]
major
IT personnel
insufficient access control
lack of competence
misconfiguration of system [possible]
slow system [possible]
moderate
provision of telecardiology service
telecardiology service

Figure 4.3: Example of a CORAS Threat Diagram [43]

The sixth step is risk estimation using the threat diagrams that were created in the step before. Unwanted incidents are assigned a likelihood based on the scale by the target team in step four. The likelihood assessment should be based on evidence and data gathered by the analysis team beforehand. The target team further estimates the consequence of each unwanted incident with respect to a critical asset using the scale from step four. This consequence together with the likelihood of the incident results in a risk, whose level can be determined by using the defined risk function [40].

The next step is risk evaluation. After having the customer check the documentation of the previous steps, the target team including decision makers review the suitability of the risk acceptance level and adjust it if necessary. Risk refinement takes place, where different similar risks are accumulated to one bigger if possible. The finalized risks are then compared to the acceptable risk level and it is determined if further steps for treatment are taken [40].

Finally, risk treatments are determined through CORAS treatment diagrams. The analysis team first identifies similarities regarding threats and vulnerabilities in the different risk diagrams to be able to group risks together that can be treated by the same measures. The target team holds a brainstorming session to come up with treatments for each individual risk. Options are transferring the risk, avoiding the business process responsible for the risk, or reducing the likelihood or impact. The treatment actions themselves are then evaluated to check the feasibility of the solution in terms of cost-benefit ratio [40].

Even though CORAS is an asset-driven method, Shameli-Sendi, Aghababaei-Barzegar, and Cheriet [16] noticed that no help regarding detailed assets identification can be found in the CORAS documentation [40]. The lack thereof can make it harder for novice assessors. Agrawal [11] categorizes CORAS as a functional approach and therefore its output is especially valuable to non-technical stakeholders, which can be a notable advantage. The disadvantages that he mentions are the need for expertise in CORAS and the length of the assessment process. Not only is the process scheduled over several meetings and workshops but two teams need to coordinate together [40], which often results in planning and communication overhead. Wangen, Hallstensen, and Snekkenes [3] showed in their work that the risk identification phase of CORAS is extensive compared to other ISRA methods. Unfortunately, it has the worst completeness score in the risk estimation phase. This stems mainly from the superficial analysis of threats and the lack of consideration of existing controls. On the other hand, the discussion and evaluation treatment actions are part of the CORAS method [40]. CORAS comes with free online [41] tools and desktops [42] applications, which makes the CORAS language easy to apply. Nevertheless, one needs to learn the language before being able to function as an analysis leader, which is a heavy initial commitment. If an organization has one or several people willing to get into the CORAS method, the documentation provides examples for each step, short summaries for all the deliverables, and detailed guidance for the language and the different diagram types. If a RAR is needed, the CORAS documentation provides a translation process to turn the diagrams into English prose [40].

4.5 CRAMM

The CRAMM [28] method is the oldest approach treated in the related work being created in 1985 by the UK government. CRAMM comes with tool support but is difficult to use without this specific tool. It would have been interesting to compare such a mature approach with newer methods, but because the last version was issued in 2003 [44], the decision was made to omit CRAMM from the selection of candidates.

4.6 FAIR

FAIR is the abbreviation of Factor Analysis of Information Risk [39] and is an ISRA method with a quantitative assessment approach. The fair method builds on its own ontology, in which the risk concept is defined as an interplay of FAIR factors in various layers. When talking about frequency in this context, the probable frequency within a given time frame is meant. Risk is the combination of loss event frequency and loss magnitude. Loss event frequency in turn is split into threat event frequency and vulnerability, where vulnerability is the probability that loss is suffered through an activity of a specified threat source. Those measures are further divided into contact frequency and probability of action, respectively threat capability of a threat actor and the difficulty that said must overcome. Loss magnitude on the other hand is split into primary loss and secondary risk, where the latter is made up of secondary loss frequency and magnitude. These refinements can help to think about controls in more detail in the sense that controls can be analyzed whether they are fit to specifically reduce one of these measures. Moreover, those measures can enable a deep level of detail in the quantification of the risk if needed. Of course, it is still possible to estimate a measure directly and not through its components, when an advanced level of detail is not needed [39].

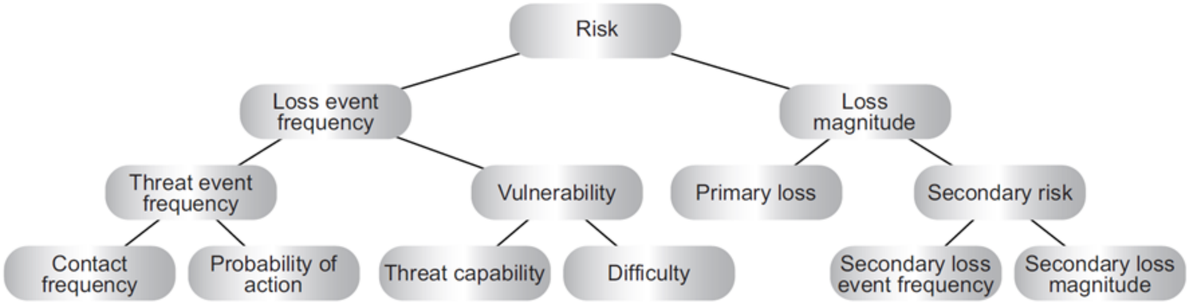


Figure 4.4: The FAIR Ontology [39]

The process of the risk assessment itself starts with building risk scenarios. To scope the assessment one identifies the critical assets at stake, the threat communities that can have a negative impact on them, the threat type, and the effect on the CIA-triad. Threat communities are threats that have a similar treatment and can therefore be grouped together. Examples of threat types are malicious, error, natural, and process failure. For each realistic combination, a risk scenario entry is created in a table. Even though it seems at first that the sheer number of combinations that have to be separately assessed is overwhelming, many steps in the calculations can be reused across various risk scenarios. At this point, a first check is done, whether it is even necessary to conduct an analysis or it is already clear that the risk needs to be treated [39].

Next is collecting data to estimate the FAIR factors. It is important to take a closer look at assets, threat communities, threat types, and effects to plan the gathering of intelligence.

For assets, it is important to consider the landscape they are in to identify controls that provide valuable insight. Analysis of threat communities often yields information about threat event frequency and threat capability. Threat type indicates threat event frequency and loss magnitude. Effect and asset should be considered together, to anticipate both frequency and magnitude. These are only a few examples given by the FAIR book and depending on the situation more assumptions can or must be made to enable gathering data [39].

After gathering the data, estimates are made using PERT distributions [45] to account for subjective estimates. According to the FAIR method, it is recommended to involve the person with the most expertise on the subject for estimating the FAIR factors. Additionally, it is crucial that they are familiar with PERT or they work in a team where knowledge about the use of such distributions is present. Documentation at this point is crucial. Reasons behind different estimations need to be documented with rigor to ensure the reproducibility of the results. The estimates are then put into a Monte Carlo function, to come up with the final quantitative values for the FAIR factors and the overall risk using a high number of simulations [39].

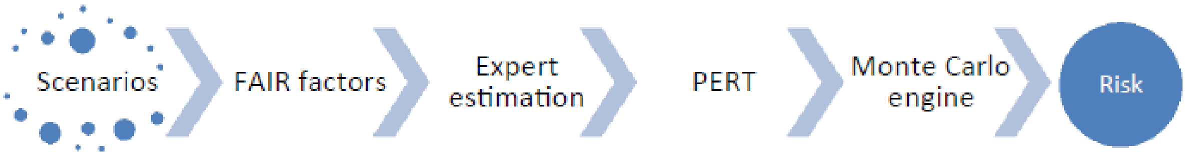


Figure 4.5: The FAIR Process [39]

Wangen, Hallstensen, and Snekkenes [3] showed that relative to other ISRA methods FAIR is an extensive approach with good completeness in the risk identification phase and excellent completeness in the risk estimation phase. It is the second most complete ISRA method after the very standardized ISO/IEC:27005 [2] approach. A feature FAIR struggles with is accessibility. Quantitative methods not only require more time [16] but also demand expertise and tool support [13]. The FAIR method itself even mentions that estimation should be made by corresponding experts and a person with knowledge about PERT distribution should be available [39]. This impedes the use of this method in small- to middle-sized companies. Another difficulty is the lack of documentation and tool support for establishing the basis of the estimation calculations, there is no real guidance on how to collect valuable data. Organizations, therefore, need experts who not only know how to read required information but also know how to establish systems and processes for collection. Additionally, FAIR must be supported by mathematics tools to be effective, especially when results are fortified using Monte Carlo simulation. Even though it is mentioned in the FAIR book that one can build its own private software to do so, it advises purchasing said software from a third-party vendor, which results in additional cost [39]. There also exists an online platform from RiskLens [46], which guides the FAIR risk assessment workflow. Unfortunately, no further information could be gathered about what this platform offers because demonstrations must be scheduled. The FAIR institute offers courses with costs that are certifiable [47] [48]. Alternatively, one can get hold of the FAIR book and use the free FAIR training application [49]. The Open Group [50] also offers certification independent of the courses with cost. If the implementation of the

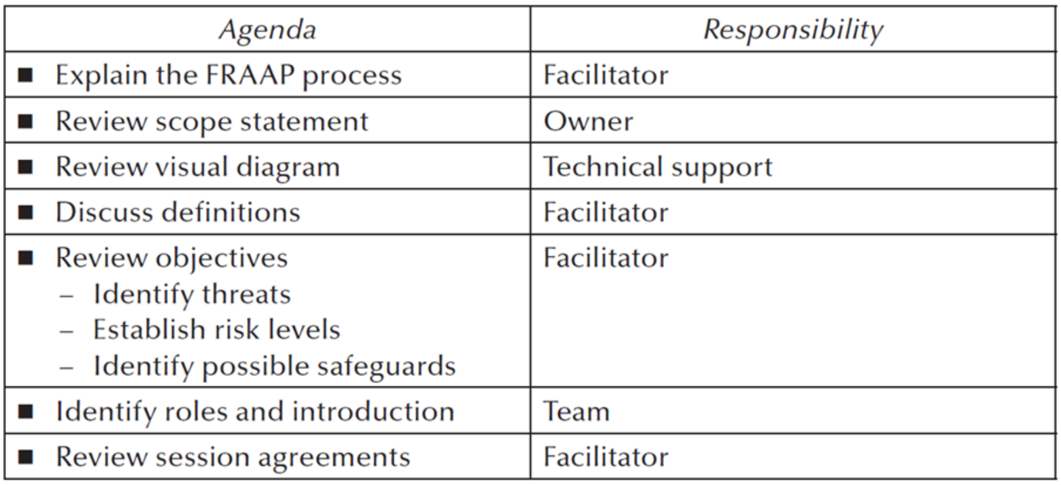
FAIR method is feasible despite the need for considerable human expertise, then it offers a complete quantitative risk assessment method, that can yield rigorous and reproducible results as such [13].

4.7 FRAAP

The FRAAP [12] method is a project-focused risk assessment approach that is conducted in a team during one FRAAP session guided by a role named the facilitator. Additionally, there is a short pre-FRAAP meeting for preparations and a longer post-FRAAP stage, where a RAR can be compiled. Owners resemble the higher management and invite to a FRAAP session. They are responsible for the creation of safeguards that should protect users while accessing authorized data. Custodians are the human resources of the organization, whose duty it is to support these safeguards. There are two additional FRAAP-specific roles: The facilitator and the scribe. The facilitator guides the FRAAP session and is responsible for achieving consensus during the pre-FRAAP and FRAAP sessions. The scribe's responsibility is that all of the orally discussed contents are converted into written form. The FRAAP method is available in book form and summarized in the following.

The pre-FRAAP meeting is an hour and a half long meeting, which is attended by the owner, the project lead, the facilitator, and the scribe. The output of this meeting is seven deliverables that are necessary for the FRAAP session. Pre-screening results from an earlier stage must be made accessible. Pre-screening involves the review of existing controls and is described in detail with several examples in the FRAAP book [12]. The scope of the assessment including relevant threat categories has to be determined by the owner and project lead. A document for guidance is given in the appendix. For the FRAAP session, a visual model is needed to give the FRAAP team an understanding of what needs to be assessed. This team is also established during the pre-FRAAP session and normally consists of fifteen to thirty members from different areas such as development, infrastructure, compliance, and HR. This is also reviewed in more detail in the appendix of the book. Further, the FRAAP meeting itself should be scheduled and responsibilities to invite the team members and provide a meeting place are assigned. Definitions of risk terms important for the assessment are agreed upon and in the end, a short brainstorming session is held, where high-level threat identification is done. The reader is provided with an example output of the brainstorm session and a pre-FRAAP session checklist with task to fulfill prior and during the meeting. [12].

The actual FRAAP session should take about four hours. At first, the meeting agenda is explained by the facilitator and the exact deliverables for each stage are presented. The owner then takes over and presents the scope of the assessment defined in the pre-FRAAP session. People that were assigned the role of technical support give the rest of the team a short overview of the subject of the assessment using the prepared visual diagram. Then the definition of the risk terms is explained in the plenary. The actual assessment starts with threat identification through brainstorming for each attribute of the CIA-triad. A worksheet with all the identified threats and the corresponding CIA attribute is compiled. In the appendix, an extensive checklist of threats is given for guidance. The identified



Agenda	*Responsibility*
■ Explain the FRAAP process	Facilitator
■ Review scope statement	Owner
■ Review visual diagram	Technical support
■ Discuss definitions	Facilitator
■ Review objectives – Identify threats – Establish risk levels – Identify possible safeguards	Facilitator
■ Identify roles and introduction	Team
■ Review session agreements	Facilitator

Figure 4.6: The FRAAP Session Agenda [12]

threats are mapped onto existing controls and safeguards by the team members working in infrastructure and security area of the organization. An example control list is provided in the book. Next comes the definition of levels for probability and impact, how they are mapped to risk levels, and what risk levels are acceptable or not. For that several scales and risk matrices with different levels of detail are provided in the appendix as examples. In plenary every threat then gets assigned a value for probability and impact on the subject of the assessment. From that the overall risk is determined and it is decided whether further action must be taken or not. For the risks that have an unacceptable level, enhancement of existing controls or new controls must be suggested until the is a consensus that the residual risk is on an acceptable level. The output is a worksheet that connects a CIA attribute with threats, existing controls, enhancement of controls, probability and impact levels, overall risk, and acceptability after mitigation [12].

The goal of the post-FRAAP process is to compile a RAR. Before that, the worksheet from the FRAAP session must be completed with an action plan. For each new control or control enhancement, one has to employ human resources for implementation and to set a deadline for completion. A summary report should consist of: Scope, methodology, findings, action plan, and a conclusion. To help with compiling a RAR, an example is provided in the book. This stage of the process should take maximally five work days. [12].

Unfortunately, none of the related academic work considered the FRAAP method. Nevertheless, Wheeler [4] did a high-level comparison of the approach with NIST SP 800-30 [13], OCTAVE Allegro [51] and FAIR [39]. He highlights three characteristics of FRAAP that sets it apart from the other methods: Project-focused, process/meeting style is adaptable to other ISRA methods, and interactive development of risk awareness through brainstorming sessions. Additional advantages are the shortness and the clear schedule of the process. The possibility to finish an assessment within two or three days makes it a good fit for the ISRA of smaller projects. The book also provides a decent amount of complementary material and explains each step of the process in a clear manner. Risk treatment is also a part of the method [12]. Unfortunately, only mitigation is considered as an action and the reader is left alone on finding out how to decide on and communicate risk acceptance, avoidance, or transfer.

4.8 ISO 27005:2018

The ISO 27005:2018 [2] is a standardized ISRA method that is embedded into the ISO 31000:2018 [52] ISRM. The document ISO 27005:2018 [2] provides a short background chapter and starts off with presenting an overview of ISO 31000:2018 [52] ISRM. The overview of ISO 31000:2018 [52] was already discussed in the background chapter, therefore we start directly with talking about the ISRA process. ISO 27005:2018 [2] is divided into three stages: Risk identification, risk analysis, and risk evaluation (see Figure 2.3). Those three are analyzed in more detail in the next paragraphs.

