University of Economics, Prague
Faculty of Informatics and Statistics

CYBERSECURITY AUDIT IN THE SME'S

MASTER´S THESIS

Study program: Applied Informatics
Field of study: Information Systems Management

Author: Magzumov Timur
Supervisor: doc. Ing. Vlasta Svatá, CSc.
Prague, May 2020

Abstract

Nowadays, digitalization of the 21st century has changed the way of how businesses operate. It provides companies with numerous incentives to innovate their service delivery by technological opportunities, but at the same time, it contributes to the growing potential of cybercriminals. Information technology concerns also draw keen interest from both computer security and audit professionals as well as from various applications, including businesses working in the area of e-business.

New findings in information protection suggest that the most susceptible companies are small and medium-sized businesses because there is a shortage of interest in their data defence systems.

The thesis will focus on the SMESEC framework and how it can be beneficial for small-medium enterprises. It will explain how its application brings value to businesses and customers; the practical part of this work will concentrate on the chapters of usage of SMESEC and its auditable outcomes.

Keywords: Cybersecurity; Audit; SMESEC; Framework.

Acknowledgement

I wish to express my appreciation and gratitude to the supervisor of my thesis, doc. Ing. Vlasta Svatá for her continuous support and patience.

Moreover, I would like to thank everyone who was a part of my student journey during my studies for their kindness and faith.

Table of content

List of Figures

List of Tables

Chapter 1: Introduction

Digitalization in the 21st century is changing the way how businesses operate today. It allows us to transfer money online through the bank, which doesn't have any physical branches (Tinkoff Bank) or to order a taxi from a company, which doesn't have any cars in their taxi park (Uber). These types of modernization give companies new opportunities to improve their business processes, as well as it can contribute to the increase of cybercriminals. Therefore, information security problems attract the close attention of both - cybersecurity and audit specialists and numerous users, including companies operating in the area of e-business. Without knowledge and qualified application of modern technologies, standards, protocols, and information security tools, it is impossible to achieve the required level of information security of computer systems and networks, which is a must in the case of contemporary business organizations.

The latest cybersecurity trends demonstrate that the most vulnerable organizations are small and medium-sized enterprises since there is a lack of investments in their cybersecurity infrastructure. For SMEs, investing in security does not provide clear, measurable profits besides the perception of safety (Amrin, 2014).

The purpose of this work is to analyze the latest policies, concepts, frameworks, as well as software and hardware cybersecurity solutions, which might be suitable for organizations with limited human and financial resources. Research findings will answer the following questions: "What is the role of cybersecurity in modern SMEs?" and "What are the benefits of adopting SMESEC cybersecurity framework for European SMEs?".

Finally, the thesis aims to cover the possible adoption of SMESEC framework, developed by the international group of experts and proved a recommendation to its desired state.

Chapter 2: Information Security and Cybersecurity

There are a few reasons why criminals are attacking organizations digitally, yet the leading cause of those cyber actions is intelligence gathering, which occurs in 89% of the cases. The remaining attacks made for business disruption (10%) and financial profitability (1%), according to the Internet Security Threat Report, published in 2019 (Symantec, 2019 Internet Security Threat Report, 2019). Another interesting fact that all these attacks in the majority of the cases (48%) targeted small organizations (Verizon, 2019). But it doesn't mean that cybercriminals only attack small companies; in the past decade alone, huge corporations like Sony, Google, and Microsoft have been experienced cyberattacks. (Symantec, 10 cyber security facts and statistics for 2018, 2018). Along with the improved cybersecurity in organizations, hackers are improving their techniques as well. As an example, WannaCry "ransomworm" attack in 2017, which affected more than 500000 PCs worldwide, owed by private users, government institutions, and commercial organizations (Ackerman, 2017). All those digital attacks have led to the new cybersecurity infrastructure in the organizations.

Now, let's have a look into a brief history of how informational and cybersecurity has evolved.

With the appearance of the earliest methods for correspondence, politicians and military commanders understood the need to create instruments for ensuring secret communication and approaches to distinguish endeavours to distort it. For instance, Julius Caesar credited with developing his own cypher around 50 BC., which was proposed to avoid the reading of his secret letters, by his detractors (V.A., 2002). However, during that time, the protection of sensitive information was done mainly by controlling and monitoring of secret information handling. Confidential correspondence was explicitly marked to be delivered and protected by trusted envoys, accompanied by the guards (Singh, 2009).

With the development of post correspondence, governmental organizations began to emerge to intercept, decrypt, read, and re-seal letters. Thereby for these purposes in 1653, the Secret Office appeared in England. The systemic nature of the practice of secretly copying the correspondence of almost all foreign diplomats so that the addressee does not have any suspicions, acquired in the mid-18th century - the so-called "dark rooms" appeared (V.C., 2015). After the autopsy, cryptanalysis of the message became very important, and for this purpose, many famous mathematicians of their time participated in the activity of dark rooms.

The most outstanding results were achieved by Christian Goldbach, who managed to decrypt 61 letters of the Prussian and French ministers in six months of work. In some cases, after successful decryption of the message, its content was replaced – analogue of contemporary "man in the middle" cyber-attack (V.C., 2015).

During World War I, multilevel classification and encryption systems used to transmit information by all warring parties, which contributed to the emergence and intensive use of encryption and cryptanalysis units. Thus, by the end of 1914, one of the sections of the British Admiralty was formed - "Room 40", which became the leading cryptographic authority in Great Britain. At the time of World War II, a set of secrecy stamps was created. They were accessible only to the insiders, which specifies who may handle documents (usually it is officers rather than ordinary ones) and the places it should be kept, taking into account the existence of increasingly complex safes and vaults. Also, the warring parties developed procedures for the guaranteed destruction of classified documents (Gannon, 2014).

The second half of the 20th and early beginning of the 21st century represents the rapid development of telecommunications, hardware, and software, as well as data encryption. The advent of portable, powerful, and affordable computer equipment has made electronic data processing available for small businesses and home users. Eventually, PCs had connected to the Internet, which led to rapid growth in the new e-business sector. All these factors, combined with the advent of cybercrime and many cases of international terrorism, has created a need for better methods of protecting computers and the information that they store, process, and transmit. Therefore, scientific disciplines have arisen, such as "Cybersecurity" and "Information Security" (The History of Information Security : A Comprehensive Handbook, 2007).

After we outlined significant historical events in informational security, let's focus on evolutional steps in the new area of cybersecurity:

2.1. 1960-1970's: Password Protection and First Virus

During the early 1960s, passwords were easily accessible by any legitimate user, unlike nowadays, where only users can get access to the information they hold. (Paul, 2013). In the 1960s, companies were focused only on physical security protection, such as fire safety

systems, but didn’t care about restricting access digitally, since no virus existed at that time. However, it is all changed in 1971, when Bob Thomas, who was a researcher for BBN Technologies in Cambridge, created the first “worm,” which replicated itself in ARPANEN (internet predecessor) network, displaying for network users’ phrase in their monitors. "I'M THE CREEPER: CATCH ME IF YOU CAN.." Besides the strange message, “worm” was utterly harmless, unlike its modern analogues (Writer, 2018).

2.2. The 1980s: First Massive Viruses

In 1981, the first genuinely massive viral digital epidemic occurred. The Apple II computers that were popular at that time were affected. The “Elk Clone” virus was written to the boot sectors of floppy disks when a user accessed them. Elk Clone distorted the image on the monitor, displayed various text messages, and made the text blink. Inexperienced users felt numb from the actions of the virus, while the virus itself continued to "move" from one computer to another (Leyden, 2012).

In 1984, Fred Cohen, one of the most respected virologists, gave a clear definition of the term "computer virus": "a program that can" infect "other programs by modifying them to introduce their copies." (Computer Security and the Internet, 2019)

In 1986, 19-year-old Pakistani Basit Farouk Alvi created the “Brain” virus. Like Elk Clone, “Brain” hit the boot sectors of floppy disks. The program didn’t focus on any destructive functions, and it only changed the name of all diskettes to “(C) Brain.” According to the author, he pursued only one goal - to find out the level of computer piracy in his country. But virus activation led to the fact that within a few weeks, thousands of computers around the world turned out to be infected, and it caused a real commotion among users and a storm of discussions in the media. In Brain, a technique was first used, when reading the infected sector of a disk, the virus substituted an uninfected section instead of this section (The History Of Computer Virus, 2008).

In 1988, was created a first malicious program that not only infected a computer but also caused real harm to it. By the way, the virus was created at Lehigh University, where worked previously mentioned, Fred Cohen. The Lehigh virus destroyed information on hard drives, targeting the COMMAND.COM system files. The presence of qualified specialists at the

university turned out to be salvation - he never made his way beyond the walls of the educational institution. However, the Lehigh algorithm itself played a significant role in eliminating the epidemic threat - during the formatting of hard drives, and it destroyed itself along with the rest of the information (Wyk, 1989).

2.3. The 1990s: The Era of Firewalls

The first device that performs the function of filtering network traffic appeared in the late 1980s when the Internet was an innovation, and it was impossible to use it globally. These devices were routers that inspect the traffic based on the data contained in the headers of the network layer protocols. Subsequently, with the development of network technologies, these devices were able to filter traffic using protocol data of a higher transport layer. Routers can be considered the first hardware-software implementation of the firewall (Ingham & Forrest, 2014).

Software firewalls appeared much later and were much younger than antivirus programs. For example, the Netfilter / iptables project (one of the first software firewalls built into the Linux kernel since version 2.4) was founded in 1998. Such a late appearance is understandable since, for a long time, the antivirus solved the problem of protecting personal computers from malware. However, in the late 1990s, viruses began to actively use the lack of firewalls on computers, which led to increased user interest in this class of devices (A., 2016).

2.4. 2000-2010s: The Era of First Great Cybercrimes

- **Citibank fraud in 1994.** This attack was one of the first significant cybercrimes known. It all started, when several bank clients found out that they are missing $400 000 in their accounts. FBI later tracked missing funds and found out that attack was organized by Vladimir Levin and his wife from St. Petersburg computer firm. Cybersecurity breaches allowed them to steal more than $10 million (FBI, 2014) .

- **PlayStation Network outage in 2011.** During the PSN hack, the number of registered accounts on its network was 77 million, which makes this incident the largest in history (the previous “record” belongs to the TJX Companies hacking, which resulted in 45 million users being affected) (Shane Richmond & Williams, 2011). During the attack, PSN user credit cards, emails,

and other personal data were stolen. According to Sony, the company lost around $171 million in revenue due to its network outage (Schreier, 2011).

- **Snowden & The NSA, 2013.** In June of 2013, Snowden handed over NASA secret information. It was the total surveillance of American intelligence services for information communications between citizens of many countries around the world using existing information and communication networks, including information about the PRISM project, as well as X-Keyscore and Tempora to the famous publishers of newspaper. According to a Pentagon closed-door report, Snowden stole 1.7 million secret files, most of the documents related to "vital operations of the US Army, Navy, Marines and Air Force." Some say that his actions were against his own government and were illegal when others call him a “hero” and “freedom fighter” (Edward Snowden: Leaks that exposed US spy programme, 2014).

- **Yahoo, 2013 – 2014.** The cyber-attack on Yahoo services in 2013 was the largest in history: 3 billion users were affected. During this attack, encrypted personal information was stolen, such as birth date, phone numbers, and user passwords of Yahoo services (Perlroth, 2017). Another attack occurred in 2014, which affected 500 million users.

- **WannaCry, 2017.** WannaCry is a malicious program, a network worm, and a ransomware program that infected only computers running on Microsoft Windows operating system. After the machine had been attacked, the worm program code encrypted almost all the files stored on the computer’s hard drive and offered its victim to pay a ransom in Bitcoin for decrypting them. In case the user didn’t transfer cryptocurrency to the displayed wallet, within seven days from the moment of infection, the ability to decrypt files was lost forever.

All these historical milestones showed us the importance of information and cybersecurity not only for small and large enterprises but for the average users. Modern digital threads have led cybersecurity to develop new tools to proactively and actively protect their digital infrastructure, namely: AI, deep learning, Cloud security.

Chapter 3: Specifics of the Small and Medium-Sized Enterprises

There is no concrete generally accepted definition of SMEs, the definition varies from country to country, but in most cases, the allocation of an enterprise depends on the number of people being employed. For instance, according to European Union recommendation 2003/361, SME’s

considered as companies with up to 250 employees, while Canadian term to SME's refers to up to 500 employees (Katua, 2014). Small-sized companies are those with up to 50 employees, while micro-companies have at most ten, or in some cases five, employees (OECD, 2014).

Other European Union members use a simplified legal definition depended on the number of employees and their turnover. Likewise, the case with Hungary and Moldova. A few EU members do not have a generally accepted legal definition; this is the case for Spain and Netherlands. Correspondingly, in New Zealand, there is no generally accepted definition; turnover is used by some, taxes on employee earnings and wages by other administrations (OECD, 2014).

According to the European Commission, the main factors for SME's are:

1. Number of employees
2. Annual turnover or Balance sheet

- For legal and administrative purposes:

Enterprises	Employees	Annual Turnover	Annual Balance sheet	Autonomous
Micro enterprise	1 to 9	< 2 million euro	< 2 million euro	25% or more of the capital or voting rights of another enterprise
Small enterprise	10 to 49	< 10 million euro	< 10 million euro	
Medium enterprise	50 to 249	< 50 million euro	< 43 million euro	
Large enterprise	More than 250	> 50 million euro	> 43 million euro	

- For statistical purposes:

The main criteria of SME statistics for statistical purposes are the number of persons employed.

