University of Zurich[UZH]

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

A System for Cost-Efficient Cybersecurity Planning, Compliance, and Investment Prioritization

Bulin Shaqiri
Zurich, Switzerland
Student ID: 17-701-442

Supervisor: Dr. Muriel Franco, Jan von der Assen
Date of Submission: August 9, 2023

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

ifi

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

Abstract

While the digital era provides many advantages, it also comes with significant risks related to cybersecurity. Organizations must be proactive in reducing the risks involved with conducting business in a connected and complex digital world. However, despite the abundance of available resources on cybersecurity guidelines, frameworks, and certifications, Small and Medium-sized Enterprises (SMEs) still struggle to understand their unique cybersecurity requirements and develop tailored cybersecurity strategies. Most notably, existing resources are often too abstract, geared towards larger and more mature organizations, or lack practical guidance. Moreover, they often focus on technical aspects and neglect essential dimensions of cybersecurity, such as the economic and societal dimensions. This is especially apparent in case of cybersecurity certifications. To address these gaps, this Master Thesis introduces three key contributions.

Firstly, the CyberTEA methodology is extended to provide SMEs with practical cybersecurity guidelines and allow them to verify compliance with a set of baseline cybersecurity requirements, all while getting formally acknowledged for that. This, in turn, ensures a more holistic approach that incorporates technical, economic, and societal aspects. This methodology is further validated by mapping it against the components of the NIST Cybersecurity Framework (CSF). Secondly, a novel lightweight cybersecurity certification scheme called CERTSec is proposed to offer SMEs an invaluable entry point into the complex world of cybersecurity. This three-tiered certification scheme takes into account key dimensions of cybersecurity and allows businesses to continuously enhance their cybersecurity posture. CERTSec also underscores the importance of annual reassessments within an ever-evolving threat landscape. The final contribution of this work lies in the development of a prototype that automates processes within the proposed certification scheme.

Three technical requirements have been selected and automated, making the prototype able to *(i)* determine whether Websites establish secure connections, *(ii)* perform network reachability analysis, and *(iii)* conduct comprehensive vulnerability analyses on the networks, technologies and software provided. Evaluations have been conducted to highlight the feasibility of key features used for the automation of the certification scheme processes. The results suggest that it is possible to conduct automation for risk analysis without significant impacts (in terms of resource consumption and overall time spent) on the entire process. Furthermore, a detailed case study is shown to demonstrate the feasibility and application of CERTSec for SMEs.

Zusammenfassung

Das digitale Zeitalter bietet zwar viele Vorteile, birgt aber auch erhebliche Risiken im Bereich der Cybersicherheit. Unternehmen müssen proaktiv vorgehen, um die Risiken zu verringern, die mit der Abwicklung von Geschäften in einer vernetzten und komplexen digitalen Welt verbunden sind. Trotz der Fülle an verfügbaren Ressourcen zu Cybersicherheitsrichtlinien, -rahmen und -zertifizierungen fällt es kleinen und mittleren Unternehmen (KMU) immer noch schwer, ihre speziellen Cybersicherheitsanforderungen zu verstehen und massgeschneiderte Cybersicherheitsstrategien zu entwickeln. Vor allem sind die vorhandenen Ressourcen oft zu abstrakt, auf grössere und reifere Unternehmen ausgerichtet oder es fehlen praktische Anleitungen. Ausserdem konzentrieren sie sich häufig ausschliesslich auf technische Aspekte und vernachlässigen wesentliche Dimensionen der Cybersicherheit, wie die wirtschaftliche und gesellschaftliche Dimension. Dies ist besonders bei Zertifizierungen im Bereich der Cybersicherheit zu beobachten. Um diese Lücken zu schliessen, stellt diese Masterarbeit drei Schlüsselbeiträge vor.

Als erstes wird die CyberTEA-Methode erweitert, um KMU praktische Leitlinien für die Cybersicherheit bereitzustellen und ihnen die Möglichkeit zu geben, die Einhaltung einer Reihe von grundlegenden Cybersicherheitsanforderungen zu überprüfen und sich dafür offiziell anerkennen zu lassen. Dies wiederum gewährleistet einen ganzheitlicheren Ansatz, der technische, wirtschaftliche und gesellschaftliche Aspekte einbezieht. Diese Methodik wird weiter validiert, indem sie mit den Komponenten des NIST Cybersecurity Framework (CSF) abgeglichen wird. Zweitens wird ein neuartiges, leichtgewichtiges Zertifizierungssystem für Cybersicherheit namens CERTSec vorgeschlagen, um KMU einen wertvollen Einstieg in die komplexe Welt der Cybersicherheit zu bieten. Dieses dreistufige Zertifizierungssystem berücksichtigt wichtige Dimensionen der Cybersicherheit und ermöglicht es Unternehmen, ihre Cybersicherheitslage kontinuierlich zu verbessern. CERTSec unterstreicht auch die Bedeutung jährlicher Neuprüfungen in einer sich ständig weiterentwickelnden Bedrohungslandschaft. Der letzte Beitrag dieser Arbeit liegt in der Entwicklung eines Prototyps, der Prozesse innerhalb des vorgeschlagenen Zertifizierungssystems automatisiert.

Drei technische Anforderungen wurden ausgewählt und automatisiert, so dass der Prototyp in der Lage ist, *(i)* festzustellen, ob Websites sichere Verbindungen herstellen, *(ii)* Netzwerkerreichbarkeitsanalysen durchzuführen und *(iii)* umfassende Schwachstellenanalysen für die bereitgestellten Netzwerke, Technologien und Software durchzuführen. Es wurden Evaluierungen durchgeführt, um die Durchführbarkeit von Schlüsselfunktionen für die Automatisierung der Prozesse des Zertifizierungssystems aufzuzeigen. Die Ergebnisse deuten darauf hin, dass die Automatisierung für Risikoanalysen ohne signifikante Auswirkungen

(in Bezug auf Ressourcenverbrauch und Gesamtzeitaufwand) auf den gesamten Prozess durchgeführt werden kann. Darüber hinaus wird anhand einer detaillierten Fallstudie die Machbarkeit und Anwendung von CERTSec für KMU aufgezeigt.

Acknowledgments

First and foremost, I would like to express my deepest gratitude to my supervisor, Dr. Muriel Franco. His invaluable feedback, continuous support, and expert mentorship have been crucial throughout the process of this thesis. His enthusiasm has been both a source of inspiration and a driving force in maintaining my motivation and commitment.

Furthermore, I would like to extend my sincere thanks to Prof. Dr. Burkhard Stiller, head of the Communication System Research Group (CSG) at the University of Zurich, for providing me with the opportunity to work on such an exciting topic and to expose myself to an enriching academic environment.

Finally, I would also like to thank my family and friends for their endless support and encouragement throughout this time.

Contents

Chapter 1

Introduction

As organizations of all sizes undergo digital transformation, the globe has recently become increasingly connected. In the current digital era, it has become for businesses a necessity to digitize their internal operations in order to increase efficiency, cut costs, improve customer service, and, most importantly, maintain competitiveness. The recent COVID-19 pandemic has accelerated this trend, with more companies than ever moving for remote operation. Global spending on digital transformation is expected to more than double by 2026, hitting a staggering US$ 3.4 trillion [1].

While there are numerous advantages to this change, such as the increased efficiency in terms of costs and speed for innovation, it has also brought many new difficulties, notably in the area of cybersecurity. With a variety of new threats emerging in recent years, the complexity of the cybersecurity area has greatly increased. For example, adversaries are taking advantage of the increased connectivity and complexity to exploit vulnerabilities and gain unauthorized access to sensitive information.

In its annual threat landscape report [2], the European Union Agency for Cybersecurity (ENISA) has identified top threats, with Ransomware and Denial-of-Service (DoS) attacks topping the list in its latest edition. Especially threats against the availability of systems or data are on the rise again. In July 2022, cloud services and Content Delivery Network (CDN) provider Akamai reported the largest Distributed DoS (DDoS) attack that has ever been launched in Europe. The distributed attack traffic peaked at 853.7 Gbps and 659.6 Mbps over a 14-hour period [3]. Moreover, the report also points to the increasing sophistication of phishing techniques and the growing interest in supply chain attacks. A prominent example for the latter one is the SolarWinds hack, which saw cybercriminals infiltrate the computer networks of several U.S. government agencies and numerous high-profile organizations by injecting malicious code into SolarWinds' network management tool [2].

These insights clearly show that cybersecurity has become a critical requirement for governments and organizations of all sizes and can not be considered as a nice-to-have anymore. Insufficient protection measures against cybersecurity risks can lead to the compromise of the confidentiality, integrity and availability of information being processed by organizations, thereby resulting in significant financial losses or reputational damage.

Organizations must thus be proactive in reducing the risks related to their operations in the increasingly complex and connected digital world.

However, due to various factors, investing in cybersecurity can be particularly challenging for Small and Medium-sized Enterprises (SMEs). With the help of a survey conducted among 249 SMEs across Europe, ENISA identified key challenges that SMEs face [4]. The results highlight that one of the biggest challenges for SMEs is their limited budget. Many SMEs operate on tight margins and may not have the resources to invest in cybersecurity solutions.

Moreover, awareness of cybersecurity among employees is often low. This is all the more concerning given that they are often the weakest link in an organization's security. Without adequate training, the personnel may not be aware of basic security practices or potential threats, leaving organizations vulnerable to cyber attacks. On top of that, acquiring the necessary in-house expertise can become a major obstacle, as there is generally a shortage of qualified cybersecurity professionals in the marketplace, resulting in having to compete with larger organizations for talents [4, 5].

Besides, there is also the common misconception among SMEs that they are not interesting targets for attackers due to their small size or limited resources - an assumption which is far from being true. In fact, SMEs are often targeted by adversaries precisely because they lack the ability to implement a defense-in-depth approach [5]. [4] points also out that due to budget and expertise constraints, business owners fail to understand the cybersecurity risks they face and may not realize the importance of investing in cybersecurity. This is an underlying issue and leads to cybersecurity being perceived as additional cost rather than an investment. With this in mind, many of the SMEs surveyed reported their reliance only on basic security controls such as firewalls, backups, and antivirus programs, as well as the security controls included in the IT products they purchase.

Nevertheless, even with the various challenges, it is of critical importance for organizations to be able to manage and respond to cybersecurity attacks. A thorough understanding of potential risks and effective strategies to mitigate them, such as robust cybersecurity measures and incident response plans, are required. To help organizations improve their cybersecurity posture, standardization institutes, certification bodies, and regulations have emerged to provide guidelines and best practices for cybersecurity. For instance, in 2019, the European Union (EU) Cybersecurity Act was adopted to reinforce ENISA and also establish an EU-wide cybersecurity certification scheme that aims to promote trust and confidence in digital products and services [6].

There exist also a number of regulations that companies around the world must comply with. One example is the General Data Protection Regulation (GDPR) [7]. It provides a set of compliance criteria for companies to follow in order to protect the personal data of individuals within the EU and imposes fines for violations of certain requirements. Apart from regulations, standardization institutes have also developed recognized approaches. For instance, the National Institute of Standards and Technology (NIST) has introduced a framework that helps guide cybersecurity activities as part of the organization's risk management process [8].

The so-called ISO 27k standard, which is actually a collection of information security management standards created by the International Organization for Standardization (ISO), is another noteworthy standard. For example, the ISO 27001 is a well-known and auditable standard outlining the requirements for establishing, implementing, and maintaining information security management systems (ISMS). It allows for a well-known certification throughout the industry, but is more commonly pursued by organizationally mature organizations due to its complexity, cost, and certification process [9].

Over the past few years, ENISA has also made significant efforts to contribute to a stronger cybersecurity ecosystem. These endeavours have led to valuable outcomes for various sectors, including the development of new risk management frameworks [10] and national cybersecurity strategies [11].

Nevertheless, even with several frameworks, guidelines, and information available, it is still a complex task for SMEs to understand requirements and achieve an adequate level of protection while ensuring basic compliance with certain standards [5, 12]. The resources available are often either too abstract or geared towards larger organizations. This can leave SMEs feeling overwhelmed and unsure of where to start. Moreover, the resources often lack practical guidelines and step-by-step instructions, which adds to the difficulty of implementing effective security measures [4].

To address these issues, it is crucial to propose suitable, user-friendly and easy-to-follow solutions that are specifically tailored to the needs of SMEs, so that SMEs are able to understand their cybersecurity risks and know about the ways to protect themselves and their stakeholders. Additionally, automating critical information gathering for the planning process can further simplify the implementation of cybersecurity measures.

1.1 Description of Work

This Master Thesis defines a novel lightweight cybersecurity certification scheme in addition to extending the CyberTEA methodology [5] to offer an user-friendly and straightforward way of assessing and improving the cybersecurity posture of SMEs. The proposed methodology serves as an entry point for SMEs into the complex world of cybersecurity. Also, a novel certification scheme is proposed to enable companies to implement efficient cybersecurity strategies and demonstrate the compliance with needs of different stakeholders, including technical, economic, and societal baselines.

A survey of existing guidelines, frameworks and certifications for cybersecurity was conducted, followed by a more comprehensive analysis of selected frameworks and certifications, including the CyberTEA methodology [5, 13]. This analysis helps to identify the key elements necessary for compliance. Using the results of these analyses, the initial CyberTEA methodology is first extended to include new and relevant phases for compliance and certification. Thus, the CERTSec is proposed as an approach for cybersecurity planning, compliance, and investment prioritization. This approach is based on established methodologies, frameworks and recent research findings, and it is tailored to the specific

needs of SMEs. A novel cybersecurity certification scheme was also proposed as a core part of the approach.

A fully operational system is designed and implemented to support companies to apply the CERTSec approach and assess their cybersecurity posture in an automated way. This helps to provide a proof of compliance when applying the proposed certification scheme. Furthermore, the developed system generates supplementary artifacts (*e.g.,* insightful technical and management reports based on collected and analysed information) that provide valuable and actionable insights for informed decision-making and identification of gaps and issues, which serve as middleware for other well-known certifications (*e.g.,* ISO 27001 and CyberEssentials) and tools.

Key elements of the developed prototype are the collection of business-relevant information and the automation of processes involved in the certification scheme. In this sense, the prototype is able to *(i)* determine whether Websites establish secure connections, *(ii)* perform network reachability analysis, and *(iii)* conduct thorough vulnerability analyses on networks, technologies and software provided.

To determine the feasibility of key features used for the automation of the certification scheme processes, different evaluations were performed. This includes a comparative analysis with a real-world tool, scalability and overall performance analyses, as well as a practical case study demonstrating the potential application and its usefulness in real-world scenarios.

1.2 Thesis Outline

The rest of this thesis is organized as follows. **Chapter 2** provides the reader with a theoretical foundation required to understand the subsequent chapters. It introduces key dimensions of cybersecurity, cybersecurity planning and certification, and cybersecurity cost management. Subsequently, the analyzed related work is highlighted in **Chapter 3**. Various cybersecurity guidelines, frameworks, and certifications from standardization institutes, certification bodies, and the research community are examined and compared. Among these, three resources are selected for a more in-depth analysis.

Chapter 4 introduces the main contributions of this Master Thesis. First, key pillars of cybersecurity are mapped and the resulting methodology is described. Afterwards, the proposed cybersecurity certification scheme is thoroughly explained and the developed prototype is also presented. **Chapter 5** presents the evaluation of the developed prototype, detailing the conducted experiments, discussing the results, and addressing limitations observed. Finally, **Chapter 6** concludes this Master Thesis by providing a summary of the work accomplished and highlighting key findings. Also, a discussion on future work is provided as part of the conclusions.

Chapter 2

Background

Due to the complexity and multi-faceted nature of cybersecurity, it is almost impossible to achieve utmost protection against cyber threats. Therefore, informed and carefully thought-through decisions must be made about how and where to invest money. This chapter therefore begins by exploring the different dimensions of cybersecurity. Then, an introduction to cybersecurity planning and certification, which are essential elements of a robust cybersecurity program, is provided. Finally, this chapter examines the importance of cybersecurity cost management and the challenges of balancing cybersecurity investments with budget constraints.

2.1 Dimensions of Cybersecurity

Cybersecurity is a complex and multi-faceted field that ecompassess several dimensions, as illustrated in Figure 2.1. Although the technical aspect of cybersecurity might appear predominant, it is imperative to recognize that each of the presented dimensions contributes significantly to safeguarding individuals, companies, and the broader society from cyber threats. To convey a more encompassing perspective, the upcoming subsections will delve into the technical, economic, and societal dimensions of cybersecurity. Notwithstanding the importance of the legal aspect, due to a lack of legal expertise, it is not possible to exhaustively cover this topic within the scope of this Master Thesis. For this reason, the legal dimension is not discussed in this work.

2.1.1 Technical Dimension

As the name implies, the technical dimension of cybersecurity deals with the technological aspects of protecting information and systems. According to NIST, cybersecurity is defined as a process that involves preventing, detecting, and responding to cyber attacks in order to safeguard information [14]. NIST further introduces security pillars that are also known as the CIA triad, which encompasses three key objectives of cybersecurity [15]:

- **Confidentiality:** This objective aims to ensure that private or confidential information is not made available or disclosed to unauthorized individuals.
- **Integrity:** The integrity objective consists of two components. Data integrity ensures that information and programs are only modified in a specified and authorized manner, both when stored (*i.e.,* at rest) and when transmitted in packets (*i.e.,* in transit). System integrity, on the other hand, ensures that a system operates as intended and is not intentionally or accidentally manipulated.
- **Availability:** This objective aims to ensure that authorized users have prompt access to the systems, services and information they need, without any denial of service.

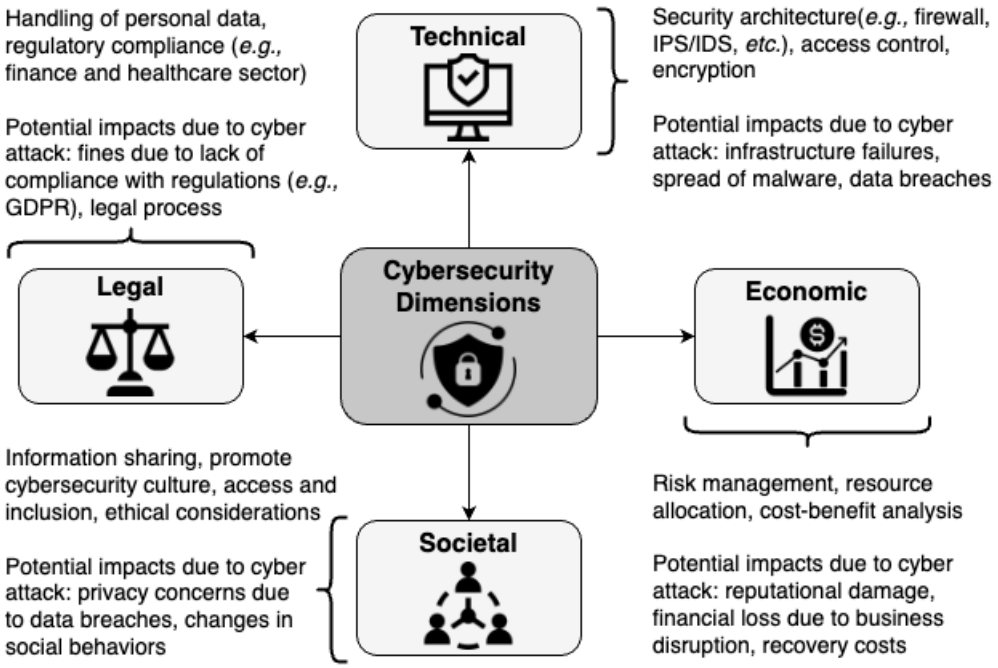


Figure 2.1: Overview of Cybersecurity Dimensions Based on [5]

To achieve these objectives, and therefore protect information and systems from a variety of threats such as unauthorized access, business disruption or data breaches, companies can employ a complex array of methods, tools, technologies and practices. For example, organizations can use penetration testing [16] as a tool to uncover vulnerabilities and establish security policies [17] (*e.g.,* enforce strong passwords or classify data based on sensitivity) to orchestrate their cybersecurity approach.

Other defensive tools such as firewalls [18] can be deployed to monitor and regulate network traffic, anti-virus software [19] can detect and remove malware, and intrusion detection systems (IDS) [20] can indicate potential security breaches by detecting network patterns that match known malware signatures (*i.e.,* signature-based IDS) or by pinpointing unusual activity that deviates from the typical baseline (*i.e.,* anomaly-based IDS).

Moreover, the technical dimension also includes the adoption of practices such as cybersecurity awareness training for employees or regular application of security patches [21], in

addition to deploying cutting-edge technologies like encryption algorithms to ensure data security or multi-factor authentication to reinforce access control mechanisms.

Although there exist a variety of measures that can help protecting businesses and their assets, it is important to emphasize that it is almost not possible to achieve utmost protection against all cyber attacks. The relentless digitalization, continuous technological advancements, and the varied motivations of adversaries (e.g., financial gains, hacktivism or nation-state actors) lead to the emergence of new vulnerabilities and attack surfaces, thus offering new opportunities for exploitation of unexpected loopholes and weaknesses.

Bearing this in mind, the technical dimension ought to be regarded as the foundational step, given that technical safeguards must be in place in order to be able to protect businesses from cyber threats. However, due to the complex, dynamic and multi-faceted nature of cybersecurity, it is necessary to move away from the naïve view of only focusing on the technical aspects and also considering other dimensions such as the economic (*cf.* Section 2.1.2) and societal (*cf.* Section 2.1.3) dimensions, especially since technical failure to avoid or mitigate attacks is also the precursor to economic and societal consequences that are often even much more severe.

2.1.2 Economic Dimension

While the technical dimension deals with ensuring the confidentiality, integrity and availability of data and systems, the economic dimension focuses on financial and business-related aspects of cybersecurity. This includes the costs associated with the protection of a company's assets and infrastructure. Businesses are required to allocate resources towards implementing and maintaining security controls, hiring skilled professionals, educating current personnel about strong cybersecurity hygiene and prevalent cyber threats, and conducting regularly routine security audits and risk assessments.

However, given that budgets are often limited, companies must assess the costs and benefits of various investment options to ascertain the most economical and efficient approach for mitigating cyber threats. Nevertheless, the economic dimension of cybersecurity is also intricate and dynamic, with the cost-effectiveness of different cybersecurity measures and investments varying considerably across companies, industries, and threat landscapes [5]. Thus, determining the most effective and efficient approach to mitigating cyber threats is therefore a non-trivial task, as it requires careful analysis and consideration of the costs and benefits of the various alternatives (*cf.* Section 2.3).

Moreover, apart from the costs arising from *e.g.,* implementing preventive measures, the economic dimension also encompasses the financial impact that cyber threats can have on companies. This includes the cost associated with actual data breaches and other security incidents, where a distinction is made between direct and indirect costs [5].

Direct costs pertain to the immediate expenses that companies incur as a consequence of a cyber attack, which includes but isn't limited to data theft, recovery costs, legal fees, or even ransom payments. Indirect costs, conversely, represent the potential losses a company sustains following a security breach. These encompass, for example, decreased

productivity, decline in future revenues, or damage to reputation. Given that these types of costs are more challenging to quantify, they could exert a more significant impact on the business in the long run than direct costs [22].

2.1.3 Societal Dimension

With the rapid proliferation of new technologies and increasing digitalization in businesses, there has been a major focus on the technical facets of cybersecurity. However, this intense emphasis on the technical aspects can sometimes eclipse the wider impacts cybersecurity can have on individuals, communities, and society as a whole. As people become increasingly reliant on technology in their daily lives (*e.g.,* social media, online shopping, cashless payments), robust cybersecurity is becoming increasingly important as it plays a vital role in protecting individuals' sensitive information and their inherent privacy, which is a fundamental human right [23].

The inability to implement effective cybersecurity measures may lead to security breaches that may result in the unauthorised acquisition of personal and sensitive information, such as financial information or medical records. This could subsequently erode customers' trust in a company, potentially causing them to cut ties with the impacted company or brand [24].

Moreover, cyber attacks compromising critical infrastructures can have a direct and severe impact on society as well. A prominent example is the WannaCry ransomware attack that took down the National Health System of the United Kingdom in 2017 [25]. By exploiting a vulnerability in outdated Windows operating systems this attack caused significant disruptions to patient care and services. As a result, many hospitals were forced to cancel appointments and procedures, or even turn away or redirect patients to other facilities.

This showcases that such cyber attacks can have serious impacts on the safety of individuals and can therefore also easily cause psychological distress such as anxiety among the population, especially considering that most of the damage could have been prevented if people were more aware of such cyber threats and the necessary software patches had been implemented [24].

Besides, there is also an increasing sophistication and frequency in social engineering and phishing techniques [26]. Adversaries try to exploit the lack of awareness and human vulnerabilities to gain sensitive information or install malicious software, for instance. As a result, these threats can have implications on the social behavior, with humans becoming more cautious and skeptical, even during legitimate interactions [5]. The fear of becoming victim of phishing attacks has thus become a widespread concern, adding to the psychological effects mentioned before. To date, the most effective countermeasure remains human education and awareness training. Therefore, as phishing and social engineering attacks continue to evolve it is all the more important to continuously educate and train the population to protect them against these threats [24, 27].

2.2 Cybersecurity Planning and Certification

Nowadays, we live in a digital age, where almost every aspect of our lives and businesses depends on technology. While this brings remarkable benefits, it also introduces a myriad of risks. Cyber threats are constantly evolving and make it therefore an ongoing challenge to protect sensitive data and maintain business operations.

With this in mind, implementing a well-designed cybersecurity plan is critical, since it serves as a shield against these risks and protects critical personal and business information. When developing a cybersecurity plan, it is invaluable to use cybersecurity frameworks as they provide a structured way to manage such risks. Chapter 3 therefore provides a detailed overview of various frameworks, guidelines, and certifications such as the NIST CSF [28] and ISO 27001 [9] that guide the development of effective cybersecurity strategies.

Moreover, it is worth noting that understanding the unique risk landscape the business operates in is a crucial aspect of developing such effective cybersecurity plans. In this context, risk management, and especially risk assessment, is of great importance. Risk management essentialy involves to continuously analyze and understand potential threats and deciding on the most appropriate mitigation strategy.

Figure 2.2 outlines the general steps of risk management. The first step is to establish the context, which sets the stage for the entire risk management process. More specifically, it defines the scope and criteria that will guide the assessment of risks. Subsequently, the risk assessment phase is started, which is comprised of several crucial steps including the identification, analysis and evaluation of risks. During this phase, companies should recognize potential threats, analyze their potential impacts and determine their risk tolerance levels [5]. The next step then involves treating the risks, which means deciding whether to mitigate, transfer, avoid, or accept the risks based on the outcomes such as risk type, nature and priority. Finally, continuous monitoring is necessary to ensure that the risk management strategies remain effective over time. This iterative process ensures that the company is well equipped to tackle and respond to any cybersecurity threats that may arise [5].

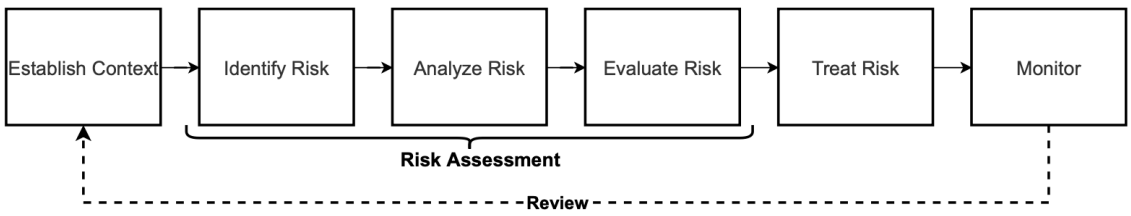


Figure 2.2: General Steps in Risk Management [5]

Another noteworthy topic are investments in cybersecurity. Cybersecurity is not just a cost center but rather a critical investment for businesses. In this sense, it is crucial that when allocating resources for cybersecurity, businesses should consider the financial

implications of potential security incidents. Section 2.3 provides more insights on this topic.

In addition to investment considerations, the concept of cybersecurity certification for businesses also demands attention. While certain industries have mandatory standards to comply with, such as the PCI Data Security Standard (PCI-DSS) [29] for businesses accepting credit card payments or the Health Insurance Portability and Accountability Act (HIPAA) [30] for healthcare organizations managing sensitive health information, certifications are encouraged across various sectors.

They serve as concrete evidence that a business is committed to cybersecurity and possesses the necessary skills and knowledge embodied by the respective certifications. Beyond enhancing professional credibility, certifications can also provide a competitive advantage in the market. For instance, the UK government expects applicant companies to hold at least the Cyber Essentials certification for certain job offers [31].

However, the significance of certifications goes beyond reputation and market advantages. They play a vital role in mitigating risks. In this sense, certifications also validate that a company has implemented robust security measures and adheres to industry best practices. By going through the certification process, organizations undergo thorough assessments, identifying and addressing vulnerabilities, thus bolstering their overall cybersecurity posture.

Nevertheless, it is important to note that not all issued certifications offer the same assurance, transparency and trust. The process of verifying adherence to specific standards, regulations or requirements is called conformity assessment (CA) [32]. Depending on the type of conformity assessment carried out, the resulting certification may vary in in terms of assurance (*i.e.,* confidence that can be placed in respective certifications), transparency (*i.e.,* clarity and opennes of process) and trust (*i.e.,* credibility and reliability) [33].

Bearing this in mind, the International Electrotechnical Commission (IEC) distinguishes between three types of conformity assessments for products [34]:

- **First-party CA:** The first-party CA essentially describes companies affirming that their products comply with a chosen standard. Since it is a self-declaration, it usually transmits a low level of trust.
- **Second-party CA:** For this CA, the assessment is conducted by external entities with whom a company has business with (*i.e.,* important stakeholders). This kind of CA yields a mid-level of trust.
- **Third-party CA:** This CA is the most reliable and widely recognized form of certification and is done by independent, external organizations such as ISO or IEC. It offers a high level of trustworthiness, which in the end depends on the reputation of the associated certification body.

Although these classifications are primarily intended for product assessments, they can be adapted and applied to the evaluation of companies as well.

2.3 Cybersecurity Cost Management

Implementing robust cybersecurity measures comes with associated costs. To optimize resources and make informed decisions, organizations need to engage in cybersecurity cost management. This practice involves evaluating the financial aspects of cybersecurity investments and determining the most cost-effective approaches to protect against cyber threats. There are a multiple approaches available, but this chapter will explore two of the most well-accepted models: the Gordon-Loeb Model and Return on Security Investments.

2.3.1 Gordon-Loeb (GL) Model

In the light of exploring how much should be invested in cybersecurity related activities, Gordon and Loeb introduced a mathematical economic model (*i.e.,* GL model) in 2002 that helps to determine the optimal level of investment in cybersecurity [35]. Since then, the model has become one of the most well accepted model in the field of cybersecurity economics and has also been widely referenced in academia [36, 37, 38, 39]. Specifically, the GL model comprises three key elements:

- **Potential Loss:** This element describes the financial impact of an information set that has been compromised by a cyber attack. In particular, the estimated value of the respective asset is considered as the potential loss L.
- **Vulnerability:** The vulnerability element v describes the likelihood of a successful cyber attack on a company, resulting in the compromise of the information set.
- **Security Breach Probability Function:** This function is defined as $S(z,v)$ and describes the productivity of additional cybersecurity investments on the likelyhood of a system being breached, or put in other terms, the reduction of the vulnerability v to a cyber attack after a cybersecurity investment z has been made.