The risk identification needs to yield input for the risk assessment phase. Those are lists of assets, business processes, threats, existing controls, vulnerabilities, and consequences relevant to the assessed situation. The asset identification is split into the identification of primary and secondary assets. Primary assets are information or business processes that depend on the secondary assets, which support business functions, and store or process data like hardware, software, network devices, people, and work environments. The primary assets are identified by a working group of managers, specialists, and maybe even users. To guide the assessor characteristic of critical primary assets are given. For each critical primary asset, the supporting secondary assets are now identified. For each type of secondary asset, examples are provided to give the assessor a feeling of what needs to be searched for. Each asset should have a designated asset owner who is responsible and capable of assessing it. Next is the identification of relevant threats. Threats can be identified by either discussing with the asset owner the threats their assets experienced in the past or by consulting threat catalogs that list typical threats. The document provides such a catalog in the appendix. Existing controls are identified by reading documentation or audits, consulting the information security team, or by on-site reviews. While doing so existing controls are also already assessed to ensure their necessity. The removal of controls that fail should be initiated. In the appendix, many example vulnerabilities are listed with their corresponding secondary asset group and an example threat. This can help the assessor with the initial identification of vulnerabilities. The document also advises the use of vulnerability scanning tools, penetration testing, and code reviews for searching for technical vulnerabilities. One can create incident scenarios based on these connections, in which threats exploit vulnerabilities leading to the compromise of a CIA attribute of assets. For each scenario, possible consequences for the assets are identified. This concludes the risk identification phase [2].

Analyzing the risks starts with taking a closer look at the assets that are provided from the last phase. First criteria are defined, which are used to assign a value measure to an asset. Examples are the replacement cost or damage control cost caused by CIA compromise. Those criteria must be accurately documented. The next challenge is coming up with a set of criteria that can be used to assess all of the assets. The document provides a suggestion based on reducing value to impact through CIA compromise. Before being able to assess the assets, a scale needs to be defined. Scales are advised to have between three and ten different levels, which are defined by a set of criteria. The document also provides a way to integrate the fact that some assets depend on others and therefore have increased value. Based on the asset assessment consequences need to be assigned values to determine their possible negative impact. Several ways to either directly or indirectly determine the impact are given in the document. The incident scenarios from the last phase need to be assigned likelihood measures before determining the overall risk. Experience or even statistics can be used to analyze threats or vulnerabilities and control exploit likelihood. The competence and capacity of threat actors can also be considered if corresponding data is available. To finish the risk analysis phase each incident scenario is mapped to an overall risk score. Four different ways to do so are presented in form of examples in the appendix of the document [2].

The different risks from the last phase are now ranked by priority and compared against risk evaluation criteria that were defined before the start of the assessment based on the level of risk acceptance of the organization. This phase also includes considering the clustering of low- to medium-level risks. If several such risks affect the same CIA-triad attribute or the same important business process, it should be considered whether the score of those risks should be increased collectively. For risk evaluation guidance the document refers to the same examples as for the overall risk determination [2].

Wangen, Hallstensen, and Snekkenes [3] determined the ISO 27005:2011 as the most complete ISRA method in their study. Under the assumption that not many features were removed for the 2018 version of the document, it is plausible to assume that ISO 27005:2018 is still a very extensive method compared to most other ISRA methods. This is reinforced by the fact that the document also includes guidance for context establishment and risk treatment even though they are strictly speaking not part of the assessment process. Another advantage is that the appendix provides adequate complementary material for most of the steps in the assessment process. An exception is the support for the risk analysis phase. The assessor is given no help in form of default scales for assessing assets, consequences, or likelihood. Nevertheless, there are four complete examples that illustrate the conduction of the method and can give the assessor a high-level understanding of the risk analysis process. In the ISO 27005:2018 document [2] it is mentioned that both qualitative and quantitative approaches can be employed. Unfortunately, examples only show qualitative analysis, and the reader is left by himself to integrate a quantitative approach into the process. Before each step input and deliverables are clearly defined, which leads the reader smoothly through the process. Not providing templates for such deliverables can be seen as a missed opportunity. Also, no official automation or tool support could be discovered. Instead, there are many options to certify the ISO 27005:2018 method [53] [54].

4.9 MCRDF

The Microsoft Cloud Risk Decision Framework [55] is a risk assessment method devised to support cloud provider selection from an InfoSec point of view and the general assessment of cloud-specific risks. The document of the approach states that it is based on the ISO 31000 [52] ISRM. This is because this process also includes context establishment and risk treatment. The composition of the document and the complementary material suggests that it is rather an ISRA method and is also identified as such by other authors like Wangen, Hallstensen, and Snekkenes [3]. The different phases of the method are: Context establishment, risk identification, risk analysis, risk evaluation, risk treatment, and review & consider [55]. The document describing the process comes with an Excel workbook, which includes templates, scales, and functionality to automate the risk assessment [56].

The context establishment is the same as in ISO 31000 [52], with the exception that cloud-specific considerations need to be made. Those are for example compliance with privacy laws or recordkeeping regulations that depend on the operating country [55]. For risk identification, a list of cloud-specific risks is provided. In the risk analysis process, the likelihood and impact of each identified risk are evaluated, and the workbook automatically calculates an overall risk score [56]. Scales with five levels for both likelihood and impact are given and can be adapted to the organization's needs if necessary. Risks are then evaluated using the risk evaluation criteria defined during context establishment. If a risk is at a critical level, the assessor must choose to reduce, accept, avoid, or transfer the risk. If it is proposed to mitigate the risk, a description of the implemented control or process must be given. The residual risk with consideration of the mitigation action needs to be reassessed. The final risk scores are again automatically calculated inside the workbook. The updated workbook can now be used in the review stage to make a decision about whether or not to adopt the cloud service that was assessed [55].

The MCRDF does not score well in terms of completeness as Wangen, Hallstensen, and Snekkenes [3] asserted. They explain this by MCRDF being a subject-specific ISRA method. This specification is also an advantage compared to other methods if the situation to be assessed is cloud-related. Another advantage is the complementary material and ease of use. The process is guided and partly automated by a well-put-together Excel workbook [56] that comes with an integrated example that is described in detail in the appendix of the MCRDF document. The method also explicitly includes risk treatment as part of the process, because Stone and Noel [55] argue that risk mitigation must already be considered, when selecting a cloud solution. The MCRDF approach has a notable limitation, as it is primarily applicable to cloud environments and may not be suitable for assessing risks in non-cloud-related settings, due to its focus on cloud-specific risk factors. The link text of the Excel workbook hints that the method is based on CSA STAR, which is certifiable [57]. Unfortunately, on the CSA website, no further indication that MCRDF is certifiable was discovered [58].

4.10 NIST Special Publication 800-30

The NIST Special Publication 800-30 [13] is an elaborate ISRA method developed by the U.S. national institute of standards and technology. Next to the detailed explanation of the process, it includes an introduction to the fundamentals of ISRM, ISRA, and risk. The process is supplemented with over thirty pages of complementary material for conducting the assessment, like assessment scales or report guidance. The method can be used at different Tiers, from 1 to 3. These tiers correspond to different levels: the organization level, the business process level, and the information system level. The last level deals with operational and implementation details and is the least abstract of the three. The risk factors that are taken into consideration are: Threat sources, threat events, vulnerabilities, predisposing conditions, likelihood, and impact [13].

The process is divided into four parts: Preparation, conduction, communication, and maintenance (see Figure 4.7). The preparation phase itself starts with defining the intentions of the assessment, in other words, which information it should yield and which decisions it should back. The publication assists by giving examples for Tiers from 1 to 3 and where to integrate it within their guide for a risk assessment report, which is provided in the appendix of the publication. Additionally, it differs between initial assessments, those resulting from a risk response, and the ones triggered by monitoring. Corresponding examples for possible purposes are provided as well. Next, the scope of the assessment has to be defined in terms of the impacted area within the organization, the duration of usability of won information and analyzed infrastructure or processes. Examples are directly given within their RAR guidance. To continue framing the conditions of the assessment assumptions and constraints are considered. Besides the rather obvious limitations on resources and knowledge needed to conduct the assessment, one is recommended to sort out several important premises, such as which and to what extent threat sources, threat events, vulnerabilities, and predisposing conditions are considered, how the likelihood of events is determined, how the organization's operations and assets could be negatively impacted, and generally what the risk tolerance within the organization is. Complementary material in the appendix includes elaborated taxonomies for threat sources and vulnerabilities/predisposing conditions and inventories of adverse threat events and impact examples. It would be impossible to conduct any assessment without sources of information. The special publication [13] gives five detailed tables for threat sources and events, vulnerabilities and predisposing conditions, impacts, and risks in which it describes what inputs are needed from which Tier level and how to communicate them. Having done the information source identification, the only step left in the preparation phase is determining how to model risk and what analytic approach to use, if the proposed risk factors are insufficient and if the provided assistance in the form of a collection of qualitative and semi-qualitative assessment scales does not suit the analytic needs [13].

The second part resembles the risk analysis and the desired output of this stage is a list of adversarial and non-adversarial risks, where a risk is linked to each relevant individually assessed risk factor and their corresponding artifacts. For each risk factor gathering the information from the sources that were determined in the preparation phase is necessary. Assessing a risk factor encompasses mapping the gathered information or data about it to a measurement, which can be qualitative, semi-qualitative, or quantitative. As mentioned before every assessment task in this whole assessment part qualitative, semi-qualitative scales for guidance are provided but of course can be replaced by adaptions. Further for all the assessments of each risk factor, a separate artifact should be created and used to update the desired output list. In the appendix of the publication are templates for artifact creation that mention the findings that should be written down. The creating and updating of these artifacts should be done continuously and is not explicitly mentioned in the following description. One can start by identifying threat sources, assessing these, and checking if they are relevant for this risk assessment using the gathered intelligence. For adversarial threats, it is advised to assess capability, intent, and targeting separately. For non-adversarial threats one measure is sufficient. Next, threat events need to be

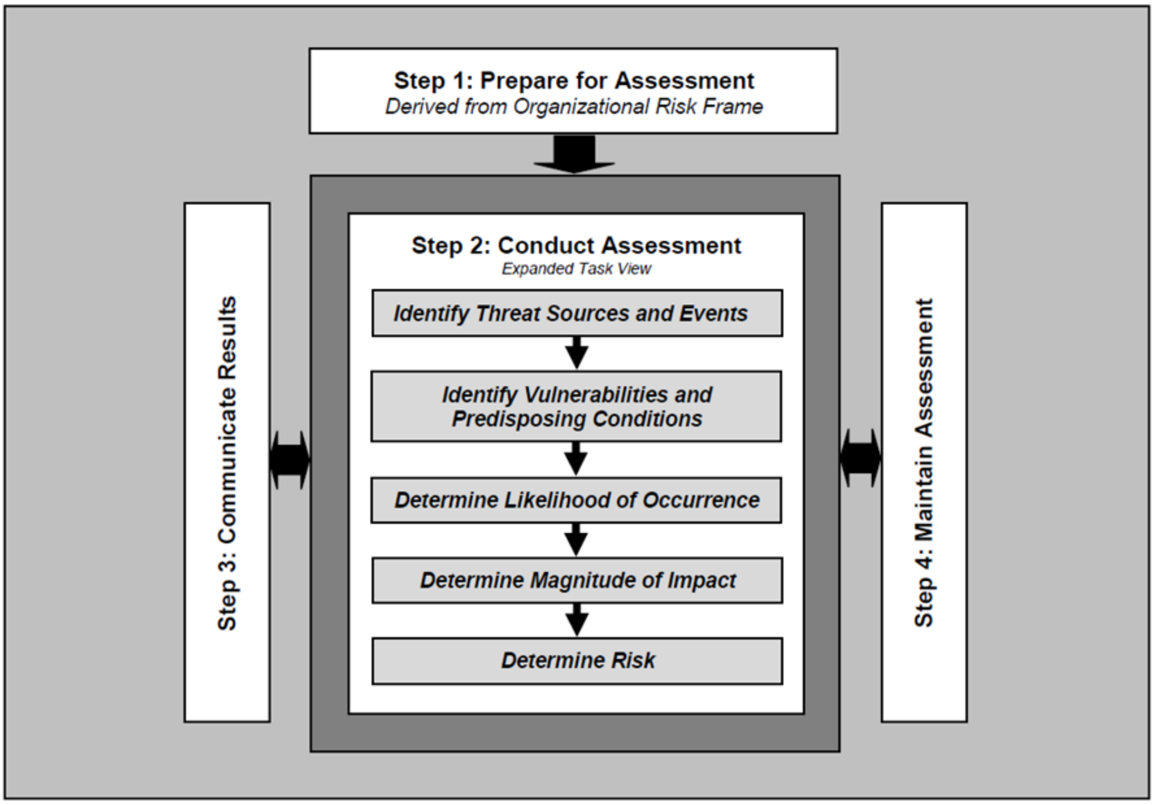

Step 1: Prepare for Assessment
Derived from Organizational Risk Frame
Step 2: Conduct Assessment
Expanded Task View
Identify Threat Sources and Events
Identify Vulnerabilities and Predisposing Conditions
Determine Likelihood of Occurrence
Determine Magnitude of Impact
Determine Risk
Step 3: Communicate Results
Step 4: Maintain Assessment

Figure 4.7: NIST Special Publication 800-30 Overview [13]

identified, connected to one or more threat sources, and assessed. Similar vulnerabilities and predisposing conditions are identified, assessed, and connected to one or more threat events. For each event the likelihood, that the threat sources whether adversarial or non-adversarial cause it, is determined. This is combined with the likelihood of an adverse impact given the threat event takes place to come up with the overall likelihood of the event. The combination of the two likelihoods can be achieved by using a matrix that maps two qualitative measures onto a single one. As with the assessment scales such matrices are provided in the NIST publication. The last factor needed to assess the risk corresponding to a threat event is its maximal adverse impact. To do this, all the adverse impacts of an event are identified, assessed, and the maximum is determined. The overall risk of a threat event can then be calculated as a combination of overall likelihood and maximal adverse impact. For determination in using a qualitative approach, a matrix is given at the end of the document. This should yield all the desired artifacts and a list containing all the analyzed risks relevant to this risk assessment. The tasks of the assessment part were listed in a linear manner in this paragraph. The reader must be aware that this does not reflect reality, where certain steps must be repeated to achieve the target level of rigor or reordered for enhanced efficiency [13].

Communicating the findings of the assessment is the third phase. It is divided into two tasks: Sharing the newly gathered intelligence with management and other stakeholders responsible for decision-making and sharing the information horizontally within the organization. To inform decision making the publication provides both a guide for refining the gathered information and a template for a risk assessment report itself. Refining the risk helps by grouping risks and making more general statements about impact and synergies within that group. This is an important step for the risk response which is not part of this publication but the separate NIST Special Publication 800-39 [59]. Sharing of information at the same organizational level doesn't happen after but already during the conduction of the assignment. The information sharing is supported by the artifacts that are created, continuously updated, and shared during the conduction. Meetings and intermediate reports must also be utilized but no further information on how to conduct respectively produce these is given [13].

The three before-mentioned phases are supplemented by one last step: Maintaining the assessment. This contains monitoring risk factors such that shifts in risk are quickly detected and updating outdated risk assessment results. One has to decide on key risk factors, a schedule when to check for shifts in risk, conditions that trigger an update, and depending on that in which depth the assessment should be revised [13]. No complementary material is given since the risk-monitoring process is more extensively covered in the Special Publication 800-39 [59].