Figure 1: EU enterprise classification. Source: (EU recommendation 2003/361., 2003)

SME state of an organization, which is part of an enterprise group, can be determined based on actual personnel number, turnover, or the balance sheet. The data should be taken from the whole group, and not only on data of the organization itself (Statistics on small and medium-sized enterprises, 2018). 9 out of 10 companies are considered as SME in the European Union (EU recommendation 2003/361., 2003). If we look at the worldwide data, we can see a similarity, where SMEs represent over 90% of commercial organizations and more than 50% of employment globally (Small and Medium Enterprises (SMEs) Finance, 2019).

SME's internationally have a massive commitment to the supply of goods and services worldwide (Bilal & Nawal Said , 2015). Small enterprises have specific characteristics that affect the methods of organizing and conducting business. Those characteristics include the structure of enterprise management, the structure of transactions for the sale of such a business, the quality of information support for capital market participants, and the methods (sometimes quite specific) that are used to evaluate them on the risks accompanying small business, etc.

Access to capital for small enterprises is quite limited (Comission, 2017). These companies, due to their characteristics, cannot fully use many capital market instruments. As a result, the cost of attracting additional financing for small enterprises is a priori higher than for large corporations with the full range of capabilities and tools for obtaining the necessary funds (Gert, 2014).

Small businesses are more mobile than large corporations. They respond more quickly and flexibly to changing market conditions. The low capital intensity of small companies allows re-profiling or liquidating the enterprise with the least losses.

The age of small companies is relatively young. The lack of historical data on the results of activities due to their absence makes it impossible to forecast the further development of the situation, which is perceived by the appraisers as an additional factor of uncertainty (risk).

It was found, that usually, the average lifetime of SME's is only five years (Jonas, 2014). The low average life expectancy of SMEs can be caused not only by high risks, lack of stability in the market, or a highly competitive environment. Some business types (e.g., in the gastronomy sector) have such a short lifespan due to the very logic of undertaking such an idea and periodic changes of its concept or liquidation of the business.

According to the Symantec cybersecurity report published in 2018, 93% of SMEs, which were attacked digitally, reported a severe effect on their daily operations. Nearly all reported a loss of funds and financial reserves. 31% announced harm to their reputation, which led to a loss of customers, as well as difficulty attracting new. Almost 50% of companies reported partial blackout in their daily business operations. Regardless of those figures, under 3 % have insurance against cyber-attacks (Millaire, 2017).

Chapter 4: Audit/Assurance Basics

Any company wants to achieve its business goals, monitor its own financial success, prevent possible frauds directed to its activities, and restrain the misapplication of its assets. Maintaining efficient systems of internal controls is essential for supporting the implementation of the processes mentioned above. There is a systematic method of collecting and analyzing proof of economic activities known as auditing. It assesses the degree of compliance between presented statements and the parameters defined and to convey the results to the concerned users (Donald & Turney, 1990). In other words, auditing is a sophisticated mechanism that reduces different kinds of risks for the organization and can fairly evaluate its correspondence with internal and external requirements.

Audits are beneficial to potential corporate partners, such as stakeholders and creditors, because when there are some problems, they provide additional assurance of investment choices. The primary objective is to determine the validity of the accountant's financial statements, and the secondary aim is to identify and avoid mistakes and fraud.

Auditing could be conducted in 2 ways, and those are internal and external audits. According to Howard F. Stettler, internal auditing is an independent evaluation activity within an organization for the examination of operations as a management service (Steller, 2011). The primary purpose of it is to assist management in the successful execution of its duties by providing them with objective analysis, evaluations, feedback and related opinions on the activities examined.

Besides, an external audit is an independent auditor's review of the company's account books of the company and the reporting that the profit and loss account and the balance sheet are drawn by the provisions of law. The financial statements reveal an accurate and fair view of the company's operations and financial statement results (Kirti, 2016). In this case, the external auditor is concerned with the legality and correspondence of the business transactions based on the presented financial statements.

Etymologically, the word "audit" comes from the Latin word “audire” - to “hear” (Auditing and Assurance, 2016). Accounting scholars state that ancient practices of auditing are mentioned during the Zhou dynasty (1122–256 BC) in China and Greek-Roman history of the 5th and 4th centuries BC (Wei & Aiken, 2003). Mainly, these governments were concerned about incompetent

clerks who were inclined to make bookkeeping mistakes and corrupt officials who were potentially motivated to commit fraud. Fraud refers to intentional financial misrepresentation to deceive by manipulating accounts and misappropriating money and goods. According to Ramamoorti, significant fraud cases like the South Sea bubble of the 18th century, and the tulip mania in the Dutch Golden Age caused a need for exercising greater control over the bookkeepers in Europe, after that those European practices of auditing were introduced into the United States (Ramamoorti, 2003).

Logically, businesses grew, and their activities on the market become more complex, which required some kind of assurance information when making serious decisions. Therefore to ensure the flow of funds from investors to businesses and the smooth functioning of the financial market, it was important for each company to persuade financial market participants that their financial statements are a fair representation of the financial position and results of the particular business (B, Simon, & Hatherly, 2005).

Consequently, the main objective of the audit function became adding credibility to the financial statements rather than identifying mistakes. At the end of the XX century, the auditor became an essential figure in affirming the truthfulness of the financial statements and in ensuring the fair presentation of the financial report (Leung & Cooper, 2004)

By 2000, series of financial scandals and the collapse of giant corporations such as Sunbeam, Xerox, Enron, and WorldCom resulted in a crisis of confidence in auditors ' work (Boynton, Johnson, & Kell, 2006). Such kind of malfunctions has been shaping and adding more value to the general role of the auditors in different countries for many years. As a result of continuous improvements made on the description of this profession, Leung stated that “The role of auditors is expected to converge: refocusing on the public interest, redefining audit relationship, ensuring the integrity of financial reports, separation of non-audit function and other advisory services” (Leung & Cooper, 2004).

Teck-Heang and Ali found that the “traditional conformance role of auditing” implies the audit practices between the 1800s and 1900s when it mostly was about verifying account accuracy and detecting fraud and mistakes (Teck-heang & Azham, 2008). But in the modern world, auditors are enhancing the integrity of financial information by disclosing irregularities, recognizing business risks, and consulting on internal control environment management (Cosserat , Leung, &

Cooper, 2004). Moreover, global companies need to improve the transparency of their financial information and raise investor confidence through independent auditing of accounting firms.

In recent years, accounting firms and audit failure cases have arisen one after another due to the lack of credibility and accuracy of corporate financial data, causing social groups to start paying attention to audit performance. Business development needs risk management, but risk management development requires internal audit support. Comparing to the past, nowadays, most of the business risks are closely related to audit risks; thus, it's necessary to increase the amount of audit work to ensure the accuracy of audit risk financial statements and certain operating risks (Huang, 2019). Gerrit Sarens et al. suggested that Internal auditors should make suggestions and assist managers in fulfilling their responsibilities by monitoring risk management adequacy and effectiveness (Sarens, De Beelde, & Evaraert, 2009). Thereby if the audit committee of the company doesn't have financial and non-accounting expertise, it has a higher chance of being found with a lack of internal control. As Jianjun Zou pointed out, improving the company's internal audit can help prevent the fraud of senior management staff and protecting the interests of shareholders and investors; it is conducive to understand the company's issues on time. Also, it contributes to the prompt correction and improvement of the company's operational efficiency; it is helpful to safeguard the company's property security (Zou, 2019).

Quality of internal audit and qualifications of auditors is an essential issue for the economy of every company and even country. Many researchers made statements about the importance of the auditor's skills, experience, and continuous education to ensure the sustainable development of the enterprises. Moreover, it was proven that the different personal characteristics of the auditors also affects the quality of the work done (Auditing Multiple Public Clients, Partner-Client Tenure and Audit Quality. , 2012). Additionally, that Ghosh and Moon stated that auditor tenure negatively affects the subjectivity of the results, thus the independence of the specialist is very crucial (Ghosh & Moon, 2005). Experts have increasingly stressed the importance of critically evaluating the evidence provided by clients to enhance the professional scepticism of auditors, given that auditors are increasingly responsible for preventing and detecting fraud. As we see, several factors have an impact on the auditing processes, and this topic is yet to be studied in the future.

In 21 centuries, while discussing the factors affecting any business process or activity, it is impossible not to mention technological change. Automation and digitization of business

information are reshaping the financial means, transforming consumers' and employers' views about jobs. According to McKinsey Global Institute's analysis of International Automation, 78% of the global labour market has about 60% of automation potential. It means that half of the workplace activities could be replaced by new technologies (Institute, 2017). Respectively, it started integrating Internal Audit (IA) robotic process automation (RPA) into the third defence line by expanding the use of conventional analytics. That includes predictive, RPA, and cognitive intelligence (CI) models (Deloitte, Adopting robotic process automation in Internal Audit, 2018).

As the large transaction populations can be tested, automation leads to a higher level of assurance. Finally, it allows transferring assurance-related activities to the front lines - to compliance, cybersecurity, risk management - where the risks should be handled and where the results can be implemented (Deloitte, "Internal audit future trends and innovation", 2019)

Forbes Insights and KPMG report on 2017 identified future trends in audit and requirements for the modern auditors. They conducted a survey of 200 financial executives from different industries in the US, asking their vision and expectation from the future of auditing. Research findings defined three primary auditor skills that clients value the most: technology, communication, and critical thinking (KPMG F. I., 2017). Clients stressed out the importance of technology skills for the specialist because they believe it could be a value-added observation that may define future opportunities for their businesses. Such requirements force auditors to go through the continuous evolvement of the skills in information technology and data science. According to King, audit firms have already expanded the new assurance service line, like SOC for cybersecurity, due to the qualified auditors of the modern era (Mervin, 2018).

Chapter 5: The Components of the Cybersecurity Audit/Assurance in SMEs

Among the national standards and guidelines on the basics of IS audit and self-assessment of IS compliance with established requirements, I would like to highlight the following documents for consideration because of their practical orientation:

- NIST 800-26: Security Self-Assessment Guide for Information Technology Systems

- NIST 800-55: Security Metrics Guide for Information Technology Systems

- NIST Special Publication 800-26 Security Self-Assessment Guide for Information Technology Systems

5.1. NIST Special Publication 800-26

The NIST Special Publication 800-26 Security Self-Assessment Guide for Information Technology Systems defines a method for self-assessing the security of systems or groups of related systems. Besides, there is a guide for the use of self-assessment results to determine the status of an organization-wide information security program. Acquired results are presented in the firm easy to determine which of the five levels established in the Federal Information Technology Security Assessment Framework document, the organization achieves for each thematic area of management tools covered in the questionnaire (NIST Special Publication 800-26, 2017).

This document is an addition to the National Institute of Standards and Technology, NIST, for the Federal Chief Information Officer. It provides information on the application of the "Federal Information Technology Security Assessment Framework" by identifying seventeen areas of management tools (Swanson, 2001).

Also, this Guide defines objectives and management practices that can be measured for each area.

The document can be used by the managers of any level or by people responsible for IT security system at organizational levels. Moreover, internal and external auditors can use the questionnaire as a guide when conducting a security analysis of IT systems.

This document contains an extensive questionnaire that defines specific goals and control methods, the use of which allows you to test and measure the security of a system or group of interconnected networks.

The proposed questionnaire is a tool for performing an internal assessment of available controls for the main application or general support system. Before its implementation, it is necessary to determine system restrictions, as well as the sensitivity and criticality of the information contained in it, processed or transmitted by the system (s).

A system is identified by defining boundaries around a set of processes, communications, memory, and related resources. Elements within these boundaries constitute a single system, each component of which must:

- be under the same administrative management tool
- have the same function or purpose
- have the same operational characteristics and safety requirements.
- be in the same shared operating environment (Swanson, 2001)

A vital element of the assessment is the determination of the effectiveness of the boundary safety management tools if the system is part of interconnected systems. Boundary controls should protect a system or group of systems from unauthorized influences. If such boundary controls are ineffective, then the security of the systems under analysis depends on the protection of other operations associated with them. If there are no adequate boundary controls, then management indicates the need to determine and document the adequacy of controls for each system that is associated with the system in question.

Effective use of the questionnaire implies an understanding of the significance of the evaluated systems and information. The assessment can be expressed by the level of sensitivity or criticality of operations and information regarding each of the five protection categories:

- integrity,
- confidentiality,
- availability,
- authenticity,
- non-repudiation.

Moreover, authenticity and non-repudiation are considered as properties of integrity. The guide indicates three degrees of sensitivity: high, medium, and low. For example, a system and its information may require a high degree of integrity and availability, but a moderate degree of confidentiality (NIST Special Publication 800-26, 2017).

The evaluation questionnaire contains three sections: title page, questions, and notes. The survey begins with a title page that requires descriptive information about the main application,

the general support system, or a group of evaluated interconnected systems. The questionnaire provides a hierarchical approach to the assessment of the system by including critical elements and secondary issues. The level of essential components should be determined based on answers to secondary questions. Minor issues reflect goals and management practices that can be implemented to meet the critical element. As an example, figure 2 below shows a part of the questionnaire from this guide.

An organization may supplement questions, but it is not permitted to remove questions or modify them from the questionnaire. Each question is followed by a comment field and a first field. The comment field can be used to link to supporting documentation that is attached to the questionnaire. The first field can be used if a decision is made (based on the results of a risk assessment) not to implement a control tool or if the control tool does not apply to the system.

Questions are divided into three main areas of management:

1) administrative controls.
2) operational controls.
3) technical controls.