Figure 2.3 represents the GL model by illustrating the relationship between security investments z and the corresponding expected loss vL, which is a product of vulnerability v and potential loss L, in case of a successful cyberattack. In particular, it shows that the Expected Benefits of Investment in Information Security (EBIS) is increasing in a decreasing rate, therefore yielding positive yet diminishing returns. In this sense, at some point, additional investments in cybersecurity are no longer worthwhile, as they cannot significantly improve the existing protection.

Consequently, the model assumes that it is not possible to achieve ultimate security by increasing the investments as there will always be some residual vulnerability that cannot be covered. The optimal investment z^*, on the other hand, can be calculated by maximizing the Expected Net Benefit of Investment in Information Security (ENBIS), *i.e.,* maximizing the difference between EBIS and the cost of the investment [40].

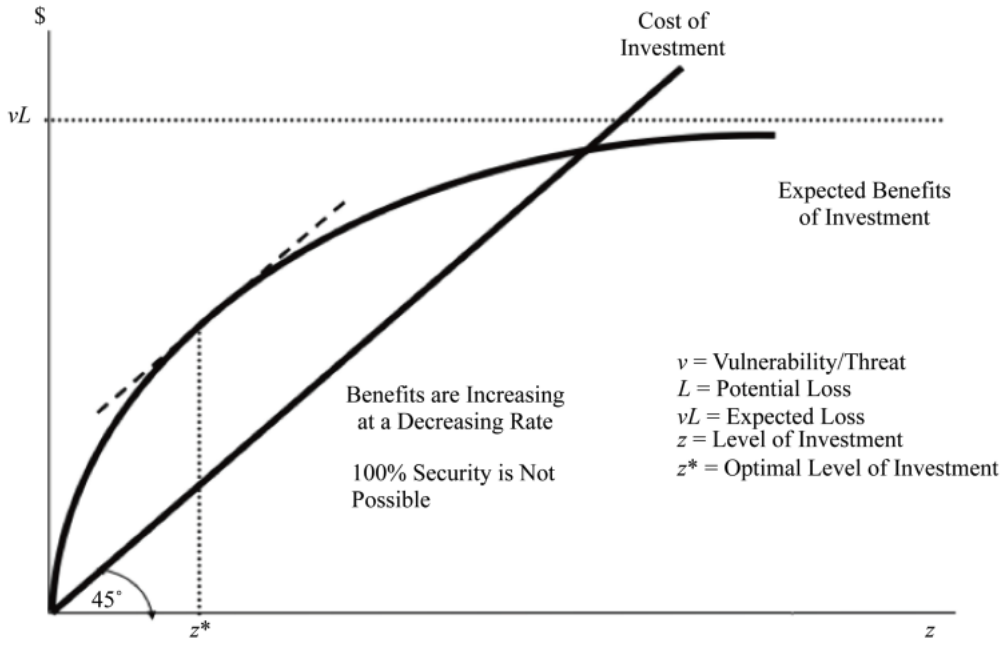


Figure 2.3: Level of Investments in Cybersecurity [40]

The above explanations can also be summarized in mathematical equations [35]. In this sense, EBIS, *i.e.,* the reduction of the expected loss due to the additional cyberesecurity investment, can be calculated as shown in Equation 2.1.

$$EBIS(z) = [v - S(z, v)]L \tag{2.1}$$

To determine the corresponding ENBIS value, the cost of the investment made must be subtracted. This is demonstrated in equation 2.2.

$$ENBIS(z) = EBIS - z \tag{2.2}$$

By applying further calculations, the GL model manages to show that companies should invest at most 37% of the expected loss that could arise from a cyber attack in cybersecurity. [35] expresses this finding mathematically, as shown in Equation 2.3.

$$z^*(v) < (1/e)vL \tag{2.3}$$

Another interesting finding of the GL model is that the optimal investment level in cybersecurity does not always increase proportionally to the level of vulnerability [40]. This, in turn, means that it may be more beneficial for a company to invest in cybersecurity measures for assets with a medium level of vulnerability rather than those with a high level of vulnerability. In this sense, protecting assets with very low or very high vulnerability may not be as cost-effective, given that the former may not face significant threats and

the latter might require unreasonably large investments in order to achieve meaningful vulnerability reduction.

Since its introduction in 2002, the GL model has been widely analysed and extended to include important concepts. [38], for instance, modified the model so that it also takes into account externalities, *i.e.,* the impacts that a cyber attack may have on other parties (*e.g.,* unknowing participation in a botnet attack, privacy effects on customers due to data leaks, or cascading effects of successful attacks on critical infrastructures). Moreover, in 2021, [37] expanded the GL model by incorporating the concept of information segmentation. This approach involves categorizing information, networks and databases into smaller and better manageable segments, allowing companies to implement more effective access controls that restrict access to authorized users only and also establish additional safeguards for more valuable segments. In this sense, [37] suggests using information segmentation to derive a more cost-effective and accurate overall cybersecurity investment strategy. The following four steps are therefore suggested to determine the optimal investment per segment:

- **Step 1:** Estimate the value and hence the potential loss L_i for each segment i.
- **Step 2:** Estimate the vulnerability v_i for each segment i to a successful cyber attack.
- **Step 3:** Estimate the productivity of investments (*i.e.,* the potential benefits in terms of exptected loss reduction) by calculating the security breach probability function $S_i(z_i, v_i)$.
- **Step 4:** Determine the optimal level of cybersecurity investment z_i^* by increasing investment as long as the benefit of the additional investment is greater than or equal to the cost of the additional investment. Since not all cybersecurity investments have the same productivity, the optimal amount will be different between investments in different segments.

2.3.2 Return On Security Investment (ROSI)

ROSI describes another concept in the field of cybersecurity economics that is used to evaluate the cost-effectiveness of cybersecurity measures [41]. It is similar to the well-known concept of Return on Investment (ROI), which helps calculate the profitability of an investment. However, since cybersecurity is not really an investment that yields a profit, the focus is rather on the loss prevention or risk reduction achieved by the implemented security measure. In addition to determining whether or not a solution is cost-effective, ROSI can also be used to compare different security measure and thereby determine the most appropriate one from an economic standpoint. A solution is considered to be cost-efficient if the ROSI index is greater than or equal to 1 (*i.e.,* ROSI ≥ 1), indicating that the investment is expected to generate more value than its cost (*i.e.,* positive payback). Equation 2.4 provides the general calculation formula [41].

$$ROSI = \frac{Risk_{Reduction} - Solution_{Cost}}{Solution_{Cost}}, where$$
$$Risk_{Reduction} = ALE \times Mitigation_{Ratio} \tag{2.4}$$

To calculate the ROSI index the equation considers the cost of the selected solution, its efficiency (*i.e.,* $Mitigation_{Ratio}$) as well as the Annual Loss Expectancy (ALE). The ALE describes the annual monetary loss that can be expected from a specific risk on a specific asset and can be calculated as shown in Equation 2.5 [41].

$$ALE = ARO \times SLE \tag{2.5}$$

In this sense, in order to estimate ALE, we need to determine the Annual Rate of Occurrence (ARO) of cybersecurity attacks (*i.e.,* the probability that an attack will occur in a year) in addition to the Single Loss Expectancy (SLE), which includes the total cost (*i.e.,* direct and indirect costs) of a single successful cyber attack.

Chapter 3

Related Work

This chapter provides an overview of various cybersecurity guidelines, frameworks, and certifications (*i.e.,* approaches) that assist organizations in developing sound cybersecurity strategies and assessing their cybersecurity posture. With this in mind, the first section examines a broad range of recent efforts that include contributions from standardization institutes, certification bodies, and the academic research community. Following this review, three key resources are then selected for more in-depth analysis, focusing on their practical applications and impact on the cybersecurity field.

3.1 Approaches

In the context of cybersecurity, NIST is known for its collaborative efforts involving industry, government and academia, which have led to the development of various frameworks, guidelines, and standards that are nowadays widely recognized and used in the industry. One great example is the well-known NIST Cybersecurity Framework (NIST CSF) [28] that helps guide cybersecurity activities as part of the organization's overall risk management process.

The NIST CSF [28] consists of three main components. The first component (*i.e.,* Framework Core) represents a set of cybersecurity activities and references that help achieve better cybersecurity outcomes. It is organized around five key functions, namely *Identify*, *Protect*, *Detect*, *Respond*, and *Recover*, which address the basic ideas behind a successful cybersecurity strategy and therefore cover aspects ranging from identification of potential cybersecurity risks to cybersecurity incident response and recovery processes.

The second component (*i.e.,* Framework Implementation Tiers) helps to determine how a company manages its cybersecurity risks and the degree to which cybersecurity risk management is incorporated into the overall risk management practices (ranging from *Partial* to *Adaptive*). The final component (*i.e.,* Framework Profile) helps then to create a roadmap for improving an organization's cybersecurity posture from the *as-is* state to the targeted *to-be* state, thus aligning and prioritizing cybersecurity outcomes based on company-specific goals.

Besides, NIST has also published various documents called Special Publications (SPs), with the 800 series focusing on cybersecurity. For example, the NIST SP 800-53 [42] is a document that provides a comprehensive set of security and privacy controls that help manage cybersecurity risks and thus safeguard information as well as systems from cyber threats. NIST SP 800-30 [43], on the other hand, is a document that provides detailed and systematic guidance for conducting cybersecurity risk assessments for information systems. However, due to its complexity, it is one of the most difficult concepts to execute.

Another well-known standard is the so-called ISO 27001 [9], which is an essential part of the comprehensive ISO 27k series. This standard outlines the requirements for the establishment, implementation and continuous maintainance of Information Security Management Systems (ISMSs) and, with a strong emphasis on risk management, aims to protect the confidentiality, integrity and availability within these systems. In addition, this standard is also auditable and therefore offers assurance in form of a well-known certification. However, because of its complexity, associated costs and strict certification process, this certification is typically pursued by larger and more mature organizations.

Apart from ISO 27001, the ISO 27002 [44] standard is also of great importance. It serves as a complementary advisory document to ISO 27001 and provides a set of best practices and comprehensive implementation guidelines. As such, ISO 27002 provides invaluable information that aids businesses in effectively implementing the cybersecurity controls outlined in the requirements of ISO 27001.

At the European level, ENISA ISMS [45] is proving to be a key component of information security. In this sense, the European Union Agency for Cybersecurity has developed a systematic approach to managing and protecting information based on a risk management process that includes policies, procedures, and various measures to protect and manage information in a very secure manner.

Moreover, in 2021, the European Telecommunications Standards Institute (ETSI) published another important document known as ETSI TR 103 787-1 [46]. This technical report addresses the key aspects of cybersecurity standardization for SMEs and provides a comparative analysis of five well-known cybersecurity standards and frameworks (*e.g.,* [44][47][48]). One of the report's key findings is the presentation of 17 unified cybersecurity controls that provide SMEs with a useful reference for their cybersecurity efforts.

Shifting focus towards more light-weight cybersecurity certifications compared to the ISO 27001, the CyberRisk Rating [33] is the first to get underway. Developed collaboratively by the Austrian Security Board, Kompetenzzentrum Sicheres Österreich (KSÖ), and Austria's largest rating agency KSV1870, the CyberRisk Rating represents a cybersecurity certification scheme that is designed to assess the cybersecurity posture of organizations. More specifically, the scheme outlines a set of 25 requirements to be met by applicants as part of a self-assessment, which is then professionally validated by experts. The streamlined process is efficient and only needs to be conducted annually.

Another particularly light-weight cybersecurity certification is the United Kingdom's Cyber Essentials [48]. This certification is designed to ensure that organizations have implemented essential security controls to protect themselves against the most common cyber

threats. Specifically, it focuses on the fundamental aspects of cybersecurity, including firewalls, secure configurations, malware protection and patch management. As such, Cyber Essentials is particularly valued by SMEs for its simplicity and cost-effectiveness, which allows them to demonstrate their commitment to cybersecurity without engaging in the more expensive and burdensome certification process of ISO 27001.

The European Watch on Cybersecurity and Privacy offers another cost-effective solution known as the Cybersecurity Label, which is designed to assist SMEs in evaluating and demonstrating their cybersecurity readiness [49]. This initiative provides an online questionnaire tool that enables SMEs to assess themselves across eight domains, encompassing requirements for software, hardware, and services. With this in mind, the tool identifies areas for improvement based on scoring, and upon meeting all requirements, SMEs are then awarded the Cybersecurity Label with which they can demonstrate their cybersecurity posture.

In addressing the complex and multi-faceted nature of cybersecurity, it is crucial to consider aspects beyond technical perspectives, especially when formulating and implementing cybersecurity strategies. In this sense, Franco [5][13] introduces an innovative approach called Cybersecurity Technical and Economic Approach (CyberTEA), which focuses on the cybersecurity planning and investments of SMEs, aiming to assist them in achieving an optimal level of protection without excessive investments. Specifically, CyberTEA provides a methodology that identifies key elements and provides guidance for SMEs in the critical early stages of cybersecurity planning. Moreover, it also provides a framework that outlines the components that solutions must implement, as well as a set of novel solutions that perform specific steps within the proposed methodology.

Finally, in their 2020 paper, the authors present a Cybersecurity Maturity Assessment Framework (CMAF) that is compliant with the NIS Directive [50]. This framework assesses and improves the cybersecurity maturity of organizations by considering key areas such as risk management, access control, and technical measures. More specifically, the framework consists of 20 security requirements and 6 maturity levels and can serve as both a self-assessment and external audit tool. In this sense, it provides a structured approach for organizations to assess their cybersecurity capabilities, benchmark themselves against industry best practices, and improve their cybersecurity resilience in line with the NIS Directive.

Table 3.1 provides an overview and comparison of the different approaches discussed within this section. These approaches are categorized by type (*i.e., Guidelines*, *Framework*, or *Certification*) and the associated costs of documents and certifications. Moreover, they are also classified by their level of complexity (*i.e., Low*, *Moderate*, or *High*). In this sense, an approach designated as *Low* complexity typically indicates that it covers fundamental concepts or generally provides clear guidance and tools for the execution of their concepts, as in the case of CyberTEA. Conversely, a *High* complexity classification means that the approach is rather comprehensive and difficult to execute, such as NIST SP 800-30. Finally, the table also provides a concise summary of each approach and the involved stakeholders.

Table 3.1: Description and Overview of Guidelines, Frameworks and Certifications

Work	Type	Characteristics	Complexity	Costs	Stakeholders
NIST CSF	Guidelines / Framework	A guide that provides a structured approach to manage cybersecurity activities in business while considering cyber risks as part of the organization's risk management process	Moderate	Free	Government and Companies
NIST SP 800-53	Guidelines	A comprehensive set of security and privacy controls to safeguard the confidentiality, integrity, and availability of systems and its information	High	Free	Professionals
NIST SP 800-30	Guidelines	A guide for conducting risk assessments that provides organizations with a structured and flexible approach to identifying, assessing, and prioritizing information security risks	High	Free	Professionals
ISO 27001	Guidelines and Certification	Outlines requirements for implementing information security management systems (ISMS) to safeguard sensitive information and processes within organizations	High	$5400 - $20'000+	Companies
ISO 27002	Guidelines	Provides guidelines and general principles for implementing the requirements defined for an ISMS in ISO 27001	Moderate	$200	Companies, Auditors, and Professionals
ENISA ISMS	Guidelines / Framework	A guide to help organizations establish and maintain an effective ISMS	High	Free	EU Member States, Companies
ETSI TR 103 787-1	Guidelines	A where-to-start guideline for cybersecurity concepts, processes, standards, and frameworks for SMEs	Moderate	Free	SMEs

Work	Type	Characteristics	Complexity	Costs	Stakeholders
CyberRisk Rating & Cyber Trust Label	Certification	Provides independent evaluation of an organization's cybersecurity posture based on a set of predefined criteria and assigns a corresponding cyber risk rating	Low	Free	Large Companies and Critical Infrastructures
Cyber Essentials	Certification	A UK government-backed certification scheme that outlines a set of basic security controls and cybersecurity best practices to help organizations protect against common cyber threats	Low	£300-£500 + VAT	Companies
Cybersecurity Label	Certification	A low-cost and user-friendly self-assessment tool to evaluate and improve an organization's cybersecurity posture	Low	150€	Companies
CyberTEA	Guideline/ Framework	A guide for cost-efficient cybersecurity planning and investments that helps companies with technical and economic constraints achieve a suitable level of protection	Low	Free	SMEs
CMAF	Framework	A novel cybersecurity maturity assessment model that is compliant with NIS Directive	High	Free	Academics, Companies, Regulators, Auditors, and Professionals

Table 3.2 delves into a more detailed analysis and comparison of the different approaches, focusing on both technical characteristics and risk-related aspects. In this sense, the approaches are first classified whether they help organizations prioritizing risks. Additionally, the table also provides information on the type of risk management strategies adhered to in these approaches. In this case, *None* implies that the approach does not adopt any risk management strategy, a trait which is commonly seen in certifications. When labeled as *Flexible*, it indicates that the user can select a risk management strategy on their own. *Prescriptive*, on the other hand, implies that there exist a well-defined set of instructions that are mandatory to be followed, such as in the case of NIST SP 800-30.

Moreover, the *Integration Support* column indicates whether an approach is designed to be interoperable with other ones. For instance, NIST SPs are known to be designed so that they can be used in conjunction with multiple of those documents. Finally, the table also assesses the maturity of the approaches by gauging their acceptance within the industry and the cybersecurity community. The *Well-established* tag is used for approaches that are already established and therefore have a solid presence, such as NIST CSF and ISO 27001. Approaches that are rather new and have yet to gain acceptance (compared to *Well-established* approaches) are labelled as *Early-stage*. *Research & Prototypes*, on the other hand, is then used for innovative solutions that are predominantly from academia.

Table 3.2: Technical and Risk Feature Analysis of Guidelines, Frameworks and Certifications

Work	**Risk Prioritization**	**Risk Management Approach**	**Integration Support**	**Maturity**
NIST CSF	Yes	Flexible	Yes	Well-established
NIST SP 800-53	No	None	Yes	Well-established
NIST SP 800-30	Yes	Prescriptive	Yes	Well-established
ISO 27001	Yes	Flexible	Yes	Well-established
ISO 27002	No	None	Yes	Well-established
ENISA ISMS	Yes	Flexible	Yes	Well-established
ETSI TR 103 787-1	Yes	Flexible	Yes	Early-stage
CyberRisk Rating & Cyber Trust Label	No	None	No	Early-stage

Work	Risk Prioritization	Risk Management Approach	Integration Support	Maturity
Cyber Essentials	No	None	No	Early-stage
Cybersecurity Label	No	None	No	Research and Prototype
CyberTEA	Yes	Flexible	Yes	Research and Prototype
CMAF	Yes	Prescriptive	Yes	Research and Prototype

3.2 Analysis of Selected Approaches

The surveys conducted in the previous section yielded a plethora of insights regarding various approaches that are relevant for strengthening an organization's cybersecurity efforts and in the assessment of its cybersecurity posture. For a more comprehensive analysis, three approaches have been carefully selected based on their respective stages of maturity.

Thus, this subsection further examines one approach from each category: NIST CSF representing the *Well-established* category, Cyber Essentials as an example of the *Early-stage*, and CyberTEA embodying the *Research & Prototype* category. The goal of this research is to provide possible applications of these approaches in industry and academia.

A first example comes from the Government of Bermuda, which successfully applied the NIST CSF to address challenges in managing cybersecurity risks in a consistent manner across all departments [51]. The process included a self-assessment using the NIST CSF to identify gaps and weaknesses, which then led to the development of prioritized action plans. The implementation of the NIST CSF then resulted in a consistent, standardized approach to business security across all departments, making complex cybersecurity risks more manageable. With this in mind, the government was able to develop policies and processes for the risk management program, link them closely to records management and privacy policies, and conduct regular training for employees and information security professionals.

Saudi Aramco, one of the world's largest and most valuable companies, serves as another notable example of successfully implementing the NIST CSF to enhance its cybersecurity posture [52]. The adoption of the framework has fostered improved communication about

cybersecurity throughout the organization, enabling effective collaboration between IT and operational technology leaders. This, in turn, resulted in addressing gaps identified during the assessment phase.

Moreover, aligning with the NIST framework has also prepared Saudi Aramco for compliance with national and international regulations, incorporating various best practices and frameworks into their cybersecurity processes. To facilitate knowledge dissemination and utilization, the framework has also been translated into Arabic, so that companies in Arab countries can access cybersecurity insights and use the framework to improve their own cybersecurity capabilities.

However, the NIST CSF has not only gained significant attention and application in industry, but also in academia. For instance, [53] presents a high-level comparison of NIST CSF with the well-known ISO 27001 standard. In this analysis, the author focused on the overall structure, essential components, and implementation strategies (risk-based vs systematic approach) of these two frameworks. The paper underscores the shared emphasis of both resources on asset management and risk management amongst other aspects. However, it also highlights the differences, including NIST CSF's specific focus on cybersecurity and its detailed categorization, in contrast to ISO 27001's broader scope and formal certification process. Therefore, by providing these useful insights, the paper serves as a valuable resource for practitioners and decision-makers in choosing the most suitable cybersecurity framework for their organizations, offering a solid foundation for improving cybersecurity posture and effectively managing associated risks.

Another notable example is [54], which presents a novel tool called Cyber Threat Dictionary (CTD) that leverages the MITRE ATT&CK Matrix [55] and maps it to the NIST CSF. The MITRE ATT&CK Matrix is a widely adopted framework that catalogs various tactics, techniques, and procedures used by adversaries. This study focuses on mapping the identified cyber threats from the MITRE ATT&CK matrix to the core components of the NIST CSF. By establishing this mapping, the authors effectively bridge the gap between the technical details of cyber threats and the strategic guidelines of the cybersecurity framework. This CTD can therefore serve as a valuable resource for cybersecurity practitioners, facilitating both reactive and proactive approaches. For instance, it enables them to take appropriate actions upon detecting attacks and helps identify potential vulnerabilities to implement suitable security controls before exploitation occurs.

As a UK government-backed certification scheme, Cyber Essentials provides a set of basic security controls and cybersecurity best practices to help organizations safeguard against prevalent cyber threats [48][31]. More specifically, there are two types of certifications offered. The first one is *Cyber Essentials* and describes a first-party conformity assessment where businesses can complete an online questionnaire on their own. *Cyber Essentials Plus* builds on the previous certification type and requires an external technical expert to conduct an audit of the company's IT systems. As a consequence, *Cyber Essentials Plus* provides higher assurance regarding compliance with the certification scheme.

Such Cyber Essentials certification demonstrates to stakeholders the commitment to cybersecurity and is also required for some government contracts in the UK. The IASME Consortium serves as the official partner for Cyber Essentials, offering certification [56] and an automated tool that generates an action plan based on a business' responses [57].

This tool provides guidance to meet specific requirements and thus help achieve the certification. Additionally, the IASME Consortium also allows for searching and verifying whether companies have obtained either of the two certifications within the past year [58].

In 2015, [59] conducted a qualitative evaluation of the effectiveness of the Cyber Essentials scheme on four different SME networks. The results demonstrate that in the absence of Cyber Essentials controls, none of the evaluated attacks were successfully addressed on any network. This emphasizes the necessity for SMEs to take proactive measures against cyber threats, as neglecting security is not a viable option. Conversely, when employing the Cyber Essentials tools, more than 99% of vulnerabilities within SME networks were effectively mitigated. However, a smaller portion (around 30%) of vulnerabilities that were only partially mitigated relied on timely patches from hardware or software vendors. The study also analyzed high-profile vulnerabilities like ShellShock [60] and Heartbleed [61] and demonstrated the varying effectiveness of the Cyber Essential controls in mitigating these threats.

Being only published in 2023, CyberTEA [5][13] presents a rather recent scientific work that introduces a methodology and framework aimed at simplifying cybersecurity planning and investments for SMEs. This research not only offers innovative solutions but also validates its effectiveness in practice. As part of this work, [62] presents a novel visual system called SecGrid that enables the analysis and machine learning-based classification of cyber attack traffic. Traditional approaches to cybersecurity often rely on complex log files and textual data, making it challenging for analysts to efficiently detect and understand cyber threats. The SecGrid system addresses this challenge by incorporating interactive visualizations that provide an intuitive representation of network traffic data, aiding analysts in identifying patterns and anomalies associated with cyber attacks.

Furthermore, SecGrid also integrates machine learning algorithms to automate the classification of attack traffic, thereby improving the efficiency and accuracy of threat detection. The paper emphasizes the usability and effectiveness of SecGrid through experiments and evaluations, demonstrating its potential to enhance cybersecurity operations.

Moreover, [63] introduces SecBot, an innovative conversational agent designed to support cybersecurity planning and management in organizations. SecBot is a business-driven solution that uses machine learning and natural language processing to provide users with a user-friendly and intuitive interface for communicating technical knowledge about cybersecurity. In this sense, the conversational agent enables users, especially non-technical personnel, to engage in intuitive and productive conversations regarding cybersecurity issues, allowing them to make informed decisions and take appropriate actions.

Through case studies and evaluations, the study also highlights SecBot's applicability and efficacy, demonstrating how it may simplify cybersecurity operations, improve risk management, and boost organisational resilience in general.

[64] presents another unique and innovative solution for cybersecurity planning. In particular, SECAdvisor assists digitized businesses in achieving effective protection while minimizing unnecessary security investments. By using economic models such as GL and ROSI (*cf.* Section 2.3), the tool optimizes cybersecurity spending, provides quantitative risk estimations (*e.g.,* ROSI), and aids decision-making. It also features a user-friendly

interface that makes it accessible to non-technical personnel. Case studies and evaluations demonstrate SECAdvisor's effectiveness in improving cybersecurity operations, risk management, and organizational resilience, thus bridging the gap between technical security measures and their respective economic impacts.

Finally, [65] introduces another valuable support tool for cybersecurity management called MENTOR. MENTOR is a protection service recommender system that aims to recommend services for preventing and mitigating cyber attacks by correlating customer information with available service options. To do so, MENTOR considers different factors like budget constraints, service requirements, or deployment time to suggest suitable protection services. The paper also evaluates the performance and accuracy of the different similarity measure techniques used and concludes that the proposed solution is able to recommend adequate protections based on user requirements, thus offering a practical solution that aids the decision-making process.

This chapter has provided an extensive overview over a broad range of guidelines, frameworks and certifications, all of which have been designed to help organizations assess and improve their cybersecurity. However, despite the widespread availability and accessibility of these approaches, SMEs continue to struggle with a number of challenges including understanding requirements and achieving an adequate level of cybersecurity protection that is able to safeguard against contemporary cyber threats.

This holds especially true when it comes to certifications. The globally recognized certification of ISO 27001, for instance, is known for its complicated and resource-intensive process. While this certification is widely used by larger and more established organizations, it is often viewed as a daunting undertaking by SMEs. They often find themselves constrained by limited time, resources and technical expertise, thus making the pursuit of such a demanding certification a major challenge.

On the other hand, more light-weight certifications such as Cyber Essentials offer a less stringent certification process and more practical and feasible requirements. However, such certifications, like most of the approaches examined in this literature review, focus predominantly on the technical aspects of cybersecurity, thereby unintentionally neglecting the multi-faceted nature of cybersecurity (*cf.* Section 2.1). This shortcoming, in turn, limits the ability of these approaches to provide more comprehensive and holistic protection.

Chapter 4

CERTSec

Chapter 3 provided a comprehensive overview over various approaches developed by public sector entities, the private sector, and researchers, all aimed at supporting organizations in assessing or improving their cybersecurity posture. However, it also became clear that these resources are often too abstract or geared towards larger and more mature organizations and, as a result, fail to meet the unique needs of SMEs. Moreover, many of these exisiting approaches tend to focus their attention only on the technical aspects of cybersecurity. This, in turn, leads to overlooking the multi-faceted nature of cybersecurity and therefore neglecting the other important pillars (*cf.* Section 2.1) of this highly complex field.

Given these shortcomings in the current landscape, this chapter therefore focuses on the lack of such cybersecurity certifications and guidelines specifically tailored to the needs of SMEs. With this in mind, an appropriate methodology is first proposed that not only provides SMEs with practical guidelines to strengthen their cybersecurity efforts, but also enables them to verify compliance with a set of baseline cybersecurity requirements. Subsequently, a novel cybersecurity certification scheme is introduced that takes into account key pillars of cybersecurity (*cf.* Section 2.1) and facilitates a more balanced and holistic approach to assessing a company's cybersecurity posture. Finally, a prototype is presented that demonstrates the feasibility of automating the processes involved in the certification scheme.

4.1 Mapping of Key Pillars

To comprehensively address key pillars of cybersecurity, more holistic and complete cybersecurity guidelines are needed. In this context, CyberTEA [5][13] serves as an excellent foundation, as it offers a structured step-by-step approach for cybersecurity planning and investment that is particularly tailored to the needs of SMEs.

More specifically, CyberTEA aims to help SMEs achieve an adequate level of protection by providing support for understanding and defining cybersecurity requirements, determining their budget and investment path to achieve a proper level of cybersecurity, and

selecting cost-efficient safeguards, all while at the same time meeting specific business needs. CyberTEA therefore explicitly addresses the technical and economic dimensions of cybersecurity, making it the ideal candidate for a foundational basis.

Nevertheless, the existing five-phase methodology of CyberTEA lacks dedicated phases that check for compliance and provide appropriate assurances in the form of certifications based on the results. Such phases are of great importance in assessing the cybersecurity posture in order to ensure that an integral baseline security level is achieved and to analyze potential gaps in cybersecurity strategies in terms of technical, economic and societal dimensions. For this reason, the Extended CyberTEA is proposed in order to fulfill all of the requirements of the novel cybersecurity certification scheme being proposed in Section 4.2. In this sense, the Extended CyberTEA adds two new phases (*i.e.,* Compliance and Certification) to the current five-phase methodology.

While the initial CyberTEA implicitly addresses societal aspects of cybersecurity, the Extended CyberTEA explicitly incorporates the societal dimension along with the technical and economic aspects. This expansion fosters a more comprehensive and holistic assessment of the cybersecurity posture and emphasizes the multi-faceted nature of cybersecurity.