Shamala, Ahmad, and Yusoff [19] already noted no instructions or further material could be found concerning improving risk management which includes activities such as training, raising awareness, and holding meetings or workshops. As mentioned by Wangen, Hallstensen, and Snekkenes [3] concerning the completeness of the method in the risk identification phase, the method lacks assessments of the stakeholders and assets, because of its threat-based nature. In the paper, the absence of a quantitative measurement during the risk estimation phase is also demonstrated. Nevertheless, the process is adaptable to a quantitative assessment approach but one would need to develop a weighting scheme for the scoring of risk factors tailored to the need of the organization [13]. Using a qualitative approach the SP 800-30 is deemed beginner friendly, because of an introduction to the risk assessment field and extensive complementary material, which is especially useful to new practitioners [21]. NIST SP 800-30 is versatile since it can be applied at different Tier levels of the organization and the complementary material can be tailored or even replaced to fit the organizations' specific needs [13]. Regarding the risk evaluation phase of the approach, the approach caters to composing a detailed risk assessment report, which could be an overkill for smaller companies where results are discussed together in meetings and decisions are made in an interactive manner. No tool support or automation for the SP 800-30 was found. NIST only provides two tools for assessing privacy risks, of which one is based on the FAIR [39] approach and the other is based on a privacy-specific risk model of NIST document [60].

4.11 NSMROS and RAIS

The Norwegian Security Authority Risk and Vulnerability Assessment (NSMROS) and the Privacy Risk Assessment of Information Systems (RAIS) are both Norwegian risk assessment frameworks that were part of building the CURF framework [3]. Both are published in Norwegian by government agencies with the latter having a special focus on privacy risk. Unfortunately, only one document [25] regarding those two methods could be found and no official English translation appeared on the website of the agencies.

Therefore those two approaches are not taken into account in the further continuation of this work.

4.12 OCTAVE Allegro

The OCTAVE Allegro [51] approach is a collaborative, workshop-style risk assessment method by the European Union Agency for Cybersecurity. It consists of four phases, which are divided into eight steps in total (see Figure 4.8). The first phase only includes one step, in which risk impact criteria are established. Phases two and three correspond to asset identification, respectively threat identification and each is made up of two separate steps. The last phase then identifies risks, analyses risks, and ends with selecting treatment.

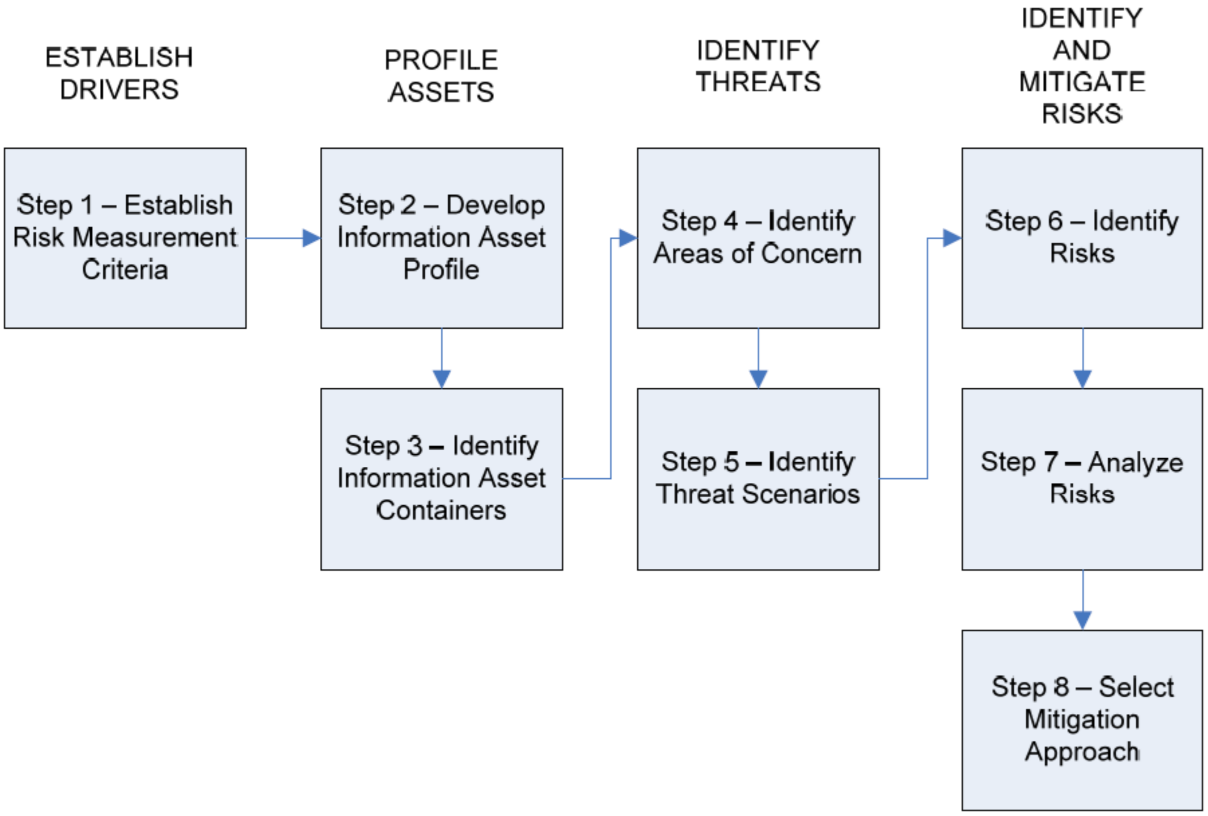

ESTABLISH DRIVERS
PROFILE ASSETS
IDENTIFY THREATS
IDENTIFY AND MITIGATE RISKS
Step 1 – Establish Risk Measurement Criteria
Step 2 – Develop Information Asset Profile
Step 3 – Identify Information Asset Containers
Step 4 – Identify Areas of Concern
Step 5 – Identify Threat Scenarios
Step 6 – Identify Risks
Step 7 – Analyze Risks
Step 8 – Select Mitigation Approach

Figure 4.8: The OCTAVE Allegro process [51]

Risk in the Allegro context is defined by an impact score. Optionally, a probability factor can be integrated into the assessment. Depending on the risk factors in use, one needs to define scales for impact and probability. By default, a qualitative scale with three levels for probability assessment is used. The criteria to assess impact are established in the first phase. The impact factor is further divided at minimum into reputation, finance, productivity, safety, and legal. For each, a qualitative scale with three levels must be defined, but default templates are provided. Prioritizing these impact criteria concludes the first phase [51].

The second phase is about asset and asset container identification. The method provides a set of questions to determine critical assets relevant to the assessment. For each of the critical assets, an extensive asset profile is compiled. The profile contains information like name, the reason for being critical, a short description, owner, and security requirements. More specifically, the security requirements determine the needs of the asset in terms of CIA attributes and the most important attribute is chosen. The Allegro document provides a template for the compilation of the critical asset profiles. Next, the asset containers are identified, in which the critical assets are stored, transported, or processed. This is crucial to be able to analyze threats, vulnerabilities, and existing controls at the right level. OCTAVE differs between technical, physical, and people containers. Containers of each of these categories have to be listed for each critical asset. Questionnaires for each container type are provided to guide the container identification [51].

Threat identification starts with identifying areas of concern, which are potential situations and conditions that endanger critical assets. Guided by provided examples, each asset container connected to a critical asset is analyzed and possible areas of concern are listed. For each area of concern threat actors, access points, reasons, immediate results, and effects on CIA attributes are documented. Those characteristics form together a threat scenario. Afterward, the areas of concern are mapped onto critical assets. As in the steps before, templates are provided to facilitate the process. In the next step, additional threat scenarios are identified through the use of given questionnaires. For each extra threat scenario note down the determining characteristics as before for the areas of concern. Optionally, each threat scenario can be assigned a probability score. The use of a probability score must be consistent over all threat scenarios and omitted if this is not possible [51].

Risk identification initiates the last phase of the OCTAVE Allegro process. It entails documenting the consequences of each threat scenario in detail. Based on the description of the consequences, each factor of impact as defined in the first phase is assessed as an impact score. This score is then multiplied by a factor that depends on the importance ranking of said impact type. The scores of all impact factors are then summed up and yield the overall risk score. Described scoring is documented on the same templates as used in the phase before. This risk score is then used to prioritize the risks to see, where immediate action is necessary. For considering treatment options risks can be divided into different risk pools using the overall risk score or a combination of the overall risk score and the probability measure. An example of such a division is given in the document. For each of those pools, a generalized treatment approach is suggested. Proposed treatment actions are accepting, mitigating, or deferring. Where deferring entails postponing the treatment decision such that the risk can be further monitored and re-assessed later on. The risks that are mitigated, controls that are implemented and the containers they affect must be documented. After implementation, residual risk needs to be assessed and documented as well [51].

Regarding the completeness of the OCTAVE Allegro method, Wangen, Hallstensen, and Snekkenes [3] assigned it an overall average score. This has to be taken with a grain of salt since the approach provides a complete risk identification and risk treatment stage, but scores very low compared to the other methods in the risk estimation phase. This is explained by the fact that its risk definition only depends on the impact of a threat scenario. The OCTAVE Allegro [51] document describes the method as having low minimal requirements regarding InfoSec risk knowledge and human resources. This seems plausible since the method document provides very granular instructions, background and definitions, and complementary material in form of templates for each step. Additionally, a completely worked-out example based on a use case is provided in the appendix of the document. It is unfortunate on the other hand, that the main source [51] calls the method collaborative and applicable in a workshop style but does not provide any information on how to do so. Concerning certification and education, Carnegie Mellon University offers an e-learning course [61] and an in-person workshop [62], where it is taught how to use the OCTAVE Allegro approach.

4.13 RISK IT

RISK IT [29] is an ISRM framework by ISACA that includes means to evaluate risks. Wangen, Hallstensen, and Snekkenes [3] assessed the ISRA approach within this framework as a process with a good completeness score compared to other ISRA methods. Unfortunately, the author of this work had problems isolating the ISRA approach without going into the details of the ISRM framework. Compared to the BSI-Standard 200-3 [24], which is also tightly coupled to its ISRM framework, no separate document for the ISRA approach is given. Additionally, the author of this thesis deems it questionable whether the use of the RISK IT risk evaluation is feasible outside its ISRM framework as with BSI-Standard 200-3, because of its risk analysis process depending on several inputs from other phases of the ISRM and the COBIT [63] framework [29]. It is worth mentioning at this point that the BSI approach would also have been omitted if it wasn't for the fact that it is described in a separate document and is the only German ISRA method found. This led the author to make the decision of omitting RISK IT as a possible candidate in the ISRA method selection framework.

Table 4.1: Overview of Risk Assessment Method Candidates

ISRA Method	**Authors/Institution**	**Year***
OCTAVE Allegro [51]	Richard Caralli, James Stevens, Lisa Young, and William Wilson (Carnegie Mellon University)	2007
CORAS [40]	Mass Soldal Lund, Bjørnar Solhaug, and Ketil Stølen	2010
FRAAP [12]	Thomas R. Peltier	2010
NIST SP 800-30 [13]	National Institute of Standards and Technology	2012
FAIR [39]	Jack Freund and Jack Jones (FAIR INSTITUTE)	2014
MCRDF [55]	Greg Stone and Pierre Noel (Microsoft)	2015
BSI-Standard 200-3 [24]	Bundesamt für Sicherheit in der Informationstechnik	2017
ISO 27005:2018 [2]	International Organization for Standardization	2018
CIS RAM [5]	Center for Internet Security	2022

* Publication year of main source

Chapter 5

Developing a Comparison Framework

As discussed in Section 3.3 the approach was chosen to develop ISRA method selection support by producing a comparison framework as defined in section 3.3. The first part of this chapter discusses each ISRA characteristic that is part of this comparison framework and lists the evaluations for each of the nine ISRA method candidates. The second part describes how a navigable user interface was created using the third-party knowledge base software LoqSeq [64].

5.1 A Comparison Framework for Selection-Support

In the following, the evaluation criteria and additional information used by the comparison framework are presented. For each, the motivation for inclusion is given and the evaluation of the ISRA method with respect to the evaluation criteria is listed. All the criteria and additional information of an ISRA approach make up the corresponding method profile. The approximate size and price of resources need to be documented. Both should be written inside parenthesis after the resource with the page volume, a comma added, and the price. If the information is not available *N/A* should be used instead. Prices of books are estimated based on prices on Amazon for new copies. Everywhere if not explicitly mentioned otherwise, the evaluation of the ISRA methods was based on their main source.

5.1.1 Description

Each ISRA method profile should have a short description of the method to give the user an understanding of what the method is about. The description should be at most three sentences. It is required to list the name, list the stages of the process, and can be complemented with other inherent characteristics. Such characteristics could be necessary preliminary work, the field of application, or tool support. The description should be at most three sentences long. The descriptions of the ISRA method candidates can be found in Table 5.1.

Table 5.1: Descriptions

ISRA Method	Description
BSI-Standard 200-3 [24]	The BSI-Standard 200-3[24] is a risk assessment method for organizations familiar with the IT-Grundschutz concept. The process entails the identification of threats, risk analysis, risk treatment, and consolidation. It builds on the identification of IT-Grundschutz Elements as described in the BSI-Standard 200-2.
CIS RAM [5]	The CIS RAM [5] is a risk assessment method based on the CIS Controls v8 [15]. The method is provided in three different versions fitted to the InfoSec resources an organization has available. All versions come with Excel workbooks, which assist the full process and automate calculations.
CORAS [40]	CORAS [40] is a risk assessment method, which uses its own UML-like risk modeling language. The method consists of an extensive preparation phase, which is followed by risk identification, estimation, evaluation, and treatment. The assessment is conducted in a meeting-style collaborative environment by an analysis team, decision-makers, and experts.
FAIR [39]	FAIR [39] is a quantitative risk assessment method that uses a detailed breakdown of risk into FAIR factors. Next to risk identification and the use of FAIR factors, the method entails expert estimations, the use of PERT distribution, and Monte Carlo simulations.
FRAAP [12]	FRAAP [12] is a risk assessment method tailored to project-scope and can be conducted within a week. The process consists of a short preparation meeting, a four-hour-long collaborative session attended by management personnel as well as technical support, and the documentation of the results in a report.
ISO 27005:2018 [2]	ISO 27005:2018 is a standardized risk assessment method entailing risk identification, risk analysis, and risk evaluation. Because of its generality and extensiveness, the method can be used for guiding the creation of new approaches, benchmarking against existing methods, or conducting detailed assessments.
MCRDF [55]	The MCRDF [55] is a risk assessment method tailored to cloud-related situations and cloud provider selection. Next to risk identification, estimation, and evaluation, it entails context establishment with cloud-specific considerations and a consider & review phase in the end.

Continued on next page

Table 5.1 – continued from previous page

ISRA Method	Description
NIST SP 800-30 [13]	The NIST Special Publication 800-30 [13] is a risk assessment method that uses information about threat sources, threat events, vulnerabilities, predisposing conditions, likelihood, and impact to measure risk. It is divided into four parts: Preparation, conduction, communication, and maintenance.
OCTAVE Allegro [51]	OCTAVE Allegro [51] is a risk assessment method that approximates the overall risk by analyzing the reputation, finance, productivity, safety, and legal impact of threats. The process starts with context establishment, is followed by a longer risk identification phase, a quick risk analysis, and ends with selecting mitigation approaches.

5.1.2 Approach

The approach specifies the assessment approach as defined in the NIST SP 800-3 [13]. Shukla and Kumar [10] as well as Agrawal [11] documented whether the methods are qualitative, quantitative. We also allow the approach to be hybrid, as in the work of Shameli-Sendi, Aghababaei-Barzegar, and Cheriet [16]. If a method deems itself feasible to work with a quantitative approach but does not provide complementary material to guide the user, it is not recognized as such. The approach characteristics of the ISRA method candidates can be found in Table 5.2.