There are several topics in each of the three management areas: for example, personnel safety, emergency planning, and incident response are topics within the operational area of management. The questionnaire has a total of seventeen subjects; each item contains critical elements and supporting goals and methods of security management (questions) regarding the system. If some goals and management methods are not realized, this does not satisfy the requirements of critical elements (NIST Special Publication 800-26, 2017).

Each goal and management method may or may not be realized depending on the system and the risk associated with the system. For each issue regarding goals and management methods, a reference is made to one or more source documents (Ross, Katzke, & Johnson, 2015).

The safety management areas proposed by this Guide for evaluation are following:

Management Controls

1. Risk Management

2. Review of Security Controls
3. Life Cycle
4. Authorize Processing (Certification and Accreditation)
5. System Security Plan

Operational Controls

6. Personnel Security
7. Physical Security
8. Production, Input/Output Controls
9. Contingency Planning
10. Hardware and Systems Software Maintenance
11. Data Integrity
12. Documentation
13. Security Awareness, Training, and Education
14. Incident Response Capability

Technical Controls

15. Identification and Authentication
16. Logical Access Controls
17. Audit Trails

In order to measure the implementation of the required security management tool, five levels of effectiveness are proposed for each answer to the question about the security management tool:

• Level 1: The purpose of the control is documented in a security policy.
• Level 2: Security controls are documented as procedures.
• Level 3: Procedures are implemented.
• Level 4: Safety management procedures and tools are tested and analyzed.
• Level 5: Security management procedures and tools are fully integrated into a comprehensive program (NIST Special Publication 800-26, 2017).

The method for answering questions can be based primarily on the examination of documents related to the issues and thorough research and testing of controls. An analysis, for example, should consist of:

- testing existing access control methods by performing a penetration test
- consideration of system documentation, like request forms for software changes, tests, and acceptance plans
- viewing security logs and audit records.

Experts and system owners should be assigned to determine whether the level of sensitivity of the system confirms the implementation of the control tool defined in the question. The main features you should pay attention to while using management tools are: to check whether there are documented policies (level 1), procedures for implementing the management tool (level 2), whether the management tool is implemented (level 3), whether the management tool is tested, and if it is ineffective, is corrected whether (level 4) and whether the control is part of the organization's culture (level 5).

Based on answers to questions regarding management goals and methods, together with the system owner and those who are responsible for system administration, the expert should conclude the level of a critical element. It should consider the relative importance of each goal/method to achieve a critical element and the accuracy with which the process is implemented, operated, and tested.

The questionnaire can be used for two purposes. Firstly, by the leaders of the organization, who know their organization's systems and safety management tools, to determine where security is required for the system, group of operations, or the whole organization. Secondly, it can be used as a guide for a comprehensive assessment of the security level of a system (NIST Special Publication 800-26, 2017).

The results of such analyzes can serve for:

- report on compliance with requirements

- preparation for audits

- identification of resource requirements

Completed self-assessment questionnaires can be a source for compiling safety reports required by the organization.

The report should address the following organizational-wide security topics:

- security management
- administrative controls
- operational controls
- technical controls
- planned actions

The report includes a brief summary of planned steps related to informational security. The review should consist of goals, actions needed to achieve goals, planned resources, and their estimated dates for completion (NIST Special Publication 800-26, 2017).

5.2. NIST 800-55 Security Metrics Guide for Information Technology Systems

The purpose of the document is to provide a standardized approach to the development, selection, and implementation of IT security metrics to be used to measure the effectiveness of IS management tools used in the organization. The Guidelines provide a recommended methodology for quantitatively measuring the seventeen thematic areas of security management tools defined in NIST 800-26, Security Self-Assessment Guide for Information Technology Systems. The measurement methodology can be used to confirm the fulfilment of system safety tasks and confirm the effectiveness of information security controls (NIST, 2008).

The manual describes how an organization, by metrics, can assess the adequacy of appropriate IS controls, policies, and procedures. This document helps management decide whether to fund additional security resources or to identify and evaluate unproductive controls. The paper explains the process of developing and implementing metrics, defines the roles and responsibilities of the organization's personnel responsible for the development and implementation of IT security metrics, and shows how parameters can be used to justify investments in information security management adequately. The target audience for the Guide is IT managers and security professionals at all levels.

An organization's IT security metrics program consists of four interrelated parts:

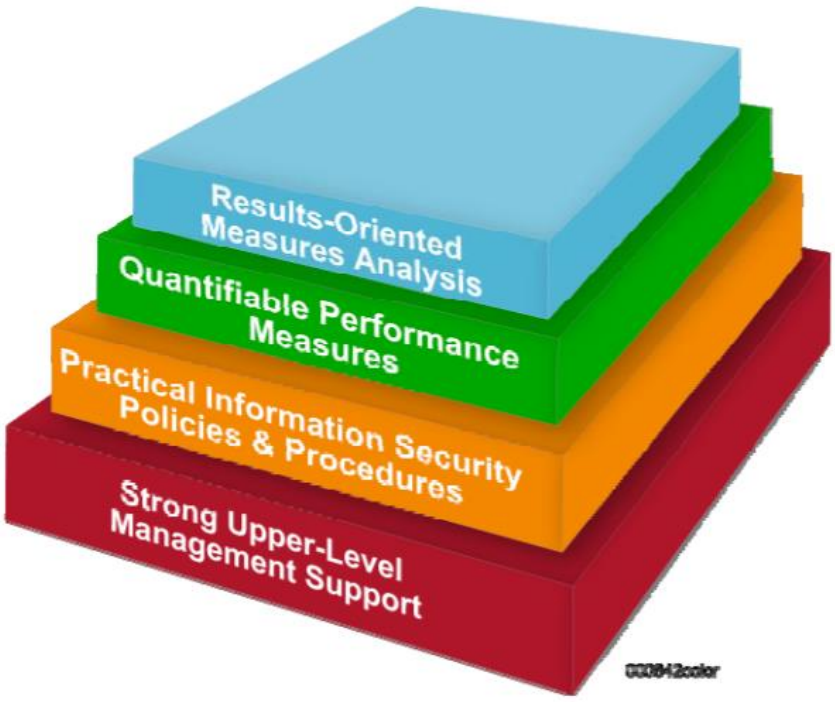

Figure 2: Security metric. Source: (NIST, 2008)

• first, basic, level - strong support of the program by top management of the organization. Without this support, not only the implementation of the security metrics program is impossible, but also an implementation of the information security program of the organization as a whole. This element draws the attention of representatives of the highest levels of management of the organization to its information security. As noted, without the support of officials managing IT

resources, the implementation of a security metrics program in an organization can be completely ineffective due to possible political pressure and budget constraints.

The second component of an effective program is the practical security policies and procedures developed by the body responsible for ensuring compliance. Such policies and procedures should, in the first place, be practicable and ensure reasonable security through appropriate management tools (protective measures). If these procedures and policies are not implemented, it can be extremely challenging to obtain metrics.

The third component of the program is the development and implementation of quantitative metrics that are designed to collect and provide meaningful information about the effectiveness of the security of the organization's IT systems. For quantitative security metrics to offer useful information, they must be based on the goals and objectives of adequate protection. At the same time, they must be easy to form and allow measurement.

The fourth component of the program is the periodic analysis of data obtained by the usage of metrics (NIST, 2008).

Research results can be used: to further use the experience gained to increase the effectiveness of the used safety controls (protective measures) and to plan new controls to ensure compliance with new safety requirements. If it is assumed that the data collected should be meaningful for the management and improvement of the information security program of the organization, the collection of accurate data should be a priority for stakeholders and users.

Metrics are tools that simplify decision-making and, at the same time, improve the quality of work and reporting system of the organization. It can be achieved by the collection and analysis of the necessary data on the quality of work and the preparation of relevant reports. The basis of metrics is the goals and objectives of effective IT security. The purposes of effective IT security provide the necessary results that are expected from the implementation of the information security program in the organization. The realization of goals helps to implement the tasks of effective IT security. Tasks determine the practices (according to the provisions of security policies and procedures) by which it is proposed to implement protective measures throughout the organization. Monitoring the process of fulfilling tasks and achieving goals is carried out using IT security measures. When monitoring is carried out, the level of implementation, the effectiveness, and

efficiency of protective measures are analyzed, the adequacy of safety activities is tested, and possible actions for improvement are determined (NIST, 2008).

When developing and implementing IT security measures, the following conditions must be met:

- They should produce results in a quantifiable form (percentages, averages, and absolute values);
- Data to support measures should be easily accessible;
- Dimension is applicable only to repeat the process;
- Measures should be useful for tracking the effectiveness of protective measures and resource management.

The given document provides examples of metrics based on critical security controls and methods contained in NIST 800-26. The presented models of metrics can be used either as it is or can be corrected or supplemented according to the existing goals and objectives of effective IT security in the organization.

NIST 800-55 defines three types of IT security measures:

* implementation measures-to assess the implementation of adopted policies, standards, and is procedures in an organization.

* performance/performance measures to assess the results that depend on the security services provided.

* impact measures-to assess the impact of security-related events on an organization's business operations or its mission (NIST, 2008).

The types of measures that can be obtained and that can be useful for improving efficiency depend on the maturity of the company's security program and the maturity of the implementation of system security controls.

Different types of measures can be used at the same time. Still, the initial focus of the standards changes as the maturity of the implementation of security management tools develops (i.e., there is a gradual transition from the use of the first type of metrics to the use of the third type of metrics).

Management defines the approach and process for developing IT security measures for the organization. The implementation and use of the IT security measures in an organization are accomplished through two processes: measures development process and the measures implementation process.

The measures development process defines the initial set of measures and allows you to select its subset that is appropriate for the organization at a given time.

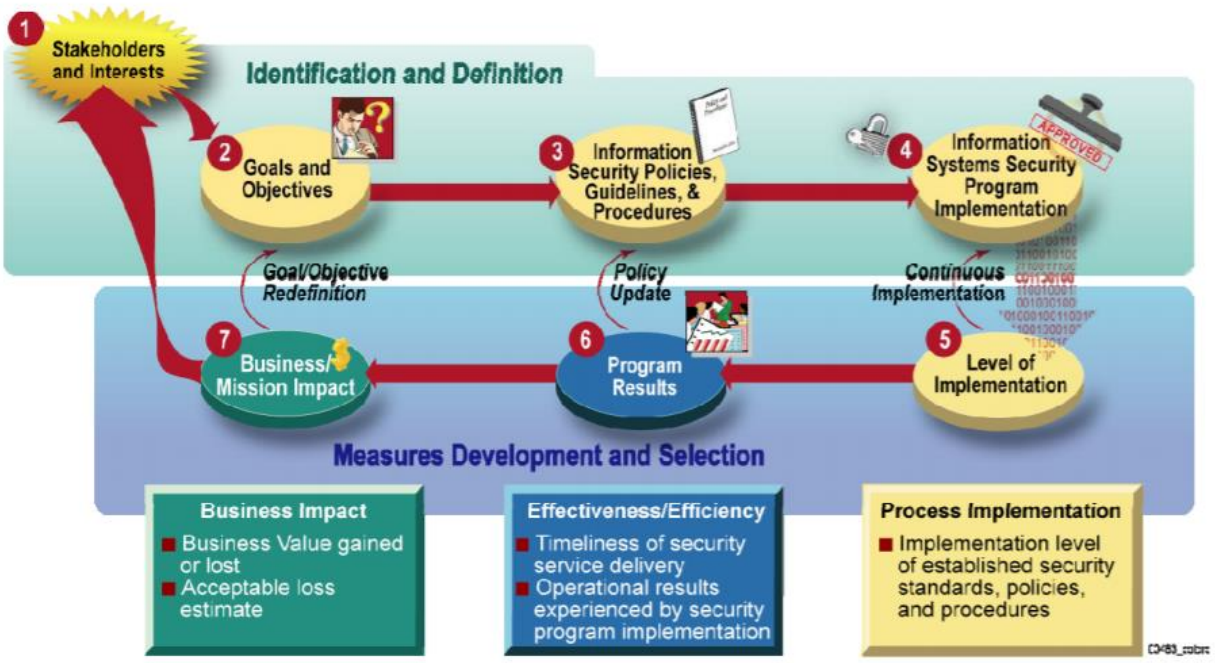

Figure 3: Information Security Measures Development Process. Source: (NIST, 2008)

The process of developing IT security measures consists of two main activities:

- Identification and definition of a valid IT security program (elements 1-4 in figure 1);

- Develop and select specific measures to assess the implementation, effectiveness, efficiency, and business impact of security management tools (elements 5-7 in Fig. 13, which correspond to the three types of metrics listed above).

As noted in the document, the order of the steps of the measure's development process may deviate from the specified sequence. Furthermore, the process shown in figure 14 provides a framework for understanding standards and simplifies the identification of measures to be developed for each system. The type of actions depends on the IT system lifecycle stage and the maturity of its system security program. The presented structure simplifies the adaptation of measures to the needs of a particular organization and the needs of various stakeholders.

The second activity in the measures development process (elements 5 - 7 in figure 14) involves the development of measures to assess the implementation of standards, policies, and procedures to ensure the security of the organization's IT systems, their effectiveness, and impact on the organization's mission. The specific aspect of its security that measures focus on at a given point in time depends on the level of security effectiveness as defined in NIST SP 800-26 (i.e., the maturity level of an organization is the program). Measures can be developed from the examples of its security measures in Appendix A of this document (or used directly without further development).

The guide suggests forming metrics in the template presented in the table below.