Figure 4.1 presents the Extended CyberTEA, including all its phases from A to G. Moreover, this figure also provides a comparative mapping of the components of the NIST CSF [28] onto the Extended CyberTEA, which serves two purposes. First, the mapping confirms that the initial CyberTEA encompasses crucial steps that are also advocated by this well-established industry guide, but simply tailored to the needs of SMEs, thus demonstrating adherence to recognized best practices. Second, the mapping also highlights that key phases such as Cost Management, Compliance as well as Certification, which are essential components in defining a holistic cybersecurity strategy and assessing an organization's cybersecurity posture, are not explicitly covered by the NIST CSF. This

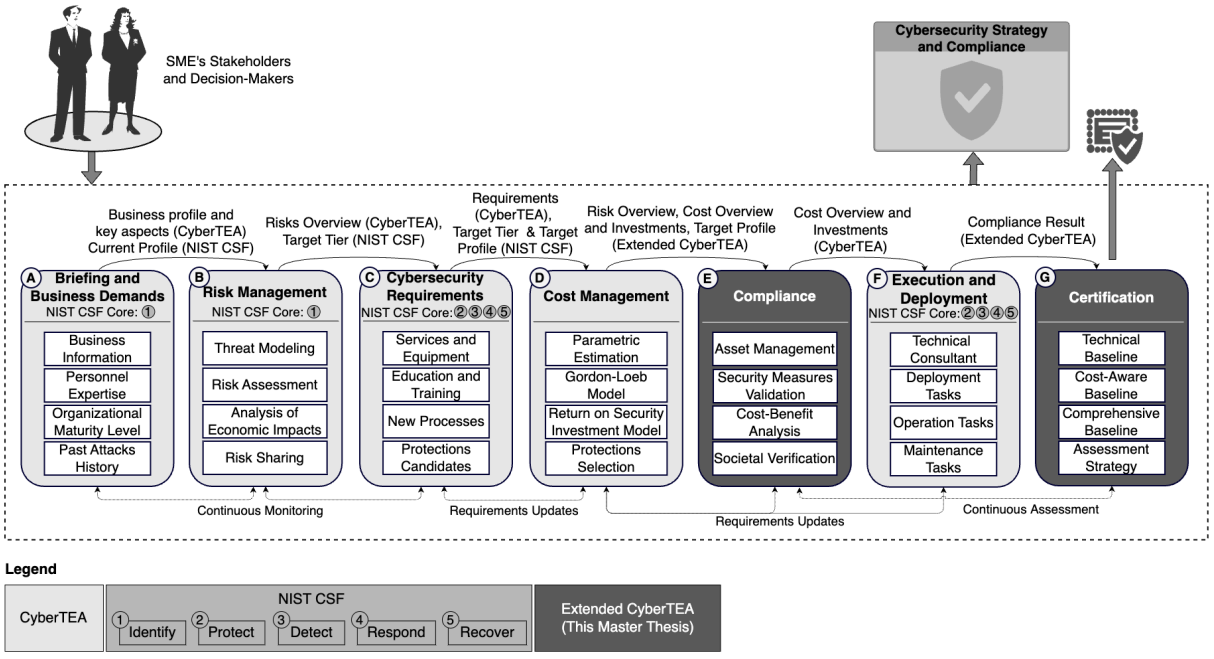


Figure 4.1: Extended CyberTEA and NIST CSF Components Mapping

observation therefore emphasizes the unique contributions of CyberTEA and its extended counterpart, as it addresses these gaps and provides a more comprehensive approach to cybersecurity, thus demonstrating its relevance, comprehensiveness, and innovative nature.

In the subsequent paragraphs, the various phases are briefly outlined, along with how they relate to the various NIST CSF components. As such, the methodology begins with the crucial **Phase A** (*i.e.,* Briefing and Business Demands), which lays the foundation for all the subsequent phases and tasks. The objective of this phase is to gather all relevant information about the business in order to be able to gain insights into the unique needs, objectives, and constraints in relation to cybersecurity and to then bring all stakeholders on the same page. Therefore, apart from key information such as the business sector, data processed and technologies in use, businesses also need to evaluate the cybersecurity skills of their employees, understand their company's maturity level and gather all information about previous cybersecurity incidents.

Upon completion of this phase, companies have created a business profile that includes all relevant aspects, which can be defined under NIST CSF terms as the **Current Profile**. Moreover, the **Identify** function of the NIST CSF focuses on developing an understanding of a company's business context, assets and capabilities, which aligns with the tasks of Phase A. Hence, the Identify function can be directly mapped to the Briefing and Business Demands phase.

Moreover, the Identify function also covers risk management related activities and can therefore also be mapped to **Phase B** (*i.e.,* Risk Management), whose emphasize is on understanding and managing a company's cybersecurity risk landscape. Conducting risk assessments and threat modeling, as well as analyzing the economic impact of potential attacks, are therefore tasks that must be considered. Additionally, businesses can also use this phase to preliminary determine a **Target Tier**, which describes a company's desired state for its cybersecurity risk management practices. However, the defined Target Tier needs to be refined in the subsequent phases (C and D), as advancing to a higher tier is only recommended if a cost-benefit analysis shows a feasible and cost-effective reduction in cybersecurity risks.

After gaining an understanding of the business profile and its associated risks, the methodology moves on with **Phase C** (*i.e.,* Cybersecurity Requirements). This phase focuses on identifying the necessary measures and practices that help mitigating the identified risks and achieve an adequate level of protection. The result of this phase is a list of cybersecurity requirements that has been carefully compiled to address the company's unique risk landscape. By focusing on identifying protective security measures and mechanisms for timely detection, quick response, and effective recovery from cyber attacks, this phase demonstrates alignment with several core functions of the NIST CSF, namely **Protect**, **Detect**, **Respond**, and **Recover**. Moreover, within the context of NIST CSF, this phase also produces a **Target Profile** that descibes the desired cybersecurity state of the company after all cybersecurity requirements are implemented.

The next phase on the line is **Phase D** (*i.e.,* Cost Management), the objective of which is to estimate and adjust the cost of implementing the cybersecurity strategy and allocate budget accordingly. For this purpose, CyberTEA explores the use of two of the most

recognized economic models (*i.e.,* GL model and ROSI) to determine the optimal level of investment and select cost-effective protection measures. The NIST CSF, on the other hand, does not explicitly address Cost Management, but emphasizes that cost-effectiveness can be achieved through its flexible nature, which allows it to adapt to an organization's unique needs and circumstances (*e.g.,* prioritize the implementation of controls that address the most important risks first). However, this explicit approach by CyberTEA adds a level of detail that is particularly useful and critical for SMEs, as they often need to make careful decisions about how to allocate their limited resources.

Once a clear understanding of optimal and cost-efficient investments is achieved, the process moves on to the novel **Phase E** (*i.e.,* Compliance). This phase assesses the proposed cybersecurity strategy of SMEs (*i.e.,* current protections along with the defined or updated cybersecurity strategy if implemented) against a set of baseline cybersecurity requirements even before the implementation of the specific measures. Such a proactive approach enables SMEs to verify and update their internal requirements and cost-efficient solutions already at an early stage. The compliance phase itself involves a multi-faceted approach that not only examines the technical aspects of cybersecurity but also considers the economic and societal implications.

In this regard, to ensure that critical assets within a company are adequately protected, a cornerstone of good cybersecurity practice is having proper asset management in place. This not only allows identification of what needs to be protected, but also streamlines other critical business operations. Moreover, this phase also requires validating the existing and additionally selected security measures against the technical baseline requirements to check whether they fulfill the minimum set of technical requirements. This includes, for instance, checking whether companies have processes or safeguards in place to deny unauthorized access to their networks, monitor suspicious activities or encrypt sensitive information in transit to preserve their confidentiality and thus minimize the risk of data breaches.

Economic considerations form another critical component of the Compliance phase, aimed at ensuring that businesses have a comprehensive understanding of their requirements and have made well-informed decisions about the selection of safeguards, which, in turn, should yield satisfactory returns in terms of risk reduction, all while meeting budgetary constraints. Finally, this phase also includes a verification process to ensure that the organization's cybersecurity practices align with societal expectations and requirements. This includes expectations such as promoting cybersecurity awareness, being transparent about cybersecurity practices as well as contributing to the broader cybersecurity community through activities like information sharing. For instance, it is expected that companies have the necessary measures in place to adequately protect the personal data that they hold. This includes not only protecting against unauthorized access, but also ensuring that individuals' privacy rights are respected when data is collected and processed.

Such a compliance component does not exist in NIST CSF. As discussed, the framework is designed to be a flexible guide that can be adapted to any company's unique needs. This in turn means that businesses can use this framework to define its own cybersecurity requirements rather than demonstrating compliance with a set of fixed rules.

After obtaining the results from the Compliance phase, the methodology continuous with **Phase F** (*i.e.,* Execution and Deployment). This phase represents the practical application of the carefully planned and validated cybersecurity measures derived from the previous phases. To this end, companies can engage external technical consultants or schedule technical tasks to deploy, configure and maintain the new cybersecurity strategy. In the context of NIST CSF, this phase therefore perfectly aligns with the **Protect**, **Detect**, **Respond** and **Recover** functions.

The final phase of the Extended CyberTEA is **Phase G** (*i.e.,* Certification). In this phase, companies receive formal recognition of their cybersecurity posture and level of compliance, which not only serves as proof of their commitment to cybersecurity, but can also provide a competitive advantage in the marketplace, *e.g.,* by establishing trust and confidence among stakeholders and differentiate themselves from competitors that have no certification at all.

Another unique characteristic of this certification phase is its hierarchical structure, which includes three level of certifications. Each level addresses one of the key dimensions of cybersecurity, with the higher levels building on the requirements of the lower ones. This structured approach enables SMEs to progressively improve their cybersecurity posture by starting from a foundational level where basic technical requirements are addressed, moving over to considering financial and business related aspects and ultimately advancing towards a more comprehensive and holistic cybersecurity strategy that also considers societal implications.

Moreover, the certification phase also includes an assessment strategy that focuses on the continuous evaluation of businesses. In this sense, the certification is not a one-time event, but a continuous process to gradually progress to the third certification, and to regularly conduct reassessments to ensure ongoing compliance and address the evolving cybersecurity threat landscape, therefore reflecting the complex and dynamic nature of cybersecurity.

4.2 Certification Scheme

Figure 4.2 illustrates how the proposed certification scheme is structured. To begin with, the lightweight certification scheme is based on three main pillars, which are driven by the selected approaches (*cf.* Section 3.2) as well as the cybersecurity dimensions introduced in Section 2.1. In this sense, the **Technical Pillar** focuses on the implementation and management of cybersecurity measures and practices, while the **Economic Pillar** examines financial and business related aspects. Finally, the **Societal Pillar** evaluates the contribution towards the security of a company's stakeholders and the wider society.

Furthermore, each pillar consists of a number of categories addressing a particular aspect of the corresponding pillar. The categories, in turn, are comprised of multiple different requirements that are defined in a broader way, so that applicants can choose, rather than impose, the specific implementation of technologies and practices. Since each of the pillars

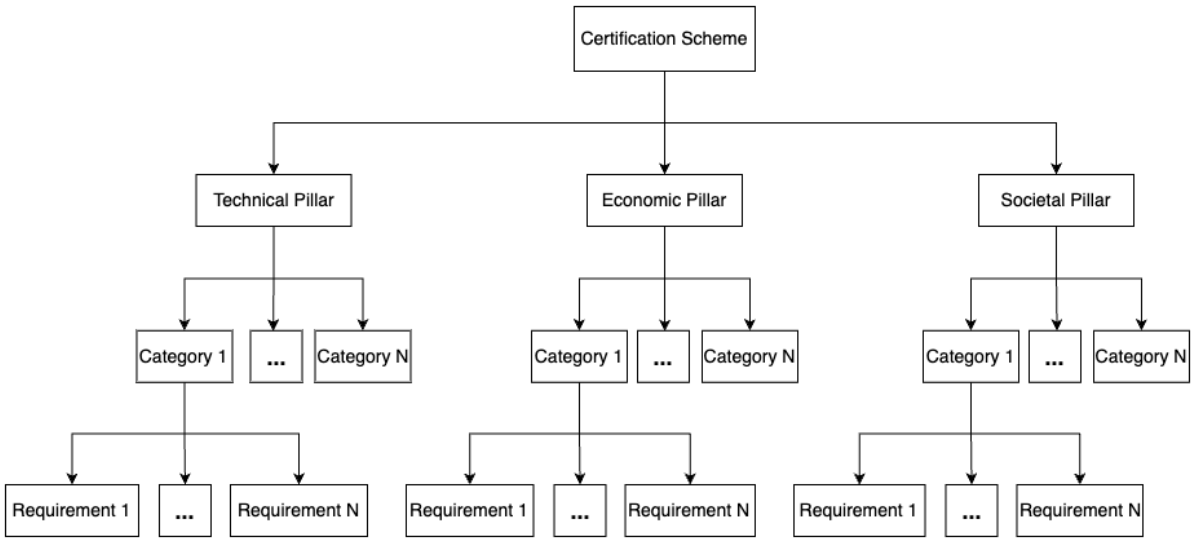


Figure 4.2: Data Structure of Proposed Certification Scheme

has a different nature, the number of categories, and hence the number of requirements per category, may vary for each pillar.

Figure 4.3 outlines the certification flow of the proposed lightweight certification scheme. The assessment starts with the examination of the technical requirements (*cf.* Subsection 4.2.1) and offers businesses a total of three different but interdependent certificates. The first certificate on the list is the **Technical Baseline (TB)**. It certifies that a company has basic cybersecurity measures and practices in place, and can only be achieved if all requirements of every category of the Technical Pillar are met. However, if there is even a single requirement that is not satisfied, the whole assessment is considered failed.

Once the TB certificate is obtained, the process moves on with the verification of the economic requirements (*cf.* Subsection 4.2.2) that are part of the Economic Pillar. The same rules apply here as well. By fulfilling all the requirements of every category of the Economic Pillar, businesses can attain the **Cost-Aware Baseline (CAB)** certificate. This certification verifies that a business has analyzed its cybersecurity risks and made informed decisions about which security measures to employ in accordance with its budget. However, to be eligible for the CAB certificate, the TB must be achieved first. At the same time, this also means that even if a company does not meet the economic requirements for the CAB certificate, it can still use the TB certificate to demonstrate its compliance with the baseline technical security measures and practices.

The final certificate on the list is the **Comprehensive Baseline (COB)**, which can be achieved by satisfying all societal requirements (*cf.* Subsection 4.2.3) in addition to the preconditioned TB and CAB. In this sense, the COB strives to provide a more comprehensive and holistic assessment of the cybersecurity posture of a business that goes beyond the technical and economic dimensions by taking into account the social and human factors as well. Again, if even a single societal requirement is not met, the assessment for the COB certificate is considered failed. The TB and CAB certificates, however, can then

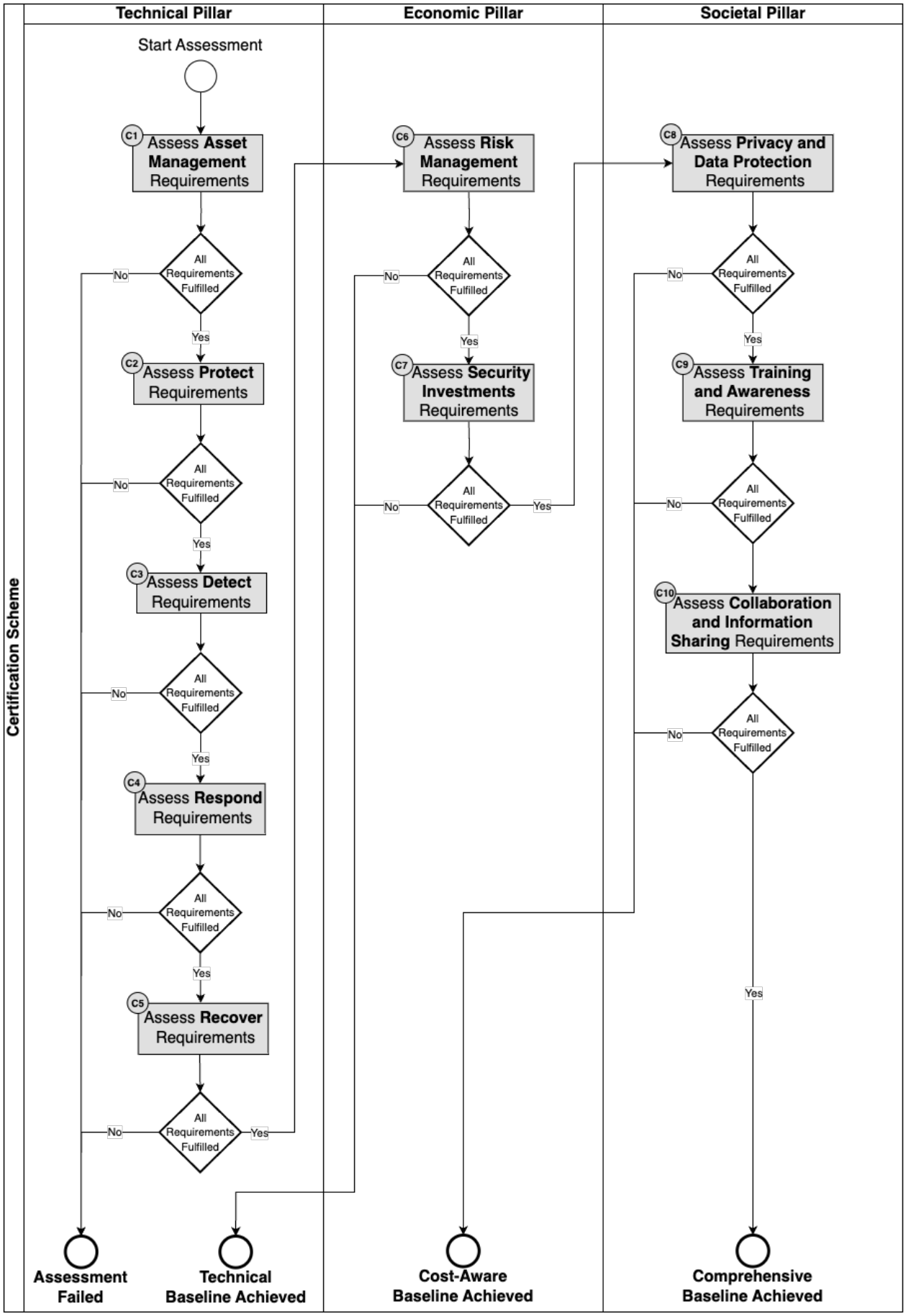


Figure 4.3: Certification Flow of Proposed Certification Scheme

still be used by companies to demonstrate their technical and financial management capabilities they have in place.

The proposed cybersecurity certification scheme therefore provides SMEs with an entry point into the complex world of cybersecurity. By offering three levels of certification, it allows businesses to gradually assess and improve their cybersecurity posture. The first and most important step is obtaining the TB certificate. Without having any security measures in place, the economic and societal impacts of cyber attacks cannot be contained. By continuously improving their cybersecurity posture (*i.e.,* by focusing on one certificate at a time), businesses can demonstrate to stakeholders their commitment to cybersecurity and their awareness of its wider implications on society. Therefore, this motivation can be used to gradually progress to the COB certification, which is the ultimate goal, as it benefits both the businesses and the broader society. On top of that, by addressing the requirements of all three pillars, companies can also develop new cybersecurity competencies that they can continue to build upon, thus continuously improving their cybersecurity posture.

The evaluation method of the proposed certification scheme is a first-party conformity assessment that allows companies to self-assess their own cybersecurity posture against a set of technical, economic and societal requirements. The relevant categories and requirements have been developed based on a variety of sources, including cybersecurity guidelines/best practices [28, 66], certifications [48, 33], and research [5, 35]. As mentioned, the requirements are formulated broadly enough to not impose any implementation rules, but to such an extent that they can still be mapped by SMEs. Since businesses can verify compliance with the requirements through self-assessment, the requirements are defined as closed questions (*i.e.,* yes or no), thus allowing for straightforward evaluation.

Furthermore, due to the dynamic and complex world of cybersecurity in which cyber attacks evolve every day, the issued certificates become valid for only one year. In this sense, after the 12-month expiry date, the whole assessment must be completed again. This approach ensures that businesses remain informed about the ever-changing threat landscape and adapt their cybersecurity practices and measures accordingly. By updating their knowledge and defenses on a regular basis, companies can then better protect their critical assets and hence reduce the risks posed by emerging cyber threats.

Moreover, due to the nature of the underlying data structure, the proposed certification scheme becomes highly customizable and extensible. In this sense, the certification scheme can, for instance, be extended to include an additional pillar such as the Legal Pillar, which covers categories and requirements related to the legal dimension. Some aspects of the legal dimension, on the other hand, can also be viewed through a societal lens and can therefore also be directly mapped to the Societal Pillar, as has been done in the case of Category C8 (*i.e.,* Privacy and Data Protection) in Figure 4.3. As such, existing categories and requirements can therefore also be adjusted and new ones can be added.

As a result, other customization possibilities can also be considered, such as tailoring the categories and requirements to fit the needs of Multi-National Enterprises (MNEs) or becoming even more specific to industries or sectors that have increased security requirements. For the latter one, the proposed data structure can be extended with another level that offers specific assessment criteria for the proposed requirements to check whether

companies meet the industry or sector standards. Ultimately, the proposed certification scheme is designed to be self-contained in the sense that it can be used on its own. Simultaneously, it can also be seamlessly integrated in existing methodologies or guidelines to ensure that a specific set of baseline requirements are met, as illustrated in Section 4.1.

In the following subsections, the categories and requirements of the Technical, Economic, and Societal Pillars are presented in greater detail. For this purpose, a table is provided for each category listing its associated requirements. It must be highlighted that the specified requirements are not meant to be exhaustive. In addition, dependencies to other categories are noted and sources for verifying the requirements are listed.

4.2.1 Technical Requirements

The evaluation of the proposed certification scheme starts by reviewing the requirements of the Technical Pillar, which are grouped into five categories (*cf.* Categories C1 to C5 in Figure 4.3). The first category to be addressed is **Category C1** (*i.e.,* Asset Management), which covers the practice of identifying and managing a company's assets such as information, technology and personnel. This category is extremely important as it facilitates not only cybersecurity but streamlines also other relevant business operations such as financial accounting. Yet, when looking at asset management through a technical lens, it quickly becomes clear that a company needs to be aware of its assets in order to have a clear understanding of what needs to be protected.

With this in mind, Table 4.1 outlines relevant requirements for this category and dependencies to other categories. There are many reasons why Requirement 1.1 is important. For example, by understanding what information a company uses facilitates the implementation of appropriate security measures for more sensitive information. Moreover, sensitive information like credit card, banking and personally identifiable information (*e.g.,* health information, passwords or social security numbers) are required by law to be adequately protected. In this sense, by complying with the respective regulations companies can avoid hefty penalties for non-compliance. Creating and maintaining an up-to-date inventory, as

Table 4.1: Requirements for Asset Management Category (C1)

Asset Management			
#	**Requirements**	**Relationships**	**Sources**
1.1	Do you know what information your business collects, processes and stores?	C2, C3, C4, C5, C6, C7, C8, C9, C10	[21][47]
1.2	Do you maintain an up-to-date inventory that lists all your assets, such as data (*cf.* Requirement 1.1), IT systems and processes (software and hardware), external technologies (*e.g.,* Cloud Services), and cybersecurity related responsibilities (*e.g.,* reporting incidents and suspicious activities)?		[48][33] [67]
1.3	Do you have a process for safe disposal of outdated computers or media such as CDs or USB drives?		[47]

suggested by Requirement 1.2, can therefore help keeping track of all relevant assets. This includes besides the information also resources such as hardware (*e.g.,* computers) and software (*e.g.,* anti-virus). Moreover, by identifying the important business assets (*i.e.,* data, services, resources), companies can prioritize its recovery in the event of business disruption due to a cyber attack or even a disaster (*cf.* Category C5). Besides, maintaining an asset inventory allows for identifying outdated resources such as computers or softwares. In this regard, Requirement 1.3 emphasizes that hardware resources must be carefully disposed of in order to prevent unauthorized parties from gaining access to a company's sensitive information (*e.g.,* business or customer information) and thus proactively countering potential data breaches.

Category C2 (*i.e.,* Protect) is the next category on the list that is addressed upon successful achievement of the requirements of Category C1. The objective of the Protect category is to develop and implement suitable security measures to safeguard a company's assets and consequently ensure the confidentiality, integrity, and availability of business critical data and services.

Table 4.2 presents requirements that help limiting or containing the impact of potential cyber attacks. For instance, Requirement 2.1 focuses on data security and suggests using encryption techniques to protect the confidentiality and integrity of sensitive and confidential information. In this sense, encryption of stored data ensures that the sensitive information cannot be accessed by unauthorized users and can therefore reduce the risk of a data breach. This also applies to data that is transmitted over the network. Encryption, in this case, not only protects the data from Eavesdropping attacks, where adversaries try to intercept and read the requests, but it also prevents attackers from tampering the data without being noticed.

Table 4.2: Requirements for Protect Category (C2)

Protect			
#	**Requirements**	**Relationships**	**Sources**
2.1	Do you encrypt sensitive and confidential data at rest (*i.e.,* stored on servers, databases, etc.) and in transit (*i.e.,* during the transmission over the Internet)?	C1, C6, C7, C8, C9	[33][47]
2.2	Is your network protected against unauthorized access from external sources by using *e.g.,* firewalls or routers?		[66] [33]
2.3	Do you use multi-factor authentication (MFA) in addition to secure passwords whenever possible?		[48][68]
2.4	Do you ensure that all IT systems are securely configured (*e.g.,* remove unnecessary user accounts, change default passwords, use of authentication to access data or services, etc.)?		[21][48] [33][68]
2.5	Do you perform periodic security updates on all your IT systems and applications?		[69][70]

Requirements 2.2 and 2.3, on the other hand, strive to improve the access control of businesses, *i.e.,* who has access to which resources and what operations are allowed to be performed involving these assets. Requirement 2.2 specifically emphasises that network traffic from the Internet should be restricted to authorized parties only. A deny by default approach for firewalls should be considered that blocks all traffic that has not been explicitly permitted. Requirement 2.3 helps then reducing the risk of account takeovers considerably, as it requires employees to use multiple forms of authentication in addition to strong and secure passwords in order to verify their identity and thus gain access to the corporate networks and systems.

Moreover, malicious actors often take advantage of misconfigured systems or networks to perform cyber attacks. It is therefore important that companies establish procedures for secure configuration, as pointed out by Requirement 2.4. These include, among others, changing default passwords for administrator accounts and also for all applications, disabling unused accounts, close unused ports, as well as isolating the guest WLAN network from the corporate network. Finally, as cyber attacks evolve every day, Requirement 2.5 specifies that security updates should be performed on a regular basis to addresss known vulnerabilities in software, application or operating systems and thus reduce the risk of exploitation by adversaries.

The third category on the list is **Category C3** (*i.e.,* Detect). This category focuses on the development and adoption of activities and processes that help detecting cybersecurity incidents in order to be able to react to them. Table 4.3 therefore provides requirements that help in identifying such cybersecurity events in a timely manner in order to be able to mitigate the damage and respond with appropriate actions.

With this in mind, the first requirement (*i.e.,* Requirement 3.1) requires implementing measures specifically targeting malware, which comes in various forms (*e.g.,* Virus, Worms or Ransomware). Such malware can cause serious damage to businesses, such as by encrypting a company's critical information and demanding a ransom for the decryption key. It is therefore of primary importance to mitigate the risk posed by such cyber attacks.

Table 4.3: Requirements for Detect Category (C3)

Detect			
#	**Requirements**	**Relationships**	**Sources**
3.1	Do you actively monitor your IT systems for malware (*e.g.,* by utilizing up-to-date anti-virus, anti-spyware, or anti-malware software)?	C1, C2, C7, C9, C10	[48][67]
3.2	Is the use of IT systems logged and are these logs maintained and monitored to make security incidents traceable?		[33][47] [71]
3.3	Do you regularly monitor your network traffic and system logs for unusual or suspicious traffic (using *e.g.,* IPS/IDS, SIEM, etc.)?		[66][33]
3.4	Have you established procedures for reporting security incidents and suspicious activities?		[67]

Moreover, Requirement 3.2 specifies the urgent need to develop and implement a logging strategy, since security monitoring as well as a company's situational awareness rely on effective logging practices. By continuously logging the use of IT systems, companies can identify and consequently analyze patterns of activity. In the event of a cyber security incident, these data can then aid forensic investigations to identify the source of the attack and the extent of the compromise.

Requirement 3.3 builds on top of the previous requirement as it focuses on identifying suspicious activities and anomalies on the corporate network and systems. Examples of unusual activities include, for example, sudden increase in network traffics at unusual times which might be an indication for (D)DoS attacks, unrecognized devices on the network, or numerous failed attempts to access (critical) resources. Finally, the last requirement of this category (*i.e.,* Requirement 3.4) aims to provide employees with straightforward ways to report cybersecurity incidents or suspicious activities in general. Having such procedures in place allows companies to analyze incoming reports and thus quickly respond to potential threats. As a result, cyber attacks may be spotted as quickly as possible, which in turn can help reduce the impact of the incident.

In the event where a business has detected a cybersecurity incident, appropriate measures must be taken. In this sense, **Category C4** (*i.e.,* Respond) comprises requirements that aim to support companies in their ability to respond to and mitigate detected cybersecurity incidents. A non-exhaustive set of requirements is therefore outlined in Table 4.4, and relations to other categories are also listed. Requirement 4.1, for example, is highly important. It urges SMEs to develop a plan beforehand on how they intend to respond to security incidents (*e.g.,* disconnect network of affected systems, shut down computers, run anti-virus software, and change passwords). This approach, in turn, ensures that businesses are prepared for such real-life scenarios, which means that they are able to respond to security events in a more timely and more efficient manner and thus limiting potential damage.

Table 4.4: Requirements for Respond Category (C4)

Respond			
#	**Requirements**	**Relationships**	**Sources**
4.1	Do you have a documented response plan in place for security incidents such as system failure, malware attack or data leakage?	C1, C3, C6, C9, C10	[33][47]
4.2	Do all employees know who is the contact point for reporting incidents?		[67][68]
4.3	Are employees aware of the appropriate ways for reporting potential security incidents?		[67][70]
4.4	Have you identified who is responsible for conducting security incident investigations and applying appropriate remediation?(*e.g.,* trained personnel, contracted company, cyber insurance, etc.)		[47][69]
4.5	Do you update your incident response plan based on lessons learned from past incidents?		[67]

As discussed, Requirement 3.4 of the Detect category requires companies to establish procedures for reporting suspicious activities or actual incidents. Requirements 4.2 and 4.3 both build on this requirement and relate to the communication of such suspicious events. It is therefore critical that employees know who to contact and how to report an incident, as proper response depends on timely action. Moreover, a documented response plan defines further roles and responsibilities in the case of cyber attacks. As outlined in Requirement 4.4, companies should be aware of who is going to investigate the attack and respond accordingly with appropriate measures. Businesses without qualified personnel are strongly advised to contract external companies in such cases. Also, for cases where sensitive data is at stake, it is recommended to seek advise from legal counsel. The last requirement of this category (*i.e.,* Requirement 4.5) promotes the idea of continuous improvement. No response plan is perfect. It is therefore important to update the current plan with lessons learned from past incidents. This enables businesses to address gaps and better prepare for future incidents.

The final requirements on the way of obtaining the TB certification are presented in Table 4.5 and belong to **Category C5** (*i.e.,* Recover). This category involves designing and implementing suitable strategies to maintain business continuity and recover any compromised capabilities or services resulting from cybersecurity events or natural disasters. In this sense, a successful Ransomware attack, for instance, can encrypt all critical business information, thus rendering them inaccessible and causing significant business disruption. In such cases, whether and how quickly a company can resume operations depends on proper preparation and response.

With this in mind, Requirement 5.1 highlights the importance of having the internal knowledge to address such scenarios and initiate timely recovery efforts. One important and effective way to restore business data and operations is by creating and maintaining backups. Since this is a practice that even SMEs can easily adopt, requirements 5.2 to 5.5 therefore aim to ensure that businesses do establish a backup strategy that is tailored to their needs and resources.

As companies do not know beforehand if and when a cyber attack is going to be launched, it is essential to create backups on a regular basis. Moreover, to ensure the confidentiality

Table 4.5: Requirements for Recover Category (C5)

Recover			
#	**Requirements**	**Relationships**	**Sources**
5.1	Do you have in-house knowledge to resume operations after a cyberattack or disaster?	C1, C2, C3, C4, C6, C9, C10	[67]
5.2	Do you perform regular backups for your critical business information?		[48][47]
5.3	Do you keep backups outside the business environment in a protected location?		[68][69]
5.4	Do you encrypt your backups?		[66][70]
5.5	Do regularly check whether data can be fully restored from your backups?		[21][68]

and integrity of the backed-up information, the copies should be encrypted and stored in remote and safe locations. And finally, companies must periodically verify that the backups can be fully restored. Failing to do so would leave businesses with no guarantee that the backups can be used in the event of a disaster or security incident.