Table 5.2: Approach

ISRA Method	Approach
BSI-Standard 200-3 [24]	Qualitative
CIS RAM [5]	Hybrid
CORAS [40]	Qualitative [16]
FAIR [39]	Quantitative [3]
FRAAP [12]	Qualitative
ISO 27005:2018 [2]	Hybrid [16]
MCRDF [55]	Qualitative [3]
NIST SP 800-30 [13]	Hybrid [16]
OCTAVE Allegro [51]	Hybrid [16]

5.1.3 Target Organization Size

Shukla and Kumar [10] assessed the skills needed to implement an ISRA method. Agrawal [11] assessed effort, which included next to skill also a measure of how time-consuming an approach is. In this thesis, the target organization size is determined. The values that can be assigned for this evaluation criteria are based on the definition of implementation groups of the CIS framework [15] as mentioned in section 4.3. Since the CIS RAM [5] is available for each implementation group it is used as a benchmark. The target organization size is assessed by considering how much input or personnel is needed, how much assistance is given, and how detailed the assessment output is. Multiple implementation groups can be assigned to the same ISRA method. The target organization size of the ISRA method candidates can be found in Table 5.3.

Table 5.3: Target Organization Size

ISRA Method	**Target Organization Size**
BSI-Standard 200-3 [24]	- Implementation Group 2 & 3
CIS RAM [5]	- Implementation Group 1, 2 & 3
CORAS [40]	- Implementation Group 2 & 3
FAIR [39]	- Implementation Group 3
FRAAP [12]	- Implementation Group 2 & 3
ISO 27005:2018 [2]	- Implementation Group 2 & 3
MCRDF [55]	- Implementation Group 1 & 2
NIST SP 800-30 [13]	- Implementation Group 2 & 3
OCTAVE Allegro [51]	- Implementation Group 1 & 2

5.1.4 Relative Completeness

Wangen, Hallstensen, and Snekkenes [3] assessed different ISRA methods regarding their completeness, which is correlated to the RAR completeness as discovered by Wangen [21]. Based on the completeness scores of the identification phase, estimation phase, evaluation phase, and the overall score, an own qualitative relative completeness measure was calculated (see Appendix B 5). For each phase, the range between the minimum and maximum values was divided into three parts. ISRA methods with scores in the lowest quarter were assigned the label *Bad*, methods with scores in the highest quarter the label *Average*, and the rest were assigned the label *Average*. There are three limitations to this measure. First, not all the ISRA method candidates were asses in the work of Wangen, Hallstensen, and Snekkenes [3]. Second, some ISRA methods were assessed in the work but are not ISRA method candidates. Third, if a user wants to add a new method, it first needs to be assessed using the CURF [3] framework and afterward, the relative scores of all methods need to be reevaluated. Nevertheless, the author of this work deems the measure useful to give the user an impression of where methods are lacking and where they have their strength. The relative completeness rating of the ISRA method candidates can be found in Table 5.4.

5.1.5 Language

Shukla and Kumar [10] already included the language in their comparison framework. This is especially crucial for organizations, where not all people responsible for ISRA

Table 5.4: Relative Completeness

ISRA Method	**Relative Completeness**
BSI-Standard 200-3 [24]	N/A
CIS RAM [5]	N/A
CORAS [40]	Risk identification: Good Risk estimation: Bad Risk evaluation: Average Overall: Average
FAIR [39]	Risk identification: Average Risk estimation: Good Risk evaluation: Bad Overall: Average
FRAAP [12]	N/A
ISO 27005:2018 [2]	Risk identification: Good Risk estimation: Good Risk evaluation: Average Overall: Good
MCRDF [55]	Risk identification: Bad Risk estimation: Average Risk evaluation: Bad Overall: Bad
NIST SP 800-30 [13]	Risk identification: Average Risk estimation: Good Risk evaluation: Bad Overall: Average
OCTAVE Allegro [51]	Risk identification: Average Risk estimation: Bad Risk evaluation: Good Overall: Average

have sufficient English skills. All of the ISRA method candidates are only available in English with the BSI-Standard 200-3 [24] being the exception, which is also provided in German.

5.1.6 Input and Output

The two evaluation criteria input and output are adopted from the work of Agrawal [11]. Input describes deliverables like lists, inventories, diagrams, etc. that need to be produced before or during the ISRA process to be able to conduct the assessment. Only things that take significant effort to compile should be listed under input. A prominent example is a list of critical assets. The output should briefly characterize what the risk assessment yields. The input and output of the ISRA method candidates can be found in Table 5.5, respectively Table 5.6.

Table 5.5: Input

ISRA Method	**Input**
BSI-Standard 200-3 [24]	List of critical target assets and their IT-Grundschutz elements as described by BSI-Standard-200-2 [31], List of threats mapped onto relevant IT-Grundschutz elements, List of threats independent of IT-Grundschutz elements
CIS RAM [5]	Answers to impact analysis questionnaire (IG2 & IG3) [36] [37], Description of implementation for all safeguards (IG2 & IG3), List of vulnerabilities for all safeguards (IG2 & IG3), List of threats for all safeguards (IG3)
CORAS [40]	Meeting schedule, Presentation of the target, List of critical assets and corresponding threats and threat actors, Threat diagrams
FAIR [39]	List of risk scenarios consisting of assets, threats, threat type, and impacted CIA-attribute, Data to be able to quantitatively assess threats, vulnerabilities, and loss
FRAAP [12]	List of existing controls including their review, List of threats connected to existing controls
ISO 27005:2018 [2]	List of critical assets, List of threats, List of existing controls, Results of vulnerability scanning, Asset evaluation criteria, Impact evaluation criteria
MCRDF [55]	Answers to Enterprise risk appetite questionnaire, List of cloud risk mitigating controls
NIST SP 800-30 [13]	List of threat sources, List of threat events, List of vulnerabilities and predisposing conditions
OCTAVE Allegro [51]	Additional impact areas (optional), List of critical assets, List of asset containers, List of threats including threat actor and consequences

Table 5.6: Output

ISRA Method	**Output**
BSI-Standard 200-3 [24]	List of IT-Grundschutz elements with corresponding threats, vulnerabilities, treatment options, and residual risks
CIS RAM [5]	List of evaluated risks with treatment option and residual risk measured by impact to mission, operational objectives, and obligations (IG1, IG2 & IG3) [35] [36] [37], Cost plan for next years (optional)
CORAS [40]	Treatment diagrams showing threat actors, threats, vulnerabilities, critical assets, and feasible treatments
FAIR [39]	Quantitative measures for each risk scenario displayed using heat maps
FRAAP [12]	Worksheet connecting CIA-attributes with threats, existing controls, enhancement of controls, risks and acceptability after mitigation, Risk Assessment report including findings as mention above and an action plan
ISO 27005:2018 [2]	List of evaluated risks with consideration of risk aggregation
MCRDF [55]	List of evaluated cloud risks with mitigating controls and residual risk
NIST SP 800-30 [13]	List of risks connected to threat events, threat sources, vulnerabilities, and predisposing conditions, Risk Assessment report including findings as mentioned above
OCTAVE Allegro [51]	Profiles for risks with detailed impact analysis, List of risks with corresponding treatments and residual risks

5.1.7 Main Features

The main features evaluation criteria are inspired by the listing of pros and cons in the work of Agrawal [11]. Pros and cons were not chosen as criteria since many characteristics can be an advantage or a disadvantage depending on the situation. These criteria should list up to four inherent characteristics of the ISRA method that give a user an understanding of what the pros and cons of a method could be, depending on the situation. The special features of the ISRA method candidates can be found in Table 5.7.

Table 5.7: Main Features

ISRA Method	**Main Features**
BSI-Standard 200-3 [24]	Available in German, Dependent on IT-Grundschutz framework (see ISRM Framework), Dissection of critical assets through IT-Grundschutz elements
CIS RAM [5]	Available for all implementation groups [35] [36] [37], Assessment done inside detailed Excel template, Assessment based on the implementation of CIS Controls v8, Some inputs can be supplied by a control assessment tool (see Tool-Support)[15]
CORAS [40]	Uses own UML-like threat modeling language, which is tool-supported, Collaborative assessment conduction during several meetings, Needs analysis team responsible for analysis consisting of a leader and a secretary, Includes decision makers into process
FAIR [39]	Yields detailed and objective quantitative risk measures, Able to make use of many risk factors to quantify risk, Depends on expert estimation and complex mathematics
FRAAP [12]	Tailored to assess InfoSec risks of projects Collaborative assessment conduction during two meetings (approx. 6h total), Style is adaptable to other ISRA methods [4], Includes decision makers into process
ISO 27005:2018 [2]	Standard method with several options for certification, Very complete method [3] that even considers risk aggregation, Can be used for benchmarking other ISRA methods and as a basis for developing new ISRA methods, because of its completeness
MCRDF [55]	Tailored to assist cloud provider selection or assess cloud-related risks, Assessment done inside Excel template
NIST SP 800-30 [13]	Document with the detailed process, lots of complementary material and templates for documentation, Has very detailed risk estimation phase [3] and considers risk aggregation, Part of renowned information security risk management framework
OCTAVE Allegro [51]	Simple risk assessment that is only based on impact measure, Detailed analysis of consequences and impact, Low minimal requirements regarding InfoSec risk knowledge and human resources

5.1.8 Documents

In each ISRA method profile, the main source of the ISRA method is named, and a short summary of the complementary materials that help the user conduct the assessment is provided, like examples, risk factor scales, or risk determination matrices. If possible a rough estimation of the page volume of the complementary material should be given. Any additional documents important to the conduction of the ISRA can also be documented here after the main source. The overview of the documents is supposed to give the user an approximate measure of the level of detail, assistance provision, and comprehensiveness. The information on the documents of the ISRA method candidates can be found in Table 5.8.

Table 5.8: Documents

ISRA Method	**Documents**
BSI-Standard 200-3 [24]	The BSI-Standard 200-3 [24] (54 pp., free) - Two examples (15 pp.) - List of fundamental threats (1 p.) - Risk factor scales and risk determination matrix (1 p.) - Guide to risk appetite (7 p.)
CIS RAM [5]	The CIS RAM core document [5] (27 pp., free) - Impact scale (1 p.) A document for each version of CIS RAM (38/53/53 pp., free) - Detailed guide on how to fill corresponding Excel workbook - Control Maturity scale (1 p.), - Expectancy scale (1 p.)
CORAS [40]	The CORAS [40] book (458 pp., $100) - High-level example (24 pp.) - CORAS UML language core guide (26 pp.) - Process explanation (130 pp.) - Likelihood estimation guide (38 pp.) - CORAS tool guide (8 pp.)
FAIR [39]	The FAIR book [39] (410 pp., $50) - Explanation of FAIR risk concept (50 pp.) - Guidance on quantitative measurements (16 pp.) - Process explanation (14 pp.) - Guidance on result interpretation (18 pp.) - Examples (70 pp.)

Continued on next page

Table 5.8 – continued from previous page

ISRA Method	**Documents**
FRAAP [12]	The FRAAP book [12] (458 pp., $110) - Process explanation (57 pp.) - Pre-FRAAP meeting checklist (3 pp.) - Probability, impact scales, and risk matrix (1 p.) - Example FRAAP worksheets (13 pp.) - FRAAP control list (5 pp.) - Team member example list (1 p.) - Guidance on project scope statement (3 pp.) - Sample threat lists (10 pp.)
ISO 27005:2018 [2]	The ISO 27005:2018 [2] white paper (61 pp., $198 for 2022 version on ISO website) - Guidance for Context establishment (3 pp.) - Process explanation (8 pp.) - Guidance for risk treatment (3 pp.) - Guidance and examples for asset identification (4 pp.) - Threat examples (3 pp.) - Vulnerability examples (3 pp.) - Three assessment examples (4 pp.)
MCRDF [55]	The MCRDF [55] white paper (30 pp., free) - Impact and likelihood scales (2 pp.) - Cloud-related example risks (1 p.) - Examples (9 pp.)
NIST SP 800-30 [13]	The NIST Special Publication 800-30 [13] (95 pp., free) - Guidance for process inputs (3 pp.) - Threat sources examples (1 p.) - Scales for threat sources (1 p.) - Examples of threat events (6 pp.) - Scales for vulnerability and predisposing conditions (1 p.) - Examples of predisposing conditions (1 p.) - Scales for likelihood (1 p.) - Examples of threat impacts (1 p.) - Scales for impact (1 p.) - Scales for overall risk (1 p.) - Templates for documentation (3 pp.) - Guidance for risk assessment report (2 p.)
OCTAVE Allegro [51]	The OCTAVE Allegro [51] white paper (154 pp., free) - Complementary examples to individual steps (3 pp.) - Templates for documentation (7 pp.) - Impact scale templates (6 pp.) - Threat scenario questionnaires (8 pp.) - Filled out example worksheets (40 pp.)

5.1.9 Tool-Support

Shukla and Kumar [10] as well as Agrawal [11] already documented whether tool-support is available in their comparison frameworks, but only give minimal information about it. Examples of tool support include Excel workbooks to automate the ISRA process and tools for gathering data or for risk score calculations. Unofficial tool support from a third party that is not approved by the author or issuing institution is not recognized. When evaluating tool support in this work, each resource should be documented with a description and a brief list of its functionalities. The tool support of the ISRA method candidates can be found in Table 5.9.

5.1.10 ISRM Framework

If the ISRA method is embedded into an ISRM framework then it should be part of the ISRA method profile. It should also be noted if the ISRA method is tightly coupled to its ISRM framework. The resources that make up the ISRM framework must be documented. This information can be useful to estimate additional effort or provide information if the user is searching for an ISRM framework based on the ISRA approach. The ISRM frameworks of the ISRA method candidates can be found in Table 5.10.

5.1.11 Certification

Certification should indicate whether an ISRA method is certifiable or not. In the scope of this work courses, workshops, and seminars are recognized as yielding a certificate. The certification means of the ISRA method candidates can be found in Table 5.11.

Table 5.9: Tool-Support

ISRA Method	**Tool-Support**
BSI-Standard 200-3 [24]	None
CIS RAM [5]	Excel workbooks for each version of CIS RAM (12/16/15 pp., free) [35] [36] [37] - Impact criteria survey (1 pp.) - Impact criteria survey example (1 pp.) - Risk assessment sheets (1-3 pp.) - Legend (1 p.), - Lookup tables (1 p.) - Tool-support explanation (2 pp.), - Examples (1-2 pp.) - Tool-supported examples (2 pp.) CIS CSTAR (free) and CIS CSTAR PRO (+$1400/Y) [38] - Tracks implementation of CIS Controls - Provides Excel workbook CIS Control implementation data
CORAS [40]	Online tool [41] (free) - Asset modelling - Thread modelling - Risk modelling - Treatment modelling - Download of created graphics Desktop application tool [42] (free) for Windows, Mac, and Linux - Full support for all CORAS language features
FAIR [39]	RiskLens Enterprise online platform (N/A) - A product demonstration must be scheduled FAIR-U online training tool (free) - Simple example to illustrate the FAIR assessment
FRAAP [12]	None
ISO 27005:2018 [2]	None
MCRDF [55]	Excel workbook (9 pp., free) - Impact and likelihood scales (2 pp.) - Enterprise risk appetite sheet (1 p.) - Detailed risk assessment sheet (1 p.) - Summary sheet (1 p.) - Filled out example (1 p.)
NIST SP 800-30 [13]	None
OCTAVE Allegro [51]	None

Table 5.10: ISRM Framework

ISRA Method	**ISRM Frameworks**
BSI-Standard 200-3 [24]	Tightly coupled to IT-Grundschutz, which consists of: - IT-Grundschutz-Kompendium [30] (858 pp., free) - BSI-Standard 200-2 [31] (180 pp., free)
CIS RAM [5]	Coupled to CIS Controls v8 [15] (87 pp., free) - Mapping of security controls onto CIS Controls needed
CORAS [40]	None
FAIR [39]	Loosely coupled to FAIR ISRM Framework [39]
FRAAP [12]	None
ISO 27005:2018 [2]	Loosely coupled to ISO 31000:2018 [52] (24 pp., $97)
MCRDF [55]	None
NIST SP 800-30 [13]	Loosely coupled to NIST SP 800-39 [59] (183 pp., free)
OCTAVE Allegro [51]	None