Field	Data
Measure ID	State the unique identifier used for measure tracking and sorting. The unique identifier can be from an organization-specific naming convention or can directly reference another

Goal	Statement of strategic or information security goal. For system-level security control measures, the goal would guide security control implementation for that information system. For program-level actions, both strategic goals and information security goals can be included. For example, information security goals can be derived from enterprise-level goals in support of the organization's mission. These goals are usually articulated in strategic and performance plans. When possible, include both the enterprise-level goal and the specific information security goal extracted from agency documentation, or identify an information security program goal that would contribute to the accomplishment of the selected strategic goal.
Measure	Statement of measurement. Use a numeric account that begins with the word "percentage," "number," "frequency," "average," or a similar term. If applicable, list the MST SP 800-53 security control(s) being measured. Security controls that provide supporting data should be stated in Implementation Evidence if the measure applies to a specific FIPS 199 impact level (high, moderate, or low). State this level within the proposal.
Type	Statement of whether the measure is implementation,
Formula	The calculation to be performed that results in a numeric expression of a measure. The information gathered through listing implementation evidence serves as an input into the formula for calculating the ratio.
Target	Threshold satisfactory rating for the milestone completion or a statistical measure. The target can be expressed in percentages, time, dollars, or other appropriate units of measure. Target may be tied to a required completion time frame. Select the final and interim target to enable tracking of progress toward a stated goal.

Implementation evidence	Implementation evidence is used to compute the measure, validate that the activity is performed, and identify probable causes of unsatisfactory results for a specific measure. For manual data collection, identify questions and data elements that would provide the data inputs necessary to calculate the measure's formula, qualify the measure for acceptance, and validate provided information. For each question or query, state the security control number from NIST SP 800-53 that provides information, if applicable. If the measure is relevant to a specific FIPS 199 impact level, questions should state the impact level. For automated data collection, identify data elements that would be required for the formula, qualify the measure for acceptance, and validate the information provided.
Frequency	Indication of how often the data is collected and analyzed, and how often the information is reported. Select the frequency of data collection based on a rate of change in the particular security control that is being evaluated. Select the frequency of data reporting based on external reporting requirements and internal customer preferences.
Responsible Parties	Indicate the following key stakeholders: • Information Owner: Identify organizational component and individual who owns required pieces of information; • Information Collector: Identify the organizational component and an individual responsible for collecting the data. (Note: If possible, Information Collector should be a different individual or even a representative of a different organizational unit than the Information Owner, to avoid the possibility of a conflict of interest and ensure separation of duties. Smaller organizations will need to determine whether it is feasible to separate these two responsibilities.); • Information Customer: Identify the organizational component and individual who will receive the data

Data Source	Location of the data is to be used in calculating the measure. Include databases, tracking tools, organizations, or specific roles within organizations that can provide the required information.
Reporting Format	Indicates how the measure will be reported, such as a pie chart, line chart, bar graph, or other formats. State the type of format or provide a sample.

Table 1: Measures Template and Instructions. Source: (NIST, 2008)

The table below provides an example of IT security metrics contained in Appendix A of NIST 800-55.

Field	Data
Measure ID	Security Budget Measure 1
Goal	Strategic Goal: Establish an environment of comprehensive security and accountability for personnel, facilities, and products. Information Security Goal: Provide resources necessary to properly secure agency information and information systems.
Measure	Percentage (%) of the agency's information system budget devoted to information security. NIST SP 800-53 Controls — SA-2; Allocation of Resources
Measure Type	Impact
Formula	(Information security budget/total agency information technology budget) *100
Target	Should be an organizationally defined percentage.
Implementation Evidence	What is the total information security budget across all agency systems (SA-2)? What is the overall information technology budget across all agency systems (SA-2)?
Frequency	Collection Frequency: Organization-defined (example: annually) Reporting Frequency: Organization-defined (example: annually)
Responsible Parties	• Information Owner: Chief Information Officer (CIO), Chief Financial Officer (CFO). Senior Agency Information Security Officer (SAISO) (e.g., Chief Information Security Officer [CISO))

	• Information Collector: System Administrator or Information System Security Officer (ISSO), budget personnel • Information Customer: Chief Information Officer (C10), Senior Agency Information
	Security Officer (SAISO) (e.g., Chief Information Security Officer [C1SOD, external audiences (e.g., Office of Management and Budget)
Data Source	Exhibit 300s, Exhibit 53s, agency budget documentation
Reporting Format	Pic chart illustrating the total agency information technology budget and the portion of that budget devoted to information security

Table 2: IT security metrics. Source: (NIST, 2008)

The process for implementing the IT security metrics program defined in this document is illustrated in the Figure below.

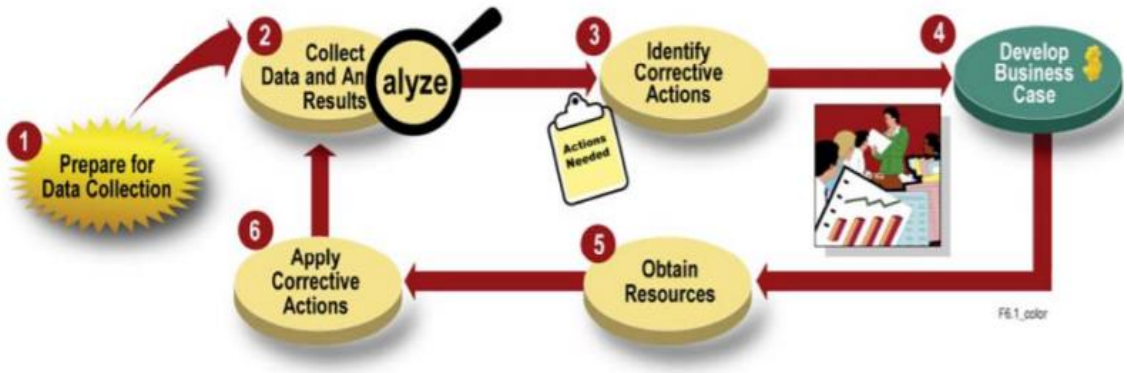

Figure 4: Information Security Management Program Implementation process. Source: (NIST, 2008)

Phase 1. "Preparing for data collection" includes the functions that are the basis for the creation and implementation of its security measures, including the definition, development, and selection of standards and the development of the measures program implementation plan. Phase 1 defines the steps to collect, analyze, and report measures. These steps should be documented in the measures program implementation plan. The procedure may include the following issues:

- roles and responsibilities of actions, including data collection, analysis, and reporting;

- the audience for the plan;

- measures collection, analysis and reporting process, adapted to organizational structure, operations, policies, and procedures;

- creation, selection, and modification of data collection and control tools;

- format of a summary report on measures;

Phase 2. "Data Collection and analysis of results" includes the following functions:

- collection of metrics data according to the processes defined in the metrics program implementation plan;

- combine the data collected and save in a format that facilitates data analysis and data reporting, such as in a database, in spreadsheets;

- conduct gap analysis-compare collected measurements with objectives and identify gaps between actual and desired performance;

- identification of causes of poor functioning;

- identification of areas that needs improvement (the improvement);

Phase 3. "Identification of corrective actions" includes the following actions:

- define the range of corrective actions;

- training of staff, system administrators or regular users;

- delivery of security tools;

- change of system architecture;

- establishment of new processes and procedures and modernization of security policies;

- prioritize corrective actions;

Phase 4. "Business portfolio Development "and **phase 5**" resource Acquisition " provide funding for the cycle needed to implement corrective actions.

Phase 6. "Application of corrective actions" includes the implementation of corrective actions in the technical, administrative, and operational areas of safety management tools.
Once corrective actions are applied, the cycle is completed and re-started with subsequent data collection and analysis. Operational data collection, analysis, and reporting will track the development of corrective actions, measure improvement, and identify areas for further growth.
NIST SP 800-55 is a necessary complement to NIST SP 800-26, its security self-assessment Guide, which is used by us Federal agencies to plan their own annual budgets, in particular the costs of informational security (NIST, 2008).

Chapter 6: The Frameworks for Cybersecurity Audit/Assurance

Nowadays, there are several cybersecurity frameworks widely used worldwide, and demand is increasing due to the different requirements necessary for each type of business. It has contributed to the introduction of many initiatives designed to help companies implement comprehensive cybersecurity programs.

- PCI DSS (47%) (htt)

PCI DSS focuses on the particular threats and risks to protection in the payments industry. It defines security criteria for protecting payment card data, as well as validation and guidance procedures to help organizations understand the purpose of the criteria. PCI DSS identifies security criteria for protecting payment card data, as well as validation and guidance protocols to help organizations understand the purpose of the requirements.

- ISO 27001/27002 (35%)

The cybersecurity architecture of ISO 27001 is composed of international standards that prescribe the criteria for managing information security systems. ISO 27001 follows a risk-based mechanism allowing businesses to put in place steps to identify security risks impacting their information

systems. The ISO 27002 specification, on the other hand, includes international standards outlining the controls an organization can use to maintain the protection of information systems. It was developed to be used together with ISO 27001 organizations use both to show their commitment to the various standards imposed by different regulations.

- CIS Critical Security Controls (32%)

CIS v7 lists 20 actionable cybersecurity specifications designed to strengthen safety performance in all organizations. Since the CIS has a credible reputation for designing baseline security systems, most organizations consider the security criteria as best practice. CIS v7 helps companies to build budget-friendly cybersecurity systems and encourages them to make cybersecurity activities a priority.

- ISACA, IS Audit/Assurance Program, USA, 2017 (www)

ISACA has established a new IS audit/assurance system, Cybersecurity: Based on the NIST Cybersecurity Framework, due to the need for audit and assurance systems and processes around cybersecurity. The purpose of this program is to provide a structured, repeatable way to validate cybersecurity controls for organizations. The software is based on the NIST Cybersecurity Framework, and it is provided as a column-created Microsoft Excel file allowing users to identify controls to be checked, as well as adding references and comments.

- NIST Framework for Improving Critical Infrastructure Security (29%) (Melanie, 2019)

The NIST framework aims to protect critical infrastructures, and private companies are adopting it to improve their cyber defences. NIST CSF outlines five functions which manage data and information security risks; they are - identify, protect, detect, respond, and recover.

- COBIT 2019 (Control Objectives for Information and Related Technologies)

This framework, which is developed by ISACA, combines the best aspects of a company into its IT security, management, and governance. The COBIT cybersecurity platform is useful for businesses that aim to increase the quality of production while at the same time adhering to improved safety practices.

- TC CYBER (Technical Committee on Cyber Security) (Mutune, 2020)

The framework was designed to enhance the quality of telecommunications across countries within European zones. It proposes a set of privacy awareness standards for individuals or

organizations, which focuses on ensuring that they can enjoy high privacy levels while using different telecommunication channels.

- KPMG's Global Cyber Maturity Framework (KPMG, 2016)

KPMG has developed a global Cyber Maturity Framework specifically to help organizations tackle significant information security challenges by incorporating the most applicable elements of existing international standards and governance structures. Compared to existing cybersecurity frameworks, KPMG's Cyber Maturity Framework is believed to be a wider, more comprehensive, and more systematic way of approaching board involvement and how boards should exercise their oversight obligations.

Czech Cyber Security legal frameworks:

- Act on Cyber Security and Change of Related Acts (Act no. 181/2014 Coll.)
- The Decree No 82/2018 Coll. on Security Measures, Cybersecurity Incidents, Reactive Measures, Cybersecurity Reporting Requirements, and Data Disposal (the Cybersecurity Decree)

Organizations with more than 10,000 personnel employed are slightly more likely to follow security framework (90%), but even smaller organizations with fewer than 1,000 employees report significant rates of adoption (77%) (Melanie, 2019).

The issue with the popular frameworks above is that they are too complicated and require certified personnel to conduct the audit, which is a financial bottleneck in the case of small enterprises. However, there is a SMESEC lightweight framework, which is specially made for small and medium-sized businesses with limited financial and human resources, which will be covered in the next parts of the thesis.

Act on Cyber Security and Change of Related Acts (Act no. 181/2014 Coll.)

Czech cybersecurity legislative framework, the Act on Cyber Security and Change of Related Acts (Act no. 181/2014 Coll.), was implemented in 2015, January 1st, and it consists of several regulations that immediately came into force on the exact day (Minárik, 2020).

It defines several types of regulated organizations and specifies their legal responsibilities as the national authority and the competencies of the NCISA (Národní úřad pro kybernetickou a informační bezpečnost)

In general, these categories represent, in descending order, the scope of the legal obligations imposed:

1. Critical information infrastructure operators
2. Operators of essential services
3. Operators of vital information systems
4. Digital service providers
5. Electronic communications service providers or electronic communications network operators
6. Operators of significant networks as specified by law (Minárik, 2020)

The document contains the definition of terms for each category, for instance, essential service means a service that relies on electronic communication networks or information systems and whose interruption may have a significant effect on the protection of social or economic operations in any of the following sectors (ACT, 2014):

1. Energy
2. Transport
3. Banking
4. Financial market infrastructures
5. Health sector
6. Water resource management
7. Digital infrastructure
8. Chemical industry (ACT, 2014)

The act is based on laws relating to the protection of critical infrastructure and crisis management, thus integrating critical technology infrastructure security into a broader context of essential infrastructure safety and inferencing requirements under crisis management regulations as well.

The act is focused on several organizational measures, divided into three main sectors:

1. Security measures: Organizational and technical
2. Organizational measures: Information security management system, Risk management, Asset Management, etc.
3. Technical measures: Physical security, Communication network integrity protection tools, Malicious code protection tools, Application Security, etc. (ACT, 2014).