4.2.2 Economic Requirements

Once all technical requirements are passed (*cf.* Subsection 4.2.1), the TB certification is issued. This assures that a company has a set of basic measures and practices for protecting, detecting, responding and recovering from cybersecurity incidents in place. The assessment then continues with verifying the financial and business related requirements of the Economic Pillar, which are grouped into two categories (*cf.* Category C6 and C7 in Figure 4.3).

In this regard, the assessment of the Economic Pillar starts by examining **Category C6** (*i.e.,* Risk Management) first, which involves the activity of identifying the level of protection for different assets, implementing the necessary safeguards, and subsequently monitoring them (*cf.* Section 2.2). Although, at this point, basic technical measures should be implemented (since TB is a precondition), companies continue to be unique and therefore may be exposed to additional unique cybersecurity risks. Thus, this category aims to help businesses to better understand their company profile, assess their unique risks, and allocate resources accordingly.

With this in mind, Table 4.6 presents the corresponding requirements and also specifies dependencies to other categories. Requirement 6.1, for instance, builds on the requirements of Category C1, in which business assets are identified. Since it is not possible to achieve utmost protection and therefore eliminate all cybersecurity risks, understanding the value of these assets helps prioritizing further risk management efforts. The value of an asset is associated with the potential impact (*i.e.,* direct and indirect costs) that a cyber attack can have. Therefore, questions related to the CIA triad (*cf.* Subsection

Table 4.6: Requirements for Risk Management Category (C6)

Risk Management			
#	**Requirements**	**Relationships**	**Sources**
6.1	Have you determined the value of all assets, including information, software and hardware, that your businesses relies on?	C1, C2, C3, C7, C8	[47]
6.2	Do you have a continuous process in place to identify and evaluate threats and vulnerabilites, and estimate the likelihood of them being exploited?		[43]
6.3	Have you prioritized the identified risks based on criticality?		[43]
6.4	Do you review your identified risks annually and whenever there is a change that can impact the risks?		[28]

2.1.1), such as *"What happens to the business if sensitive customer data is leaked?"*, can be asked to assess the potential consequences to business productivity, reputation or legal liabilities, for example.

Once the values of the different assets have been determined, it is essential for companies to understand the threats and vulnerabilities that they face, and estimate the likelihood of their exploitation (*i.e.,* Requirement 6.2). Subsequently, the assessed risks can then be prioritized based on their criticality (*i.e.,* likelihood, impact, company's risk tolerance), which in turn ensures that the most significant risks are addressed first, thus making the best use of the limited resources (*i.e.,* Requirement 6.3).

However, it still depends on the company's risk appetite and available resources whether additional controls are implemented alongside the baseline safeguards to mitigate the unique risks, or whether the company intends to share (*cf.* Requirement 7.4) or even accept them. In the end, risk management is an iterative process, and companies should continuously reassess their risks (*e.g.,* when a new technology is introduced) and adjust the treatment strategies as needed (*i.e.,* Requirement 6.4).

After complying with the Risk Management requirements, the certification process then moves on to verifying the requirements of **Category C7** (*i.e.,* Security Investments), which is intended to aid companies avoid overinvesting in cybersecurity while still achieving reasonable protection. As discussed, it is not possible to achieve utmost protection and eliminate all risks. Moreover, most SMEs operate on a tight margin anyway. The requirements in Table 4.7 therefore serve businesses in making informed decisions in terms of adequacy and cost-efficiency of cybersecurity investments.

In this regard, Requirement 7.1 requires that companies allocate a dedicated budget for cybersecurity related activities. As business continue to move their operations online, they become increasingly vulnerable to cyber attacks. It is therefore important that businesses take the necessary protective measures to mitigate their risks. Nevertheless, this requirement should be fulfilled at this stage of the certification process, since the TB

Table 4.7: Requirements for Security Investments Category (C7)

Security Investments			
#	**Requirements**	**Relationships**	**Sources**
7.1	Have you allocated a dedicated budget for cybersecurity investments in your company?	C1, C2, C3, C5, C6	[4]
7.2	Are your cybersecurity investments allocated in a manner that balances the cost of risk mitigation with the potential financial impact of cybersecurity incidents (*e.g.,* using Gordon-Loeb model)?		[35][64]
7.3	Do you use metrics (*e.g.,* ROSI) to compare potential cybersecurity solutions and prioritize the implementation of the more cost-efficient ones?		[5][41]
7.4	Have you considered investing in cyber insurance to mitigate potential financial impacts of security incidents?		[67]

that mandates the implementation of basic cybersecurity protections and processes must be achieved in order to assess the Economic Pillar.

Requirement 7.2 goes further and wants businesses help achieve a balance between risks and investments. Well-accepted models such as GL model (*cf.* Subsection 2.3.1) can be considered. This analytical model therefore helps determining the optimal investment level in cybersecurity and recommends that businesses do not allocate more than 37% of the expected loss due to a successful cyber attack to mitigation measures. Although the complex calculation might be intimidating to SMEs, there are solutions [64] available that automate and simplify the whole process.

Moreover, Requirement 7.3 mandates that businesses assess with the help of *e.g.,* ROSI (*cf.* Subsection 2.3.2) the benefits of investments in terms of how much risk for a security incident could be reduced. It also requires companies to compare solutions with different characteristics based on their cost-effectiveness to determine which one should be selected from an economic standpoint. This is extremely important as it allows businesses to make informed decisions, ensure the best use of their constrained budget as well as to justify investments to stakeholders, all while not exceeding the maximum investment in cybersecurity (*i.e.,* 37% of the expected loss).

Requirements 7.2 and 7.3 should not only be applied on the prioritized risks from the previous category, but should also be considered for the cybersecurity measures implemented as part of the TB certification. The last requirement of this category (*i.e.,* Requirement 7.4) aims to remind companies that there exist still the possibility to contract cyber insurance. Cyber attacks are costly and depending of the type of incident the direct and indirect costs can lead businesses to bankruptcy. Cyber insurance in this case can protect a company's financial stability by covering part of the associated costs of the incident.

4.2.3 Societal Requirements

After obtaining the TB and CAB certifications, the applicant can not only demonstrate that it has basic cybersecurity measures and practices in place, but also that it has made informed decisions about which measures to implement while meeting budgetary constraints. The final part of the assessment then reviews the requirements of the Societal Pillar, which addresses the **Social** component of the Environmental, Social, and Governance (ESG) criteria [72].

With this in mind, the societal requierements are grouped into three categories (*cf.* Categories C8 to C10 in Figure 4.3). The first category to be addressed is **Category C8** (*i.e.,* Privacy and Data Protection), which is concerned with today's data-driven world where vast amounts of personal and sensitive information are being collected, processed and stored. Companies need be aware that, besides legal considerations, they also have a social and ethical obligation to protect personal information against unauthorized access, misuse or disclosure in order to respect the rights and interests of the individuals whose data they process.

Table 4.8 therefore outlines requirements that contribute in protecting personal and sensitive information. In this regard, Requirement 8.1 highlights the importance of having

Table 4.8: Requirements for Privacy and Data Protection Category (C8)

Privacy and Data Protection			
#	**Requirements**	**Relationships**	**Sources**
8.1	Do you have clear and up-to-date data protection policies that align with relevant data regulations (*e.g.,* GDPR)?	C1, C2, C5	[66][73]
8.2	Do you provide individuals with clear, concise, and easy-to-understand privacy notices that explain how their information is collected, used, and shared?		[74][75] [76]
8.3	Do you collect, process, and store only the minimum amount of personal data necessary for your business operations?		
8.4	Do you securely delete or anonymize personal data when it is no longer required for business purposes?		
8.5	Do you have security controls in place that adequately protects personal information?		

clear and up-to-date data protection policies. Depending on the business and what data it collects or processes, the company might be subject to different regulations such as the GDPR or HIPAA. Compliance with such regulations not only helps considerably reducing risks, but also helps companies to improve their reputation while avoiding hefty fines or other legal consequences for non-compliance. In addition to that, such policies can motivate employees to follow outlined best practices as not adhering to policies might lead to consequences.

The remaining requirements introduce further but not exhaustive data protection principles that help strengthening the commitment to safeguarding personal information. In this sense, Requirement 8.2 focuses on the transparency of data collection and processing. Data subjects must be aware how their personal information is going to be collected, used and disclosed in order to be able to give explicit and informed consent.

Another key aspect is outlined in Requirement 8.3 and concerns the principle of data minimization. This requirement dictates that only the necessary personal information that is required to fulfill a specific purpose should be collected, processed and stored. Moreover, Requirement 8.4 concerns the principle of storage limitation which mandates that information should be deleted or anonymized as soon as they are no longer needed. This can help reduce the potential risks of holding personal data for too long.

The last requirement (*i.e.,* Requirement 8.5) specifies that a company need to have protective measures in place that addresses the confidentiality, integrity and availability of personal information, including accidental, unauthorized, or unlawful disclosure or loss of personal information. There is therefore a direct dependency to categories C1 and C2, which are responsible for identifying critical assets such as personal information and implementing the necessary safeguards, respectively.

Having met the requirements of the Privacy and Data Protection category, the next priority on the agenda is **Category C9** (*i.e.,* Training and Awareness). While cybersecurity itself represents a complex ecosystem that requires cutting-edge technologies and sophisticated algorithms to protect information and systems, these technical security measure are only one part of the puzzle. For these measures to be really effective, they need to operate in harmony with the people that use them, such as employees, management or customers. In reality, however, this is often not the case, as people are often the weakest link in a company's cybersecurity due to their susceptibility to errors, manipulation or oversight.

In its annual Data Breach Investigation Report [77], Verizon reported that in 2022, 82% of the investigated data breaches involved the human element (*e.g.,* Phishing, stolen credentials, or simply errors), which is quite alarming. This fact underlines all the more that it is crucial for companies to foster a culture of security awareness and properly train employees to be better prepared against such threats. By doing so, companies can not only significantly reduce their own risks, but these measures can also lead to better personal cybersecurity habits of individuals, therefore making society more robust against prevalent threats such as Phishing.

With this in mind, Table 4.9 presents requirements aiming at enhancing the awareness of employees and training them to respond appropriately to cybersecurity threats. Requirement 9.1, for instance, is of great importance as it addresses the aforementioned crucial role of the human factor in cybersecurity. Given that employees are often the most vulnerable to cyber attacks, their training becomes a critical part of a company's proactive defense strategy. Regular training therefore ensures that employees stay informed about the constantly evolving threat landscape, including prevalent risks such as Phishing or Social Engineering, and learn how to detect and respond to them.

Moreover, Requirement 9.1 also emphasizes that cybersecurity is not just the responsibility of the IT department or the respective employees in charge. Therefore, all employees should be equipped with the necessary knowledge to protect themselves and the business, because anyone can become a target. Furthermore, Requirement 9.2 once again highlights

Table 4.9: Requirements for Training and Awareness Category (C9)

Training and Awareness			
#	**Requirements**	**Relationships**	**Sources**
9.1	Do you provide regular security training and awareness programs for all employees that covers topics such as Phishing, Social Engineering and Password Management?	C1, C2, C3, C4, C5, C7	[47][69] [70]
9.2	Do you regularly update and improve security training to ensure employees remain aware of the latest threats and best practices?		[78][79]
9.3	Do you encourage employees to report potential security issues or incidents, therefore actively promoting a culture of security awareness?		[80]

that cybersecurity is a dynamic and rapidly evolving field, where cyber attacks evolve on a daily basis. Regularly updating and improving security training means keeping employees informed about these new threats and the latest defense strategies, which should be updated anyway after each security incident (*cf.* Requirement 4.5).

Finally, Requirement 9.3 reinforces the importance of employees feeling comfortable in reporting potential security incidents. Since they are the first point of contact for potential threats in most cases, their observations and thus their reports can be instrumental in preventing security breaches. By fostering a cybersecurity culture on a daily basis, employees can become a strong first line of defense against potential threats such as Phishing attacks or other forms of Social Engineering, and can therefore actively contribute to a company's overall cybersecurity posture.

Category C10 (*i.e.,* Collaboration and Information Sharing) represents the final phase of the verification process for obtaining the COB certification. This category deals with a complex topic which offers considerable benefits that are represented by the idea that the detection of one company can become the protection of another. However, this practice requires careful management, as it also presents a number of difficulties including establishing trust between participating companies and protecting private and sensitive information.

In this regard, Table 4.10 outlines requirements addressing different aspects of this category, including dependencies to other categories. Requirement 10.1, for instance, can help strengthening the ability of the broader community to prevent similar attacks on other companies or to enable them to react in a more effective manner in the event that they are targeted. Sharing intelligence is therefore critical, especially for SMEs, to better understand the potential risks that they face. Moreover, seeing how companies are overcoming challenges motivates businesses more to put in the effort to protect their assets than learning similar details from industry reports.

However, sharing information is not a straightforward task. Unintentional disclosure of sensitive information, for example, can lead to legal consequences, financial loss or damage to a company's reputation. Moreover, disclosing certain security and event information (*e.g.,* security logs) could also inadvertently reveal the protection or detection capabilities of a company, which, in turn, could allow adversaries to change their tactics. Therefore,

Table 4.10: Requirements for Collaboration and Information Sharing Category (C10)

Collaboration and Information Sharing			
#	**Requirements**	**Relationships**	**Sources**
10.1	Do you report and share information about security incidents or vulnerabilities with relevant external parties such as authorities or partners?	C1, C2, C3, C4, C5, C6, C9	[66][69]
10.2	Do you have rules in place about what cybersecurity information can be shared and who it can be shared with?		[81]
10.3	Have you joined any local or industry groups that share cybersecurity updates and warnings?		[81]

Requirement 10.2 mandates the establishment of clear rules that specify what may be disclosed and to whom.

The final requirement of this verification process (*i.e.,* Requirement 10.3) emphasizes the two-way nature of cybersecurity information sharing. In this sense, companies are strongly encouraged not only to provide information, but also to actively incorporate insights from cybersecurity communities [82, 83, 84]. This collaborative approach therefore allows companies to benefit from shared knowledge and experience to strengthen their own defense strategies.

Moreover, a better understanding of the threat landscape that results from this collaboration can also support the risk management phase (*cf.* Category C6). This allows companies then to refine their analysis and make informed decisions, thus strengthening their overall cybersecurity posture.

4.3 Prototype Design and Implementation

The following subsections present an overview of the prototype's architecture, technologies used, and the proposed user interface. A primary focus during the development was to create an automated solution for the compliance check, thus distinguishing CERTSec from traditional online questionnaire tools. In this sense, we will also dive into the automated features to shed light on their functioning.

4.3.1 Architecture Overview

Figure 4.4 illustrates the architecture of the CERTSec prototype. The users engage with the system through a web-based user interface (*cf.* Component C1) built with React [85] and TypeScript [86]. Next.js [87], a renowned React framework, enhances the frontend by bundling and optimizing it, while also providing useful features such as Server-Side Rendering (SSR) and Static Site Generation (SSG). To streamline development, the highly regarded UI component library, Material UI [88], was chosen for its adherence to Google's Material Design guidelines, thus ensuring the creation of modern and high-quality user interfaces. This layer interacts with the backend via REST APIs.

The backend, on the other hand, has been developed using the Python [89] programming language and Django REST Framework [90], which is a powerful and flexible toolkit for building Web APIs. Specifically, the Compliance Layer (*cf.* Component C2) processes HTTP requests from the frontend, performs the necessary computations, and responds accordingly with HTTP responses.

One of the unique features of this prototype is its automated requirements verification. However, such automated tasks can be time-consuming and must be executed asynchronously. Here, the Task Queue Layer (*cf.* Component C3) comes into play. CERTSec specifically leverages Celery [91], which is a distributed task queue system for Python

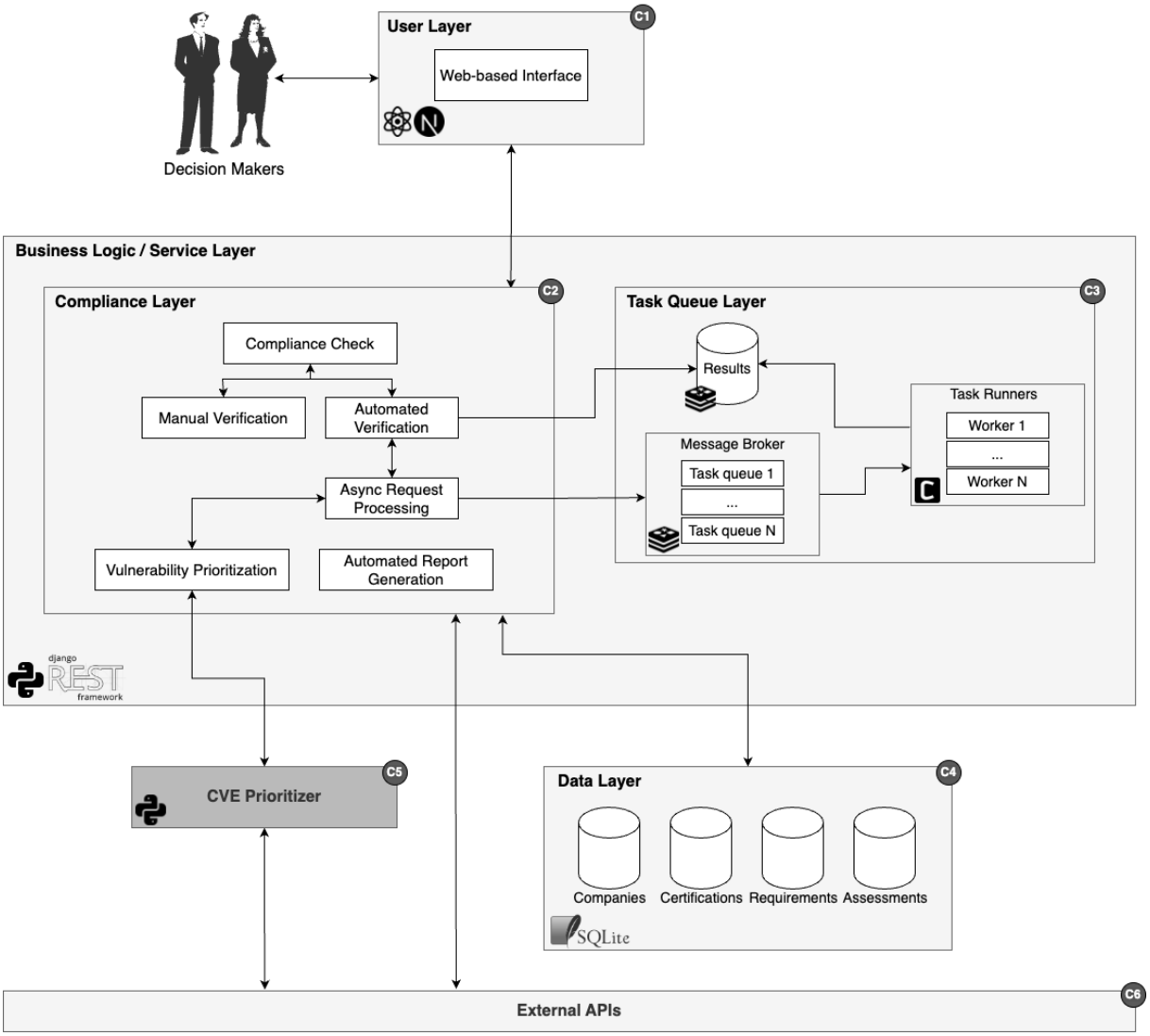


Figure 4.4: CERTSec Architecture

applications, to perform long-running tasks. This ensures that the main server thread isn't blocked by long-running operations, thereby maintaining responsiveness. Redis [92] serves as the message broker for communication between the main Django app and the worker processes responsible for executing tasks. Once the asynchronous tasks have finished, the results are then stored in Redis, which also serves as the results backend. This way, the frontend can then poll the statuses of the tasks and update the user interface accordingly.

In cases where the automated verification process identifies vulnerabilities, a prioritization process is employed. For this purpose, the CVE Prioritizer Tool v1.3.0 [93] (*cf.* Component C5) is integrated into CERTSec. The tool categorizes vulnerabilities into five categories by considering metrics such as CISA's Known Exploited Vulnerabilities (KEV), Common Vulnerability Scoring System (CVSS), and Exploit Prediction Scoring System (EPSS). The respective thresholds can be configured to reflect a company's risk appetite.

The Data Layer (*cf.* Component C4) contains the database responsible for storing relevant information. The Django application interacts with this layer to perform CRUD

operations on the data records. As this prototype is a Proof-of-Concept (POC), CERTSec utilizes a lightweight SQLite database [94], which requires no upfront configuration and offers efficient data storage and retrieval capabilities. Finally, the prototype also leverages external Application Programming Interfaces (APIs) (*cf.* Component C6), which will be discussed further in the subsequent section.

4.3.2 Automated Features

To demonstrate the feasibility of abstracting technical processes, a part of the verification for the technical requirements of the certification scheme has been automated. This means that the user only has to provide the necessary information (*e.g.,* company websites, IP addresses, technologies/software in use) before starting the assessment of the TB Certification. Then, while answering the rest of the questions, CERTSec evaluates the respective requirements. For this purpose, the following requirements from the *Protect* category (*cf.* Section 4.2.1 and Table 4.2) have been addressed:

- **Requirement 2.1**: Do you encrypt sensitive and confidential data at rest (i.e., stored on servers, databases, etc.) and in transit (i.e., during the transmission over the Internet)?
- **Requirement 2.2**: Is your network protected against unauthorized access from external sources by using *e.g.,* firewalls or routers?
- **Requirement 2.5**: Do you perform periodic security updates on all your IT systems and applications?

Secure Connections

The first feature to be addressed focuses on the second part of Requirement 2.1, which is about securing sensitive information during transmission over the Internet. In Django REST Framework, the `views.py` file typically contains the application's views, which can be either functional or class-based and define how a request should be handled. It is located under `backend/compliance` in CERTSec's GitHub repository [95].

Listing 4.1 provides the respective code snippet for the `check_https_connection` view, which receives HTTP requests, performs the necessary operations and finally returns a HTTP response.

```
@api_view(["POST"])
def check_https_connection(request):
    websites = request.data.get("websites", [])

    # Start check_https_connection_task as a background process
    task = check_https_connection_task.delay(websites)
    return Response({"task_id": task.id})
```

Listing 4.1: Check HTTPS Connections View

In particular, it is a function-based view that is decorated with the `@api_view` decorator to ensure that it is able to handle HTTP POST requests. This view itself is quite straight forward. It accepts an `HttpRequest` object as an argument from which it then can extract the data that has been sent in the body of the HTTP request. As shown on Line 3, it tries to get a list of website URLs from the request data, and if no `websites` key is present, it defaults to an empty list.

On Line 6, the `check_https_connection_task` (*cf.* Listing 4.2) is then added to the Celery task queue where Celery workers can pick it up and execute asynchronously. After scheduling the task, the view returns a HTTP response with a JSON body that contains the ID of the scheduled background task. This ID is then used in the frontend to check the status of the task.

Listing 4.2 illustrates a snapshot of the actual operations being performed in the background. Celery tasks are located inside the `backend/compliance/tasks.py` file and decorated with `@shared_task()` decorator. In essence, this method iterates over all websites. For each URL provided, the system first makes an HTTP GET request and determines based on the response URL the protocol in use. If the website is using the HTTPS protocol, the method tries to establish an SSL/TLS socket-based connection with the respective website using the secure context created (*cf.* Line 12-14). This secure context enforces some level of security by checking the server's certificate for authenticity and validity. If there is any issue with the certificate, such as it being expired or the hostname being invalid, the raised errors will be captured and handled within the corresponding `except` block.

```
1  @shared_task()
2  def check_https_connection_task(websites):
3      results = {}
4
5      for site in websites:
6          ...
7          try:
8              response = requests.get(tmp_site, timeout=(10, 60),
9                                      verify=False)
10
11             if response.url.startswith('https://'):
12                 context = ssl.create_default_context()
13                 conn = http.client.HTTPSConnection(domain, context=
14                                      context, timeout=10)
15                     ...
16             else:
17                 results[site] = {
18                     "protocol": "http",
19                     "description": "Not secure connection"
20                 }
21         except (socket.gaierror, socket.timeout, ConnectionRefusedError)
22             ...
23         except ssl.SSLError as e:
24             ...
25         except requests.exceptions.ConnectionError as e:
26             ...
27         except requests.exceptions.ReadTimeout as e:
```

```
            ...
        except http.client.HTTPException as e:
            ...

    return results
```

Listing 4.2: Check HTTPS Connection Celery Task

To check whether a background task has finished, the `get_background_process_status` view has been implemented (*cf.* Listing 4.3). If the task has successfully finished, it returns a HTTP response with a JSON body containing the status as well as the result data. Otherwise it returns only the status (*i.e.,* *PENDING*, *FAILED*, etc.).

```
@api_view(["GET"])
def get_background_process_status(request):
    task_id = request.GET.get("id")

    if task_id is None:
        return Response({'error': 'task_id is required as a query
                         parameter'}, status=status.HTTP_400_BAD_REQUEST)

    task = AsyncResult(task_id)
    response_data = {
        "status": task.status,
    }

    # include result if the task has finished
    if task.successful():
        response_data['result'] = task.result

    return Response(response_data, status=status.HTTP_200_OK)
```

Listing 4.3: Get Background Process Status View

Unauthorized Access

Determining whether a network is protected against unauthorized access (*cf.* Requirement 2.2) requires a comprehensive security assessment and penetration testing, which is out of scope for this work. However, gaining insights into a network's reachability and identifying potential firewalls or routers can still be achieved to some extent.

To accomplish this, CERTSec makes use of ICMP echo requests (*i.e.,* ping) that are sent to the target hosts. The view responsible for setting up the background task and returning the corresponding task ID is called `ping_ip` and can be found under `backend/compliance/views.py` in the code repository [95]. The corresponding Celery task, `ping_ips_task` (*cf.* `backend/compliance/tasks.py` in [95]), iterates through all provided IP addresses and sends a ping request to each one. Depending on the round-trip time returned, it determines whether the target host is reachable. If a host is unreachable, it could be due to various reasons, such as an active firewall blocking ICMP requests, the host being offline, or the IP address being invalid.

Although network reachability analysis offers a helpful overview of the network's status, it does not definitively indicate the presence of network security devices like firewalls or routers. More importantly, it does not replace a thorough security assessment and penetration test. Further reconnaissance tools and methodologies are required for a more in-depth analysis. Keeping this in mind, CERTSec extends its probing capabilities by scanning commonly used network ports, as detailed in the `nmap_top_ports_scan_task` defined under `backend/compliance/tasks.py` in CERTSecs code repository.

Summing up, similar to previous tasks, this process runs asynchronously in order to maintain system responsiveness. Moreover, the task utilizes Nmap [96] for port analysis. Upon completion of the task, users are prompted to evaluate whether there are protective measures deployed on each open port. This design approach acknowledges the constraints of CERTSec, which is not equipped to conduct automated penetration testing. Such activities would necessitate additional permissions and authorizations.

Vulnerability Scanning

To check whether Requirement 2.5 is fulfilled, CERTSec applies a two-pronged approach to identify vulnerabilities. Primarily, it relies on Nmap [96], which is an open-source network scanning tool that is used for network exploration and security auditing. More specifically, CERTSec uses the python3-nmap [97] library for this purpose.

Similarly to the previous feature, there is a functional view created inside the `views.py` file that takes care of scheduling the asynchronous task. In this sense, the `nmap_vulners_scan_task` (*cf.* `backend/compliance/tasks.py` in [95]) carries out a vulnerabilitiy scan for each provided IP address.

The Nmap results, prior to being returned, are then prioritized leveraging the CVE Prioritizer tool [93]. Version 1.3.0 has been successfully integrated within CERTSec and its code base is accessible within the `backend/cve_prioritizer` [95] directory. However, since the CVE Prioritizer tool outputs the outcome directly to the console, some modifications had to be made. With this in mind, we can now invoke the `prioritize_cves` method, located at `backend/cve_prioritizer/cve_prioritizer/cve_prioritizer_wrapper.py` in the code repository, to prioritize the vulnerabilities found by Nmap. This wrapper class returns now the results directly instead of printing them to the console.

Listing 4.4 presents a representative outcome of the network vulnerability scanning process. The structure of this result is a hierarchical dictionary where each IP address maps to its corresponding ports. For every port under each IP, it incorporates both the findings from the Nmap vulnerability scan (*cf.* Lines 4-14) and the resulting analysis from the CVE Prioritizer Tool (*cf.* Lines 15-22).

```
1 {
2     "192.168.1.14": {
3                 "80": {
4                     "protocol": "tcp",
5                     "service": {
6                         "name": "http",
```

```
7                       "product": "Apache httpd",
8                       "version": "2.4.25"
9                   },
10                  "vulnerabilities": {
11                      "CVE-2019-9517": {
12                          "type": "cve",
13                          "cvss": "7.8",
14                          "is_exploit": "false",
15                          "priority_details": {
16                              "priority": "Priority 2",
17                              "epss": 0.00345,
18                              "cvss_baseScore": 7.5,
19                              "cvss_version": "CVSS 3.1",
20                              "cvss_severity": "HIGH",
21                              "cisa_kev": "FALSE"
22                          }
23                      },
24                      ...
25                  }
26              }
27              ...
28      }
29      ...
30  }
```

Listing 4.4: Sample Outcome of Network Vulnerability Scan

The secondary approach involves examining the technologies and software products submitted by the user via the frontend. This task is handled by the `technology_vulners_scan` function-based view in `backend/compliance/views.py`, which in turn schedules the `technologies_vulnerability_scan_task` task located at `backend/compliance/task.py` [95].

Other than the primary approach, this feature uses the provided parameter to query the National Vulnerability Database (NVD) [98] for potential vulnerabilities associated with the technology. Moreover, in order to be able to make more request, a corresponding API key has been obtained [99], increasing the limit from 5 to 50 requests in a rolling 30-second window [100].

Since finding exact Common Platform Enumeration (CPE) matches for user-provided technologies or software can be challenging, the method incorporates the `virtualMatchString` parameter, enabling vulnerability searches using a CPE formatted string. As a result, by leveraging the `virtualMatchString`, the method expands the search scope and increases the likelihood of locating relevant vulnerabilities. This approach acknowledges the dynamic nature of technology descriptions and accommodates variations in CPE representations. As a result, users can obtain more comprehensive vulnerability results, even when specific CPEs are unavailable or uncertain.

Listing 4.5 showcases an example result of a vulnerability scan for Microsoft Excel 2019. As with the Common Vulnerabilities and Exposures (CVEs) identified by Nmap, all detected CVEs are prioritized using the CVE Prioritizer tool. The identified CVE IDs are then logged as keys in the `vulnerabilities` dictionary, with their corresponding priority details recorded as values (*cf.* Lines 7-14).

```
[
    {
        "product": "Excel",
        "version": "2019",
        "vendor": "Microsoft",
        "vulnerabilities": {
            "CVE-2020-0759": {
                "priority": "Priority 2",
                "epss": 0.04524,
                "cvss_baseScore": 8.8,
                "cvss_version": "CVSS 3.1",
                "cvss_severity": "HIGH",
                "cisa_kev": "FALSE"
            },
            "CVE-2019-1327": {
                "priority": "Priority 2",
                "epss": 0.03799,
                "cvss_baseScore": 8.8,
                "cvss_version": "CVSS 3.1",
                "cvss_severity": "HIGH",
                "cisa_kev": "FALSE"
            },
            ...
        }
    }
]
```

Listing 4.5: Sample Outcome of Technology Vulnerability Scan

Report Generation

Section 3.2 introduced SecBot [63], a cutting-edge tool that uses machine learning and natural language processing to simplify the cybersecurity planning and management of SMEs. Although the evaluation process highlighted many benefits of SecBot, it also revealed a significant limitation, namely its limited knowledge base. However, with the introduction of OpenAI's groundbreaking language model ChatGPT [101], this type of limitation has been effectively addressed. In this sense, as a Large Language Model (LLM), ChatGPT possesses an extensive and versatile knowledge base that helps overcoming the knowledge-based limitations typically encountered in such research prototypes.