Table 5.11: Certification

ISRA Method	**Certification**
BSI-Standard 200-3 [24]	Framework is ISO 27001 certifiable based on IT-Grundschutz [32]
CIS RAM [5]	None
CORAS [40]	None
FAIR [39]	FAIR Analysis Fundamentals training [48] (6h VoD, $1450) - Voucher for Open FAIR Certification [50] Advanced FAIR Analyst Learning Path [48] (2.5h VoD, $1450) Open FAIR Certification [50] ($360)
FRAAP [12]	None
ISO 27005:2018 [2]	Examples: - FIREBRAND ISO 27005 Risk Manager [53] - PECB ISO/IEC 27005 Risk Manager [54]
MCRDF [55]	None
NIST SP 800-30 [13]	None
OCTAVE Allegro [51]	Assessing Information Security Risk Using the OCTAVE Approach - eLearning [61] (27 VoD lectures, $700) Assessing Information Security Risk Using the OCTAVE Approach [61] (3d course, +$1900)

5.2 Implementation

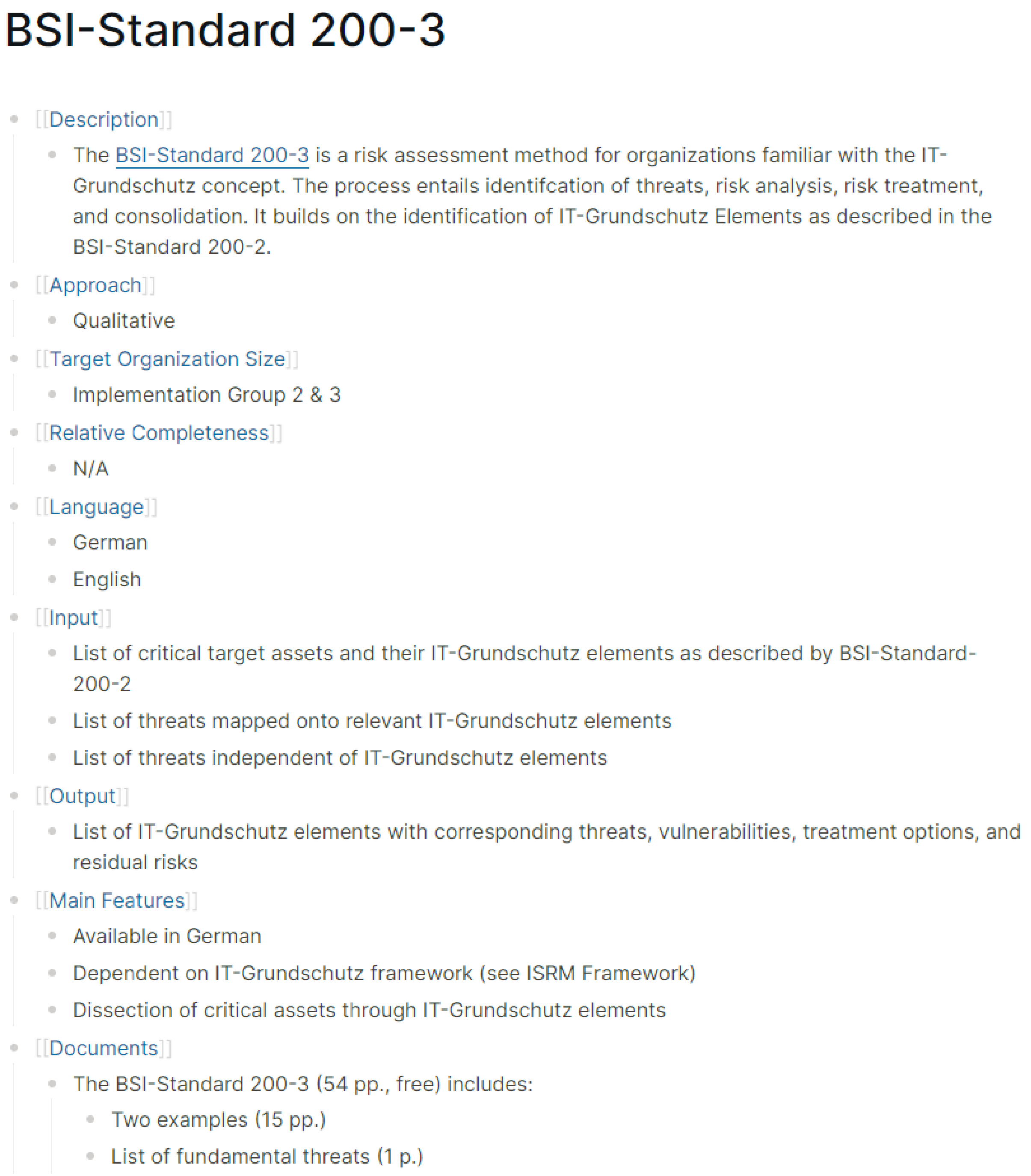
Shukla and Kumar [10] as well Agrawal [11] used a table to present their comparison framework and the evaluation of the ISRA methods. Because of the number of criteria used and the number of methods evaluated in the current framework a table is not a suitable solution to present information to a user. A prototype for a navigable dynamic user interface of the current framework was developed as part of this thesis to enable a user-friendly comparison of the ISRA methods assessed. Since the prototype does not only entail the comparison framework but also the evaluation of the ISRA method candidates, it is referred to as the ISRA knowledge base prototype. It was implemented using the free, open-source, knowledge base software Logseq [64]. The prototype comes without a tutorial or a legend explaining all terms necessary to understand the framework. Therefore it complements this thesis and is not designed for use by itself.

5.2.1 Logseq

Logseq [64] is a free, open-source software that can be used to automate daily workflows, work as a knowledge base, help with task management, or studies [65]. In the following, only the features of Logseq that were needed in the creation of the comparison framework prototype are presented and not Logseq as a whole. The knowledge presented below was acquired through the practical use of Logseq and the Logseq Community Hub [65]. Logseq enables the presentation of knowledge written into markdown files in a navigable graph structure. The graph consists of different pages, which are linked using tags. A Tag is created by enclosing words in double square brackets or putting a hashtag in front of a word. For each tag a page is created, where each appearance of the tag within the graph is listed. The backbone of the graph are journal pages (see Figure 5.1), which are markdown files that contain text and tags. To add text to a tag, the indented text must be directly written under the tag. If a tag is created below a tag in this way, those tags get connected. All the connections are shown in a graph view, which is navigable [65]. To create a navigable comparison framework, a journal page for each ISRA method was created and tags were used to denote the evaluation criteria.

5.2.2 Navigating the ISRA Knowledge Base Prototype

After following the installation guidelines in Appendix A, the user sees the knowledge base graph (see Figure 5.2). Both ISRA methods and risk evaluation criteria are represented by gray circles. The lines between the dots represent the connection between the tags. Clicking on an ISRA approach transfers the user onto the corresponding journal page. Alternatively, an evaluation criterion can be clicked. The user can now either navigate back to the graph by clicking on *Graph View* in the menu on the left-hand side or click on a tag representing an evaluation criterion. The latter option brings the user onto the page of the corresponding criteria (see Figure 5.3), where the value of each ISRA method is listed. Again the user can now either navigate back to the graph or click on a tag representing an ISRA method.



BSI-Standard 200-3

- [[Description]]
  - The BSI-Standard 200-3 is a risk assessment method for organizations familiar with the IT-Grundschutz concept. The process entails identifcation of threats, risk analysis, risk treatment, and consolidation. It builds on the identification of IT-Grundschutz Elements as described in the BSI-Standard 200-2.
- [[Approach]]
  - Qualitative
- [[Target Organization Size]]
  - Implementation Group 2 & 3
- [[Relative Completeness]]
  - N/A
- [[Language]]
  - German
  - English
- [[Input]]
  - List of critical target assets and their IT-Grundschutz elements as described by BSI-Standard-200-2
  - List of threats mapped onto relevant IT-Grundschutz elements
  - List of threats independent of IT-Grundschutz elements
- [[Output]]
  - List of IT-Grundschutz elements with corresponding threats, vulnerabilities, treatment options, and residual risks
- [[Main Features]]
  - Available in German
  - Dependent on IT-Grundschutz framework (see ISRM Framework)
  - Dissection of critical assets through IT-Grundschutz elements
- [[Documents]]
  - The BSI-Standard 200-3 (54 pp., free) includes:
    - Two examples (15 pp.)
    - List of fundamental threats (1 p.)

Figure 5.1: The BSI-Standard 200-3 Journal Page

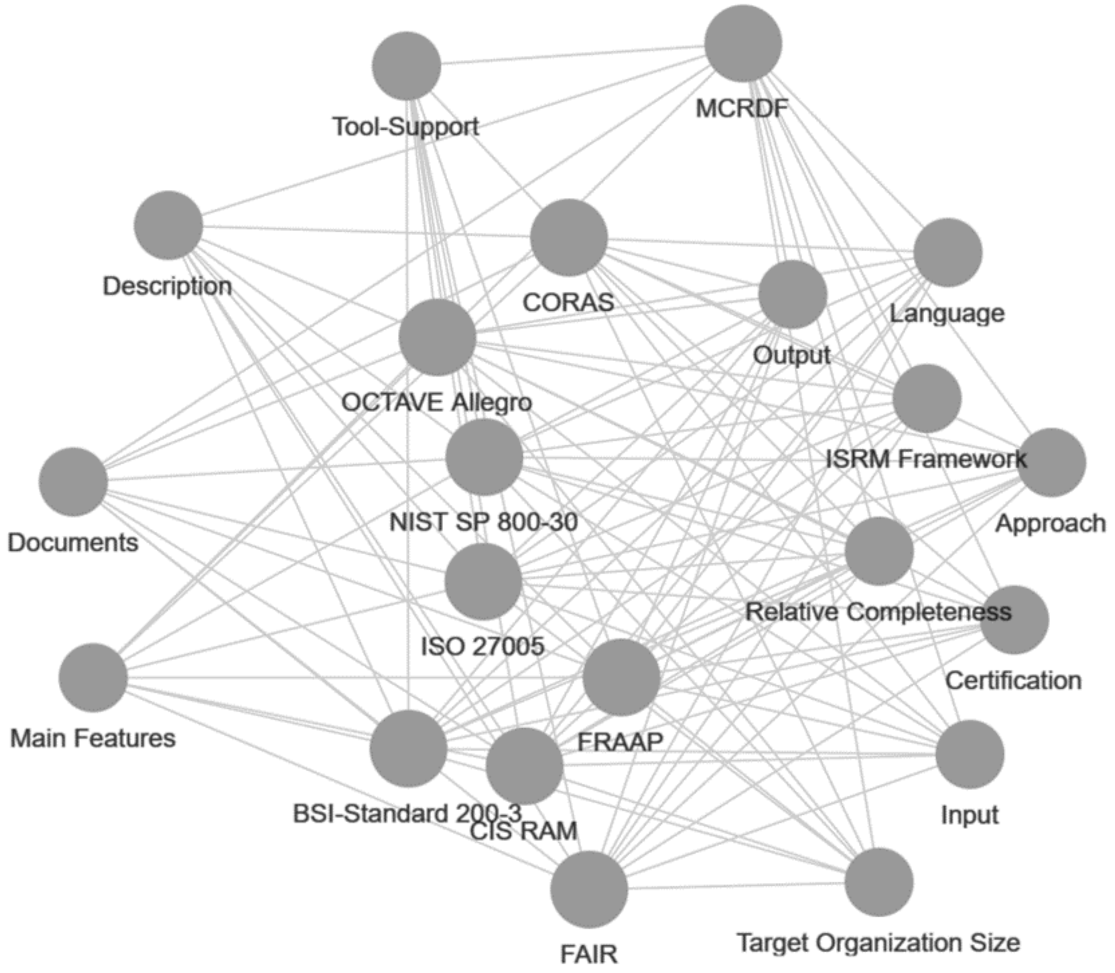
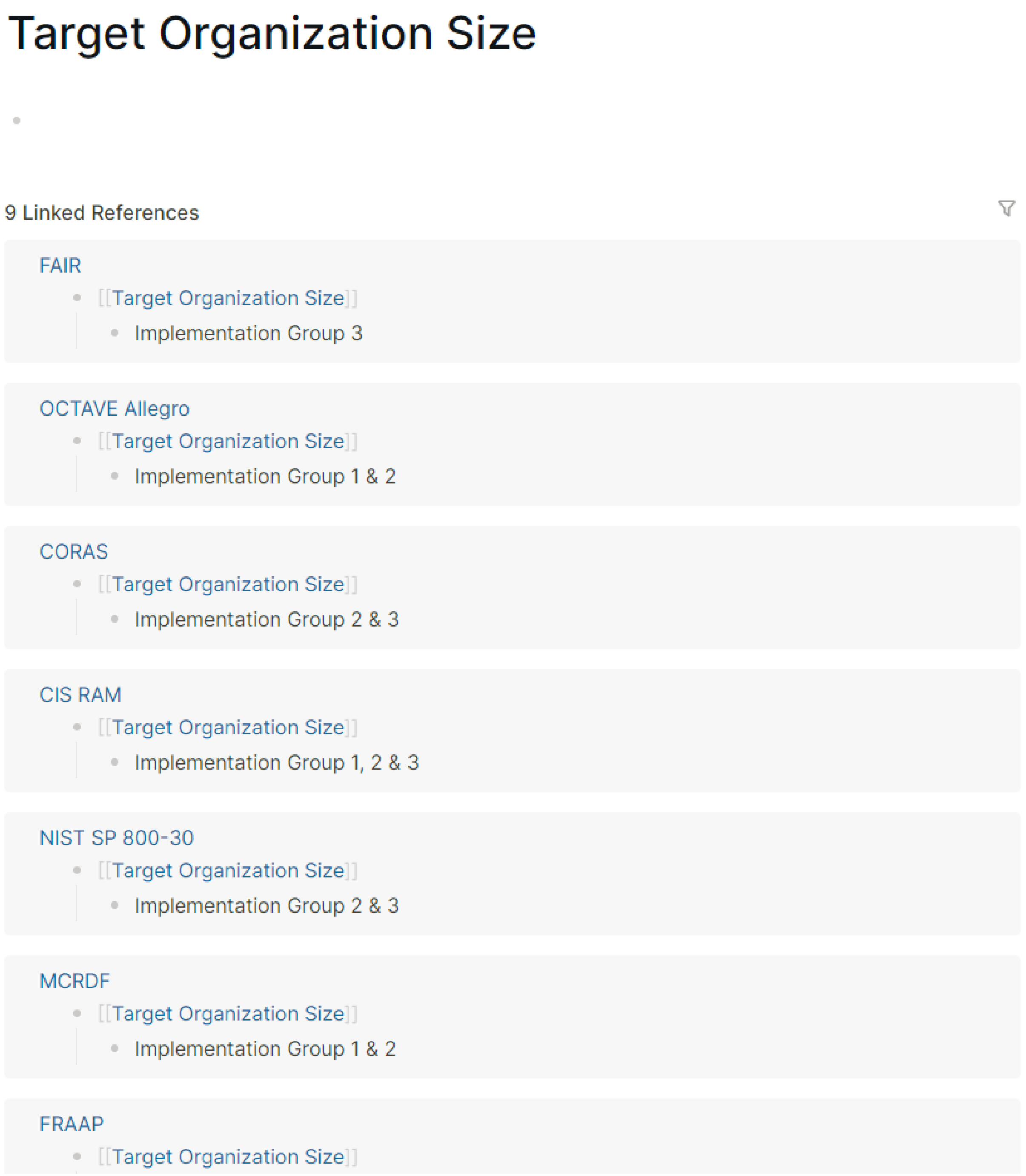


Figure 5.2: The Comparison Framework Graph



Target Organization Size

9 Linked References

FAIR
- [[Target Organization Size]]
  - Implementation Group 3

OCTAVE Allegro
- [[Target Organization Size]]
  - Implementation Group 1 & 2

CORAS
- [[Target Organization Size]]
  - Implementation Group 2 & 3

CIS RAM
- [[Target Organization Size]]
  - Implementation Group 1, 2 & 3

NIST SP 800-30
- [[Target Organization Size]]
  - Implementation Group 2 & 3

MCRDF
- [[Target Organization Size]]
  - Implementation Group 1 & 2

FRAAP
- [[Target Organization Size]]