Measures are activities that are required to safeguard information systems or services and digital communication networks from risks in the field of digital security or to resolve an already emerged cybersecurity incident (ACT, 2014)

Measures classified as:
a) Warning
b) Reactive measure
c) Protective measure

Mainly, Act on Cyber Security responsibilities, and Change of Related Acts apply to risk control, information protection, protection of the supply chain, and incident management (ACT, 2014).

The Decree No 82/2018 Coll. on Security Measures, Cybersecurity Incidents, Reactive Measures, Cybersecurity Reporting Requirements, and Data Disposal (the Cybersecurity Decree)

The aim of the Cyber Security Act No. 181/2014 Coll. is to bring into effect a series of rights and responsibilities to improve digital security and to create an active collaboration process between the private and public sectors. Clear responsibilities are given for organizations impacted by the Cyber Security Act legislation, such as the form and reporting standards for cyber-security incidents. Through meeting these responsibilities, the security of these organizations 'information or communication systems, as well as the networks they run, will be improved (Decree No. 82/2018, 2020).

Decree focuses on a certain organizational measure, such as Information security management system; Asset management; Risk management, Cybersecurity audit, etc. (Coll., 2018).

Let’s focus on Cybersecurity act within Decree No 82/2018:
Within the framework, the obliged entity should:

- Document security policy in compliance with audit, including review of technical compliance

- Asses compliance with security measures with internal regulations, best practices, and other contractual obligations

Also, Decree is obliging organizations to conduct regular cybersecurity audit intervals of at least 2 or 3 years. In case if organizations cannot meet these time intervals, they can carry out their audit continuously, in systematic units. However, in this case, organizations must finish their cybersecurity audit within five years latest. The results of the cybersecurity audit report should be submitted to the operator of the information and communication system (Coll., 2018).

Cybersecurity auditor within decree 82/2018 is defined as per the table below:

Role:	**Cybersecurity Auditor**
Key activities	Conducting cybersecurity audits
Knowledge	1. Methodology and frameworks of the information security audit. Internal audit processes and procedures. 2. Internal audit roles and functions. 3. ICT security audit conducting process. 4. Strategic and tactical ICT management. 5. ICT acquisition, development, and deployment. 6. ICT operation, maintenance, and service management. Protection of assets. 7. Cybersecurity assessment, methods for testing and sampling. Relevant legislation. 8. ICT security.
Experience:	1. Information and cybersecurity audit planning. 2. Conducting cybersecurity audits or information security management audits. 3. Analyzing audit results.

	4. Writing audit conclusions, presenting them, and proposing recommendations to remedy the findings. 5. Reporting of compliance with legal requirements. 6. Audit conduction focused on ICT, information security, or cybersecurity.
Education and practice:	1. At least three years of practice in the information or cybersecurity audits 2. Graduation at the university level and at least one year of training in the information or cybersecurity audits.
Relevant certifications	• Certified Information Systems Auditor (CISA), Certified Internal Auditor • (CIA), Certified in Risk and Information Systems Control (CRISC), Lead • Auditor Information Security Management System (Lead Auditor ISMS), Auditor of information security

Table 3: Cybersecurity auditor. Source: (Coll., 2018)

SMESEC framework

Currently, the SMESEC framework is in its Alpha status and will be fully released in the last quarter of 2020. SMESEC framework is intended to be user-friendly and can be implemented with little training. Per their description on the main page, "The SMESEC consortium is proposing to develop a cost-effective suite of cyber-security tools. The suite supports SMEs in managing network information security risks and threats and identifying opportunities for implementing secure, innovative technologies for the digital market. As a benefit, the framework shall allow SMEs not only to look at cyber-security as an obstacle but also as an opportunity for business." (SMESEC, 2019). What makes this framework unique from the traditional ones is the fact that it is aimed to provide cybersecurity training to all types of employees, and it is a particular focus on the European market, unlike any other framework.

The framework can be used not only to secure the traditional business process, yet it can be implemented for several cases given below:

- Smart city: Framework is planned to be used in Sense. City platforms used for communication between citizens and city authorities and currently aimed at urban issue solving.

- Industrial IoT: SMESEC is partnering with Worldsensing IoT company, to test on their environment their various sensors and software. SMESEC consortium aims to show the benefits of their framework by checking it in a real environment.

- Smart Grid: Partnership with PowerVAS platform to test their framework by collecting structured and unstructured data.

- E-Voting: Scytl's Online Voting platform will be using the SMESEC network for the private and secure online voting process.

SMESEC has the following components:

Framework components are divided into six main categories. For each element, within the framework, their description, responsibility, input, and output are described.

- Data collection consists of the tools, XL-SIEM agents, and EWIS agents. Given components are made explicitly to collect SME's data, which will be analyzed in the next phase. The monitoring of sources is done through Citrix ADC.

- Endpoint protection and offline tools contain Citrix ADC, Gravity Zone endpoint, TaaS, Virtual patching, Testing Platform, and Moving target. All these tools are aimed to strengthen IT infrastructures located on the SME's property, as well as to increase the security of products, developed by SME's

- Data analysis combine all information retrieved by the data collection and endpoint protection tools, studies the data, and train it for the presentation and orchestration modules. Latter are aggregators in the SMESEC Framework: Gravity Zone, XL-SIEM, EWIS, and Citrix ADC Aggregator

- Training and security measurement tools are planned to evaluate both the cyber-security level of the organizational infrastructures and the alertness and expertise in the IT security of the employees. Additionally, the SMESEC framework consists of tools like CySec that sets itself a target to increase awareness and give proper cyber-security training to the company employees. Training and security assessment tools include the following: CySec on-prem, CySec on-Cloud, Risk Assessment Engine, and training platform.

- The orchestration category consists of SMESEC Hub and extensions module. Extensions module has a variety of plugins that utilizes hardcoded rules, alongside AI-generated patterns, to analyze all the data retrieved and output alerts and proposals.

- Presentation module is the interface made explicitly for SMESEC Framework users. The interface is easily customizable per user needs (SMESEC, 2020).

Chapter 7: Practical Part

Introduction

The practical part aims to analyze the possible implementation of SMESEC in the real environment and to find its pros and cons for the organizations within the EU with the limited financial and economic resources. The analysis will be conducted using primary and secondary resources.

What makes this practical work useful for SME's that there is currently no research focused on the framework, and by analyzing its current state small and medium enterprises can decide whether to consider this framework to protect their digital assets from internal and external threats.

The practical part will mainly focus on the benefits of implementation of SMESEC in comparison with widely used frameworks, steps to implement it, costs of its adoption, and its outputs.

7.1. Goals of SMESEC

SMESEC's fundamental goal is to define what the needs are from the viewpoint of SMEs and turn them into specifications for a unified framework, which will ultimately consist of various products from the SMESEC members. The frame is targeting multiple market segments, including IoT devices and smart city solutions. Furthermore, the SMESEC framework is trying to achieve the most cost-effective way to implement its structure, which is a crucial factor for SMEs. Notably, at the beginning stage, newly founded organizations, opened by self-employed entrepreneurs, typically have survival rates in the first five years, between 30-60% and less (Carrigan, 2020).

SMESEC has identified key digital areas, where protection of cyberspace of organizations is a must, and the goal of this framework is to maximize its resistance against internal and external threats. Those areas are namely: (SMESEC, 2020)

- Web servers (front-end): Since the majority of SMEs are using multiple or at least one web service in their daily business operations, it is a must to provide the required tools to protect web-based applications and servers.

- Database servers (back-end): Contemporary businesses cannot survive without data regarding financial transactions, customer data, or data from hardware devices they use (sensors, IoT devices), hence why it is vital to protect their databases. Potential loss or damage of the sensitive information can lead to unexpected reputational and financial losses, which SME’s cannot afford with their limited financial capabilities. SMESEC is aiming to provide all tools to reduce the risk of leakage or loss of data.

- Network interconnectivity: Local network or external internet connectivity is essential for smooth daily business processes. A simple DDoS attack can shut the servers, making them unavailable for the customers, which will lead to reputational and financial losses. Firewalls and network filters recommended by the SMESEC framework will reduce the risk of such threats.

- Cloud: Since cloud services are getting more affordable for the organizations, especially compared to the traditional hardware solutions, SMESEC is considering cloud as one of the areas, to pay extra attention to and protect.

- Gateways: IoT sensors and hardware devices use gateways to share the data, and potential vulnerabilities in the system can result in their abnormal behaviour.

- Virtual Machines: With the rapid usage of Virtual Machines running on personal computers, SMESEC should provide protection tools to safeguard applications inside the virtual environment.

Various types of exploits are covered in the SMESEC framework. Antivirus software (example: “Bitdefender”) and firewalls/IDS (“CITRIX ADC” and “FORTH”) will potentially identify above mentioned in the table exploits. Per SMESEC recommendation, software source code must be invisible for the general public and inaccessible for external network users (SMESEC, 2019).

7.2. Benefits of SMESEC

One of the main advantages of the SMESEC framework is that consortium is trying to achieve the most cost-effective way to implement their solutions. The framework is designed to support small and medium organizations to manage their digital risks and threats and help them identify new market opportunities by the usage of the latest cybersecurity tools.

Benefits of SMESEC:

- Flexibility and adoption of the framework into a variety of segments, including IoT devices and e-Voting

- Simplicity: innovational protection tools should decrease the overall complexity of the system. The user-friendly UI of the dashboard is understandable by the employee without a dedicated technical background.

- Protection: SMESEC framework is aiming to provide at least the same or better level of protection currently offered by other available frames.

- Training and awareness: One of the weakest points of the cybersecurity infrastructure is personnel. Without proper training, they are not aware of how IT infrastructure can be attacked externally. By providing employees with simple training materials, SMESEC aims to decrease the risk of credential reuse or social engineering attacks (SMESEC, 2020).

Chapter 8: Implementation of SMESEC Framework to EU SME's

Currently, SMESEC in its testing phase for European SMEs, and it is organized around below five concepts:

1. Definition & Recommendations
2. Discovery & Solutions
3. Protection & Response
4. Extensive validation
5. Training & Awareness (Atos Research, 2020)

Given principles reflect the phases of a full lifecycle for cybersecurity defence, and each of them is realized through a series of processes provided by SMESEC partners. On top of that, to enhance the consistency of the proposed studies, this lifecycle is evaluated, considering four target groups through the proposed use cases (Business partners, Public Services, People, and Technicians). (Atos Research, 2020)

8.1.1. Definition & Recommendations

This phase of a framework contains current market analysis for SMEs, and it is providing a list of their standard systems and services that should be protected.

SMESEC has classified threats as internal and external.

Internal threats have been identified for small and medium-sized enterprises as potentially more harmful than external ones since a potential attacker will have closer access to its internal IT infrastructure.

- Users privacy compromise: Information of the system's users, which is stored in the database, can be compromised, and their privacy revealed.

- Alteration or deletion of sensitive data and/or software: Malicious insiders could delete or manipulate private data, which can result in reputational/financial loss.

- Internal attack to the system (Code injection, DoS attack): Attack of IT infrastructure by the usage of its own resources (software and hardware)

- Data leakage: Leakage of sensitive customer or employee data can be critical for SME's (SMESEC, 2020).

The four use cases have identified the external threats that their system may face and have grave consequences for their infrastructure. External adversaries could vary from enterprise espionage and malicious competitors up to hacktivists. Malicious competitors aim to attack the reliability and the proper operation of an enterprise for creating margins to gain a more substantial part of the market. All the groups of mentioned attackers pose the following list of potential external threats (SMESEC, 2020):

- Unauthorized use of the system: Only limited users should be granted access to sensitive information. Unauthorized access can result in threats to the system, as listed below.

- Privacy compromising: Leakage of private data of the system by server compromise is a severe hazard for all SME organizations.

- Alteration or deletion of data: Alteration or removal of sensitive data is a threat majority of SME's are facing, and SMESEC theoretically will reduce the risk of remote attack

- DDoS attacks: Small and medium-sized enterprises suffer from DDoS as often as large companies. Such attacks are harmless from the organization's point of view, and the necessary tools can be easily purchased on the Web, which is used by ill-wishers, dishonest competitors, offended customers, and other attackers. At the same time, the consequences of a DDoS attack for small organizations can be more harmful and destructive, since their business often depends entirely on the availability of online

resources, and such companies are not able to create duplicate systems during the attack (SMESEC, 2020).

8.1.2. Discovery & Solutions

This phase of the cycle contains steps and procedures of risk evaluation, vulnerabilities detection, and recommendation on cybersecurity.

Unlike other traditional frameworks, SMESEC is offering a friendly UI interface to assess the current status of cybersecurity within the organization.

Unlike traditional frameworks, usability is a must of the SMESEC Framework. It is because SMESEC is specifically designed to be used by a variety of SME employees, with diverse expertise and knowledge. For the development of appropriate user experience (UX) and identify the target personas of the SMESEC Framework, they expanded previous interviews with their use-case SME partners, that have a joint application design workshops. It was needed for the UI interpretation in a partnership with the cybersecurity responsible in these small and medium-sized enterprises.