With this in mind, CERTSec has also integrated a feature that leverages the ChatGPT API. This integration allows to automatically generate insightful reports that provide explanations, recommendations and timelines to address unfulfilled requirements for the TB, CAB, and COB certifications (*cf.* Section 4.2).

The corresponding view is illustrated in Listing 4.6. `generate_report` is a function-based view and is designed to handle HTTP POST requests. As can be observed, Line 4 invokes the `prepare_gpt_messages` function (*cf.* `backend/compliance/utils/utils.py` in [95]), which is responsible to prepare the messages for the GPT-3.5 model. In order to be able to use the ChatGPT API, users have to obtain a corresponding API key [102]. If

such a key is available, it will be set on Line 7. Subsequently, a chat completion is created using OpenAI's GPT-3.5 model with the prepared messages. The request is considered as successful if the finish reason is `stop`, as detailed in Line 15.

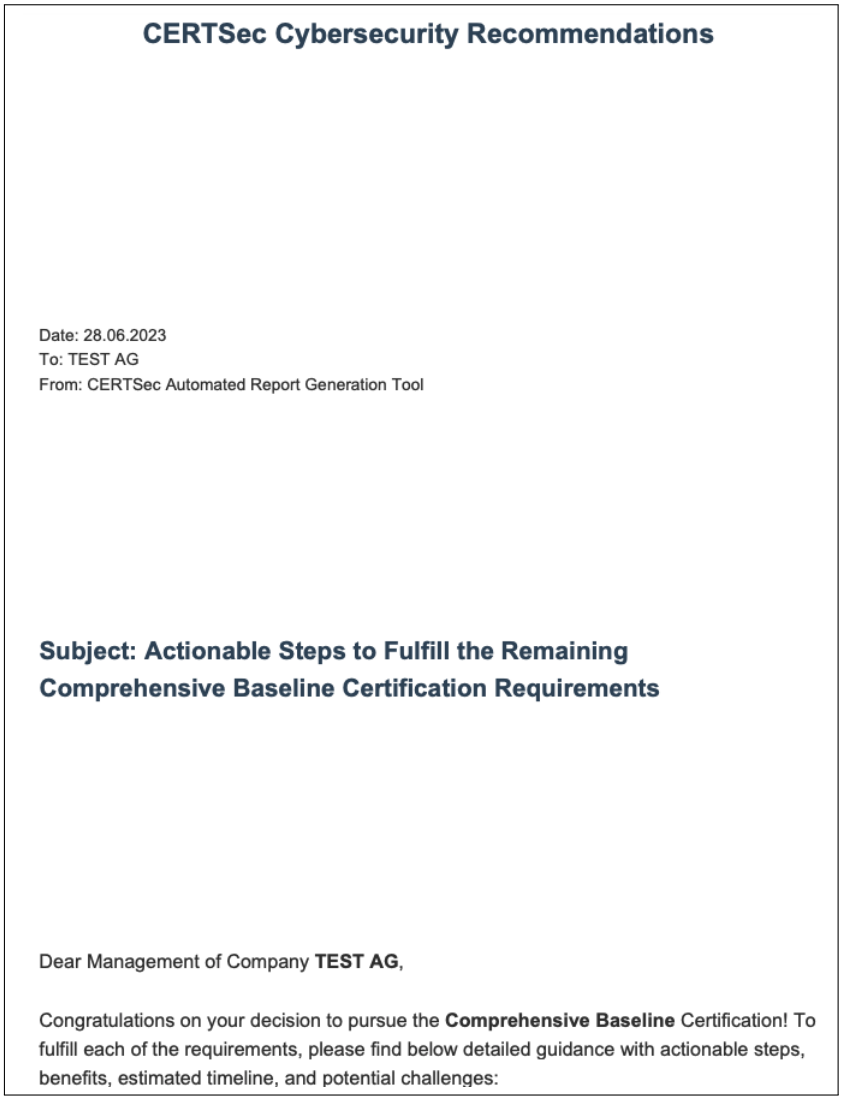
```
1  @api_view(["POST"])
2  def generate_report(request, id):
3      ...
4      prompt = prepare_gpt_messages(company, certificate,
5                                    unfulfilled_requirements)
6
7      openai.api_key = os.getenv("OPEN_AI_API")
8      response = openai.ChatCompletion
9                      .create(model="gpt-3.5-turbo-16k",
10                             messages=[{"role": "system", "content":
11                             prompt["system_msg"]},
12                             {"role": "user", "content":
13                             prompt["user_msg"]}])
14
15     if response["choices"][0]["finish_reason"] == "stop":
16         # generate pdf
17     else:
18         print(response["choices"][0]["finish_reason"] == "stop")
19     return Response({'prompt': prompt})
```

Listing 4.6: Generate Report with ChatGPT

The subsequent figures provide visual representations to demonstrate the structure and content of the generated report. For example, Figure 4.5 exhibits the design of the title page. This page comprises the title, creation date, the addressed company, the subject of the report, and a brief introduction. This introduction acknowledges the company's decision to pursue a particular certification and outlines the subsequent report content, *i.e.,* detailed guidance featuring actionable steps, benefits, estimated timelines, and potential challenges associated with fulfilling the certification requirements. Importantly, this page underscores that the report is a product of the *CERTSec Automated Report Generation Tool*.

Figure 4.6, on the other hand, showcases the conclusion and a critical disclaimer. The concluding remarks reaffirm the belief that by following the proposed actionable steps, the company can significantly bolster its cybersecurity posture and successfully achieve the targeted certification.

Moreover, the disclaimer clearly states that the report is automatically generated by ChatGPT and has not undergone review by a cybersecurity professional. This disclaimer aims to set the right expectations about the report and emphasizes that while the AI model is highly trained and advanced, human expertise may still be needed for comprehensive analysis and guidance.



CERTSec Cybersecurity Recommendations

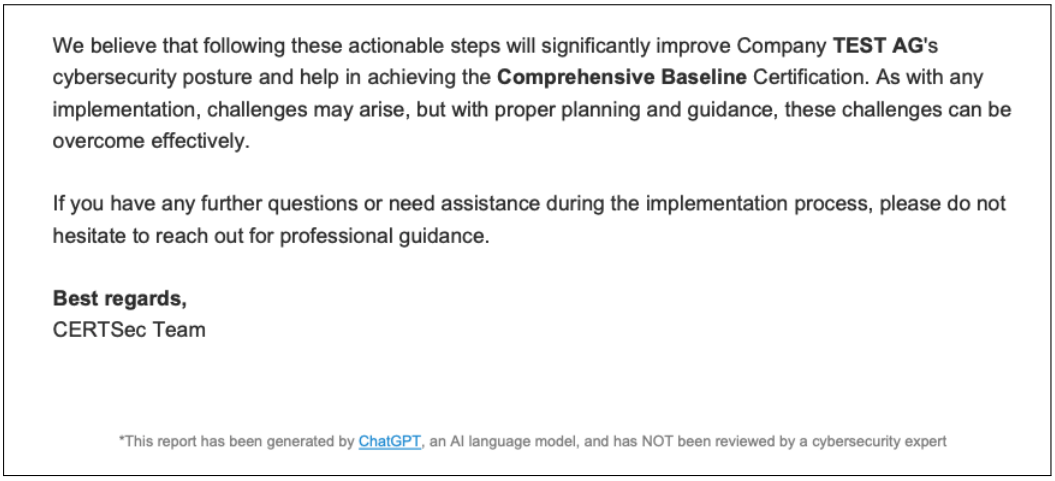
Date: 28.06.2023
To: TEST AG
From: CERTSec Automated Report Generation Tool

Subject: Actionable Steps to Fulfill the Remaining Comprehensive Baseline Certification Requirements

Dear Management of Company **TEST AG**,

Congratulations on your decision to pursue the **Comprehensive Baseline** Certification! To fulfill each of the requirements, please find below detailed guidance with actionable steps, benefits, estimated timeline, and potential challenges:

Figure 4.5: Title Page of Generated Report



We believe that following these actionable steps will significantly improve Company **TEST AG**'s cybersecurity posture and help in achieving the **Comprehensive Baseline** Certification. As with any implementation, challenges may arise, but with proper planning and guidance, these challenges can be overcome effectively.

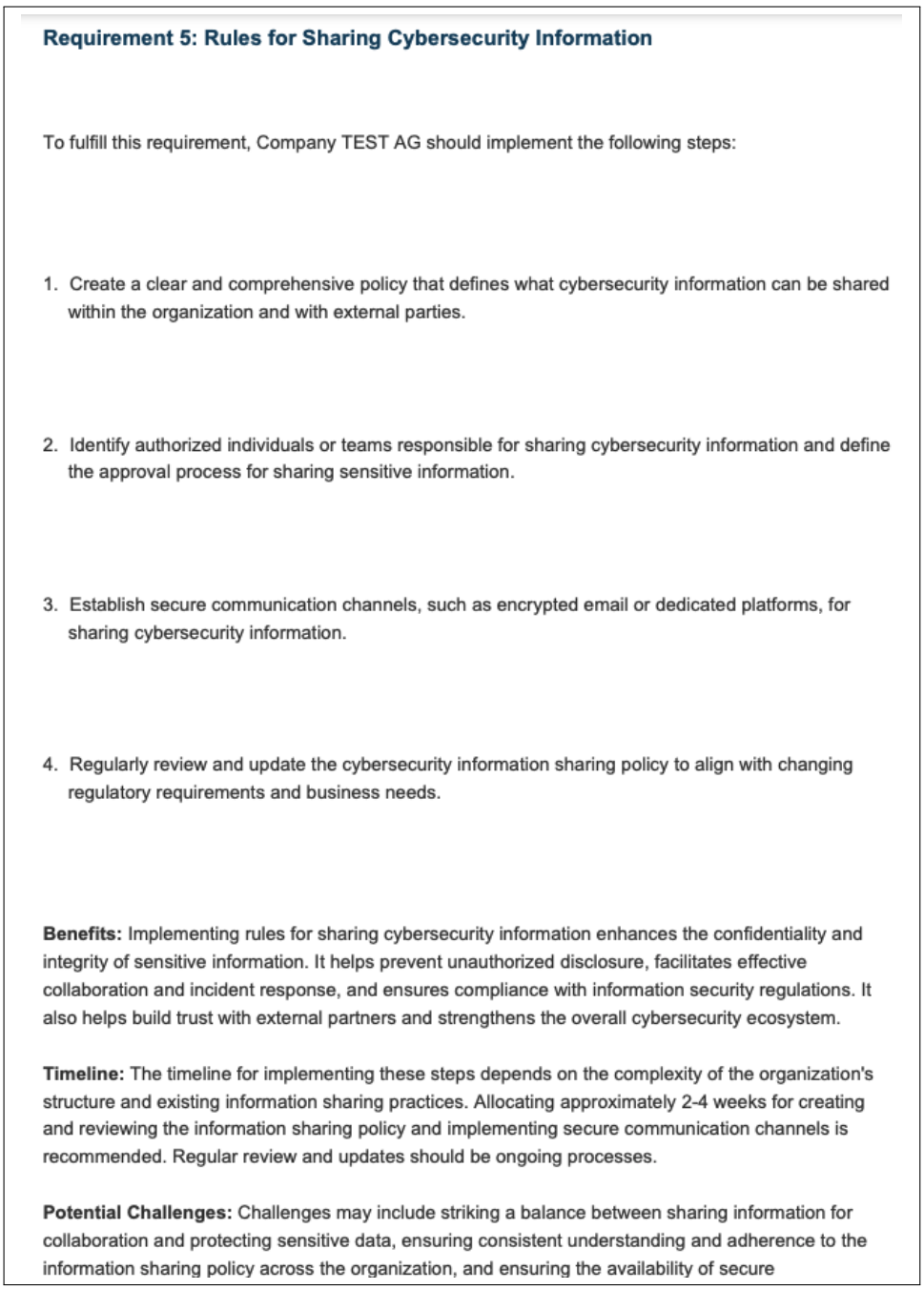
If you have any further questions or need assistance during the implementation process, please do not hesitate to reach out for professional guidance.

Best regards,
CERTSec Team

*This report has been generated by ChatGPT, an AI language model, and has NOT been reviewed by a cybersecurity expert

Figure 4.6: Final Page of Generated Report

Figure 4.7 presents a demonstrative example of the report's guidance for a specific requirement. The presentation of this guidance starts with the title of the requirement, followed by a series of recommended steps to address it. It is worth noting that due to the generative nature, the number of these steps may vary across different reports and corresponding requirements. Subsequently, benefits, timeline, and potential challenges associated with these steps are detailed. By offering this comprehensive perspective, the report equips users with a thorough understanding of the measures needed to fulfill the requirement effectively.



Requirement 5: Rules for Sharing Cybersecurity Information

To fulfill this requirement, Company TEST AG should implement the following steps:

1. Create a clear and comprehensive policy that defines what cybersecurity information can be shared within the organization and with external parties.

2. Identify authorized individuals or teams responsible for sharing cybersecurity information and define the approval process for sharing sensitive information.

3. Establish secure communication channels, such as encrypted email or dedicated platforms, for sharing cybersecurity information.

4. Regularly review and update the cybersecurity information sharing policy to align with changing regulatory requirements and business needs.

Benefits: Implementing rules for sharing cybersecurity information enhances the confidentiality and integrity of sensitive information. It helps prevent unauthorized disclosure, facilitates effective collaboration and incident response, and ensures compliance with information security regulations. It also helps build trust with external partners and strengthens the overall cybersecurity ecosystem.

Timeline: The timeline for implementing these steps depends on the complexity of the organization's structure and existing information sharing practices. Allocating approximately 2-4 weeks for creating and reviewing the information sharing policy and implementing secure communication channels is recommended. Regular review and updates should be ongoing processes.

Potential Challenges: Challenges may include striking a balance between sharing information for collaboration and protecting sensitive data, ensuring consistent understanding and adherence to the information sharing policy across the organization, and ensuring the availability of secure

Figure 4.7: Example Recommendation of Generated Report

Although the layout and content of each report are generated from scratch, certain elements such as the title and final page (excluding specific company name, date of creation, and certificate details) remain consistent across all reports. Similarly, the format for requirements guidance is also consistent across each page, encompassing essential sections such as the title, steps, benefits, timeline, and potential challenges. This consistency ensures a level of uniformity and recognizable branding, even within the dynamic nature of the generated content.

4.3.3 User Interface

The frontend of the prototype is comprised of multiple, task-specific pages. The following paragraphs will delve into a more detailed examination of the key pages that play a crucial role in the operation of the prototype. A corresponding demo video showcasing all features is provided in [95].

As described in Section 4.3.2, businesses can leverage the power of the automated features to accelerate and streamline the verification process of the proposed certification scheme. In this sense, before starting the TB certification process (*cf.* Section 4.2), companies are required to provide relevant data beforehand. The corresponding user-friendly page (*cf.* Figure 4.8) assists businesses in providing this necessary information. Beyond the company name, businesses are encouraged to provide their IP addresses, enabling the system to carry out analyses for potential network vulnerabilities.

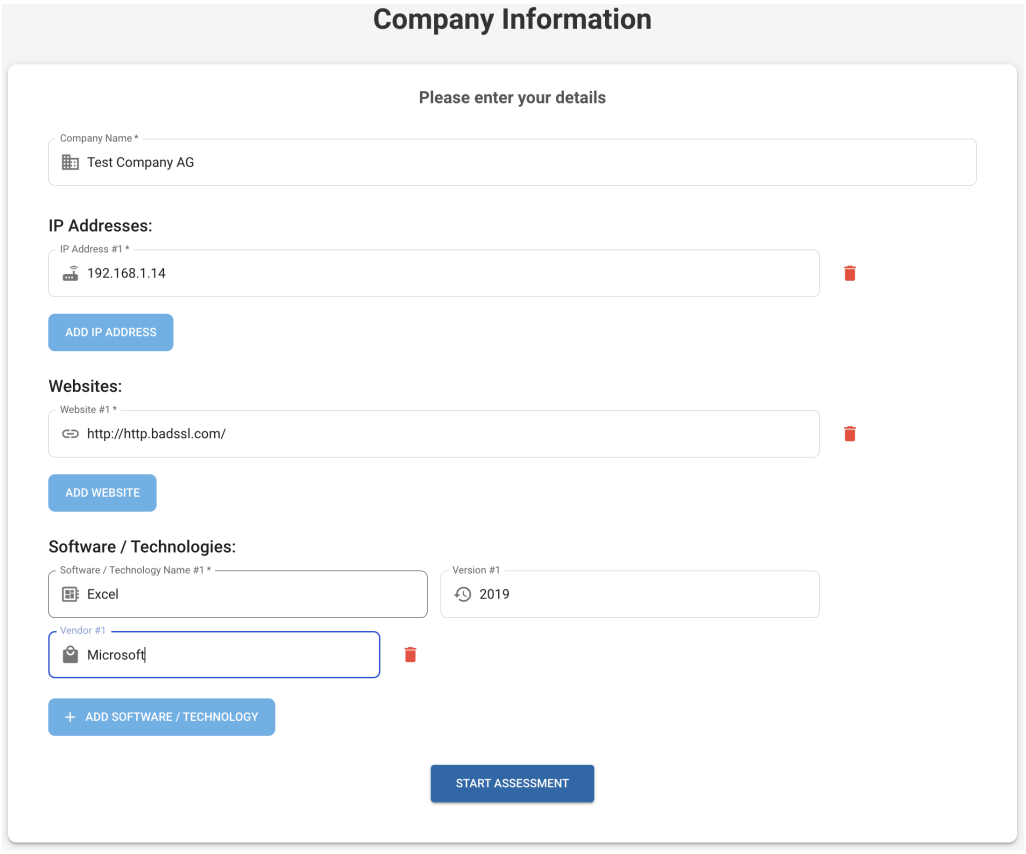


Figure 4.8: Provision of Relevant Information

Moreover, in the interest of security, the system also allows businesses to submit their public-facing websites for inspection. This allows the prototype to evaluate whether these websites establish secure connections with their stakeholder. Finally, to further strengthen security checks, the prototype also examines the technologies and software used by companies. This is important to identify and mitigate any vulnerabilities that could be exploited for cyber attacks.

Upon the provision of all relevant data, the assessment can be launched, and the user is directed to the next page, illustrated in Figure 4.9. This page features a list of all requirements for each category where users must verify their compliance with each requirement. For requirements subject to automated verification, users receive continuous visual feedback.

For example, in the case of the second requirement depicted in the figure, the verification process has concluded. The result is then displayed on the right and flagged as *No-based on automated verification*. This indicates an issue with the provided websites. During the automated verification of the subsequent requirement, the system detected the presence of well-known open ports operating services. In such cases, the verification relies on both the automated results and manual input from the user, who must now affirm the implementation of security measures to prevent unauthorized access through these ports. If the verification process is still in progress, the respective requirement will be appropriately flagged, as seen in the last requirement.

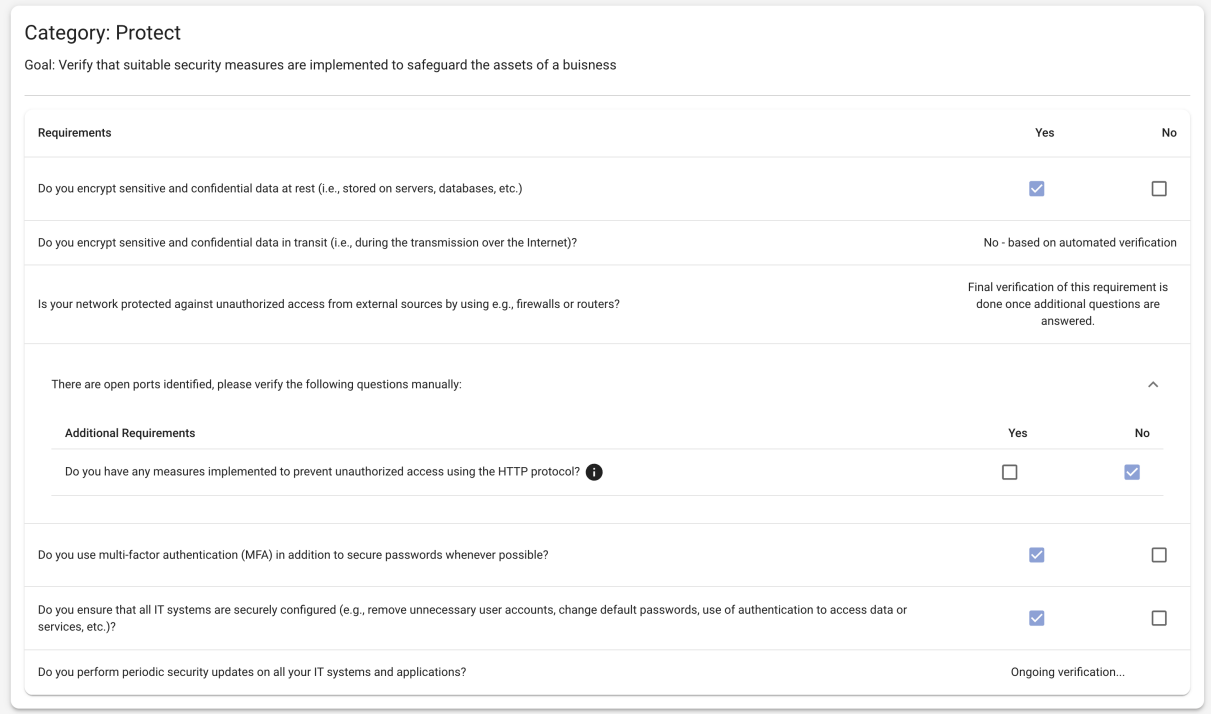


Figure 4.9: Manual and Automated Verification

Once all requirements have been addressed and the automated verification has completed, the user is redirected to the evaluation page where the results of this assessment are presented. There, the outcomes of the assessment are succinctly displayed, offering users

a clear perspective on their compliance status. Each category is evaluated separately, with clear indicators showing whether each requirement has been met or not.

As demonstrated in Figure 4.10, apart from a textual hint, color cues are also provided to enhance user understanding at a glance. The color green symbolizes fulfilled requirements, while red signifies unfulfilled ones, thereby creating an intuitive and straightforward visual guide.

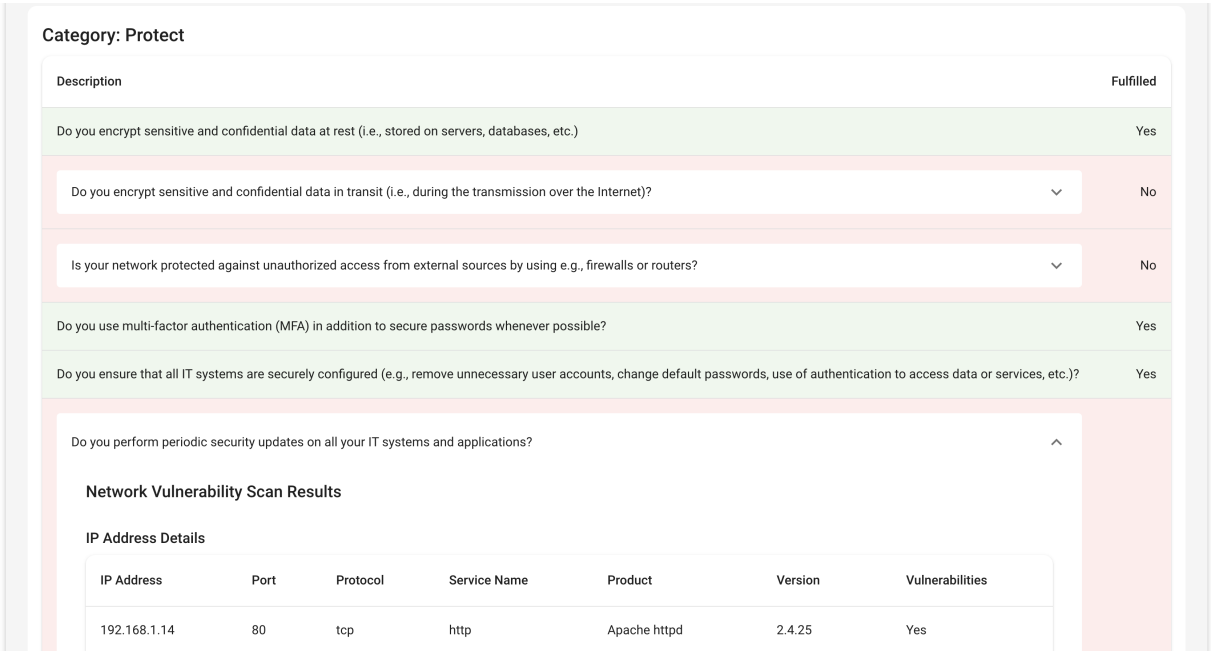


Figure 4.10: Evaluation of Automated Requirements

In instances involving automated verification, the corresponding requirements are complemented with an interactive accordion component. Users can expand this element to delve into the specifics of the results and gain an understanding of the success or failure

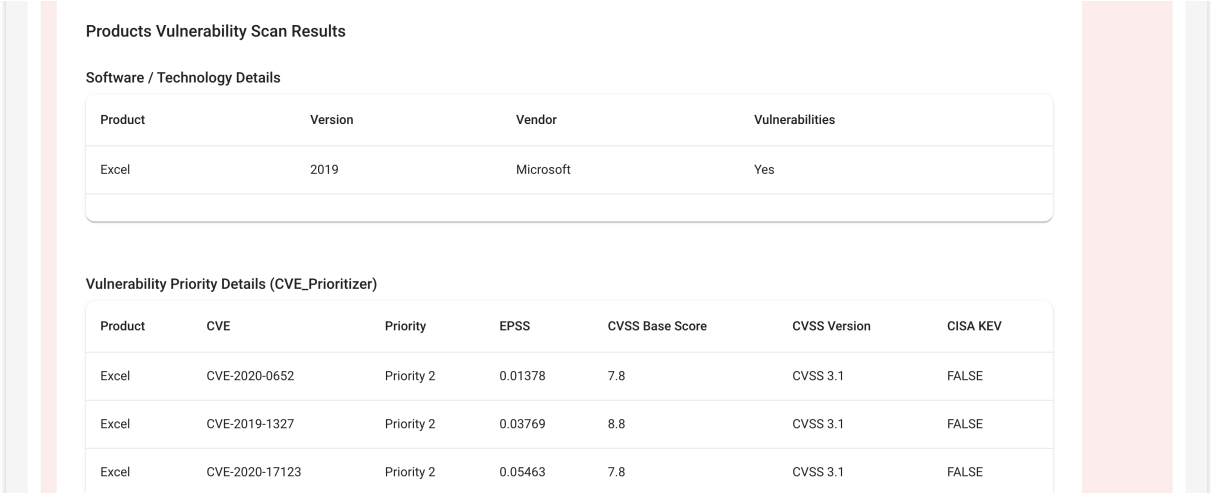


Figure 4.11: Tabular Representation of Automated Verification Results

of certain requirements. Figure 4.11 showcases the results obtained from the automated verification of the technology vulnerability analysis. The data is presented in a tabular layout, optimized for clarity and accessibility. This structure helps users to quickly assimilate critical information, providing them with actionable insights.

Moreover, the evaluation page features a summary at the top, indicating whether the evaluated company has successfully passed the assessment for the sought-after certification, as highlighted in Figure 4.12. This concise summary offers an immediate understanding of the certification status, streamlining the user's experience.

To the right, additional options are available, offering advanced functionalities. For example, users have the option to download a JSON file that encapsulates all data derived from the automated verification process, thus facilitating further automated analysis. Also, they can generate an insightful report with the help of artificial intelligence, as discussed in Section 4.3.2.

Finally, it is worth noting that the layout and structure of the pages described in this section remain consistent across all three certifications (*i.e.,* TB, CAB, and COB). This uniformity ensures a smooth and predictable user experience, reducing the learning curve while navigating different certification processes.

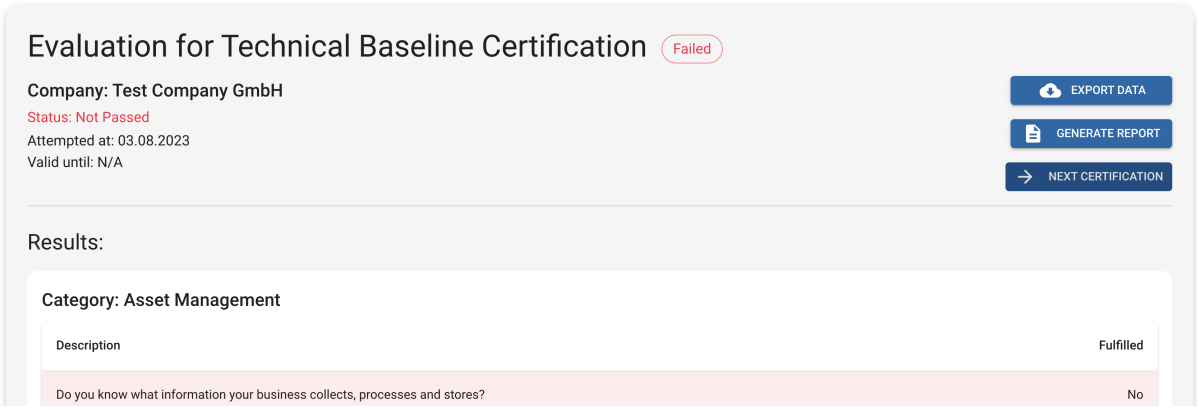


Figure 4.12: Outcome of the Assessment

4.3.4 Deployment

The deployment strategy for CERTSec is a significant aspect that can affect its usability, efficiency, and scope. Three potential deployment approaches can be considered: private, public, and hybrid.

The private deployment strategy involves offering CERTSec as a downloadable tool that businesses install and operate within their own infrastructure. This method would grant the tool comprehensive access to both public and private network components, thereby enabling a more detailed security assessment. Additionally, businesses would retain all sensitive information in-house, thus mitigating concerns regarding data storage. Nevertheless, the process of issuing certifications in such cases is an aspect that requires further consideration.

On the contrary, a public deployment would involve hosting CERTSec on a publicly accessible web server. This configuration allows businesses to easily engage with the tool by simply accessing the website, inputting the required information, and initiating the certification process. This model of deployment is the most accessible method, requiring no installation or setup on the user part. However, its scope is limited to the examination of public-facing services and IPs. This constraint could result in potential blind spots, especially when it comes to vulnerabilities residing within a company's local or internal networks that are not exposed to the public internet.

The third option, the hybrid deployment, aims to leverage the advantages offered by both private and public deployment strategies. CERTSec could be offered as a downloadable tool for a detailed local network analysis, while also maintaining a web server for probing public-facing services. The results from these parallel analyses could be integrated at the client-side. While this method maintains the comprehensive analysis capability of a private deployment and the convenience and accessibility of public deployment, it may also entail challenges inherent to both models, such as client-side setup requirements, limited scope of public-facing services for the web component and arising complexities when integrating results from both analyses.