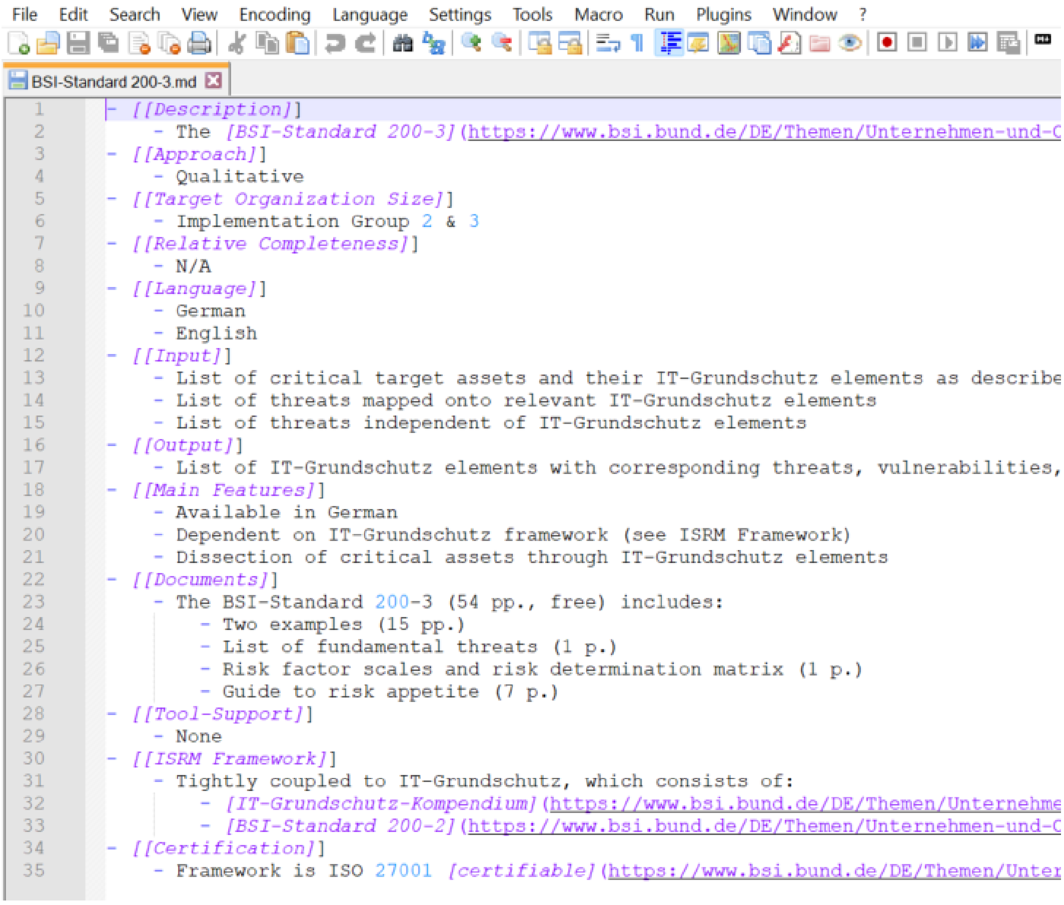
Figure 5.3: The Target Organization Size Journal Page

5.2.3 Adding an ISRA method to the Prototype

If a user wants to add an ISRA method to the ISRA knowledge base Prototype, the method first has to be evaluated in regard to the criteria described in Section 5.1. The two criteria *Target Organization Size* and Relative Completeness score are more difficult to assess, since knowledge about CIS RAM [5], respectively about the CURF [3] framework is needed. After assessing the ISRA method using the framework from section 5.1, the ISRA method template (see Appendix B 4) needs to be copied into the *journal* folder of the graph (see Appendix A). The file should then be renamed to the method name and edited using a text editor. The assessment output of an evaluation criterion should be written below the criterion tag after a tab indent and a hyphen. Indentation and hyphens can be used to layer information as seen for the *Documents* criteria in Figure 5.4. The markdown files inside the *journal* .zip file (see Appendix B 3) serve as examples. A hyperlink can be added to text by enclosing the text in square brackets and providing the link in parenthesis after closing the brackets.

5.2.4 Removing an ISRA method from the Prototype

If the information to an ISRA method is not needed anymore, the user can click *All pages* in the menu on the left-hand side. All the pages of the graph are listed here and can be selected using a checkbox next to their name. By checking the box next to an ISRA method name and subsequently clicking the *Delete* button on top of the page, the method gets removed from the knowledge base graph. This is especially helpful when eliminating ISRA methods as potential candidates during a selection process.



```
- [[Description]]
    - The [BSI-Standard 200-3](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-C
- [[Approach]]
    - Qualitative
- [[Target Organization Size]]
    - Implementation Group 2 & 3
- [[Relative Completeness]]
    - N/A
- [[Language]]
    - German
    - English
- [[Input]]
    - List of critical target assets and their IT-Grundschutz elements as describe
    - List of threats mapped onto relevant IT-Grundschutz elements
    - List of threats independent of IT-Grundschutz elements
- [[Output]]
    - List of IT-Grundschutz elements with corresponding threats, vulnerabilities,
- [[Main Features]]
    - Available in German
    - Dependent on IT-Grundschutz framework (see ISRM Framework)
    - Dissection of critical assets through IT-Grundschutz elements
- [[Documents]]
    - The BSI-Standard 200-3 (54 pp., free) includes:
        - Two examples (15 pp.)
        - List of fundamental threats (1 p.)
        - Risk factor scales and risk determination matrix (1 p.)
        - Guide to risk appetite (7 p.)
- [[Tool-Support]]
    - None
- [[ISRM Framework]]
    - Tightly coupled to IT-Grundschutz, which consists of:
        - [IT-Grundschutz-Kompendium](https://www.bsi.bund.de/DE/Themen/Unternehme
        - [BSI-Standard 200-2](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-C
- [[Certification]]
    - Framework is ISO 27001 [certifiable](https://www.bsi.bund.de/DE/Themen/Unter
```

Figure 5.4: The BSI-Standard 200-3 Markdown File inside Notepad++

Chapter 6

Evaluation

The evaluation of this thesis comprises two parts: The comparison of the current framework, which was introduced in the last chapter, against the frameworks of Shukla and Kumar [10] as well as Agrawal [11] and a case study using an imaginary organization to test the usability and efficiency of the framework.

6.1 Framework Comparison

We begin by comparing the number of evaluation criteria and methods used in the current framework, the framework of Shukla and Kumar [10] and Agrawal's [11] framework. Afterward, we assess if and how each framework implements the evaluation criteria of the others.

6.1.1 Overview

"The current framework includes more evaluation criteria and evaluated methods compared to the framework of Shukla and Kumar [10] or Agrawal [11], as shown in Table 6.1. This is due to the fact that the current framework was built upon these frameworks and adopted the most useful criteria while also introducing additional ones. While having more criteria may make the evaluation process more complex, the current work evaluated more ISRA methods than the previous works. The focus of the current work was to incorporate as many new methods as possible that are commonly used in practice.

Table 6.1: Framework Comparison Overview

	Current Framework	**Shukla and Kumar [10]**	**Agrawal [11]**
# of Evaluation Criteria	12	10	8
# of Methods Evaluated	9	6	4

6.1.2 Comparison to the Framework of Shukla and Kumar

The framework of Agrawal [11] included many evaluation criteria that were omitted by Agrawal [11] and the current framework, as shown in Table 6.2. For instance, vendor name and country of origin were deemed irrelevant for assisting the selection of an ISRA method and were omitted by both Agrawal and the current framework. Instead of date of first release, it was considered to incorporate the release date of the latest version into the current framework. This would have been more favorable for older methods like FRAAP [12], which were updated over time. However, the author of this work decided against it as the criteria would have to be continuously updated to remain relevant and with time there a discrepancy between the latest release and the release studied in this thesis would appear. Language, price, and tool support were incorporated into the current framework as they were deemed important factors for ISRA method selection. Two interesting criteria, that were not adopted were compliance with IT standards and the skill needed. Compliance with IT standards could have been adopted into the current framework, but it was decided that it was enough to know, whether an ISRA method was certifiable. Skills needed seemed like a useful criterion, but were too difficult to assess without any practical knowledge of conducting risk assessments. Instead, the target organization size was evaluated (see section 6.1.4). Availability was not considered relevant for this work as it aimed to facilitate choosing between methods that have already been officially released. The assessment approach as defined in [13], was the only evaluation criteria appearing in all of the comparison frameworks.

Table 6.2: Comparison to Shukla and Kumar

Criteria of Shukla and Kumar [10]	**Agrawal [11]**	**Current Framework**
Assessment approach	✓	✓
Vendor Name	-	-
Country of Origin	-	-
Date of First Release	-	-
Languages	-	✓
Price	-	✓
Compliance to IT Standards	-	-
Skills Needed	✓(Part of effort)	-
Availability	-	-
Tools Supporting the Method	-	✓

6.1.3 Comparison to the Framework of Agrawal

The purpose evaluation criteria of Agrawal's framework was not directly adopted by the current framework as shown in Table 6.3. If an ISRA method is specific to a use case, it should be mentioned in the description and main features criteria of the current work. The main feature criterion also provides space to list any other inherent features that were listed under the purpose criteria in Agrawal's framework. Input and outcome criteria were incorporated into the current framework. The Effort criterion similar to the skills needed factor in the work of Shukla and Kumar [10], was considered too difficult to assess without any practical knowledge of conducting risk assessments. Instead, target organization size was evaluated (see section 6.1.4). The target organization size in the current framework includes the functionality of determining scalability, by assessing whether the ISRA method is suitable to be used by organizations of the implementation group 3, as defined in [15]. As explained in section 5.1.7, many characteristics of an ISRA method can be seen as advantages or disadvantages depending on the situation. For example, a simple risk estimation model is advantageous, when conducting a quick assessment with limited resources, but a clear drawback when more granularity is required. Therefore, the current framework did not adopt pros and cons but provided a criterion called main features under which key characteristics of an ISRA method can be listed.

Table 6.3: Comparison to Agrawal

Criteria of Agrawal [11]	**Shukla and Kumar [10]**	**Current Framework**
Assessment approach	✓	✓
Purpose	-	(✓) (Description and main feature)
Input	-	✓
Effort	(✓) (Only skills needed)	-
Outcome	-	✓
Scalability	-	(✓) (Target Organization Size)
Pros	-	(✓) (Main features)
Cons	-	(✓) (Main features)

6.1.4 Novel Aspects of the Current Framework

It is questionable, whether the description in the ISRA profiles of the current framework is can be seen as a comparison criterion. However, it does serve the purpose of providing a brief introduction to an ISRA method for users. In contrast, Shukla and Kumar [10] do not offer such an introduction in their comparison framework, making it difficult for users to become quickly familiar with the methods. On the other hand, Agrawal [11] uses the purpose criterion to briefly mention the key features of an ISRA method in one sentence, which gives users an idea of what to expect. Providing a few sentence-long descriptions of ISRA methods is more effective in generating interest in the method and facilitating a smoother introduction. This is especially useful when a framework is used to compare a vast amount of ISRA methods, and users may feel overwhelmed by technicalities initially.

Target organization size as discussed in section 5.1.3, is a novel comparison criterion that allows users to quickly evaluate whether an organization has the necessary knowledge and resources to implement the assessment method. The criteria used by Shukla and Kumar [10] or Agrawal [11] to describe the skill and effort required were not expressive enough to guide users effectively. For Instance, a system administrator working alone in a small fifteen-employee retail company may be searching for a risk assessment method. The employee is now considering an ISRA method that needs standard-level expertise but a team of several people to conduct the assessment. The latter fact is reflected in the target organization size criterion, whereas the admin might make a wrong decision if presented only information about time consumption and skill required.

Another novel evaluation criterion is relative completeness as discussed in section 5.1.4. Relative completeness provides the user with a rough estimate of the extent to which each phase of an ISRA method is covered. This allows for quick filtering of methods that do not meet an organization's requirements. For example, if a large organization of implementation group 3, as defined in [15], is searching for an ISRA method with a detailed risk model, it can immediately eliminate all methods that do not have good relative completeness in the risk estimation phase. This shortens the selection process and provides more time to explore suitable methods. If no information is provided about the risk model in criteria like purpose, outcome, pros or cons [11], there is a risk that an inappropriate method may be considered.

Unfortunately, the frameworks presented by Shukla and Kumar [10] or Agrawal [11] do not provide information about the volume of the ISRA method material and what it entails. The documents criterion (see Section 5.1.8), on the other hand, presents the media provided to assist with conducting the ISRA method and lists the important complementary materials. These materials are especially useful for organizations with limited knowledge [21]. For example, the IT personnel of a medium-sized company in implementation group 2, as defined in [15], recently adopted their first ISRA method. Unfortunately, the newly adopted method was too high-level and the employees struggled with the definition of risk factor levels. Using the current framework the employees, chose NIST SP 800-30 [13] and OCTAVE Allegro as [51] as their main choices because they both provide several pages of risk factor scales. The fact that only impact scale templates are provided in the OCTAVE Allegro white paper, led the responsible decision maker to prefer NIST SP 800-30 over OCTAVE Allegro because they had bad experiences with less detailed methods and did not want to settle for such an approach. This decision would not have been possible without reading the ISRA method white papers, had the other frameworks been used.

Since Shukla and Kumar [10] as well as Agrawal [11] only evaluated methods that are not part of an ISRM, they had no reason to include that evaluation criterion. However, this criterion is useful when evaluating ISRA methods that are integrated into a framework for two reasons. Firstly, it helps prevent a user from selecting an ISRA approach that is tightly coupled to an ISRM that the user's organization has not implemented. Secondly, it can help pitch an ISRM to an organization that has not yet employed one. For Instance, a small organization in implementation group 1, as defined in [15], is searching for an ISRA method for a quick risk assessment of their new customer website. After assessing their company size and comparing it with the target organization size, they narrow down their options to the CIS RAM for implementation group one [35] and OCTAVE Allegro [51], but prefer CIS RAM because of the automatic tool support. The ISRM criterion now helps the organization to realize that if they want to employ the CIS RAM method, they need to map their existing controls onto the CIS controls. The organization can choose OCTAVE Allegro if they do not want to invest the extra effort of the control mapping, do the control mapping and work with CIS RAM or even consider implementing the CIS Controls [15] framework.

An important factor when choosing an InfoSec solution is whether it is possible to attain a certificate that proves to governmental or otherwise overseeing bodies that the knowledge to implement the solution. However, neither Shukla and Kumar [10] nor Agrawal [11] mention certification in their work. While Shukla and Kumar [10] use compliance to IT standards as a criterion, which can be used as a baseline for compliance, this is still not suitable to prove competence to an overseeing entity.

The current comparison framework adopted the useful evaluation criteria from both Shukla and Kumar [10] as well as Agrawal [11]. Additionally, it added criteria like target organization size, relative completeness, documents, ISRM framework, and certification. One could argue that these criteria could also be covered in the criteria purpose or pros and cons of Agrawal [11]. Indeed, sometimes they do cover aspects like organization size. However, those criteria are not well-defined and may not provide sufficient information. The current framework clearly defines what should be included under each criterion, except for the description and main features criteria. These criteria give a method assessor the necessary freedom to mention information that does not belong to any other criteria. The adoption of useful criteria and the incorporation of new, well-defined criteria, make the current framework superior to its predecessors. In the next chapter, a use case will demonstrate the usability of the comparison framework when implemented by its prototype.