Below, you can see an example of the UI:

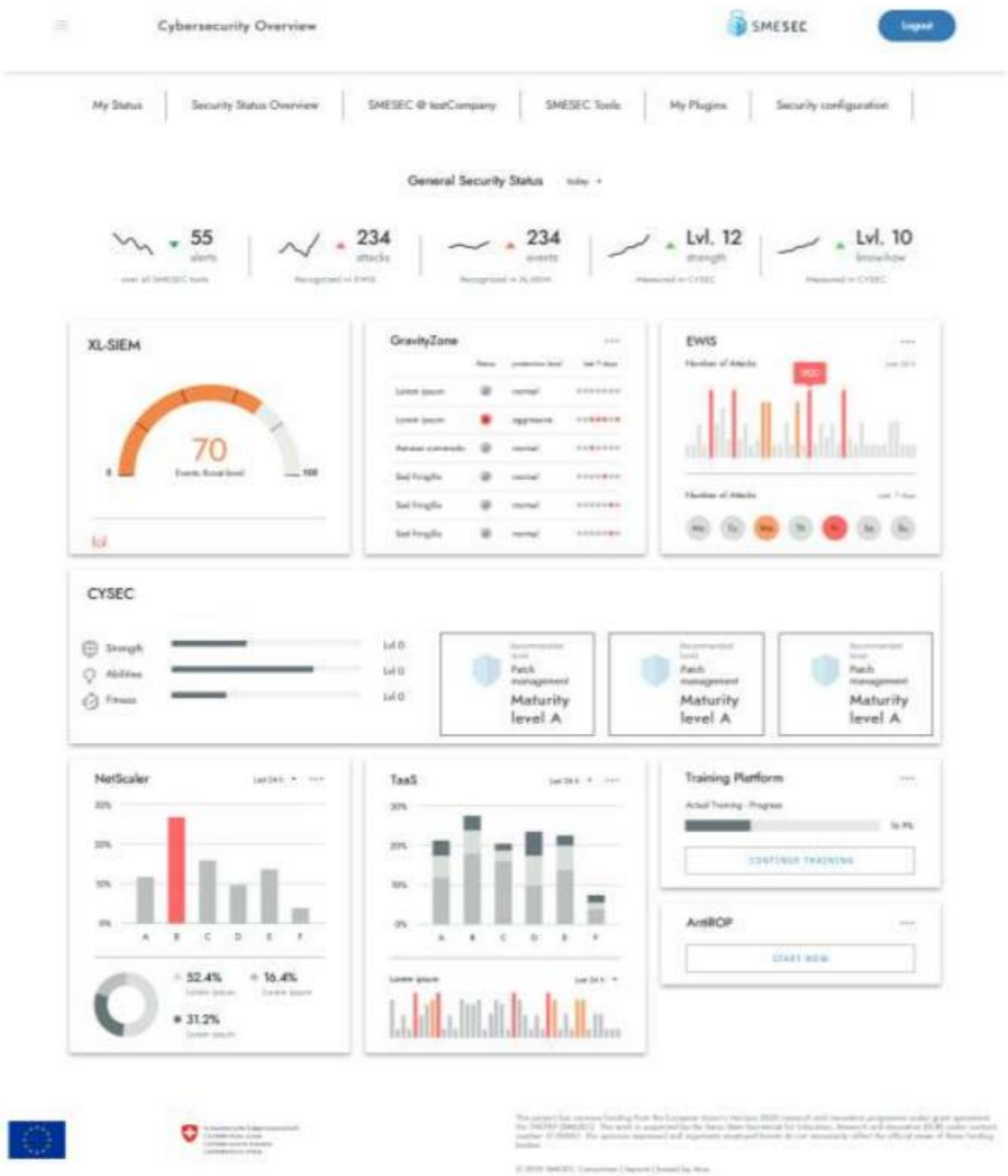

Figure 5: Cybersecurity overview. Source: (SMESEC, 2020)

UI can be accessed by using Windows or Mac OS users through browsers such as Mozilla Firefox, Google Chrome, and Safari.

Users who visit the framework will get on the main page a one-page overview of the cybersecurity status of their SME (1) that answers the questions of how secure your SME is and how to improve the security of your SME. The first question is answered with a score of the SME's safety, an overview of recent attacks, and the timeline of recent security events detected

by the SMESEC framework. The second question is answered with the current status of self-assessment, capability improvement, and training provision and recommendations of next steps (SMESEC, 2020).

SMESEC framework users, while visiting the UI main page, users will see an overview of their current cybersecurity status in their organization. The Main page is useful to answer the following questions:

- How secure is my organization?
- How to improve its current cybersecurity infrastructure?

For the first question, the overall score of SME cybersecurity is shown, with all the recent incidents and timelines they have occurred.

The second question is answered through the status of self-assessment, capability improvement, and future steps recommendations.

8.1.3. Protection & Response

This phase is designed to deploy its protection tools and to monitor the overall performance of the system. SMESEC is offering below endpoint solutions for their protection:

- System resistance against malware attacks
- System resistance against viruses
- Intrusion detection
- Information management etc.

Example of protection tools are given below:

Bitdefender Endpoint protection and GravityZone

Bitdefender is anti-malware software of SMESEC framework and consists of two different components (SMESEC, 2020):

1. GravityZone server
2. Endpoint Security

Endpoint Security component should be installed on organizational machines and should provide real-time protection.

GravityZone must be deployed locally and should be connected to the endpoints. Endpoint security component designed to exchange data with GravityZone, which is sending logs to XLSIEM.

Bitdefender uses fake malware files to test the security of network hosts protected by the GravityZone. The reason for calling the file “fake” is that it is designed for test purposes only and will not cause any harm to a testing environment. The Bitdefender Endpoint protection must detect malicious files as malicious and must alert the GravityZone. An alert has to be generated, and information must be sent to the administrator and the XL-SIEM (SMESEC, 2020).

For each component, within the framework, their description, responsibility, input, and output are described. Framework components are divided into six main categories: (SMESEC, 2020)

- Data collection consists of the tools, XL-SIEM agents, and EWIS agents. Given components were specifically made to collect SME’s data, which will be analyzed in the next phase. The monitoring of sources is done through Citrix ADC.

- Endpoint protection and offline tools contain Citrix ADC, Gravity Zone endpoint, TaaS, Virtual patching, Testing Platform, and Moving target. All these tools are aimed to strengthen IT infrastructures located on the SME’s property, as well as to increase the security of products, developed by SME’s

- Data analysis combine all information retrieved by the data collection and endpoint protection tools, studies the data, and train it for the presentation and

orchestration modules. Latter are aggregators in the SMESEC Framework: Gravity Zone, XL-SIEM, EWIS, and Citrix ADC Aggregator

- Training and security measurement tools are planned to evaluate both the cyber-security level of the organizational infrastructures and the alertness and expertise in the IT security of the employees. Besides, the SMESEC framework consists of tools like CySec that sets itself a target to increase awareness and give proper cyber-security training to the company employees. Training and security assessment tools include the following: CySec on-prem, CySec on-Cloud, Risk Assessment Engine, and training platform
  .
- The orchestration category consists of SMESEC Hub and the extensions module. Extensions module has a variety of plugins that utilizes hardcoded rules, alongside AI-generated patterns, to analyze all the data retrieved and output alerts and proposals.

- The presentation module is the interface designed explicitly for SMESEC Framework users. The interface is easily customizable per user needs (SMESEC, 2020).

List of all components used by SMESEC framework to protect SME organizations from digital threats:

Component	Description and responsibility	Input	Output
Citrix ADC	Intercepts network communication	Network traffic into SME's system	Information extracted from the intercepted communication
Citrix ADC Aggregator	Collects data from Citrix ADC and outputs alerts	Information extracted from the intercepted communication	Aggregated information into data visualization
SMESEC extension	Analyze collected alerts to detect possible	Alerts collected in HUB	Attack-chain alerts, initial forensics &

	infrastructure attack areas		response, recommendations
Presentation module	Presents results to the user and receives user requests	User interaction	Present results to the user and forward user requests to SMESEC extension
Keycloak	Management of user authentication and authorization	Login request	Authorization to the tools: GravityZone, EWIS, XL-SIEM
XL-SIEM agents	Log files monitoring	CITRIX ADC log files, EWIS agents, Gravity Zone endpoint	Information extracted from log files
XL-SIEM	Aggregates data from XL-SIEM agents	Information extracted from XL-SIEM log files	Proprietary alerts or in MISP format
Risk Assessment Engine	Correlates vulnerability posture with XL-SIEM agents and produces alerts	Alerts from XL-SIEM and vulnerability overview from the user	Vulnerability assessment based on a vulnerability posture
EWIS Agents	Honey-pot integration	Traffic from the network	Extracted data sent to XL-SIEM
EWIS	Collect data from all EWIS agents and provide alerts	XMPP commands from the honeypot	All security events send to XL-SIEM and logs to EWIS database
Gravity Zone endpoint	Vulnerability management and malware detection	Data on user hard drive	All retrieved data send to Gravity Zone and XL-SIEM agents
Gravity Zone	Aggregates data from all malware detection alerts	Analysis of data retrieved from Gravity Zone endpoint	Alerts from all detected malware on a hard drive

Table 4: SMESEC tools. Source: (SMESEC, 2020)

8.1.4. Training & Awareness

Training and security measurement tools are planned to evaluate both the cyber-security level of the organizational infrastructures and the alertness and expertise in the IT security of the employees. Moreover, the SMESEC framework consists of tools like CySec that sets itself a target to increase awareness and give proper cyber-security training to the company employees. Training and security assessment tools include the following: CySec on-prem, CySec on-Cloud, Risk Assessment Engine, and training platform (SMESEC, 2020).

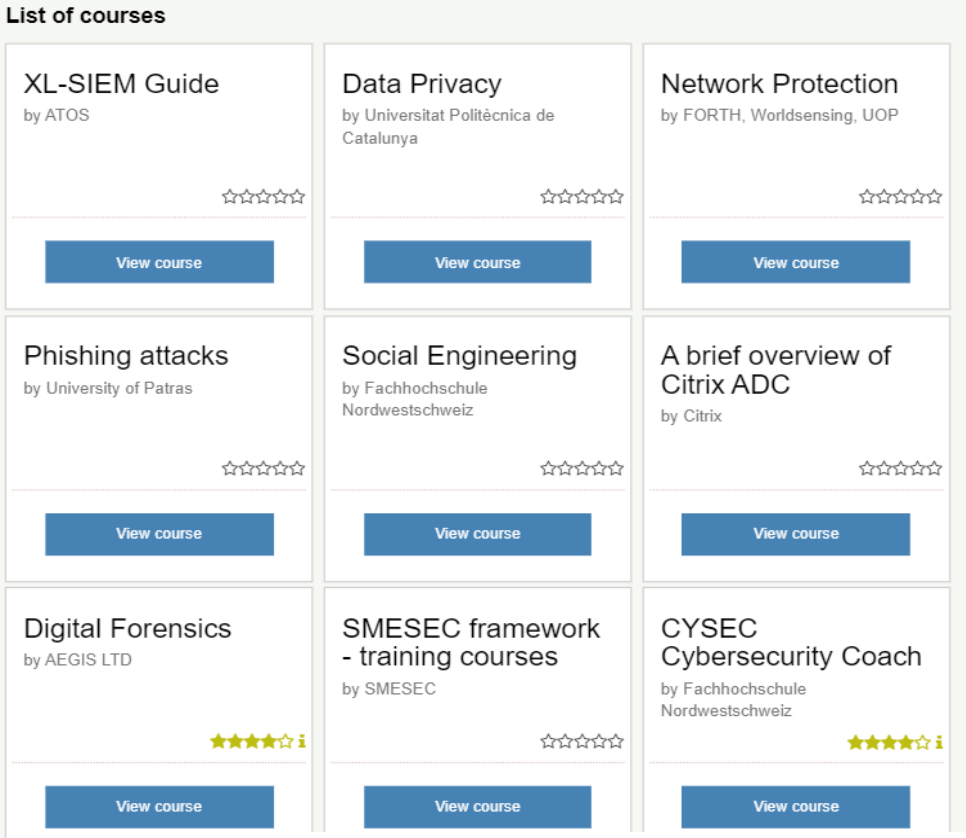

Figure 6: Training platform main page. Source: (SMESEC, 2020)

At the moment, for the training platform, all learning materials are available for registered users and completely free, they are hosted on a Securityaware.me Training Platform. The screenshot below illustrates how content is presented at their main training page:

Training courses are separated into ten categories:

1. Phishing
2. DDoS protection
3. Ethical hacking
4. Privacy
5. Hardware Security
6. Forensics
7. Antivirus
8. Antimalware
9. Ransomware
10. Social engineering

When the user interacts with the category, he is interested in, and training material window pops up. Web page explains the attack and most common examples of it, as well as how to deal with such a scenario if it occurs. Training of small and medium-sized employees is crucial, and proof of that is research conducted by CompTIA, indicating that 52 percent of all security branches in 2015 were caused by human error. According to the same study, only 54% of surveyed companies had offered any type of cybersecurity training for their employees (Maurer, 2015)