Chapter 5

Evaluation

This chapter has a three-fold objective, each designed to thoroughly evaluate CERTSec's performance and potential. Initially, the focus is on benchmarking the secure connection feature (*i.e.,* HTTP vs HTTPS) of CERTSec against a practical real-world tool to determine its comparative advantages and disadvantages. Subsequently, the efficiency of the prototype's automated assessment features is evaluated to determine its scalability and overall performance, including CPU usage and memory consumption analyses for specific tasks. The chapter concludes with a practical case study to clearly demonstrate the potential application of CERTSec and its usefulness in real-world scenarios.

These experiments were defined in order to highlight the feasibility of key features used for the automation of the certification scheme processes (*e.g.,* identifying insecure Websites, vulnerabilities, and factors that increase the risks of cyber attacks). Additional features can be implemented and evaluated similarly in order to ensure that the automation is providing complete and rich information for the certification process. Our results show that it is possible to conduct automation for risk analysis without significant impacts (in terms of resource consumption and overall time spent) on the entire process.

5.1 Analysis of Secure Websites

Securing connections between Websites and end users is of utmost importance, as it not only helps maintain user trust but also safeguards sensitive information against potential adversaries. In order to evaluate the effectiveness of CERTSec's specially designed feature, which verifies the usage of the HTTPS protocol and ensures no issues with the SSL certificate of a Website, it is crucial to compare the results with those obtained from an automated tool that is widely used in real-world scenarios. This comparison will provide valuable insights into the accuracy and reliability of CERTSec's custom-built feature.

5.1.1 Design and Experiment

For this comparative evaluation, we selected the SEO Site Checkup [103] as the automated tool to benchmark against CERTSec. It is a commercial, reputable and widely recognized tool that is known for its ability to perform comprehensive analysis and evaluation of various aspects of Website performance, with a primary focus on Search Engine Optimization (SEO), including security considerations.

To ensure a diverse and representative set of Websites, we carefully curated a list of 30 Websites for the evaluation. The selection process involved two main criteria. Firstly, we leveraged the Tranco list [104], a trusted and frequently updated ranking of top Websites based on their popularity and traffic. Specifically, we extracted 20 Websites from the Tranco list, encompassing both the top 10 most popular Websites and the 10 least popular Websites. This approach allows us to evaluate CERTSec's performance across a range of Websites with varying levels of traffic and user engagement.

Moreover, in order to specifically evaluate CERTSec's capability to detect insecure connections (*e.g.,* Websites using the HTTP protocol or facing SSL certificate-related issues) we also incorporated an additional set of 10 Websites obtained from *badssl.com* [105], which is composed of intentionally designed Websites featuring insecure connections or exhibiting various misconfigurations and vulnerabilities in their SSL certificates. By including these Websites, an ideal testing environment is created to assess CERTSec's effectiveness in accurately identifying and reporting security issues.

5.1.2 Analysis and Results

Figure 5.1 shows, for each tool compared, the number of Websites identified as using either the HTTPS or HTTP protocol. It is worth noting, however, that this representation does not take into account any SSL certificate related issues, like the employment of self-signed certificates by HTTPS-based Websites.

Reviewing this data, it can be observed that CERTSec successfully classified 18 Websites as using the HTTPS protocol and 6 as using the HTTP protocol. In contrast, the SEO Site Checkup tool was able to detect 5 Websites using HTTP and 16 using HTTPS. This represents an interesting pattern, as it highlights the different efficiency of the two tools in categorizing Websites based on the protocols used. Furthermore, out of the total 30 Websites examined, CERTSec was unable to analyze 6 of these Websites. Even more surprisingly, the commercial product, SEO Site Checkup, was unable to analyze 9 of the 30 Websites, which is 3 more than the proposed prototype.

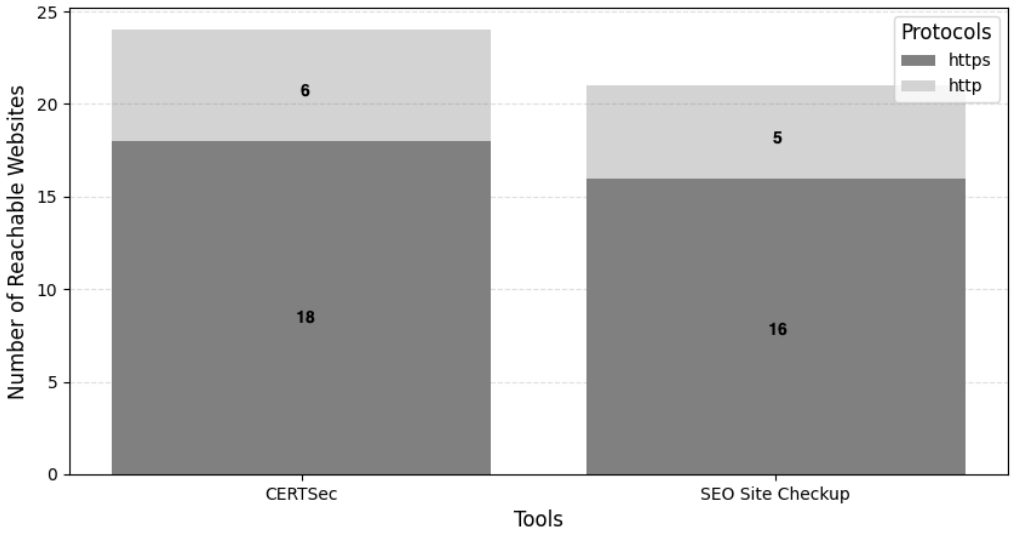


Figure 5.1: Comparison of Identified Protocols

Figure 5.2 provides an extensive comparison between the CERTSec and SEO Site Checkup tools. The first entries represent the top 10 most popular Websites (*i.e.,* from google.com to instagram.com) as per the Tranco list mentioned previously. The next set of 10 Websites showcase the least popular ones, while the final 10 display intentionally insecurely designed Websites drawn from *badssl.com*.

The second column (*i.e.,* Protocol) shows the agreement or disagreement between the two tools regarding the identification of the protocol for each Website. The term *Match* denotes instances where both tools identified the same protocol, while *Mismatch* points to disagreements. *N/A* is recorded for incomparable results, such as when one tool identifies a protocol, and the other fails, or when neither tool can analyze the protocol due to error occurrences.

Subsequently, the third column (*i.e.,* Error) highlights the agreement between the tools in identifying the same errors. For example, for *google.com*, both CERTSec and SEO Site Checkup agree on the Website's protocol, leading to a *Match* being recorded. The absence of errors is denoted accordingly by *N/A* in the corresponding error cell.

Examining *amazonaws.com* reveals that both tools failed to identify the protocol in use. However, the recorded *Mismatch* means that different errors were returned by the two tools. Another interesting example is the *https://expired.badssl.com/*, where both CERTSec and SEO Site Checkup recognized the HTTPS protocol, as well as agreed that the Website employs a self-signed certificate, leading to a *Match* in both cells. However, for *https://untrusted-root.badssl.com/*, despite the matching identified protocols, the error messages returned by the tools differed.

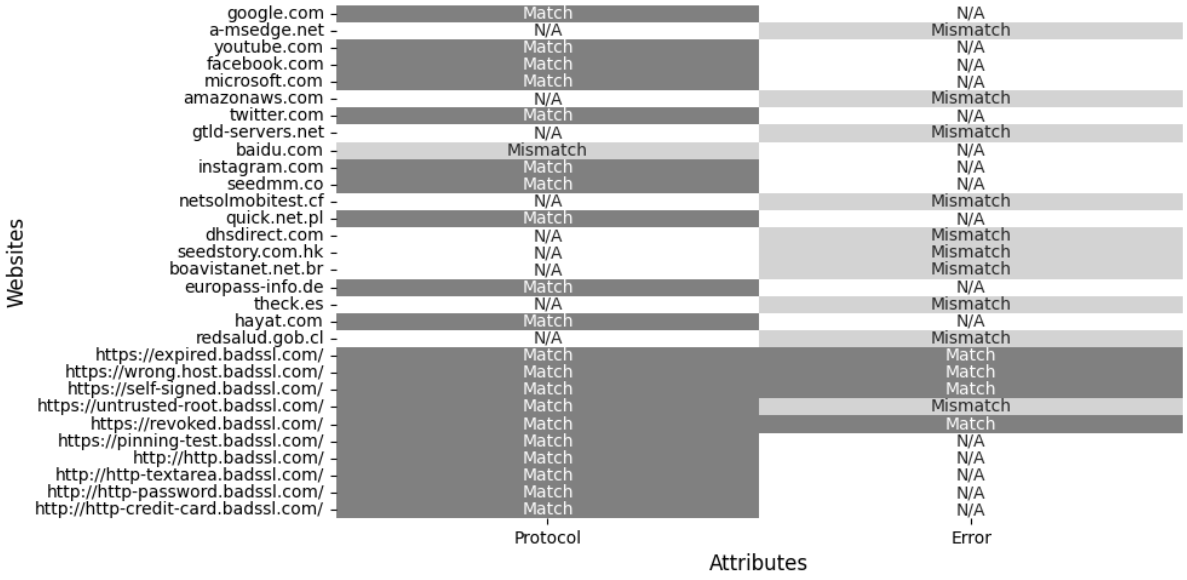


Figure 5.2: Visualization of Agreement Between CERTSec and SEO Site Checkup

Moreover, for the 10 most popular Websites, both tools agreed on the protocol for 6 sites. There was one mismatch and three non-comparable results. For the least 10 popular Websites, there was 6 non-comparable results (*i.e.,* due to errors). For the other 4 Websites, both tools agreed on the protocols. Lastly, by examining the insecure Websites, it can be observed that both tools matched on all protocols. Of the 5 comparable errors, there was agreement in four cases.

Figure 5.3 aggregates these observations and provides an overview. In summary, CERTSec and SEO Site Checkup agreed on the protocol for 20 Websites, with only one disagreement. Due to SEO Site Checkup's inability to identify the protocol for 9 Websites, only 21

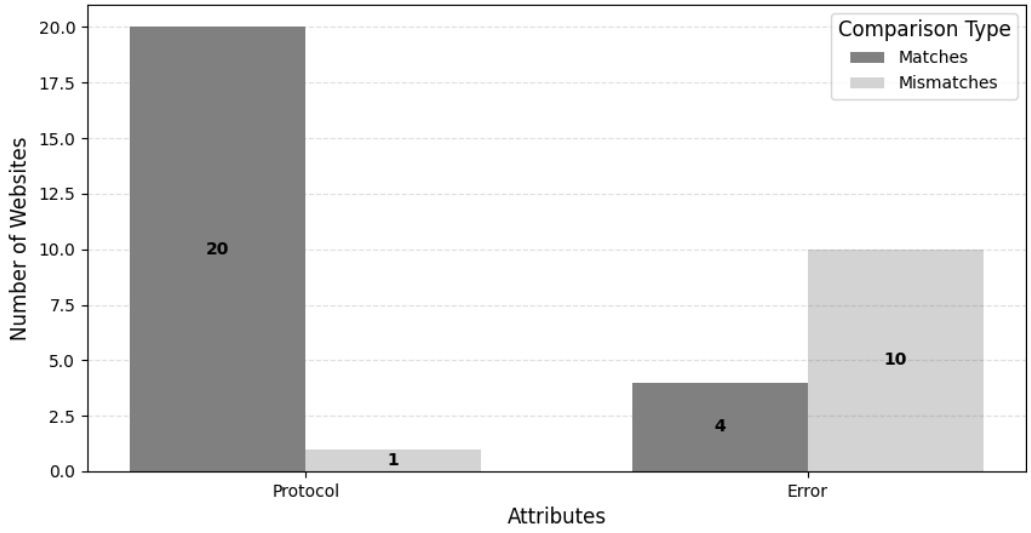


Figure 5.3: Aggregated Results of Matches and Mismatches

Websites' results could be mutually compared. In terms of errors, there were 4 matches, all relating to SSL certificate issues. Interestingly, there were 10 mismatches for the Websites from the Tranco list.

5.1.3 Discussion and Limitations

The comparison of CERTSec with SEO Site Checkup, a commercial offering, offers considerable insights into the strengths and weaknesses of both tools. The testing methodology involved evaluating these tools against Websites of diverse popularity and security profiles, obtained from the Tranco list and *badssl.com*. The former represents a wide spectrum of real-world scenarios, while the latter presents a collection of intentionally insecure Websites, thus, enabling an extensive analysis of both tools' error detection capabilities.

The analysis demonstrated that CERTSec, despite being a freely available prototype in its early stage, can deliver comprehensive and detailed results. In terms of protocol identification, both tools exhibited comparable performance, showing a consensus in 20 out of 21 mutual evaluations. These features evaluated are relevant for the certification scheme provided by CERTSec since automation of certain tasks are critical for an adequate risk analysis when conducting cybersecurity planning and certification activities.

Nevertheless, the analysis uncovered certain limitations that need consideration. The Websites selected for this study were picked based on their popularity rankings, without pre-checking their availability (*cf.* Section 5.1.1). This approach potentially undermines the real-world validity of the analysis. Specifically, CERTSec encountered difficulties when classifying 6 Websites due to unresolved domain names, refused connections, or operation timeouts, as detailed in Table 5.1. Conversely, SEO Site Checkup could not determine the protocol for 9 Websites, responding with a generic error message in each case.

Interestingly, the manner in which both tools responded to these limitations differed significantly. CERTSec offered a more detailed analysis of the encountered issues, providing specific reasons for each failure. This offers users an informative perspective and could facilitate further troubleshooting. In contrast, SEO Site Checkup responded with a generic error message that does not provide this level of clarity: *"We cannot access your Website in order to perform our test! Either the site is not online, or our tool is being blocked by your server. Try again or Try another URL".*

In terms of error detection, CERTSec outperformed SEO Site Checkup, identifying 7 SSL certificate-related issues as opposed to SEO Site Checkup's 5. This observation underscores CERTSec's potential for detecting more subtle security issues.

Overall, these findings highlight the value that CERTSec brings to the table. It not only holds its own against a commercial product but in some aspects, such as detailed error reporting and SSL certificate issue detection, it outperforms the latter.

Table 5.1: Comparison of Error Distribution

Error Type	CERTSec	SEO Site Checkup
The Website could not be resolved	3 (10.00%)	N/A
The host is refusing the connection	1 (3.33%)	N/A
Operation timeout: network issue or server unavailable	2 (6.67%)	N/A
Generic Error	N/A	9 (30.00%)
SSL Certificate Issues	7 (23.33%)	5 (16.67%)
No Errors	17 (56.67%)	16 (53.33%)

5.2 Performance of Automated Assessments

An evaluation of the performance of CERTSec's automated feature has been conducted by analyzing metrics such as CPU usage, memory usage, and/or response time across ten runs. Among the suite of features offered by CERTSec, our tests focused on the *HTTPS Check* and the *Technology Vulnerability Scan*. The *Network Vulnerability Scan* feature was deliberately excluded from our evaluation since it relies on the Nmap tool and, therefore, is out of scope. Evaluations regarding Nmap tool can be found in the literature, such as in [106] and [107].

The mean values were computed for all measured metrics. This process was automated through a script, triggered by a cron job every hour when all other system resources were idle, thus, ensuring minimal interference from other processes. The tests were conducted on a MacBook Pro equipped with an Apple M1 Pro chip and 32GB of memory.

5.2.1 HTTPS Checker

This section evaluates the performance of CERTSec's feature, which determines if a Website securely transmits data over the network. Figure 5.4 presents the average CPU usage observed while analyzing 1, 10, and 100 Websites. The tested Websites were obtained from the top 100 entries in the Tranco list and represent a diverse range of real-world Websites, each with varying traffic and availability.

Intuitively, one might expect CPU usage to increase proportionately with the number of Websites analyzed. However, the results show an inverse relationship: average CPU usage decreased as the number of Websites increased. Analysis of a single Website registered a

CPU usage of 15.94%. This figure dropped to 9.14% for ten Websites and further reduced to 5.01% when analyzing 100 Websites.

At first sight, these results seem intriguing and counter-intuitive. However, further analysis of the `check_https_connection_taks` method (*cf.* `backend/compliance/tasks.py` in [95]) provides explanations for this behavior. One influential factor is the prevalence of Input/Output (I/O) bound operations. While checking a Website, the program spends significant time awaiting the Website's response, during which CPU utilization is minimal. We make two requests: *(i)* identify the protocol used and *(ii)* establish a socket-based connection for verifying the SSL certificate. As the number of sites in the test set increases, the total time spent waiting on I/O operations also grows, leading to reduced average CPU usage.

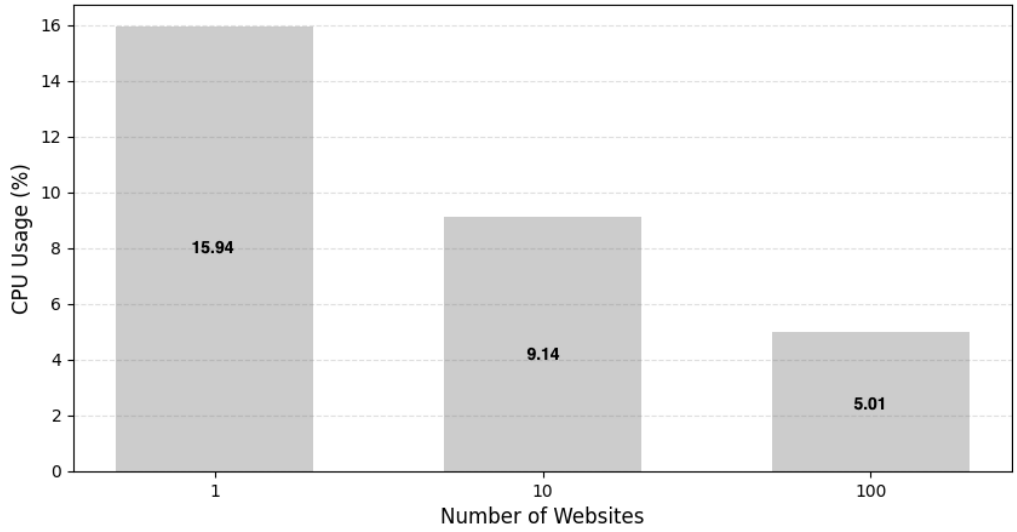


Figure 5.4: Average CPU Usage (%)

Furthermore, the data processing involved in these checks (*e.g.,* URL parsing and dictionary manipulations) is not CPU-intensive. The procedures are lightweight and do not require substantial computational resources. Consequently, as the number of Websites processed grows, the relative time the CPU spends idle (waiting for I/O) compared to the time spent processing data increases, thus, resulting in a decrease in average CPU usage.

Figure 5.5 depicts the mean memory utilization for the varying data set sizes. As can be observed, the memory usage incrementally grows with an increase in the number of Websites assessed. This behavior is expected given that the `results` dictionary keeps growing as more Websites are processed.

However, it is noteworthy to mention that the memory growth is not linear, which may be attributed to Python's garbage collection that frees up memory occupied by temporary objects. Additionally, this could also be due to certain inherent efficiencies in Python's memory management, particularly when handling large data structures.

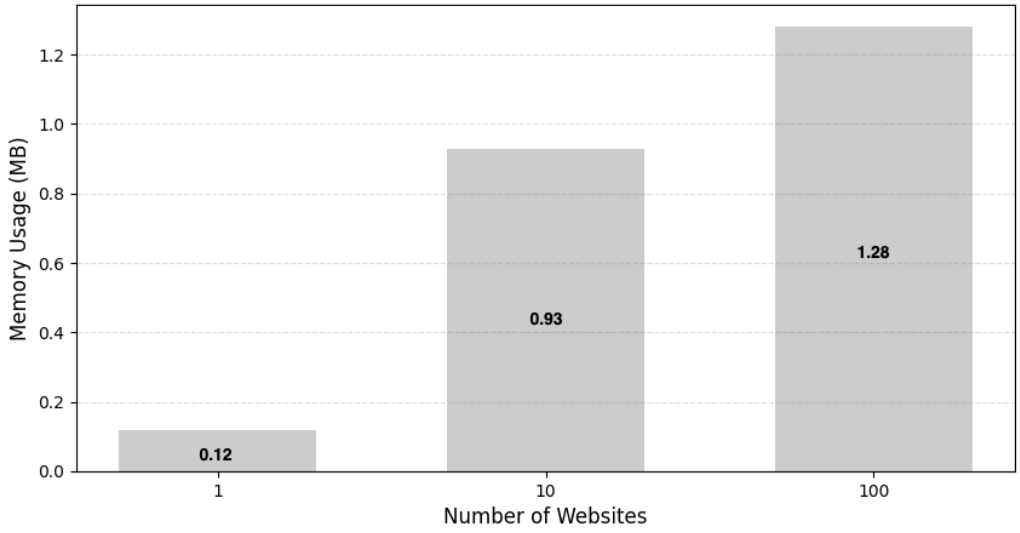


Figure 5.5: Average Memory Usage (MB)

Interestingly, despite the growth in memory utilization with larger datasets, the overall memory usage remains relatively low. Memory usage is only 0.12 MB for a single Website, increasing to 0.93 MB for 10 Websites, and further to 1.28 MB for 100 Websites. This modest memory requirement can also be attributed to the minimal creation of large and complex objects in the code. Consequently, the memory overhead remains low, even with the increasing number of Websites.

Figure 5.6 delineates the average response time for 1, 10, and 100 Websites. One observation is the significant increase in response time as the number of Websites increases. This behavior aligns with our expectations, given that the program processes each Website in

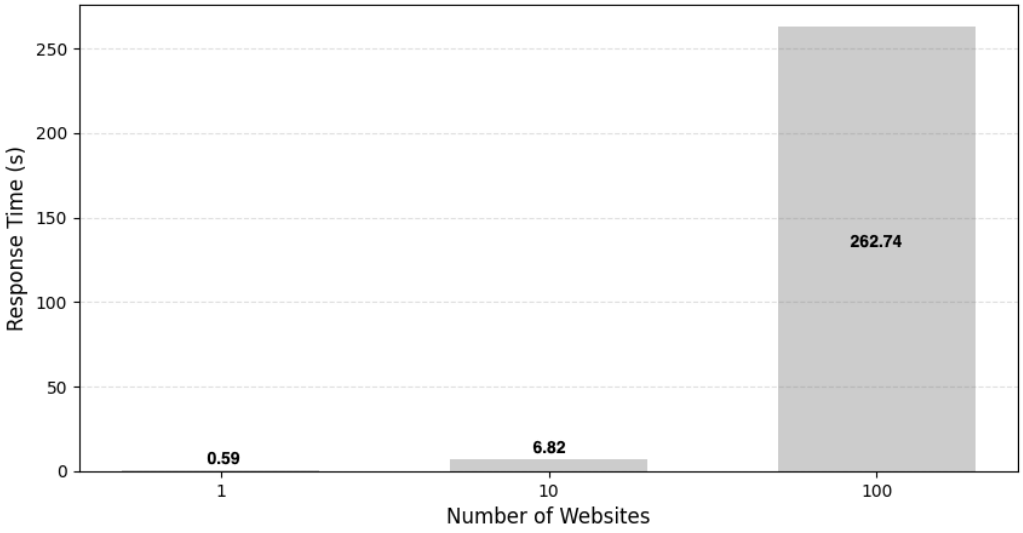


Figure 5.6: Average Response Times (s)

a sequential manner. Therefore, the total execution time should roughly be proportional to the number of Websites.

However, the unexpectedly large jump in response time when progressing from 10 to 100 Websites could be explained due to network effects, such as increased latency or rate limiting by servers. Moreover, this discrepancy could also indicate that certain Websites are slower in responding than others or do not respond at all. Although our evaluation employed the top 100 Websites from the Tranco list, their availability was not verified. This implies that the program might attempt to establish a connection with the host until reaching the specified timeout, thereby inflating the response time.

5.2.2 Technology Vulnerability Scan

The CERTSec's technology vulnerability scan feature was also evaluated as it is a core feature for the risk analysis during the certification process. As this feature relies extensively on external APIs to detect and prioritize vulnerabilities, it is notably I/O bound. Consequently, our primary focus is on the response time.

For this evaluation, three distinct scenarios depicting companies of varying sizes and their respective technologies are defined. Each experiment was conducted ten times, encompassing 1, 5, and 10 technologies, which were used as underlying infrastructure of the hypothetical companies defined in Scenario A, B, and C, respectively. Moreover, all selected technologies are known to contain vulnerabilities, allowing us to observe how the prototype manages rate limiting as enforced by the NVD API. For this experiment, a corresponding API key has been obtained which increased the limit from 5 to 50 requests in a rolling 30-second window [100]. The overall results are shown and discussed in the end of this subsection, especially in Figure 5.7.

Scenario A: Small E-Commerce Business with 1 Technology

Suppose the QuickShopster Tech is an emerging e-commerce startup with a small but motivated team of 10 employees. This start-up specializes in the online sale of gadgets and tech accessories. Despite its size, QuickShopster Tech has successfully garnered an impressive user base. Its philosophy revolves around simplicity and efficiency, which is reflected in their streamlined tech stack.

The foundation of QuickShopster's digital infrastructure is the Apache HTTP Server (*cf.* Table 5.2). This server technology is an integral part of QuickShopster's operations, delivering their e-commerce Website to their growing customer base. Its reliable performance and robustness have been pivotal in ensuring smooth and seamless user experiences, a critical factor driving the company's growth.

Table 5.2: Sample Technologies for Small E-Commerce Business

#	Vendor	Technology/Software	Version	#Vulnerabilities
1	Apache	HTTP_Server	2.4.46	34

Scenario B: Large E-Commerce Business with 5 Technologies

NextBuyDirect e-commerce is a successful online retailer offering a diverse range of products across various categories. With a workforce of 75, NextBuyDirect relies heavily on a broad array of technologies for its operations, including server software, databases, and web technologies (*cf.* Table 5.3).

At the heart of NextBuyDirect's digital operations is the Apache HTTP Server, delivering their Website's content to a wide array of users. Accompanying this, the Oracle MySQL database management system is responsible for managing their extensive product catalog and user data. For handling server-side scripting, they rely on PHP, which works seamlessly with their chosen server software and database. Microsoft's Windows Server acts as their operating system of choice for their servers, delivering reliability and ease of use. Lastly, OpenSSL plays a crucial role in ensuring secure and encrypted communication over their networks. The synergy between these technologies provides NextBuyDirect with a robust and secure platform to carry out their e-commerce operations.

Table 5.3: Sample Technologies for Larger E-Commerce Business

#	Vendor	Technology/Software	Version	#Vulnerabilities
1	Apache	HTTP_Server	2.4.46	34
2	Oracle	MySQL	8.0.19	368
3	-	PHP	7.4.11	17
4	Microsoft	windows_server	2019	1
5	OpenSSL	OpenSSL	1.1.1h	21

Scenario C: Large E-Commerce Business with 10 Technologies

MegaStoreXpert e-commerce is a dominant player in the online retail market with a large workforce of 250 employees. The company utilizes a myriad of technologies for

its vast operations, ranging from server software and databases to web technologies and operational tools (*cf.* Table 5.4).

MegaStoreXpert's digital architecture is built upon a foundation of robust technologies. Their Apache HTTP Server serves as the digital link between their e-commerce platform and their extensive customer base. Their huge inventory of product and user data is managed by the Oracle MySQL database system. PHP, their server-side scripting software, works seamlessly with their database and server software to deliver dynamic web content. Complementing this setup, the Microsoft Windows Server acts as the reliable operating system for their servers. OpenSSL, an essential piece in their security puzzle, secures their network communication with encryption.

Moreover, MegaStoreXpert's software ecosystem is further enriched with IBM's WebSphere, providing a robust application server environment, Adobe's ColdFusion for rapid web application development, and Atlassian's Jira for effective issue tracking and project management. ElasticSearch enables real-time search and analytics capabilities, ensuring quick and efficient access to critical data. Lastly, Microsoft Excel is a prerequisite in their data analysis and reporting processes.

Table 5.4: Sample Technologies for E-Commerce SME

#	**Vendor**	**Technology/Software**	**Version**	**#Vulnerabilities**
1	Apache	HTTP_Server	2.4.46	34
2	Oracle	MySQL	8.0.19	368
3	-	PHP	7.4.11	17
4	Microsoft	windows_server	2019	1
5	OpenSSL	OpenSSL	1.1.1h	21
6	IBM	WebSphere_-Application_Server	9.0.5.6	28
7	Adobe	ColdFusion	2018	49
8	Atlassian	Jira	8.13	20
9	Elastic	ElasticSearch	7.9.3	4
10	Microsoft	Excel	2019	9

Figure 5.7 presents the average response time derived from a series of experiments involving the analysis of 1, 5, and 10 technologies (*i.e.,* Scenario A, B, and C, respectively). The response time measurement encompasses both the process of querying the NVD database for known CVEs and prioritizing the discovered CVEs using the CVE Prioritizer Tool, which also relies on external APIs for the prioritization process.

This shows an anticipated rise in response time as the number of technologies analyzed increases. Notably, the rate of growth is not linear, indicating that the response time does not scale directly with the number of technologies. For a single technology (Scenario A), the average response time was registered at approximately 11.52 seconds with a standard deviation of about 3.21 seconds. As the technologies analyzed increased to 5 (Scenario B), the average response time escalated to around 77.69 seconds, marking a nearly seven-fold increase, with a standard deviation of roughly 6.78 seconds. For 10 technologies (Scenario C), the response time further grows to 115.07 seconds, which is a lesser proportionate increase despite the doubling of technologies, and with the standard deviation rising to approximately 10.33 seconds.

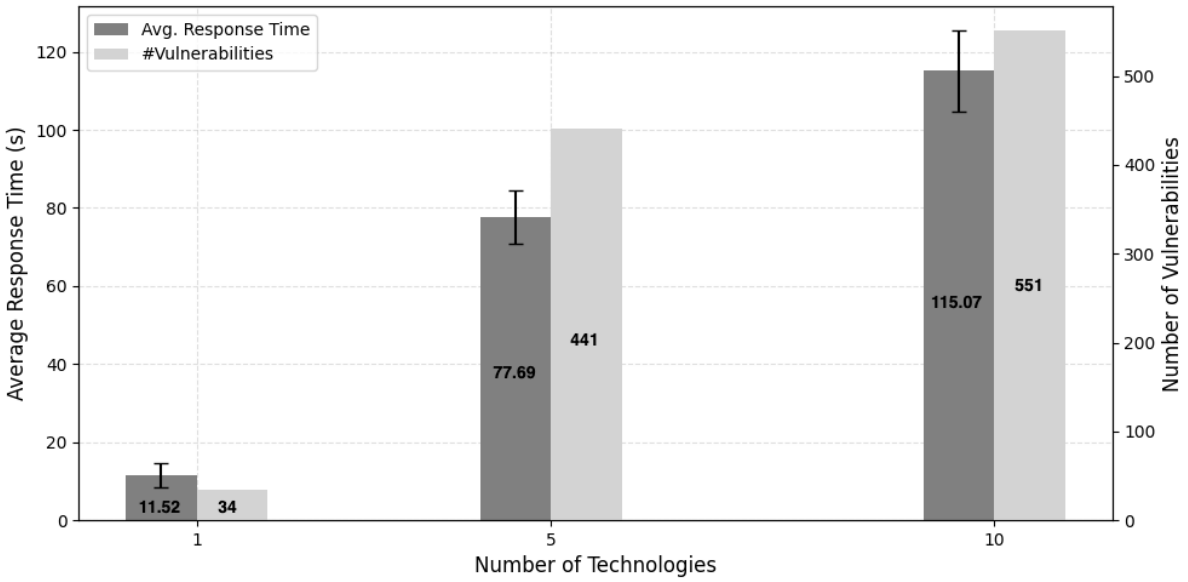


Figure 5.7: Average Response Times (s)

The non-linear growth and the increasing standard deviation suggest a greater variability in the response times when more technologies are evaluated, implying that while the mean response time provides a general estimate, the actual response time could significantly deviate from this average.