Table 6.4: Comparison to Current Framework

Criteria of Current Framework	**Shukla and Kumar [10]**	**Agrawal [11]**
Description	-	(✓) (Purpose)
Assessment Approach	✓	✓
Target Organization Size	-	-
Relative Completeness	-	-
Language	✓	-
Input	-	✓
Output	-	✓
Main features	-	(✓) (Purpose and pros)
Documents	-	-
Tool-Support	✓	-
ISRM Framework	Not relevant	Not relevant
Certification	-	-

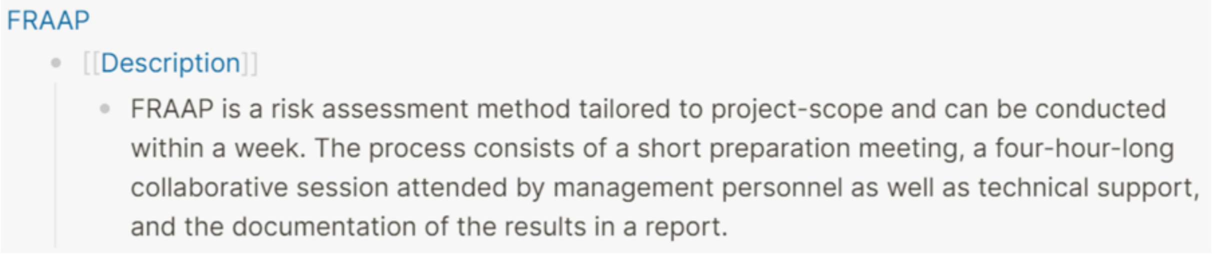
6.2 Case Study

The following use case is fictitious and should demonstrate the efficiency of selecting a suitable ISRA method using the comparison framework together with its knowledge base prototype. As mentioned in Section 5.2, the prototype does not entail explanations of the terms used and should therefore be used in combination with this thesis. The reader is invited to install the prototype as described in Appendix A and try to follow along by copying the steps of the imaginary user.

Alpanat AG is a Swiss company that specializes in the production of chemicals used in toilet refreshers. Approximately 150 employees in total work at Alpanat AG, either on the production site or in their office building close to their factory. On the factory site, there are multiple chemical reactors and synthesizers that are controlled and monitored by on-site servers. The CEO of the company also plans to integrate IOT devices into the production line. Customer and employee data is still stored on database servers in the basement of their office building and backed up in the cloud operated by a cloud provider. Their IT personnel consists of an IT manager, two system administrators, a network administrator, a newly employed InfoSec specialist called Alex, and two help desk workers. The company does not yet employ an ISRM but has information security controls and safeguards in place maintained by the system and the network administrators. Depending on the outcome of the risk assessment the company decides whether to spend the time and finances to integrate an ISRM into the organization.

The It manager wants the company to assess its information security risks for the first time and appoints Alex to do the assessment. Alex can work full-time on the assessment and has approximately a quarter to conduct it. The ISRA should yield a RAR that can be shown to the CEO of the company. The It manager tells him that it is planned for one system administrator and the network administrator to work a day per week for the assessment. Additionally, Alex can request administrative help in form of a secretary if required. After the assessment, the identified critical information security risks should be treated, within another quarter. Alex already did an ISRA at his last job but used a method, which is unavailable in this situation, because it was designed by his last employer and is not open to the public. Since the ISRA should start next week, designing a custom method is not an option, and a publicly available ISRA method should be chosen. Fortunately, an old friend working in the Communication Systems Group of the University of Zürich organizes Alex a copy of this thesis and a memory stick with the material mentioned in Appendix B.

After finishing the installation as described in Appendix A, Alex has the interactive knowledge base graph opened inside Logseq as seen in Figure 5.2. Alex clicks on the circle representing the main features criteria, eager to get more information about each method. After reading the main features of each method, Alex wants to eliminate the FRAAP [12] method as a candidate since it says it is tailored to project-scope and the assessment itself only takes two meetings (see Figure 6.1). The FRAAP page is then removed from the graph using the guidance given in Section 5.2.4. After navigating back to the graph view, the information security specialist decides to further investigate the NIST SP 800-30 [13] and clicks its tag. The information is quickly skimmed through and questions about the evaluation criteria are answered by consulting Section 5.1 of this thesis. Alex chooses to use the target organization size as an elimination criterion. Because Alex assesses the company as belonging to implementation group two (see Section 4.3), only the FAIR method can be eliminated.

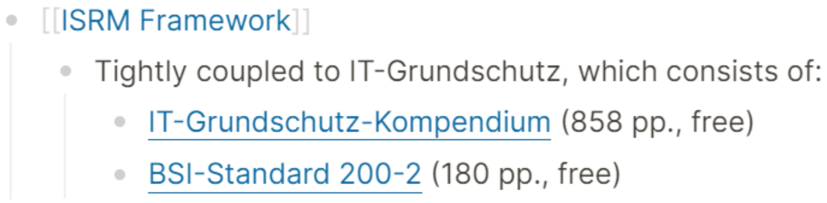


FRAAP

- [[Description]]
  - FRAAP is a risk assessment method tailored to project-scope and can be conducted within a week. The process consists of a short preparation meeting, a four-hour-long collaborative session attended by management personnel as well as technical support, and the documentation of the results in a report.

Figure 6.1: The Description of FRAAP

Alex further investigates the relative completeness of the ISRA methods. The InfoSec specialist argues that because it is the first ISRA of the company, the identification phase must have good relative completeness in the risk identification phase. The MCRDF is then eliminated because it has bad relative risk identification completeness. Methods left that do not have relative completeness values like CIS-RAM, and the BSI-Standard 200-3 are not eliminated but are further investigated. Alex navigates to the CIS RAM page and reads through it. But no information is found that immediately disqualifies this method. By clicking on the relative completeness tag, the InfoSec specialist is transferred back to the completeness overview. On the BSI-Standard 200-3 page of the knowledge base graph, the information is provided that the method is tightly coupled to the IT-Grundschutz (see Figure 6.2). Brief research using the links provided in the knowledge base prototype gave Alex the feeling that this is too much of a commitment for the company to work with this method including the components needed from the ISRM framework. Therefore, the method is removed from the graph.



- [[ISRM Framework]]
  - Tightly coupled to IT-Grundschutz, which consists of:
    - IT-Grundschutz-Kompendium (858 pp., free)
    - BSI-Standard 200-2 (180 pp., free)

Figure 6.2: The ISRM Framework of BSI-Standard 200-3

Next, the inputs needed to conduct each ISRA method are closely inspected and evaluated. The IT specialist is interested in checking whether the provided human resources are enough to yield the required inputs. From the graph view circle labeled with input is clicked and Alex is transferred to the input page, where each method can be checked one after another. The specialist realizes that most of the inputs of the CIS-RAM method are related to information security safeguards. Since most of the knowledge of existing safeguards and controls is shared between a system administrator and the network administrator, Alex is afraid that the workload is too much for the limited time these employees have available to work on the assessment. This leads to the elimination of CIS RAM as a possible candidate and the specialist now only has four methods left to choose from (see Figure 6.3).

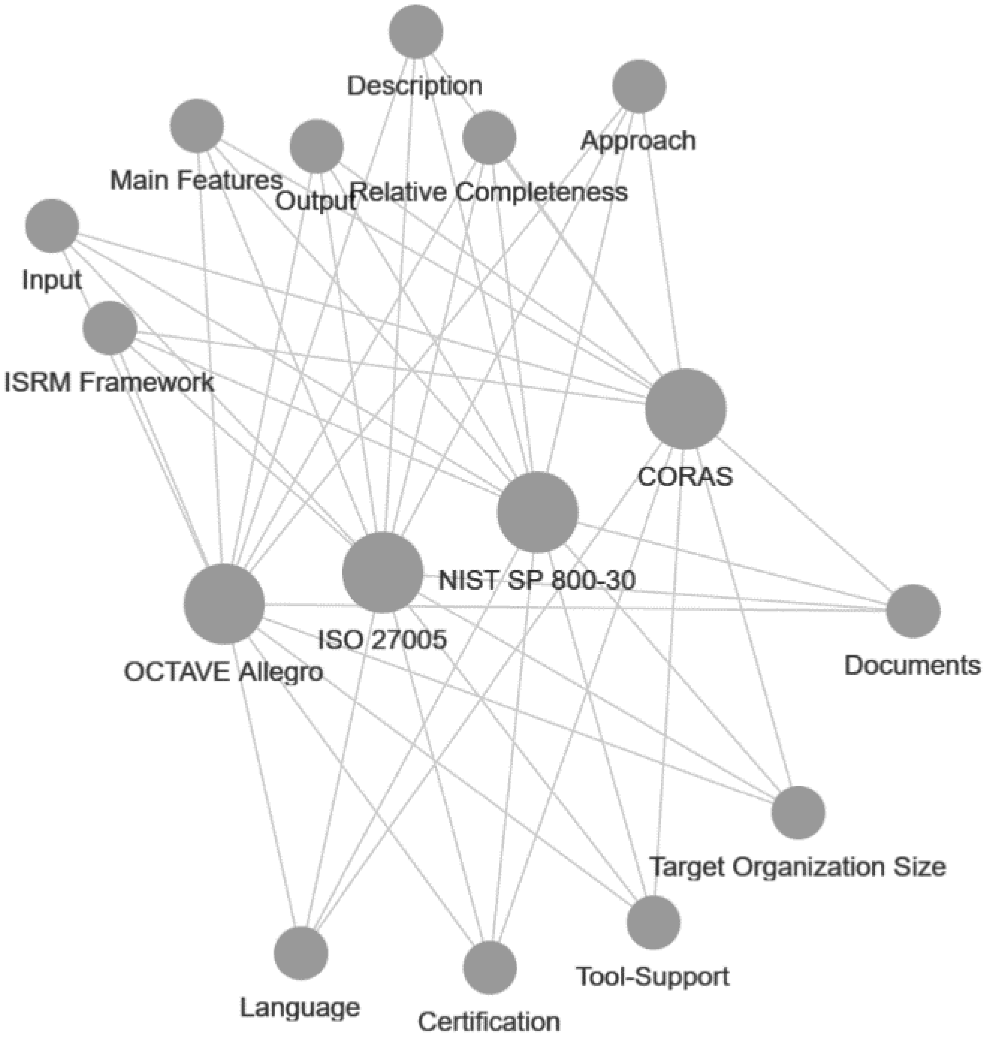


Figure 6.3: The Reduced Knowledge Base Graph

After comparing the inputs, Alex decides to compare the outputs of the ISRA methods that are still left. Looking at the output page it becomes evident that only the NIST SP 800-30 yields a RAR after following the process. This convinces the InfoSec specialist to choose this method if no other characteristics of this ISRA method eliminate it as a solution. Taking a closer look at the NIST SP page of the knowledge base graph, Alex identifies two advantages. The amount of complementary material the white paper of the method provides is extensive. Further, the method is part of an ISRM framework that could later be adapted. The coupling to the framework is loose though so it is also applicable without any other parts of the framework. Two disadvantages that are discovered are that no tool support or certification is available. Since neither tool support nor certification was a requirement, Alex thinks that the good outweighs the bad. The InfoSec specialist reads the summary and discussion of the method given in Section 4.10 to make certain that a proper method was chosen. The discussion mentions that neither stakeholder nor asset identification is part of the process. Alex sees this as a problem that has to be discussed with the IT manager but does not want to eliminate NIST SP 800-30 as a possibility for the ISRA conduction. The InfoSec specialist decides to suggest NIST SP 800-30 in the next meeting together with an alternative method.

Since the problem with NIST was the completeness of the identification phase, an alternative should be chosen with a good risk identification completeness score. This leaves CORAS and ISO 27005 as possible alternatives. Certification was identified as a strength of ISO 27005 and tool support as a strength of CORAS. Since neither of those criteria was seen as crucial in the beginning, a favorite can not be identified and Alex decides to read both summaries and discussions of the methods in Section 4.8, respectively Section 4.4. The InfoSec specialist learns that CORAS does not provide help for detailed asset identification and is therefore not a well-suited alternative to NIST SP 800-30. Reading the summary and discussion of ISO 27005 does not yield a reason to refuse the method. Alex is pleased with the two alternatives, NIST SP 800-30 and ISO 27005:2018, and is eager to propose these methods in the upcoming meeting with the IT manager.

This case study demonstrates that a user familiar with the necessary background knowledge is able to use the knowledge base prototype and the contents of this thesis to quickly find suitable ISRA methods for an organization. The quickness with which methods can be eliminated helps to invest more time in analyzing more suitable methods. Even if the criteria of the comparison framework do not suffice to assure the user that the most appropriate method was chosen, the summaries and discussions of the ISRA methods in this thesis can be consulted to make an informed decision.

Chapter 7

Summary and Future Work

The goal of this thesis was to develop a navigable ISRA method knowledge base prototype that facilitates efficiently comparing methods and therefore assists with selecting a suitable ISRA method. This prototype is complemented by the collection of summaries and discussions of the ISRA methods inside this thesis. These two elements address the need for ISRA selection tool support as identified by the review of the status quo of academia, the private or governmental sector.

After establishing the necessary background knowledge, using two standard ISRA methods, the related work was thoroughly reviewed. Only one ISRA selection tool in academia was discovered, which needed an excessive amount of expert knowledge to be used and implemented. In the private sector, two tools were identified. One of them used the same approach as the tool found in academia and the other one was rather tailored to select ISRM frameworks than ISRA methods. Thereupon, comparison methods were taken into account, because of the lack of relevant work on ISRA selection. Two frameworks were identified that could have been used to select an ISRA method for an organization. The lack of expressiveness or well-definedness of their evaluation criteria prompted the author of this thesis to devise their own improved comparison framework, based on the predecessors and related work.

Nine ISRA methods were analyzed in-depth such that new evaluation criteria could be developed and the necessary knowledge for their evaluation could be acquired. The analysis was done by reading the corresponding primary sources of the ISRA methods, because of a lack of comprehensive summaries and discussions in related work. This motivated the author to compile a collection of summaries and discussions, which could be used to assist users of the comparison framework if they doubt the outcome of their selection process or introduce students to various ISRA methods.

Based on related work and the study of ISRA methods the improved comparison framework was developed by clearly defining each evaluation criterion. The improved framework was used to evaluate all the analyzed ISRA methods. Because of the volume of the content created by the evaluation, a navigable knowledge base prototype was implemented that facilitates the selection of a suitable ISRA method.

Through a comparison of the new comparison framework with its predecessors, its superiority was demonstrated. It was argued that the crucial evaluation criteria were adopted and examples of decisions that were not resolvable with the predecessing comparison framework were presented. In the context of a case study with a fictional company, an employee used the knowledge base prototype and the contents of this thesis to select a suitable ISRA method based on various characteristics of the organization. The case study proved that this is possible in an efficient manner.

There are three main considerations for future work regarding the comparison framework and knowledge base prototype. The first one is that more methods could be added to it. An example of an interesting ISRA approach to add is the one in the RISK IT [29] framework, which was not considered because of the additional time needed to isolate the method. Next, the comparison framework could be expanded with use cases for each ISRA method. This would give a user quick guidance on when and how to apply the methods. Finally, Scalability could become a problem when expanding the knowledge base with more methods and criteria. Therefore it would be useful to be able to filter methods according to selected criteria.

Bibliography

[1] FINMA, "Annual Report", Bern, Tech. Rep., 2021, https://www.finma.ch/~/media/finma/dokumente/dokumentencenter/myfinma/finma-publikationen/geschaeftsbericht/20220405-finma_jahresbericht_2021.pdf Last visit 01.03.2023.

[2] ISO, "ISO/IEC 27005:2018", Geneva, Tech. Rep., Jul. 2018, https://www.iso.org/standard/75281.html Last visit 01.03.2023.

[3] G. Wangen, C. Hallstensen, and E. Snekkenes, "A framework for estimating information security risk assessment method completeness: Core Unified Risk Framework, CURF", *International Journal of Information Security*, vol. 17, no. 6, pp. 681–699, Nov. 2018, ISSN: 1615-5262, 1615-5270. DOI: 10.1007/s10207-017-0382-0.

[4] E. Wheeler, *Security Risk Management: Building an Information Security Risk Management Program from the Ground Up*. Syngress Publishing, May 2011, ISBN: 978-1-59749-615-5.