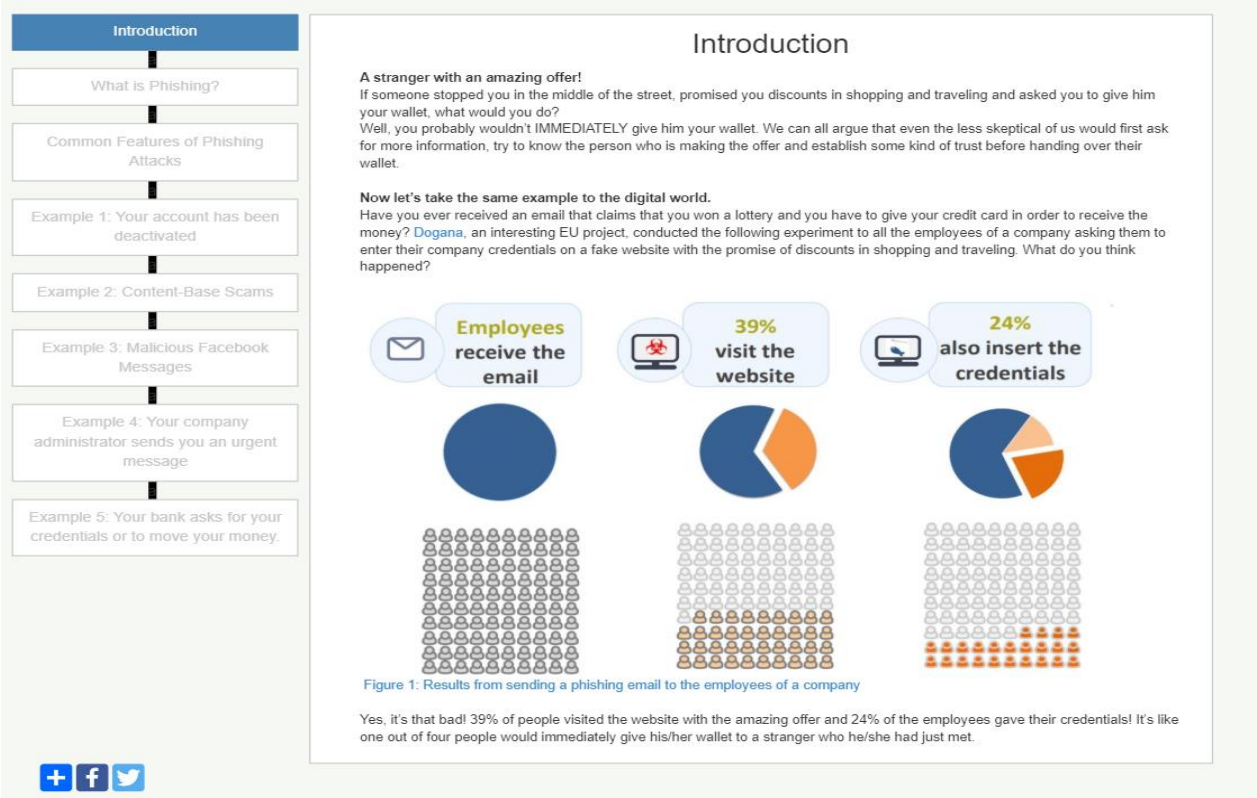

Figure 7: Training content. Source: (SMESEC, 2020)

8.1.5. Extensive Validation

During this phase of the framework, all tools mentioned are tested on a user hardware device, since hardware specifications may dramatically vary from organization to organization. They can perform differently based on an operating system installed (Windows or MacOS), the performance of the system (processing power, available RAM), and based on network connectivity (internet speed).

Currently, all tools being tested on various hardware components in those organizations, which have shown interest in the SMESEC framework.

8.2. SMESEC Personas and Users

The UI has been designed for use by specific personas in the SME. According to the so far collected survey data and by following the SMESEC fast ramp-up recommendations for cybersecurity capability improvement in the SME, we can expect that in each end-user SME, there will be a person appointed for handling cybersecurity in the SME. We call this person the Chief Information Security Officer, or CISO, referring to the corresponding formal job description that is often used in large companies. To describe in a specific way how to use the framework, we defined a user called “Ron” who has this responsibility. The table below specifies the characteristics and backgrounds of Ron, the SME CISO, which is a primary user of the SMESEC framework. It also includes framework tools. It is to be noted that personas are not identical to the user roles. User roles represent the privileges and responsibilities of a person at a given time, while personas present characteristics, goals, desires, and expectations of a person (SMESEC, 2020).

Attributes	**Values**
Name	Ron
Responsibility	Responsible for overall cybersecurity of the organization (CISO)
Characteristics	Has general curiosity about cybersecurity, cybersecurity is his side-topic work
Background	General knowledge of cybersecurity principles did not have previous experience with SMESEC.

Tasks	Monitor and evaluate the current status of secureness of the system, involve SME employees into cybersecurity controls and report all findings to the management
Expectations	Ongoing learning and guidance on how to address cybersecurity with SMESEC. Minimal effort to monitor current protection of IT infrastructure and report of any incidents.

Table 5: SMESEC personas. Source: (SMESEC, 2020)

The framework was designed to be handled by one appointed persona mainly. SMESEC decided to have one responsible person to monitor the cybersecurity status of the organization due to the surveys conducted on European SMEs. A responsible person within a framework named CISO (Chief Information Security Officer). However, the number of persons responsible for cybersecurity within the organization may vary by their financial and human resources. It can include cyber resilience team and external advisors with cybersecurity background such as auditors and members of the cybersecurity incident response team (CIRT).

Below you can see organizational chart per SMESEC personas.

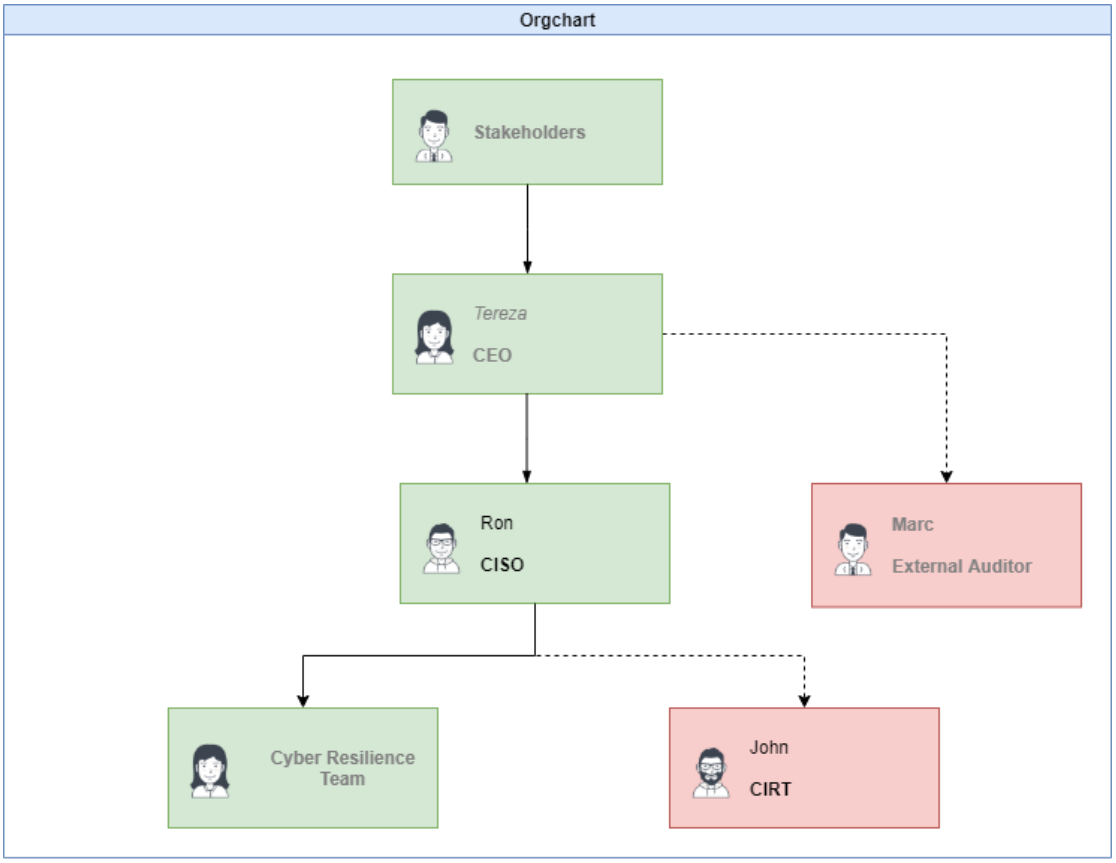

Figure 8: SMESEC organizational chart. Source: (SMESEC, 2020)

Additional to the appointed persona, in SMEs, there will be users of the framework, which must contribute to the overall cybersecurity awareness of the organization. The number of users involved will vary from organization to organization and will depend on the educational background of employees, their availability, and the total number of personnel. The table below shows the example of those users and their interaction with the Chief Information Security Officer.

Name	Role and traits	Consideration in SMESEC
Tereza	Chief Executive Officer (CEO) appointed by stakeholders is responsible for the overall wellbeing of the organization	Tereza has read-only access to the SMESEC framework. She receives regular cybersecurity reports from Ron (CISO)
Marc	Cybersecurity audit expert validating that SME is compliant with regulations	Marc works directly with (Ron) regarding audit compliance with sensitive customers. Marc advises Ron on practices and training under the SMESEC framework.
John	Cybersecurity professional and consultant advising SME's on a best practice offered in the market for cybersecurity solutions. Part of cybersecurity incident response team (CIRT)	John is closely working with the appointed CISO and consulting him on what is beyond the SMESEC framework. CISO is providing him with all data required for its analysis, such as log files, company profile, etc.
Cyber Resilience Team	Employees within SME interested in cybersecurity	Cyber Resilience team is provided with all training materials and has read-only access to the UI of the framework.

Table 6: SMESEC personas. Source: (SMESEC, 2020)

8.3. Cybersecurity Audit and its Interaction with SMESEC

Generally, a cybersecurity audit starts with audit objectives and ends with an audit report, which is reported to interested parties.

According to Scott Donaldson, cybersecurity audit consists of 3 main parts (Donaldson, Sigel, & Williams, 2018) :

1. Threat audit
2. Assessment Audit
3. Validation audit

8.3.1. Threat Audit

Aim of the threat audit is to find and analyze all occurred threats within the organization with the focus on ones, threatening confidentiality, integrity, and availability of IT the whole IT infrastructure of the organization. The result of the threat audit is a report with an evaluation of all past cyber-attacks and their impact.

By using SMESEC organization can easily pull this report by using “Security status Overview.” Unlike other frameworks, where auditors had to “hunt” for security incidents by analyzing log files manually, SMESEC can show the current cybersecurity status of the organization even for those without a dedicated technical background. By implementing this tool, an organization can keep track of security incidents daily, without need to hire external auditor, which in case of small organizations is a huge plus, because of its cost savings (average cybersecurity audit costs 10 000 $) (CSA, 2019)

The framework will offer multiple functionalities to the end-users. On one side, there is results visualization, and on the other access to tools and functions. Available functions depend on the user access level granted by an admin user. In the case of the admin user, “Security Status Overview” is shown. For the less privileged users, “My cybersecurity status” is displayed. Separation of a user interface for various users is done to show the user relevant information only. For instance, an admin needs to see the whole organizational status of their cybersecurity system, while for the ordinary user, this sensitive information can cause various risks. For average users, only cybersecurity training materials, news of cybersecurity, awareness, etc. will be available. That is an additional step to support SME’s cybersecurity at the highest level (SMESEC, 2020).

Each user has access to the tabs below:

- Standard user: “My Status.”
- Admin: “My Status”, “Security Status Overview”, “SMESEC@”, “SMESEC Tools”, “My Plugins”, “Security Configuration”
- Security Analyst: “My Status”, “Security Status Overview”, “SMESEC@” and “My Plugins”
- Auditor: “My Status”, “Security Status Overview”, “SMESEC@”, “SMESEC Tools”, “My Plugins”, “Security Configuration” (only read) (SMESEC, 2020)

Example of Security Overview you can see from below screenshot:

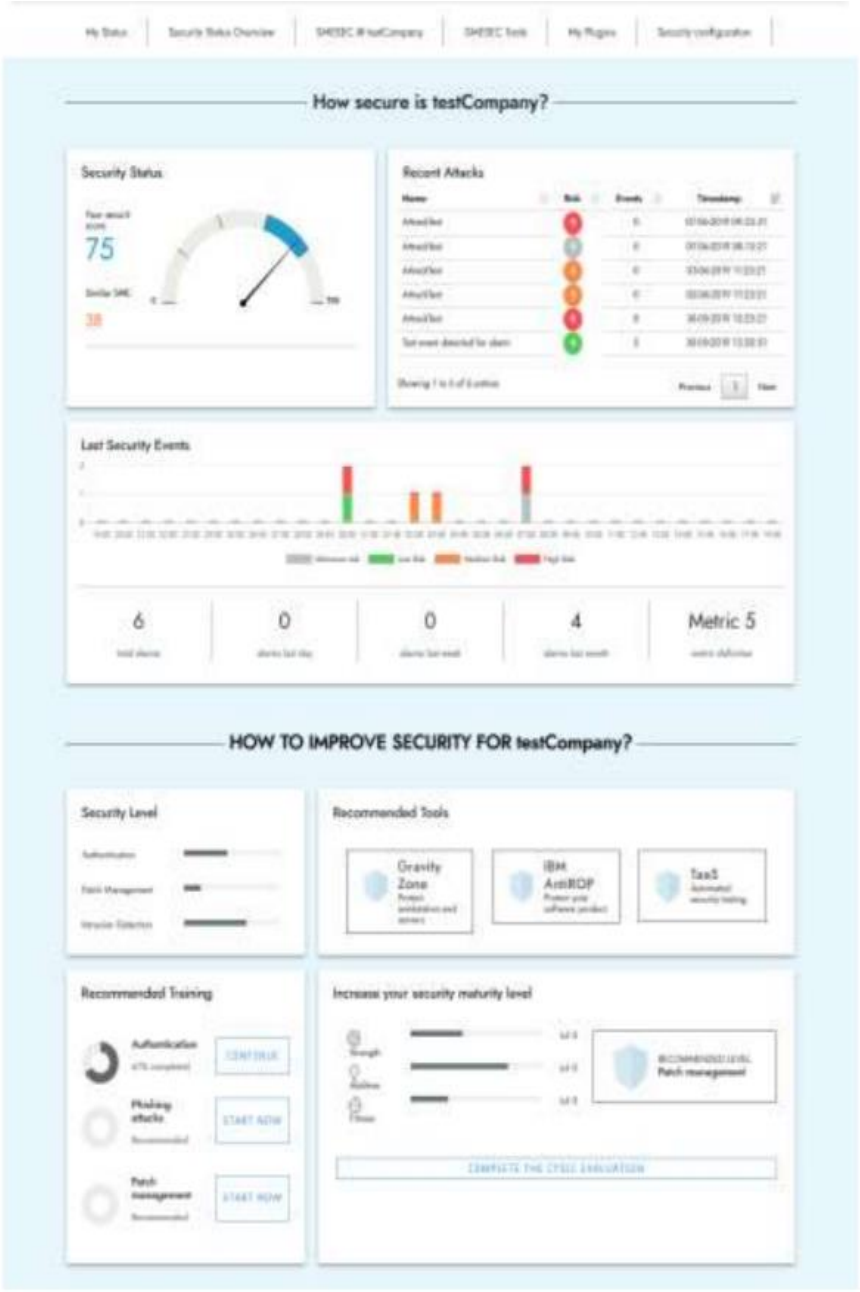

Figure 9: Security overview of SMESEC. Source: (SMESEC, 2020)

As we can see, diagrams are showing the current user status of the system. On the left top side, a high-level analysis of the system is shown. The number is calculated with the result of events received by tools monitoring, with the internal classification, which is still under development. The creation of this tool was aimed to give a simple overview to non-cybersecurity professionals about the current cybersecurity state within their SME. A high number indicates that the overall system is protected, while a low number means that system is vulnerable to internal and external threats.