Further observations reveal a correlation between the number of vulnerabilities discovered in the technologies and the response times. During the analysis of a single technology, for instance, 34 vulnerabilities were discovered and prioritized. The sharp increase in response time for 5 technologies aligns with a substantial increase in detected vulnerabilities to 441. This represents an approximately thirteen-fold escalation, suggesting the time required to analyze and prioritize vulnerabilities plays a significant role in the overall response time.

Even though the number of technologies processed doubles from 5 to 10, the hike in response time is relatively modest, *i.e.,* 37.38 seconds. Moreover, it can also be observed that the count of vulnerabilities only expanded by 110 during this increase. Considering the experiment only leveraged technologies with vulnerabilities, it seems that the response time is more significantly affected by the total number of vulnerabilities discovered and

prioritized than by the number of technologies examined. It is important to note that the same technologies were used consistently over the ten trials ensuring a uniform count of vulnerabilities for each trial and number of technologies. Therefore, this suggests that the analysis (*i.e.,* request to NVD database) and prioritization of vulnerabilities, rather than the technologies harboring them, consume the most time. Thus, the efforts to optimize response time should be primarily directed towards enhancing the efficiency of the vulnerability examination and prioritization process.

5.2.3 Discussion and Limitations

The evaluation conducted provides important insights into the performance of the automated features. However, it is essential to discuss these results in the context of their limitations and the potential implications for scalability, especially when deploying the solution in real-world scenarios.

During the analysis of the HTTPS check feature (*cf.* Section 5.2.1), a paradoxical decrease in **CPU usage** was observed as the number of Websites processed increased. This trend, while counter-intuitive, provides reassurances in terms of scalability. As the system is expected to handle an increased workload, our results suggest that CPU resources are unlikely to be a bottleneck. However, this is tightly linked to the I/O bound nature of the tasks (*e.g.,* waiting for network requests to complete), and could change if the balance between waiting time and active processing time is changed.

The **memory usage**, though increasing with the volume of data, demonstrated only modest growth. Our findings suggest that as the number of Websites increases, memory usage does not increase in a directly proportional manner, implying the system might handle large-scale data efficiently. Yet, it is important to remember that these results might be affected by Python's garbage collection and memory management. It would therefore be necessary to examine whether this trend persists as the data set grows beyond the range we have considered.

The most prominent limitation for this feature in terms of scalability lies in the **response time**, which grew significantly as the number of Websites increased. This directly ties in with the sequential design of our program, which processes Websites one at a time. For large-scale implementations, this approach could become impractical due to long execution times. Therefore, the challenges posed by this limitation provide clear direction for future work. Optimizations such as parallel processing of Websites, for instance, could significantly improve response times and overall efficiency.

The analysis for the technology vulnerability scan feature (*cf.* Section 5.2.2) indicated a clear increase in **response time** as the number of technologies scanned for vulnerabilities increases. The sequential nature of our scanning process, where technologies are scanned one at a time, contributes significantly to this rise in response time, making scalability a challenge in scenarios where a large number of technologies require simultaneous or sequential vulnerability scanning.

Moreover, the response time has been found to be influenced significantly by the total number of vulnerabilities discovered and processed. Given that larger systems might

contain a higher number of technologies with a more substantial volume of associated vulnerabilities, it is reasonable to anticipate that the response times would escalate in such scenarios. This could impact the overall efficiency of the system and its capacity to promptly identify and address vulnerabilities.

Also, the standard deviation of the response time also increases with the number of technologies. This suggests a growing inconsistency in the response time as the system scales up, which could lead to unpredictable system behavior. Consistency in performance is crucial for any scalable system, and this variability in response time could thus pose a significant challenge to scalability. From a code perspective, CERTSec relies heavily on external services (*i.e.,* NVD database and CVE Prioritizer Tool). Any rate limits, connection errors, or performance inconsistencies in these services could directly impact the scalability of our feature. Additionally, the necessity for retries in case of such issues adds an extra overhead, potentially slowing down the system in larger scales.

All in all, these findings highlight the importance of optimizing this feature for better scalability. Possible strategies could include implementing more efficient vulnerability scanning and prioritization algorithms, exploring parallel processing techniques for handling multiple technologies at once while considering API rate limits, and improving error-handling mechanisms to reduce the number of retries.

Alternatively, reducing dependencies to external services also becomes a valid option. In this sense, localizing vulnerability information (*i.e.,* keeping this data within own infrastructure) could potentially reduce response times as the need for network request to external services is eliminated. For this purpose, tools such as CVE Search [108] can be installed locally as they consolidate vulnerability information from multiple sources, including NVD, and expose them through a local API or UI. Another approach could involve creating a local database that mirrors the information contained in the NVD database. However, it is important to note that such an approach would require regular updates to the local database to keep the vulnerability information current and comprehensive.

Nevertheless, further research and testing with a broader range of technologies and under varied conditions (*e.g.,* different hardware configurations and diverse technology sets) are necessary to validate these potential solutions and to better understand the scalability of CERTSec and its features.

5.3 Case Study

This section undertakes a case study to evaluate the usability and application of CERTSec, focusing on the prototype's main features. For the purpose of this case study, we consider the hypothetical SME, MegaStoreXpert, which has been defined as Scenario C in Section 5.2.2. As a prominent player in the online retail market, MegaStoreXpert has always prided itself on its digital infrastructure (*cf.* Table 5.4). However, in the ever-evolving landscape of cyber threats, MegaStoreXpert's management team understands that their cybersecurity posture must be continuously evaluated and reinforced.

In response to the global surge in cyber attacks, MegaStoreXpert's decision-makers have decided to revisit their cybersecurity strategy. They recognize the critical importance of early stage detection of vulnerabilities and are committed to proactively addressing any potential weaknesses in their cybersecurity defenses. Moreover, they also understand that on top of protecting their business operations, cybersecurity plays a crucial role in maintaining the trust of their stakeholders, as they need to feel confident that their data is safe when interacting with MegaStoreXpert's e-commerce platform.

Motivated by this understanding, the management team has set out to pursue a cybersecurity certification. Their initial consideration was the well-known ISO 27001, but the stringent requirements and extensive resource commitment of this certification quickly made it apparent that it was not the most feasible option for them at this stage. However, their quest for a suitable certification led them to CERTSec - a lightweight cybersecurity certification designed to assess the cybersecurity posture of SMEs.

To take full advantage of CERTSec's automated features, MegaStoreXpert's management team first has to supply relevant information. As sown in Figure 5.8, this information extends beyond the basic business name. In this sense, the team needs to provide all the relevant IP addresses associated with their business. These IP addresses are crucial in identifying potential vulnerabilities in the network infrastructure. Alongside IP addresses, the management also needs to provide the domain names that are publicly associated with their e-commerce platform. These domain names serve as the public face of MegaStore-

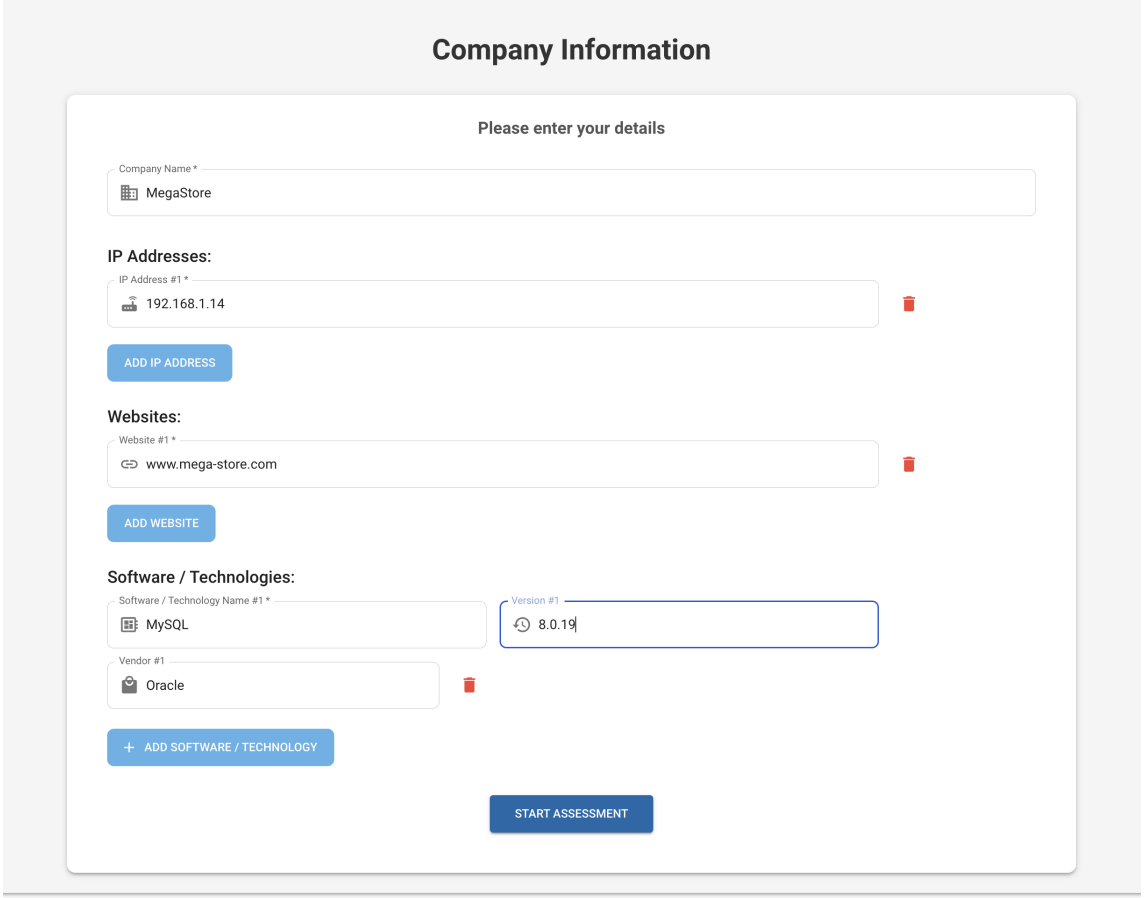


Figure 5.8: Provision of Company Information

Xpert online and are vital for assessing the security of their web presence.

Moreover, the system also allows the management team to submit a list of the software and technologies that are utilized within the company. This feature enables CERTSec to carry out a vulnerability check on these technologies, assessing whether they contain any known security issues (*i.e.,* CVEs) to be addressed. This functionality further enhances the effectiveness of CERTSec's cybersecurity assessment, providing a more comprehensive view of MegaStoreXpert's cybersecurity posture.

With all the relevant data supplied, the management team can trigger the start of the assessment. This action navigates them to the next page, as depicted in Figure 5.9. Here, MegaStoreXpert is prompted to confirm their compliance with the requirements listed under each category. While MegaStoreXpert responds to these prompts, the system simultaneously conducts its automated checking, providing real-time feedback. This automated evaluation is particularly important for the *Protect* category.

As illustrated, three questions have already been manually addressed, the rest are assessed automatically. For the second question *"Do you encrypt sensitive and confidential data in transit (i.e., during the transmission over the internet)?"*, the automated verification has already concluded, delivering a positive outcome. During the assessment of the subsequent question, CERTSec detected an open port (*i.e.,* port 80) which is commonly associated with HTTP traffic. The system prompts the management to confirm whether protective measures are in place to deny unauthorized access through this open port. For the final question in this category, CERTSec flags that the automated verification has failed, indicating a potential area of concern.

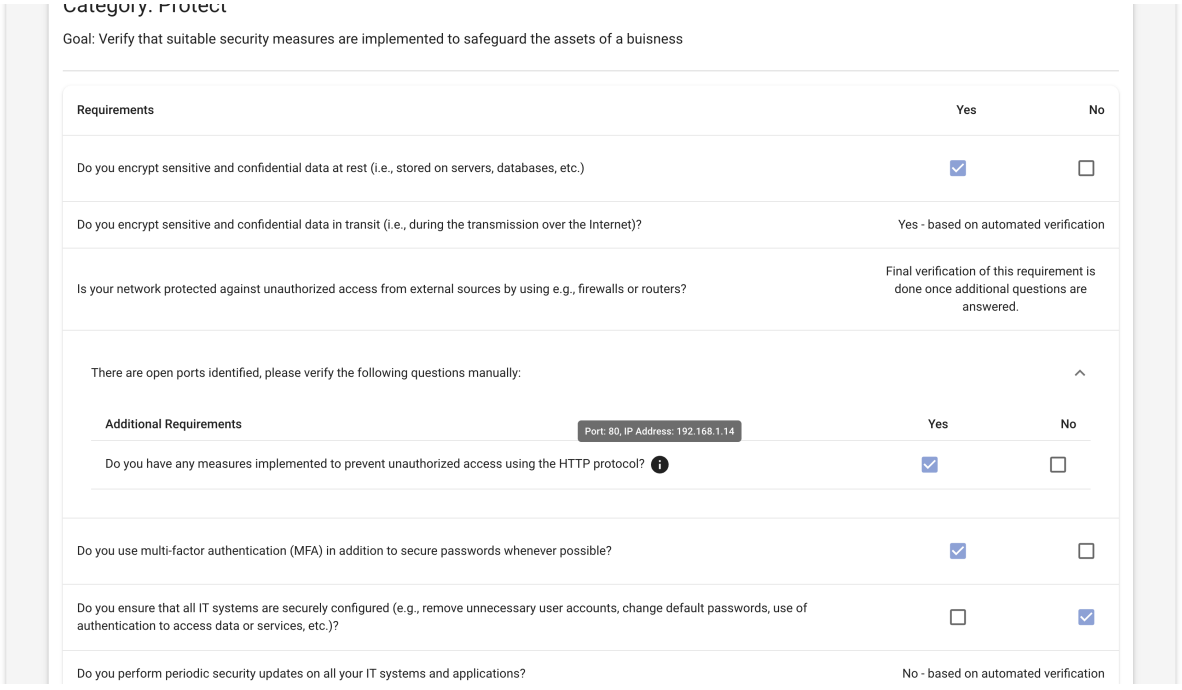


Figure 5.9: CERTSec Requirements Page

Once all the prompts for the other categories are addressed, CERTSec evaluates all the

responses to determine the success of the assessment. This process determines if MegaStoreXpert has met the outlined requirements, thus, indicating the conclusion of the assessment process.

Figure 5.10 presents the outcome of MegaStoreXpert's Technical Baseline assessment to the management team. As indicated, the online retailer did not succeed in passing the assessment, which is flagged in red under the *Status* and by the *Failed* chip component. However, the results highlight certain areas of strength, such as the *Asset Management* category, where all requirements were met.

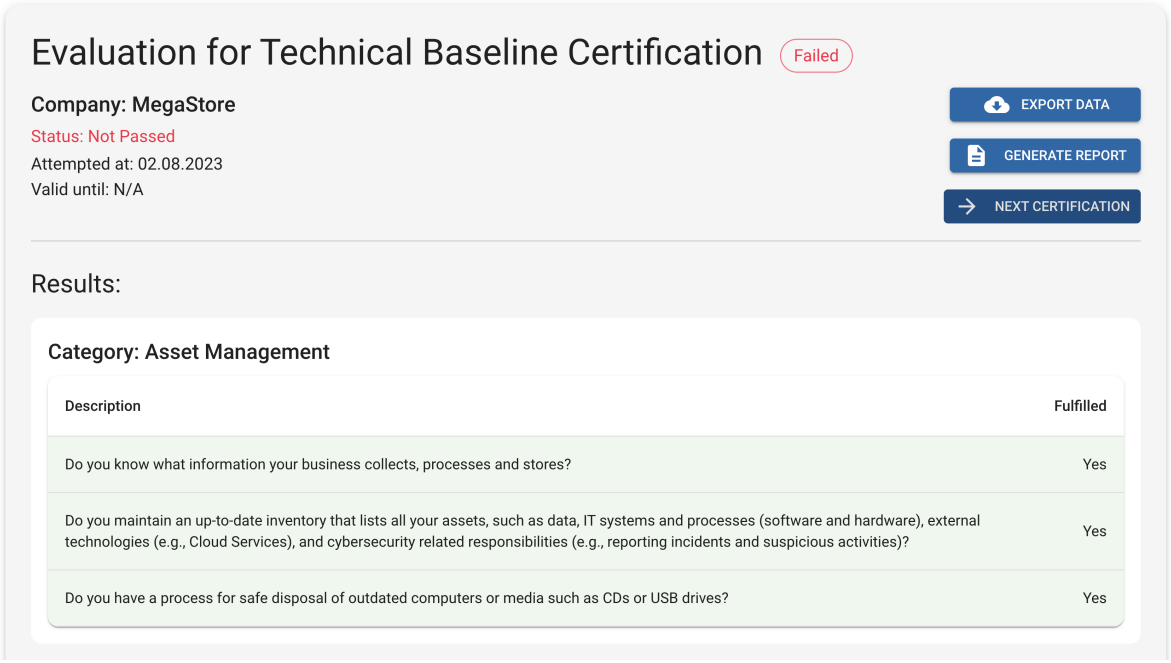


Figure 5.10: Outcome of the Technical Baseline Assessment

Moreover, on the top right side of the figure, the management team has access to several options. The button that starts the certification process for the next certification on the line is deliberately disabled, since attaining the Technical Baseline certification is a prerequisite to move on. The *EXPORT DATA* button allows MegaStoreXpert to download a JSON file detailing the results of all automated assessments. Listing 5.1 provides a snapshot of this file's structure. At the outset, it reveals the outcome of the HTTPS protocol checker. As shown in Line 3, the main Website *www.mega-store.com* passed the test, which means that the connections to its users can be considered as secure.

Following this, the file presents a detailed analysis of identified vulnerabilities across the network and technologies used by MegaStoreXpert. It enumerates services running on each port and technology assessed, including the identified vulnerabilities. Moreover, each CVE includes prioritization data (*cf.* Lines 24-30 and 46-52), providing MegaStoreXpert's management team with insights into which CVEs should be addressed first and allowing them to filter the most critical ones. In the last section, the JSON file provides a comprehensive scan report of the most commonly used ports. This valuable information

can then support MegaStoreXpert's technical staff, for instance, in identifying any open ports that should ideally be closed to enhance their network security.

In essence, this JSON file can serve as a roadmap for MegaStoreXpert's cybersecurity enhancement efforts. The company can use it to drive their strategic planning for IT upgrades, vulnerability patching, and overall security improvements. It could also serve as a reference document for any cybersecurity audits. Furthermore, the file's structured data format also makes it an ideal input for other systems to conduct further in-depth, automated analysis, thus enhancing MegaStoreXpert's ability to understand and respond to their cybersecurity landscape.


```
{
    "https_protocol_checker": {
        "www.mega-store.com": {
            "protocol": "https",
            "description": "Secure connection"
        },
        ...
    },
    "vulnerability_checker": {
        "ipVulnerabilities": {
            "192.168.1.14": {
                "80": {
                    "protocol": "tcp",
                    "service": {
                        "name": "http",
                        "product": "Apache httpd",
                        "version": "2.4.25"
                    },
                    "vulnerabilities": {
                        "CVE-2019-9517": {
                            "type": "cve",
                            "cvss": "7.8",
                            "is_exploit": "false",
                            "priority_details": {
                                "priority": "Priority 2",
                                "epss": 0.00345,
                                "cvss_baseScore": 7.5,
                                "cvss_version": "CVSS 3.1",
                                "cvss_severity": "HIGH",
                                "cisa_kev": "FALSE"
                            }
                        },
                        ...
                    }
                },
                ...
            }
        },
        "technologyVulnerabilities": [
            {
                "product": "MySQL",
                "version": "8.0.19",
                "vendor": "Oracle",
                "vulnerabilities": {
```

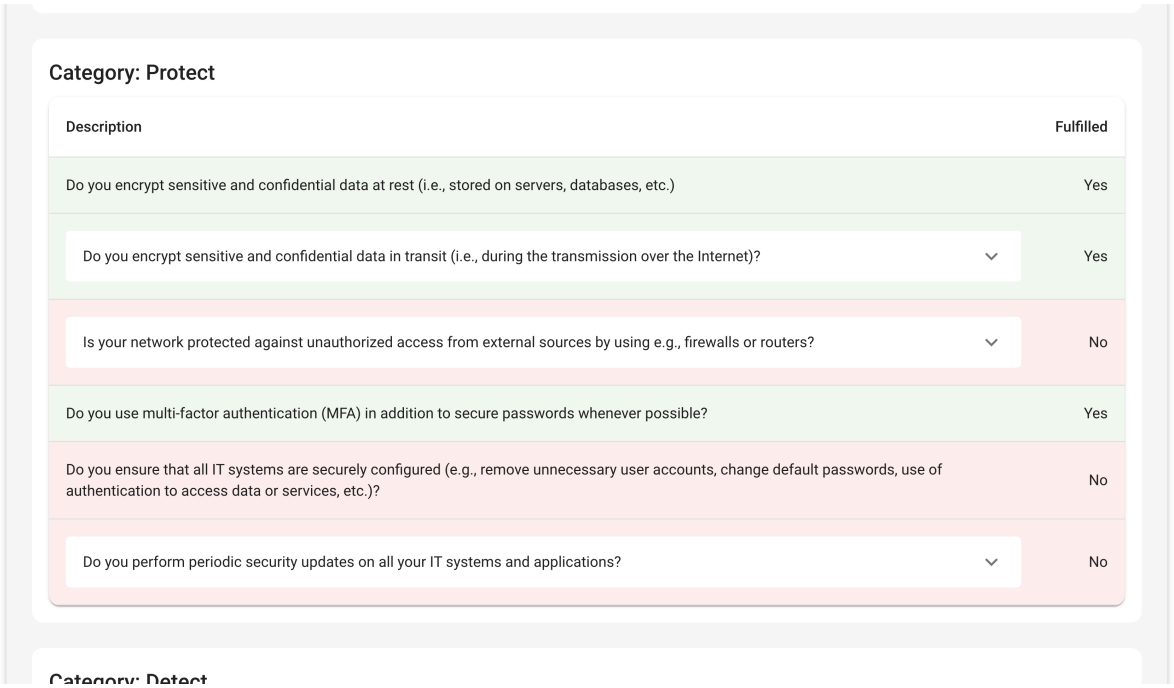
```
                    "CVE-2022-21599": {
                        "priority": "Priority 4",
                        "epss": 0.00056,
                        "cvss_baseScore": 4.9,
                        "cvss_version": "CVSS 3.1",
                        "cvss_severity": "MEDIUM",
                        "cisa_kev": "FALSE"
                    },
                    ...
                }
            },
            ...
        ]
    },
    "unauthorized_access_checker": {
        "pingCheck": {
            "192.168.1.14": {
                "connection_established": "True",
                "description": "Reachable with delay:
                                0.0004417896270751953 ms"
            }
        },
        "portScan": {
            "192.168.1.14": [
                {
                    "protocol": "tcp",
                    "portid": "21",
                    "state": "closed",
                    "reason": "conn-refused",
                    "reason_ttl": "0",
                    "service": {
                        "name": "ftp",
                        "method": "table",
                        "conf": "3"
                    },
                    "cpe": [],
                    "scripts": []
                },
                ...
            ]
        }
    }
}
```


Listing 5.1: JSON File of Automated Assessment Data

This rich set of data is also rendered visually for ease of use. As exemplified in Figure 5.11, the results from the *Protect* category are presented in an intuitive and in an user-friendly manner. Automated requirements are arranged in a collapsible accordion format that can be expanded to reveal the detailed results visually, thus, bridging the gap between raw data and actionable insights.

For instance, when the management team selects the final requirement within this category, the accordion element expands to reveal detailed insights, as depicted in Figure 5.12. This particular view provides a visual interpretation of the technology vulnerability

analysis results. In this sense, the tabular representation and clear labeling simplify the data, making it comprehensible even for those without extensive technical knowledge. At a glance, MegaStoreXpert's management team can easily discern that all three analyzed technologies harbor vulnerabilities. The Vulnerability Priority Details table further aids in understanding which CVE ID corresponds to which product, and which vulnerabilities

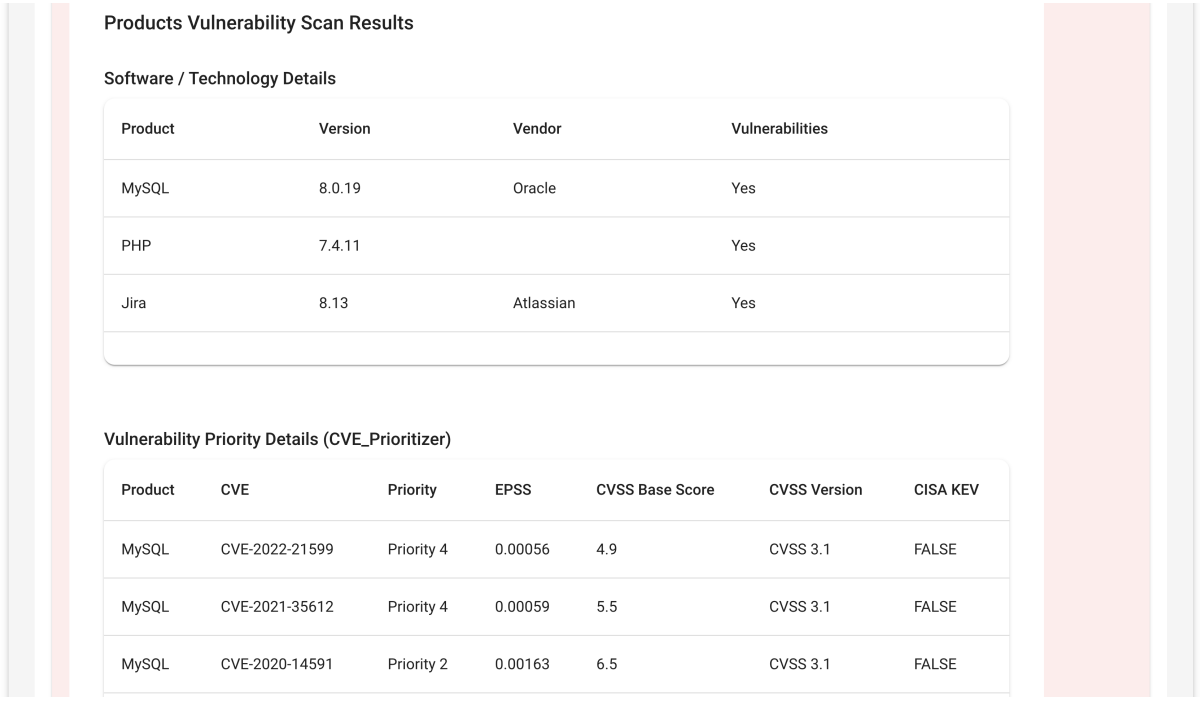


Category: Protect

Description	Fulfilled
Do you encrypt sensitive and confidential data at rest (i.e., stored on servers, databases, etc.)	Yes
Do you encrypt sensitive and confidential data in transit (i.e., during the transmission over the Internet)?	Yes
Is your network protected against unauthorized access from external sources by using e.g., firewalls or routers?	No
Do you use multi-factor authentication (MFA) in addition to secure passwords whenever possible?	Yes
Do you ensure that all IT systems are securely configured (e.g., remove unnecessary user accounts, change default passwords, use of authentication to access data or services, etc.)?	No
Do you perform periodic security updates on all your IT systems and applications?	No

Category: Detect

Figure 5.11: Outcome of the Protect Category



Products Vulnerability Scan Results

Software / Technology Details

Product	Version	Vendor	Vulnerabilities
MySQL	8.0.19	Oracle	Yes
PHP	7.4.11		Yes
Jira	8.13	Atlassian	Yes

Vulnerability Priority Details (CVE_Prioritizer)

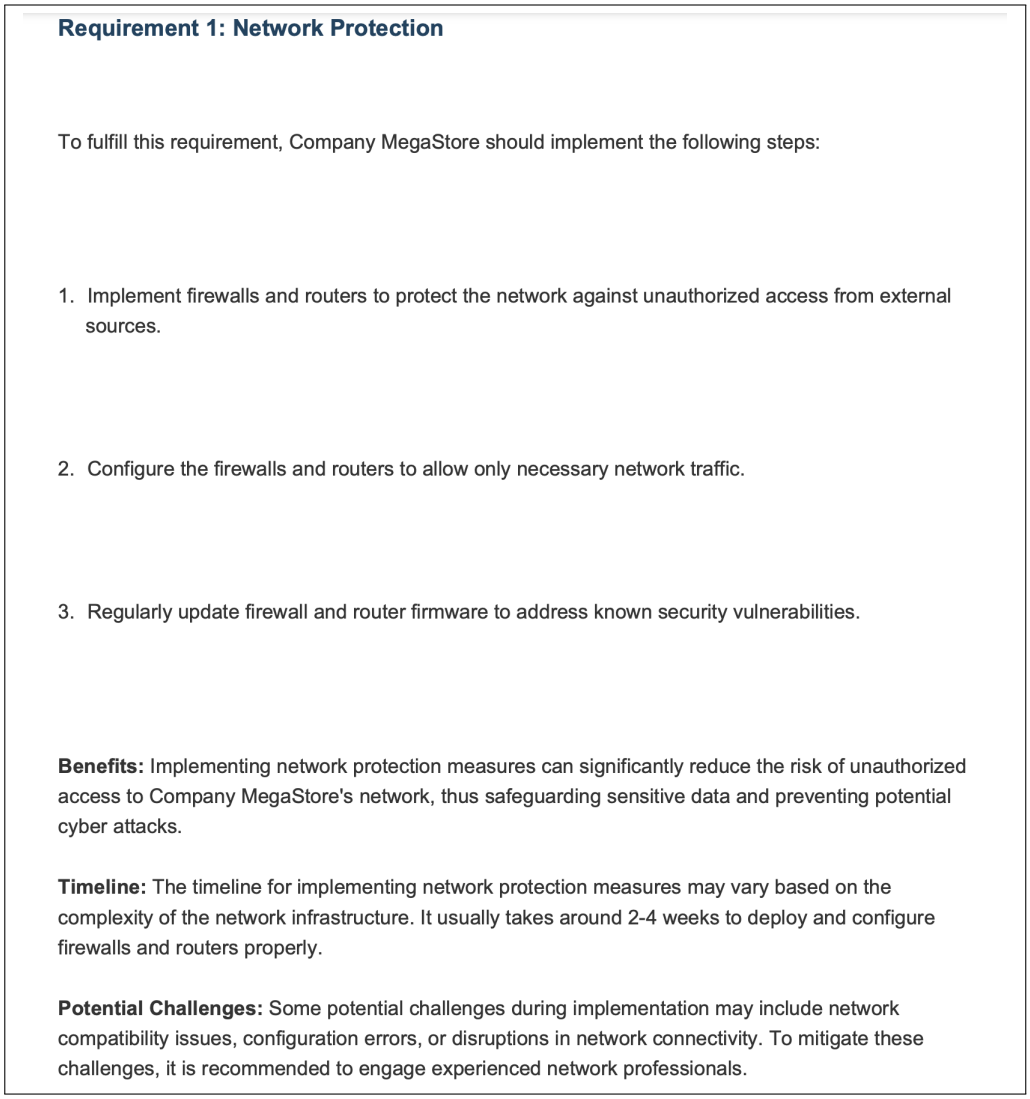
Product	CVE	Priority	EPSS	CVSS Base Score	CVSS Version	CISA KEV
MySQL	CVE-2022-21599	Priority 4	0.00056	4.9	CVSS 3.1	FALSE
MySQL	CVE-2021-35612	Priority 4	0.00059	5.5	CVSS 3.1	FALSE
MySQL	CVE-2020-14591	Priority 2	0.00163	6.5	CVSS 3.1	FALSE

Figure 5.12: Tabular Representation of Automated Results

should be prioritized for remediation.