[5] CIS, "CIS Risk Assessment Method (RAM)", East Greenbush, NY, Tech. Rep., version 2.1, Aug. 2022, https://www.cisecurity.org/insights/white-papers/cis-ram-risk-assessment-method Last visit 01.03.2023.

[6] S. Smojver, "Selection of Information Security Risk Management Method Using Analytic Hierarchy Process (AHP)", in *Proceedings of the 22nd Central European Conference on Information and Intelligent Systems*, 2011, pp. 119–126.

[7] ENISA, "Determining Your Organization's Information Risk Assessment and Management Requirements and Selecting Appropriate Methodologies", Tech. Rep., version 2.0, Sep. 2008, https://www.enisa.europa.eu/publications/archive/determining-your-organization2019s-information-risk-assessment-and-management/@@download/fullReport Last visit 01.03.2023.

[8] ENISA, "SARP - Self Assessed Risk Profiler", May 2009, https://www.enisa.europa.eu/topics/risk-management/files/tools/sarm-2009-05-10.xls Last visit 01.03.2023.

[9] M. Sajko, N. Hadjina, and D. Pešut, "Multi-criteria model for evaluation of information security risk assessment methods and tools", in *The 33rd International Convention MIPRO*, May 2010, pp. 1215–1220, ISBN: 978-9-5323-3050-2.

[10] N. Shukla and S. Kumar, "A Comparative Study on Information Security Risk Analysis Practices", *IJCA Special Issue on Issues and Challenges in Networking, Intelligence and Computing Technologies*, vol. ICNICT, no. 3, pp. 28–33, Nov. 2012.

[11] V. Agrawal, "A Comparative Study on Information Security Risk Analysis Methods", *Journal of Computers*, vol. 12, Dec. 2015. DOI: `10.17706/jcp.12.1.57-67`.

[12] T. R. Peltier, *Information Security Risk Analysis*, 3rd. Auerbach Publications, 2010, ISBN: 9780429094071. DOI: `https://doi.org/10.1201/EBK1439839560`.

[13] NIST, "NIST Special Publication 800-30", Gaithersburg, MD, Tech. Rep., Sep. 2012, `https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final` Last visit 01.03.2023.

[14] ISO, "ISO Guide 73:2009", Geneva, Tech. Rep., Nov. 2009, `https://www.iso.org/standard/44651.html` Last visit 01.03.2023.

[15] CIS, "CIS Critical Security Controls", East Greenbush, NY, Tech. Rep., version 8, May 2021, `https://www.cisecurity.org/controls` Last visit 01.03.2023.

[16] A. Shameli-Sendi, R. Aghababaei-Barzegar, and M. Cheriet, "Taxonomy of information security risk assessment (ISRA)", *Computers & Security*, vol. 57, pp. 14–30, 2016, ISSN: 0167-4048. DOI: `https://doi.org/10.1016/j.cose.2015.11.001`.

[17] T. Saaty, *Fundamentals of Decision Making and Priority Theory With the Analytic Hierarchy Process*. RWS Publications, 1994, ISBN: 978-1-88860-315-6.

[18] E. Paintsil, "Taxonomy of security risk assessment approaches for researchers", in *2012 Fourth International Conference on Computational Aspects of Social Networks (CASoN)*, Nov. 2012, pp. 257–262, ISBN: 978-1-4673-4794-5. DOI: `10.1109/CASoN.2012.6412412`.

[19] P. Shamala, R. Ahmad, and M. Yusoff, "A conceptual framework of info structure for information security risk assessment (ISRA)", *Journal of Information Security and Applications*, vol. 18, pp. 45–52, 2013. DOI: `10.1016/j.jisa.2013.07.002`.

[20] J. E. Stamp and P. L. Campbell, "A classification scheme for risk assessment methods.", Albuquerque, Tech. Rep., Aug. 2004, `https://www.osti.gov/biblio/925643` Last visit 01.03.2023. DOI: `10.2172/925643`.

[21] G. Wangen, "Information Security Risk Assessment: A Method Comparison", *Computer*, vol. 50, no. 4, pp. 52–61, 2017. DOI: `10.1109/MC.2017.107`.

[22] T. Aven, "The risk concept—historical and recent development trends", *Reliability Engineering & System Safety*, vol. 99, pp. 33–44, 2012, ISSN: 0951-8320. DOI: `https://doi.org/10.1016/j.ress.2011.11.006`.

[23] ENISA, "Methodology for evaluating usage and comparison of risk assessment and risk management items", Tech. Rep., version 1.0, Apr. 2007, `https://www.enisa.europa.eu/publications/archive/methodology-for-evaluating-usage-and-comparison-of-risk-assessment-and-risk-management-items/at_download/fullReport` Last visit 01.03.2023.

[24] BSI, "BSI-Standard 200-3", Bonn, Tech. Rep., version 1.0, Oct. 2017, `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_3.pdf?__blob=publicationFile&v=2` Last visit 01.03.2023.

[25] Datatilsynet, "Risikovurdering av informasjonssystem", Oslo, Tech. Rep., 2011, `https://www.datatilsynet.no/globalassets/global/dokumenter-pdfer-skjema-ol/regelverk/veiledere/risikovurdering_veileder.pdf` Last visit 01.03.2023.

[26] FINMA, “FINMA Guidance - Duty to report cyber attacks pursuant to Article 29 para. 2 FINMASA”, Bern, Tech. Rep., May 2021, https://www.finma.ch/en/documentation/dossier/dossier-cyberrisiken/ Last visit 01.03.2023.

[27] L. Rajbhandari and E. Snekkenes, “Intended Actions: Risk Is Conflicting Incentives”, in *Information Security*, Berlin, Heidelberg: Springer, 2012, pp. 370–386, ISBN: 978-3-642-33383-5.

[28] Z. Yazar, “A qualitative risk analysis and management tool–cramm”, *SANS InfoSec Reading Room White Paper*, vol. 11, pp. 12–32, 2002.

[29] ISACA, *Risk IT Framework.* 2009, ISBN: 978-1-60420-111-6.

[30] BSI, “IT-Grundschutz-Kompendium”, Bonn, Tech. Rep., Feb. 2023, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf?__blob=publicationFile&v=4#download=1 Last visit 01.03.2023.

[31] BSI, “BSI-Standard 200-2”, Bonn, Tech. Rep., version 1.0, Oct. 2017, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.html?nn=128640 Last visit 01.03.2023.

[32] BSI, “ISO 27001 Zertifizierung auf Basis von IT-Grundschutz”, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Managementsystemen/ISO-27001-Basis-IT-Grundschutz/iso-27001-basis-it-grundschutz_node.html Last visit 01.03.2023.

[33] L. Rajbhandari and E. Snekkenes, “Using the Conflicting Incentives Risk Analysis Method”, in *Security and Privacy Protection in Information Processing Systems*, Berlin, Heidelberg: Springer, 2013, pp. 315–329, ISBN: 978-3-642-39218-4.

[34] DoCRA Council, “Duty of Care Risk Analysis Standard”, DoCRA Council, Schaumburg, IL, Tech. Rep., version 0.6, Jun. 2021, http://www.docra.org/wp-content/uploads/2021/06/Duty-of-Care-Risk-Analysis-Standard-Draft-20200907.pdf Last visit 01.03.2023.

[35] CIS, “CIS Risk Assessment Method (RAM) – Implementation Group 1”, East Greenbush, NY, Tech. Rep., version 2.1, Aug. 2022, https://www.cisecurity.org/insights/white-papers/cis-ram-risk-assessment-method Last visit 01.03.2023.

[36] CIS, “CIS Risk Assessment Method (RAM) – Implementation Group 2”, East Greenbush, NY, Tech. Rep., version 2.1, Aug. 2022, https://www.cisecurity.org/insights/white-papers/cis-ram-risk-assessment-method Last visit 01.03.2023.

[37] CIS, “CIS Risk Assessment Method (RAM) – Implementation Group 3”, East Greenbush, NY, Tech. Rep., version 2.1, Aug. 2022, https://www.cisecurity.org/insights/white-papers/cis-ram-risk-assessment-method Last visit 01.03.02.2023.

[38] CIS, “CSAT Pro User Guide”, https://csat.readthedocs.io/en/stable/source/csat_pro_user_guide/ Last visit 01.03.2023.

[39] J. Freund and J. Jones, *Measuring and managing information risk: a FAIR approach.* Newton, MA: Butterworth-Heinemann, Aug. 2014, ISBN: 978-0-12-799932-6.

[40] M. S. Lund, B. Solhaug, and K. Stølen, *Model-driven risk analysis: The CORAS approach*. Springer, 2010, ISBN: 978-3-642-12323-8. DOI: `https://doi.org/10.1007/978-3-642-12323-8`.

[41] SINTEF, "CORAS - A risk modelling approach", `https://coras.tools/#/` Last visit 01.03.2023.

[42] SINTEF, "The CORAS Tool", Jan. 2012, `https://coras.sourceforge.net/coras_tool.html` Last visit 01.03.2023.

[43] F. Braber, I. Hogganvik, M. S. Lund, K. Stølen, and F. Vraalsen, "Model-Based Security Analysis in Seven Steps — a Guided Tour to the CORAS Method", *BT Technology Journal*, vol. 25, no. 1, pp. 101–117, Jan. 2007, ISSN: 1358-3948. DOI: `10.1007/s10550-007-0013-9`.

[44] ENISA, "Cramm", `https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html` Last visit 01.03.2023.

[45] Wikipedia contributors, "PERT distribution", Jul. 2022, `https://en.wikipedia.org/wiki/PERT_distribution` Last visit 01.03.2023.

[46] RiskLens, "RiskLens Enterprise", 2023, `https://www.risklens.com/products-services/platform` Last visit 01.03.2023.

[47] FAIR INSTITUTE, "FAIR TRAINING AND CERTIFICATION", 2023, `https://www.fairinstitute.org/fair-training-and-certification-courses` Last visit 01.03.2023.

[48] RiskLens, "Results for www.fairinstitute.org", 2023, `https://risklens-academy.myshopify.com/?utm_referrer=https%3A%2F%2Fwww.fairinstitute.org%2F` Last visit 01.03.2023.

[49] FAIR INSTITUTE, "FAIR-U", 2023, `https://www.fairinstitute.org/fair-u` Last visit 01.03.2023.

[50] The Open Group, "Open FAIR Certification Program", 2023, `https://www.opengroup.org/certifications/openfair` Last visit 01.03.2023.

[51] R. Caralli, J. Stevens, L. Young, and W. Wilson, "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process", Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, Tech. Rep. CMU/SEI-2007-TR-012, 2007, `http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=8419` Last visit 01.03.2023.

[52] ISO, "ISO/IEC 31000:2018", Geneva, Tech. Rep., Feb. 2018, `https://www.iso.org/standard/65694.html` Last visit 01.03.2023.

[53] Firebrand Training GmbH, "ISO - 27005 Risk Manager - Information Security Risk Management", 2023, `https://firebrand.training/ch/kurse/iso/27005-risk-manager-zertifizierung` Last visit 01.03.2023.

[54] Professional Evaluation and Certification Board, "ISO/IEC 27005 Risk Manager", 2023, `https://pecb.com/de/education-and-certification-for-individuals/iso-iec-27005/iso-iec-27005-risk-manager` Last visit 01.03.2023.

[55] G. Stone and P. Noel, “Cloud Risk Decision Framework”, Microsoft, Redmond, WA, Tech. Rep., 2015, `https://download.microsoft.com/documents/australia/enterprise/smic1545_pdf_v7_pdf.pdf` Last visit 01.03.2023.

[56] G. Stone, P. Noel, and J. Kavanagh, “Cloud Initiative Risk Analysis based on CSA v3”, `https://download.microsoft.com/documents/australia/enterprise/Risk_Framework_Template_Tool.xlsm` Last visit 01.03.2023.

[57] Microsoft, “Cloud Security Alliance (CSA) STAR Certification”, Jul. 2022, `https://learn.microsoft.com/en-us/azure/compliance/offerings/offering-csa-star-certification` Last visit 01.03.2023.

[58] CSA, “Search Results - For: *microsoft cloud risk decision framework*”, 2023, `https://cloudsecurityalliance.org/search/?s=microsoft+cloud+risk+decision+framework` Last visit 01.03.2023.

[59] NIST, “NIST Special Publication 800-39”, Gaithersburg, MD, Tech. Rep., Mar. 2011, `https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-39.pdf` Last visit 01.03.2023.

[60] NIST, “Risk Assessment Tools”, Mar. 2022, `https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/collaboration-space/focus-areas/risk-assessment/tools` Last visit 01.03.2023.

[61] Carnegie Mellon University, “Assessing Information Security Risk Using the OCTAVE Approach - eLearning”, 2023, `https://www.sei.cmu.edu/education-outreach/courses/course.cfm?coursecode=V22` Last visit 01.03.2023.

[62] Carnegie Mellon University, “Assessing Information Security Risk Using the OCTAVE Approach”, 2023, `https://www.sei.cmu.edu/education-outreach/courses/course.cfm?courseCode=P10B` Last visit 01.03.2023.

[63] ISACA, “COBIT - An ISACA Framework”, `https://www.isaca.org/resources/cobit` Last visit 01.03.2023.

[64] Logseq, Inc., “Logseq: A privacy-first, open-source knowledge base”, 2023, `https://logseq.com/` Last visit 01.03.2023.

[65] Logseq, Inc., “Logseq Community Hub ”, 2023, `https://hub.logseq.com/` Last visit 01.03.2023.

Abbreviations

AHP	Analytic Hierarchy Process
BSI	Bundesamt der Sicherheit in der Informationstechnik
CIA	Confidentiality, Integrity, and Availability
CIRA	Conflicting Incentives Risk Analysis
CIS	Center for Internet Security
CRAMM	Central Computer Agency Risk Analysis and Management Method
CSA STAR	Cloud Security Alliance Security, Trust, Assurance, and Risk
CURF	Core Unified Risk Framework
DoCRA	Duty of Care Risk Analysis
ENISA	European Union Agency for Cybersecurity
FAIR	Factor Analysis of Information Risk
FINMA	Swiss Financial Market Supervisory Authority
FRAAP	Facilitated Risk Analysis and Assessment Process
InfoSec	Information Security
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
ISRA	Information Security Risk Assessment
ISRM	Information Security Risk Management
MCRDF	Microsoft Cloud Risk Decision Framework
NIST	National Institute of Standards and Technology
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
RAR	Risk Assessment Report
UML	Unified Modeling Language
VoD	Video on Demand

List of Figures

List of Tables

Appendix A

Installation Guidelines

In the following it is explained how to run the prototype of the dynamic user interface for the comparison framework. The free, open-source software Logseq [64] needs to be installed to run the prototype. Logseq is available for Windows, MacOS, Linux, IOS, and Android. This installation guide was only tested for Windows, but should work analogue for MacOs and Linux. If Logseq is already installed, add a new graph and progress with Step 4. of the installation guidelines. Before downloading a release from the official website *https://logseq.com/*, create a folder on your computer, where the prototype graph will be saved. Then download the release from the Logseq website and run it. After the installation, the program starts automatically. Follow the steps below to be able to navigate the prototype graph.

1. Click *Add a graph* in the top right corner of the program. Alternatively, in the menu on the left side choose the top option, which expands a menu and click *Add new graph.*

2. The program prompts you to choose a folder, where your graph will be saved. Choose the folder that you have created beforehand.

3. Open a file navigation program.

4. Navigate to the folder, which contains your new graph and copy the contents from the *journal* .zip file (see Appendix B 3.) into the journal folder of your graph.

5. Switch to Logseq and click *Graph View* in the menu on the left hand side.

Appendix B

Contents of the CD

1. This thesis as PDF
2. This thesis as LaTeXsource in a .zip file
3. A .zip file called *journals*, which contains the ISRA method candidate pages
4. A markdown file called *ISRA_Method_Template*, which is a template for ISRA method candidate pages
5. An Excel file called *Relative_Completeness*, which contains the calculations for the relative completeness score