This visual representation of the results generally make cybersecurity assessments more accessible to a wide range of users ranging from technical experts to non-technical staff. In this particular case, CERTSec allows the MegaStoreXpert management team to quickly get an overview of the cybersecurity situation and identify problem areas without having to delve into the raw data.

CERTSec also explores chatbots and Large Language Models (LLM) [109] to provide an Automatic Report Generation Tool. By selecting the *GENERATE REPORT* option (*cf.* Figure 5.10), MegaStoreXpert's management can leverage the power of Artificial Intelligence, more specifically ChatGPT [101], to provide tailored recommendations for addressing failed requirements. In this sense, even though MegaStoreXpert failed the Technical Baseline assessment, they immediately receive insightful guidance on how to address the identified issues so they can repeat the assessment as soon as possible. Figure 5.13 shows an excerpt from the report generated for MegaStoreXpert.



Requirement 1: Network Protection

To fulfill this requirement, Company MegaStore should implement the following steps:

1. Implement firewalls and routers to protect the network against unauthorized access from external sources.

2. Configure the firewalls and routers to allow only necessary network traffic.

3. Regularly update firewall and router firmware to address known security vulnerabilities.

Benefits: Implementing network protection measures can significantly reduce the risk of unauthorized access to Company MegaStore's network, thus safeguarding sensitive data and preventing potential cyber attacks.

Timeline: The timeline for implementing network protection measures may vary based on the complexity of the network infrastructure. It usually takes around 2-4 weeks to deploy and configure firewalls and routers properly.

Potential Challenges: Some potential challenges during implementation may include network compatibility issues, configuration errors, or disruptions in network connectivity. To mitigate these challenges, it is recommended to engage experienced network professionals.

Figure 5.13: Excerpt of Generated Report

Chapter 6

Conclusions and Future Work

The age of digitalization has brought numerous benefits, such as increased efficiency, but also a number of new challenges, particularly in the field of cybersecurity. As a result, companies need to take proactive steps to mitigate the risks associated with operating in an increasingly connected and complex digital world. In this work, we thoroughly examined various cybersecurity guidelines, frameworks and certifications that are designed to help organizations formulate appropriate cybersecurity strategies and assess their cybersecurity posture.

The comprehensive analysis revealed that SMEs still face several challenges (*e.g.,* understand their own cybersecurity requirements or formulate adequate cybersecurity strategy) despite the widespread availability and accessibility of these resources. The investigated resources often prove to be too abstract, tailored to larger organizations, or lack practical step-by-step guidance. Moreover, the analysed approaches tend to excessively focus only on technical aspects, thereby overlooking other critical dimensions (*i.e.,* economic and societal) that are integral to the diverse nature of cybersecurity. This gap is especially noticeable in case of cybersecurity certifications. Given these shortcomings in the current landscape, this Master Thesis offers three main contributions to better support SMEs in their cybersecurity endeavors.

First, a methodology is proposed that not only provides SMEs with practical guidelines to strengthen their cybersecurity efforts, but also enables them to verify compliance with a set of baseline cybersecurity requirements, all while getting formally acknowledged for that. To do so, CyberTEA is used as a basis and is extended with two additional phases (*i.e.,* Compliance and Certification). The Extended CyberTEA offers now an assessment of a SME's cybersecurity posture, ensuring that an integral baseline security level is achieved while analyzing potential gaps in cybersecurity strategies in terms of technical, economic and societal dimensions. Also, a comparative mapping with NIST CSF components has been conducted, highlighting its unique and innovative contributions.

The second contribution is the CERTSec, a novel lightweight cybersecurity certification scheme that aligns with the Extended CyberTEA. Unlike other certifications, CERTSec offers a three-tiered cybersecurity certification scheme that takes into account key dimensions of cybersecurity, thereby providing a more balanced and holistic approach to assessing an organization's cybersecurity posture. In this sense, the Technical Baseline focuses

on the implementation and management of cybersecurity measures and practices (*i.e.,* Technical dimension), while the Cost-Aware Baseline examines financial and business related aspects (*i.e.,* Economic dimension). Finally, the Comprehensive Baseline evaluates the contribution towards the security of a company's stakeholders and the wider society (*i.e.,* Societal dimension).

The proposed lightweight cybersecurity certification scheme serves as an invaluable entry point for SMEs into the complex domain of cybersecurity. By offering three levels of certification, it allows businesses to gradually assess and improve their cybersecurity posture. By doing such certifications, businesses can effectively demonstrate their commitment to cybersecurity and their awareness of its wider implications on society. On top of that, by addressing the requirements of all three pillars, companies can also develop new cybersecurity competencies that they can continue to build upon, thus, continuously improving their cybersecurity posture. To this end, the scheme also emphasizes continuous verification and requires annual reassessments to ensure companies are keeping pace with the ever-changing threat landscape. Moreover, due to its flexibility, the proposed certification scheme can be adjusted for the context of MNEs and could even drive industry standards by promoting a more comprehensive and practical approach to cybersecurity.

The final contribution of this work lies in the development of a prototype that automates processes within the proposed certification scheme. For this purpose, three technical requirements were selected for automation. As a result, the prototype is able to *(i)* determine whether Websites establish secure connections to protect sensitive data during transmission over the network, *(ii)* perform network reachability analysis, and *(iii)* conduct comprehensive vulnerability analyses on the networks, technologies and software provided. Moreover, a thorough evaluation of the prototype has been conducted to demonstrate the scalability of automating processes involved in the certification scheme. The results indicate that it is possible to conduct automation for risk analysis without significant impacts in terms of resource consumption and overall time spent on the entire process.

This work has exposed significant potential for future research. Given the lack of legal expertise, the proposed certification scheme currently does not address the legal dimension of cybersecurity. To address this limitation, extending CERTSec to include a fourth pillar, *i.e.,* Legal dimension, would enable an even more comprehensive approach to cybersecurity by encompassing all key dimensions. This addition would be beneficial as it ensures that SMEs' cybersecurity efforts align with legal requirements, providing them with a more robust and compliant cybersecurity posture.

Moreover, the integration of artificial intelligence solutions could revolutionize the cybersecurity landscape, making risk analysis and mitigation even more effective. Future work could therefore focus on enhancing the CERTSec Automated Report Generation Tool to generate more comprehensive and accurate reports. In this sense, SMEs could gain even deeper insights into their cybersecurity status, resulting in more informed decision-making and better risk management. For that, LLM tailored to cybersecurity can be explored.

Also, as future work, software engineering and deployment tasks have to be performed, such as making the application production-ready and deploying it to real-world scenarios. By implementing the certification scheme in practical settings, its effectiveness and usability can be thoroughly evaluated, ensuring that it aligns with real-world cybersecurity

challenges faced by SMEs. This practical deployment would contribute to refining and optimizing CERTSec for broader adoption, potentially leading to a more secure digital environment for businesses. Finally, addressing scalability issues for the technology vulnerability feature as well as exploring the automation of more processes involved in the certification scheme can lead to a more efficient and accessible cybersecurity management for SMEs.

Bibliography

[1] J. A. Sava, "Spending on digital transformation technologies and services worldwide from 2017 to 2026," November 2022, [Online] https://www.statista.com/statistics/870924/worldwide-digital-transformation-market-size/, last visit March 2023.

[2] European Union Agency for Cybersecurity (ENISA), "ENISA Threat Landscape 2022," November 2022, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.

[3] M. G. Craig Sparling, "Largest European DDoS Attack on Record," July 2022, [Online] https://www.akamai.com/blog/security/largest-european-ddos-attack-ever, last visit March 2023.

[4] European Union Agency for Cybersecurity (ENISA), "Cybersecurity for SMEs: Challenges and Recommendations," June 2021, https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes.

[5] M. F. Franco, "CyberTEA: a Technical and Economic Approach for Cybersecurity Planning and Investment," PhD Thesis, Communication Systems Group, Department of Informatics, Universität Zürich UZH, Zürich, Switzerland, February 2023.

[6] E.-C. Davri, E. Darra, I. Monogioudis, A. Grigoriadis, C. Iliou, N. Mengidis, T. Tsikrika, S. Vrochidis, A. Peratikou, H. Gibson, D. Haskovic, D. Kavallieros, E. Chaskos, P. Zhao, S. Shiaeles, N. Savage, B. Akhgar, X. Bellekens, and M. A. B. Farah, "Cyber Security Certification Programmes," in *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, 2021, pp. 428–435.

[7] European Commission, "Data protection: Rules for the protection of personal data inside and outside the EU." [Online] https://commission.europa.eu/law/law-topic/data-protection_en, last visit March 2023.

[8] A. Amiruddin, H. G. Afiansyah, and H. A. Nugroho, "Cyber-Risk Management Planning Using NIST CSF v1.1, NIST SP 800-53 Rev. 5, and CIS Controls v8," in *2021 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS*, 2021, pp. 19–24.

[9] C. Hsu, T. Wang, and A. Lu, "The Impact of ISO 27001 Certification on Firm Performance," in *2016 49th Hawaii International Conference on System Sciences (HICSS)*, 2016, pp. 4842–4848.

[10] European Union Agency for Cybersecurity (ENISA), "Interoperable EU Risk Management Framework," January 2023, https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-framework.

[11] ——, "Highlights on the National Cybersecurity Strategies," October 2020, https://www.enisa.europa.eu/news/enisa-news/Highlights-on-the-National-Cybersecurity-Strategies.

[12] M. F. Franco, F. M. Lacerda, and B. Stiller, "A Framework for the Planning and Management of Cybersecurity Projects in Small and Medium-sized Enterprises," *Revista de Gestão e Projetos*, vol. 13, no. 3, pp. 10–37, December 2022. [Online]. Available: https://doi.org/10.5167/uzh-229378

[13] M. F. Franco, L. Z. Granville, and B. Stiller, "CyberTEA: a Technical and Economic Approach for Cybersecurity Planning and Investment," in *36th IEEE/IFIP Network Operations and Management Symposium (NOMS 2023)*, Miami, USA, 2023, pp. 1–6.

[14] Computer Security Resource Center (CSRC), "cybersecurity," [Online] https://csrc.nist.gov/glossary/term/cybersecurity, last visit April 2023.

[15] National Institute of Standards and Technology (NIST), "An Introduction to Information Security," June 2017, NIST Special Publication 800-12. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf.

[16] M. Bishop, "About penetration testing," *IEEE Security & Privacy*, vol. 5, no. 6, pp. 84–87, 2007.

[17] National Center for Education Statistics (NCES), "Security Policy: Development and Implementation," [Online] https://nces.ed.gov/pubs98/safetech/chapter3.asp, last visit April 2023.

[18] J. M. Stewart, *Network Security, Firewalls and VPNs*. Jones & Bartlett Publishers, 2013.

[19] Cybersecurity & Infrastructure Security Agency (CISA), "Understanding Anti-Virus Software," september 2019, [Online] https://www.cisa.gov/news-events/news/understanding-anti-virus-software, last visit April 2023.

[20] H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, and K.-Y. Tung, "Intrusion detection system: A comprehensive review," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 16–24, 2013.

[21] Center for Internet Security (CIS), "CIS Controls Implementation Guide for SMEs," September 2017, https://www.cisecurity.org/wp-content/uploads/2017/09/CIS-Controls-Guide-for-SMEs.pdf.

[22] J. Mendel, "Economics and business review contents," *Economics and Business Review*, vol. 5 (19), pp. 24–47, 06 2019.

[23] European Data Protection Supervisor (EDPS), "Data Protection," [Online] https://edps.europa.eu/data-protection/data-protection_en, last visit April 2023.

[24] P. Apte, "Why is the social impact of cyber security important to business?" [Online] https://edps.europa.eu/data-protection/data-protection_en, last visit April 2023.

[25] National Audit Office (NAO), "Investigation: WannaCry cyber attack and the NHS," April 2018, https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf.

[26] O. Katz, "Highly Sophisticated Phishing Scams Are Abusing Holiday Sentiment," November 2022, [Online] https://www.akamai.com/blog/security-research/sophisticated-phishing-scam-abusing-holiday-sentiment, last visit April 2023.

[27] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, "Phishing attacks: A recent comprehensive study and a new anatomy," *Frontiers in Computer Science*, vol. 3, p. 563060, 2021.

[28] National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cybersecurity," April 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[29] Payment Card Industry Security Standards Council (PCI SSC), "PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.2.1," July 2018, https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf.

[30] Centers for Disease Control and Prevention (CDC), "Health Insurance Portability and Accountability Act of 1996 (HIPAA)," [Online] https://www.cdc.gov/phlp/publications/topic/hipaa.html#:~:text=The%20Health%20Insurance%20Portability%20and,the%20patient's%20consent%20or%20knowledge., last visit July 2023.

[31] National Cyber Security Centre (NCSC), "Cyber Essentials," [Online] https://www.ncsc.gov.uk/cyberessentials/overview, last visit July 2023.

[32] International Electrotechnical Commission (IEC), "What is conformity assessment," [Online] https://www.iec.ch/conformity-assessment/what-conformity-assessment, last visit July 2023.

[33] Das Kompetenzzentrum Sicheres Österreich (KSÖ), "Cyber Risk Rating & Cyber Trust Label Scheme Policy 2023 ," 2023, https://cyberrisk-rating.at/cyberrisk-2023-schema-en.pdf.

[34] International Electrotechnical Commission (IEC), "Types of conformity assessment," [Online] https://www.iec.ch/conformity-assessment/types-conformity-assessment, last visit July 2023.

[35] L. A. Gordon and M. P. Loeb, "The economics of information security investment," *ACM Transactions on Information and System Security (TISSEC)*, vol. 5, no. 4, pp. 438–457, 2002.

[36] J. Willemson, "Extending the gordon and loeb model for information security investment," in *2010 International Conference on Availability, Reliability and Security*, 2010, pp. 258–261.

[37] L. A. Gordon, M. P. Loeb, and L. Zhou, "Information segmentation and investing in cybersecurity," *Journal of Information Security*, vol. 12, no. 1, pp. 115–136, 2020.

[38] L. A. Gordon, M. P. Loeb, W. Lucyshyn, L. Zhou *et al.*, "Externalities and the magnitude of cyber security underinvestment by private sector firms: a modification of the gordon-loeb model," *Journal of Information Security*, vol. 6, no. 01, p. 24, 2014.

[39] L. A. Gordon, M. P. Loeb, and L. Zhou, "Integrating cost–benefit analysis into the nist cybersecurity framework via the gordon–loeb model," *Journal of Cybersecurity*, vol. 6, no. 1, p. tyaa005, 2020.

[40] L. A. Gordon, M. P. Loeb, L. Zhou *et al.*, "Investing in cybersecurity: Insights from the gordon-loeb model," *Journal of Information Security*, vol. 7, no. 02, p. 49, 2016.

[41] European Union Agency for Cybersecurity (ENISA), "Introduction to Return on Security Investment," December 2012, https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment.

[42] National Institute of Standards and Technology (NIST), "Security and Privacy Controls for Information Systems and Organizations," September 2020, NIST Special Publication 800-53. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[43] ——, "Guide for Conducting Risk Assessments," September 2012, NIST Special Publication 800-30. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

[44] International Organization for Standardization (ISO), "ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls," February 2022, https://www.iso.org/standard/75652.html.

[45] European Union Agency for Cybersecurity (ENISA), "Framework," [Online] https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-isms/framework, last visit July 2023.

[46] European Telecommunications Standards Institute (ETSI), "Cybersecurity for SMEs: Cybersecurity Standardization Essentials," May 2021, ETSI TR 103 787-1, https://www.etsi.org/deliver/etsi_tr/103700_103799/10378701/01.01.01_60/tr_10378701v010101p.pdf.

[47] National Institute of Standards and Technology (NIST), "Small Business Information Security: The Fundamentals," November 2016, https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf.

[48] National Cyber Security Centre (NCSC), "Cyber Essentials: Requirements for IT infrastructure v3.1," April 2023, https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-April-2023.pdf.

[49] European Watch on Cybersecurity & Privacy, "Cybersecurity Label," 2021, https://label.cyberwatching.eu/Pages/Home.aspx.

[50] G. Drivas, A. Chatzopoulou, L. Maglaras, C. Lambrinoudakis, A. Cook, and H. Janicke, "A nis directive compliant cybersecurity maturity assessment framework," in *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)*, 2020, pp. 1641–1646.

[51] National Institute of Standards and Technology (NIST), "Success Story: Government of Bermuda," [Online], 2020, https://www.nist.gov/cyberframework/success-stories/government-bermuda, last visit July 2023.

[52] ——, "Success Story: Saudi Aramco," [Online], 2021, https://www.nist.gov/cyberframework/success-stories/saudi-aramco, last visit July 2023.

[53] P. P. Roy, "A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard," in *2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA)*, 2020, pp. 1–3.

[54] R. Kwon, T. Ashley, J. Castleberry, P. Mckenzie, and S. N. Gupta Gourisetti, "Cyber Threat Dictionary Using MITRE ATT&CK Matrix and NIST Cybersecurity Framework Mapping," in *2020 Resilience Week (RWS)*, 2020, pp. 106–112.

[55] The MITRE Corporation, "MITRE ATT&CK," 2015, https://attack.mitre.org/.

[56] IASME Consortium Ltd, "The Benefits of Certification," [Online] https://iasme.co.uk/cyber-essentials/, last visit July 2023.

[57] ——, "Get ready for CYBER ESSENTIALS," [Online] https://getreadyforcyberessentials.iasme.co.uk/, last visit July 2023.

[58] ——, "Cyber Essentials Certificate Search," [Online] https://iasme.co.uk/cyber-essentials/ncsc-certificate-search/, last visit July 2023.

[59] J. Such, J. Vidler, T. Seabrook, and A. Rashid, "Cyber security controls effectiveness: A qualitative assessment of cyber essentials," technical Report SCC-2015-02, Security Lancaster, Lancaster University, 2015.

[60] M. Stone, "Shellshock In-Depth: Why This Old Vulnerability Won't Go Away," [Online] https://securityintelligence.com/articles/shellshock-vulnerability-in-depth/, last visit August 2023.

[61] Synopsys, Inc, "The Heartbleed Bug," [Online] https://heartbleed.com/, last visit August 2023.

[62] M. Franco, J. Von der Assen, L. Boillat, C. Killer, B. Rodrigues, E. J. Scheid, L. Granville, and B. Stiller, "SecGrid: a Visual System for the Analysis and ML-based Classification of Cyberattack Traffic," in *2021 IEEE 46th Conference on Local Computer Networks (LCN)*, 2021, pp. 140–147.

[63] M. F. Franco, B. Rodrigues, E. J. Scheid, A. Jacobs, C. Killer, L. Z. Granville, and B. Stiller, "SecBot: a Business-Driven Conversational Agent for Cybersecurity Planning and Management," in *2020 16th International Conference on Network and Service Management (CNSM)*, 2020, pp. 1–7.

[64] M. F. Franco, C. Omlin, O. Kamer, E. J. Scheid, and B. Stiller, "SECAdvisor: a Tool for Cybersecurity Planning using Economic Models," 2023, 2304.07909, cs.CR, https://arxiv.org/abs/2304.07909.

[65] M. F. Franco, B. Rodrigues, and B. Stiller, "MENTOR: The Design and Evaluation of a Protection Services Recommender System," in *2019 15th International Conference on Network and Service Management (CNSM)*, 2019, pp. 1–7.

[66] European Union Agency for Cybersecurity (ENISA), "Cybersecurity guide for SMEs - 12 steps to securing your business," June 2021, https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes.

[67] Centre for Cyber Security Belgium (CCB), "CYBER SECURITY INCIDENT MANAGEMENT GUIDE," September 2021, https://ccb.belgium.be/sites/default/files/cybersecurity-incident-management-guide-EN.pdf.

[68] ——, "CYBER SECURITY GUIDE FOR SME," January 2017, https://ccb.belgium.be/sites/default/files/CCB-EN%20-C.pdf.

[69] digitalswitzerland, "Cybersecurity Guide for SME," May 2021, https://digitalswitzerland.com/wp-content/uploads/2021/05/Cyber_Guideline_for_SME.pdf.

[70] Huawei Technologies Co., Ltd., "Q&A Guide: Promoting Cybersecurity for SMEs in Europe." 2023, https://www-file.huawei.com/-/media/corp2020/media-center/pdf/facts/papers/cybersecurity%20for%20european%20smes%20a%20huawei%20study.pdf?la=en.

[71] National Cyber Security Centre (NCSC), "Introduction to logging for security purposes," https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes, last visit May 2023.

[72] A. Sarnek and C. Dolan, "Cybersecurity is an environmental, social and governance issue. Here's why," [Online] https://www.weforum.org/agenda/2022/03/three-reasons-why-cybersecurity-is-a-critical-component-of-esg/, last visit May 2023.

[73] PricewaterhouseCoopers AG (PwC), "The global footprint of data protection regulations," 2019, https://www.pwc.ch/en/publications/2019/The%20global%20footprint%20of%20data%20protection%20regulations_EN_V3-web.pdf.

[74] European Data Protection Board (EDPB), "Data protection basics," [Online] https://edpb.europa.eu/sme-data-protection-guide/data-protection-basics_en, last visit May 2023.

[75] European Commission, "What information must be given to individuals whose data is collected?" [Online] https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/what-information-must-be-given-individuals-whose-data-collected_en, last visit May 2023.

[76] ——, "What data can we process and under which conditions?" [Online] https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/overview-principles/what-data-can-we-process-and-under-which-conditions_en#:~:text=the%20company%2Forganisation%20must%20collect,if%20not%20('accuracy')%3B, last visit May 2023.

[77] S. Widup, A. Pinto, D. Hylender, G. Bassett, and p. langlois, "2022 Verizon Data Breach Investigations Report," May 2022, Technical Report, https://www.researchgate.net/publication/362160949_2022_Data_Breach_Investigations_Report, last visit May 2023.

[78] National Institute of Standards and Technology (NIST), "Building an Information Technology Security Awareness and Training Program," October 2003, NIST Special Publication 800-50. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf.

[79] European Union Agency for Cybersecurity (ENISA), "Cyber Security Culture in organisations," February 2018, https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations.

[80] Payment Card Industry Security Standards Council (PCI SSC), Security Awareness Program Special Interest Group, "Information Supplement: Best Practices for Implementing a Security Awareness Program," October 2014, https://listings.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf.

[81] National Institute of Standards and Technology (NIST), "Guide to Cyber Threat Information Sharing," October 2016, NIST Special Publication 800-150. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-150.pdf.

[82] National Cyber Security Centre (NCSC), "Welcome to the National Cyber Security Centre NCSC," [Online] https://www.ncsc.admin.ch/ncsc/en/home.html, last visit May 2023.

[83] Swiss Cyber Security Days (SCSD), "Shaping Cyber Resilience," [Online] https://scsd.ch/swisscybersecuritydays_en/, last visit May 2023.

[84] Swiss Cyber Institute, "Welcome to Swiss Cyber Institute," [Online] https://swisscyberinstitute.com/, last visit May 2023.

[85] Meta Open Source, "React - The library for web and native user interfaces," [Online] https://react.dev/, last visit July 2023.

[86] Microsoft, "TypeScript Documentation," [Online] https://www.typescriptlang.org/docs/, last visit July 2023.

[87] Vercel, "The React Framework for the Web," [Online] https://nextjs.org/, last visit July 2023.

[88] Material UI SAS, "Move faster with intuitive React UI tools," [Online] https://mui.com/, last visit July 2023.

[89] Python Software Foundation, "Python is a programming language that lets you work quickly and integrate systems more effectively," [Online] https://www.python.org/, last visit July 2023.

[90] Encode OSS Ltd., "Django REST Framework," [Online] https://www.django-rest-framework.org/#, last visit July 2023.

[91] A. Solem, "Introduction to Celery," [Online] https://docs.celeryq.dev/en/stable/index.html, last visit July 2023.

[92] Redis, "Real-time speed and simplicity," [Online] https://redis.com/, last visit July 2023.

[93] M. Rojas, "CVE Prioritizer Tool," [Online] https://github.com/TURROKS/CVE_Prioritizer, last visit July 2023.

[94] SQLite, "What Is SQLite?" [Online] https://www.sqlite.org/index.html, last visit July 2023.

[95] B. Shaqiri, "CERTSec - An Automated Cybersecurity Self-Assessment Tool," August 2023, [Online] https://github.com/cert-sec/CERTSec, last visit August 2023.

[96] G. Lyon, "Nmap: Discover your network," [Online] https://nmap.org/, last visit July 2023.

[97] J. Wangolo, "Python3-nmap converts Nmap commands into python3 methods making it very easy to use nmap in any of your python pentesting projects," [Online] https://pypi.org/project/python3-nmap/, last visit July 2023.

[98] National Institute of Standards and Technology (NIST), "NATIONAL VULNERABILITY DATABASE," [Online] https://nvd.nist.gov/, last visit July 2023.

[99] ——, "Request an API Key," [Online] https://nvd.nist.gov/developers/request-an-api-key, last visit July 2023.

[100] ——, "Getting Started," [Online] https://nvd.nist.gov/developers/start-here#:~:text=Rate%20Limits&text=The%20public%20rate%20limit%20(without,a%20rolling%2030%20second%20window., last visit August 2023.

[101] OpenAI, "Introducing ChatGPT," [Online] https://openai.com/blog/chatgpt#OpenAI, last visit July 2023.

[102] ——, "API reference," [Online] https://platform.openai.com/docs/api-reference/introduction, last visit July 2023.

[103] SEO Site Checkup, "Search Engine Optimization Made Easy," [Online] https://seositecheckup.com/, last visit July 2023.

[104] V. Le Pochat, T. Van Goethem, S. Tajalizadehkhoob, M. Korczyński, and W. Joosen, "Tranco: A Research-Oriented Top Sites Ranking Hardened Against Manipulation," in *Proceedings of the 26th Annual Network and Distributed System Security Symposium*, ser. NDSS 2019, Feb. 2019.

[105] badssl.com, "badssl.com," [Online] https://badssl.com/, last visit July 2023.

[106] S. young Im, S.-H. Shin, K. Y. Ryu, and B. hee Roh, "Performance evaluation of network scanning tools with operation of firewall," in *2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN)*, 2016, pp. 876–881.

[107] C. Dishington, D. P. Sharma, D. S. Kim, J.-H. Cho, T. J. Moore, and F. F. Nelson, "Security and performance assessment of ip multiplexing moving target defence in software defined networks," in *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. IEEE, 2019, pp. 288–295.

[108] cve-search, "cve-search - a tool to perform local searches for known vulnerabilities," [Online] https://github.com/cve-search/cve-search, last visit August 2023.

[109] E. Kasneci, K. Seßler, S. Küchemann, M. Bannert, D. Dementieva, F. Fischer, U. Gasser, G. Groh, S. Günnemann, E. Hüllermeier *et al.*, "ChatGPT for good? On Opportunities and Challenges of Large Language Models for Education," *Learning and Individual Differences*, vol. 103, p. 102274, 2023.

Abbreviations

API	Application Programming Interface
CAB	Cost-Aware Baseline
CDN	Content Delivery Network
COB	Comprehensive Baseline
CIA	Confidentiality, Integrity, Availability
CMAF	Cybersecurity Maturity Assessment Framework
CPE	Common Platform Enumeration
CTD	Cyber Threat Dictionary
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CyberTEA	Cybersecurity Technical and Economic Approach
DoS	Denial of Service
DDoS	Distributed DoS
EBIS	Expected Benefits of Investment in Information Security
ENBIS	Expected Net Benefit of Investment in Information Security
ENISA	European Union Agency for Cybersecurity
EPSS	Exploit Prediction Scoring System
ETSI	European Telecommunications Standards Institute
EU	European Union
GDPR	General Data Protection Regulation
GL Model	Gordon-Loeb Model
HIPAA	Health Insurance Portability and Accountability Act
IEC	International Electrotechnical Commission
IDS	Intrusion Detection System
ISMS	Information Security Management Systems
ISO	International Organization for Standardization
KEV	Known Exploited Vulnerabilities
KMU	Kleine und Mittlere Unternehmen
KSÖ	Kompetenzzentrum Sicheres Österreich
LLM	Large Language Model
MFA	Multi-Factor Authentication
MNE	Multi-National Enterprise
NIST	National Institute of Standards and Technology
NIST CSF	NIST Cybersecurity Framework
NIST SP	NIST Special Publication
NVD	National Vulnerability Database

ROI	Return on Investments
ROSI	Return on Security Investments
SME	Small and Medium-sized Enterprise
SSG	Static Site Generation
SSR	Server-Side Rendering
TB	Technical Baseline

List of Figures

List of Tables

Listings

Appendix A

Contents of the CD

The following deliverables are submitted for this thesis:

- **Code:**
  - Contains the source code for CERTSec, together with guidelines for its installation and usage. For convenience and enhanced accessibility, this is also made publicly available on GitHub [95].
- **Thesis:**
  - PDF version of the thesis.
  - ZIP file containing source code of the thesis.
  - Plain text files of the Abstract in English and German.
  - PDF version of the intermediate presentation.

Appendix B

Installation Guidelines

This installation guideline is based on a MacOS operating system. Therefore, the setup for Windows might differ. The source code of CERTSec including a comprehensive installation guide is also publicly available on GitHub [95].

Prerequisites

In order to be able to run the program, the following technical requirements must be met:

- Node.js v18.13.0
- NPM v8.19.3
- Python 3.x
- pip (included with Python 3.4 and later)
- Nmap
- Redis (using official docker image recommended)

Installing CERTSec

1. Clone the repository:

   `git clone https://github.com/cert-sec/CERTSec.git`

2. Install dependencies:

   (a) Frontend:

   Navigate into the frontend directory: `cd frontend`
   Install dependencies: `npm install`

(b) Backend:

Navigate into backend directory: `cd ../backend`
Create a virtual environment: `python3 -m venv venv`
Activate virtual environment: `source venv/bin/activate`
Install dependencies: `pip install -r requirements.txt`

Env Variables

Since CERTSec leverages external APIs, it is necessary to create a local `.env` file containing the key-value pairs of the corresponding environment variables.

The `.env.template` files located at `backend` and `backend/cve_prioritizer/cve_prioritizer` show which environment variables must be set (*i.e.,* NVD API [99] and OpenAI API [102])

Starting CERTSec

1. Start Redis:

   ```
   docker run -d -rm -p 6379:6379 redis
   ```

2. Start Backend:

   Navigate into backend directory: `cd backend`
   Run the following commands:
   ```
   python manage.py makemigrations
   python manage.py migrate
   python manage.py runserver
   ```
   Open a second terminal and run: `python -m celery -A backend worker -l info`

3. Start Frontend:

   Navigate into frontend directory: `cd frontend`
   Start frontend: `npm run dev`