The second graph is showing different attacks the system has been under and a small description of them.

The third graph, “Last Security Events”, highlights events that occurred for a period (day/week/month overview) with their risk level. The initial idea was to give an overall view of recent incidents in the system and their evolution in the short and long run.

The last part of the overview is designed for system admins, which contains recombinational steps about how to improve the cybersecurity of the company. The sub-section aims to give a piece of information on how employees are increasing their cybersecurity knowledge daily (SMESEC, 2020).

However, threat audit is not only covering security tools being used to protect the integrity and availability of the data but also includes physical security. It consists of server safety when located inside the organization (who has access to it, how access is limited to the server, its protection from fire and flood, etc.). And it cannot be done internally unless organizational employees have proper knowledge of how to do so.

8.3.2. Assessment Audit

An assessment audit includes the review of a set of standards, and the assessment of cybersecurity controls relevant to those requirements. Primarily, the evaluation focuses on how cybersecurity is held within the organization and then measures how they correspond to this metric. With a preemptive assessment, where there are obvious vulnerabilities or gaps, there is time and space to fix any problems. Data for a security assessment is typically obtained in a

variety of different forms, including surveys, interviews, comparison with international norms, statistics, or analysis of past assessment reports (Donaldson, Sigel, & Williams, 2018).

SMESEC has identified several international security standards by conducting surveys and identifying small and medium organizational needs. By implementation of SMESEC organizations will be compliant with below standards (SMESEC, 2020):

- ISO 27’00x
- BSI 100-X

ISO 27’00x - A series of international standards, including information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) (Abernathy & McMillan, 2018).

The series contains the best practices and recommendations in the field of information security for the creation, development, and maintenance of an Information Security Management System.

Also, it consists of below following generally applicable documentation

- ISO/IEC 27002: Code of practice for cybersecurity management
- ISO/IEC 27003: ISMS implementation guidance
- ISO/IEC 27004: Cybersecurity management – Measurement
- ISO/IEC 27005: Cybersecurity risk management (SMESEC, 2020)

Additional guidelines include the following:

- ISO/IEC 27011: Information technology – Security techniques – Cybersecurity management guidelines for telecommunications organizations based on ISO/IEC27002 ISO 27799:

- Health informatics – Cybersecurity management in health using ISO/IEC27002 (SMESEC, 2020)

BSI 100-X – BSI standard consists of the following:

- BSI standard 100-1: Information Security Management Systems. Requirements. The standard defines the general provisions of the ISMS. It is fully compatible with ISO 27001 and takes into account the recommendations of ISO 27002; (BSI, 2018)

- BSI standard 100-2: Actions and approach to the primary (basic) protection measures, practical implementation of the 100-1 standard. The standard provides practical assistance in the form of numerous tips, recommendations including examples. (BSI, 2018)

- BSI standard 100-3: Risk Analysis based on IT-Grundschutz

BSI methodology can be used not only to build an information security management system (ISMS) but also to certify companies according to the requirements of the ISO 27001 standard.

BSI standard was chosen by SMESEC due to its simplicity, which is easier to handle by SME's, even compared to the ISO 2700x standard (SMESEC, 2020).

The first step to being compliant for the organizations with the standards mentioned above is to get an initial certification. Maintaining these standards over the extended time period is a challenge for organizations due to employee tendency to lose their diligence after an annual audit. A further step is to remain compliant, for instance, in case of ISO standard requirement is to conduct an internal audit every three years. Still, it is highly recommended to perform it annually. An additional step is to train organizational employees on these standards annually. SMESEC currently does not have training materials for the mentioned standards, and having them included in a training materials section would be a considerable advantage (Peters, 2020).

8.3.3. Validation Audit

The purpose of the validation audit is to determine whether cybersecurity controls are meeting initial documented requirements.

For instance, per SMESEC framework, documented requirement against malware attacks is to deploy Bitdefender antivirus and GravityZone. Validation of these tools is conducted through "feeding" the organizational network by test malware, which should be detected and isolated/deleted by GravityZone.

As it was mentioned in "components of SMESEC", per each cybersecurity tool there are presented the inputs and outputs. Surely, all cybersecurity tools are being used in SMESEC; there is a dependency; each input and outputs should be tested per their initial state. Validation of these tools is crucial because the software can behave differently depending on an operating system, hardware capabilities, or simply how these tools were installed initially. Per each device, SMESEC is giving detailed instructions on how to deploy and test the system, and by following them, personnel appointed to conduct internal audits can run a validation audit to check if it meets its initial state.

Chapter 9: SMESEC Use Cases

This chapter will focus on one medium and one small-sized organization: Company X and company Y, both based in the European Union. The use case will bring an example of the adoption of SMESEC framework. Presently they are

9.1. Company X Description

Company X is based in Prague, Czechia. Their main business is focused on the relocation of organizational employees. They provide end-to-end service for their customers in case there is a need for the domestic or international transfer of their employees. Presently company X employs 95 people with an annual turnover of 25 million euros. Almost half of the employed personnel is working as relocation analysts, and rest employees are involved in consulting and management. Because of the nature of their business company is using its own software for their business processes, they did not focus on hiring personnel with strong IT skills, as they provide their personal training on their own internal tools. This fact led to the low cybersecurity awareness of their employees. For managing their software and hardware infrastructure, company X hired

external IT company. For resolving daily issues, the external company provided company X their two IT contractors, who are working on a shift. IT staff is mainly involved in resolving hardware issues and maintenance of the server, which is located in the same building.

9.1.1. Company X Organizational Chart

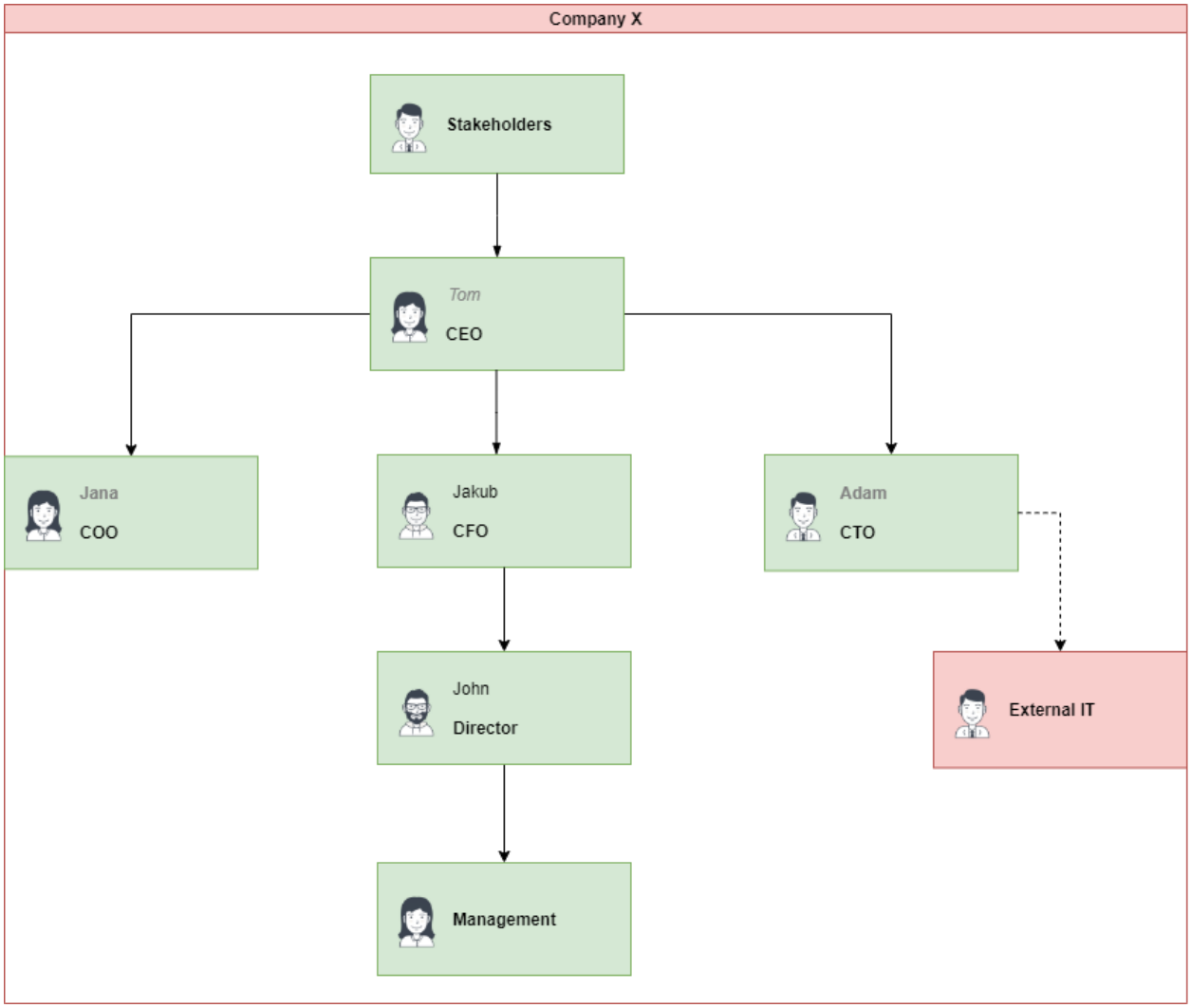

Figure 10: Company X organizational chart. Source: own data

As you can see from the chart above, Company X is following the hierarchical structure, most common in larger organizations. Company has appointed Chief Executive officer, Chief Operating Officer, Chief Technical Officer etc. Moreover, you can see external IT contractors highlighted in the red box, which are reporting critical incidents directly to CTO.

9.1.2. Company X Current State of Cybersecurity

Company X is highly dependent on the reliability of their IT systems because daily communication and service provision with their foreign European customers is based online. Company does not have access to live cybersecurity incidents overview and relies on a monthly report of all incidents by external IT consulting company. The monthly overview includes a list of all cybersecurity incidents, their impact and recommendations on how to reduce the number of critical ones. However, the report seems too technical for CTO, and he relies on an external IT company entirely.

The most recent critical cybersecurity incident happened to Company X is Ransomware attack. Relocation analysts received an external email, which contained a link that downloaded word file. The email was impersonating as a message from HR regarding new open internal opportunities. It was downloaded by ten analysts before IT staff identified suspicious actions within their network. After downloading the file, analysts could not access their personal computers anymore, as a result of all files on a hard drive being encrypted by ransomware.

Ransomware displayed a message on a victim's computers that their data was encrypted and contained details on how to restore it to the working state. Message ends with attackers' recommendations not to decrypt the data by using third-party software, as it will result in a loss of all data stored. Attackers were requesting 1000 $ in bitcoin ransom, after sending this amount to the crypto wallet they ensured to send encryption key, which would decrypt all data and allow employees to access their computers. Example of ransomware pop up window you can see below from WannaCry tool, which affected more than 150 countries.

Figure 11: Ransomware example. Source: (Avast, 2020)

After company X gave ten personal computers to an external organization to resolve this critical incident, they were informed that there is no way that they can decrypt the data. The solution is to wipe all data and install all software from scratch or simply pay the ransom. Paying the ransom was against the company's corporate policy and did not guarantee that company would get their data back, so they decided to wipe all ten hard drives.

Impact of a ransomware attack was the following:

- Financial loss - as a result of 10 revenue-generating analysts were unable to work.
- Missed clients - SLA due to unavailability of few relocation analysts, resulted in financial penalties, as well as partial loss of good reputation
- Financial loss associated with remediation efforts

Causes of a ransomware attack were the following:

1. Employees were not provided cybersecurity awareness training and did not know how to react to a ransomware attack proactively.

2. The organization was using pre-installed antivirus that was not updated frequently, could not detect and isolate/delete ransomware file

3. The organization was not using any spam filter to quarantine or execute harmful attachments.

9.1.3. Company X SMESEC Implementation

If company X at the moment of the attack were using SMESEC framework, they would avoid financial and reputational losses. As described in chapter 8.2, company X would have appointed CISO within their company, who is responsible for the protection & response of the whole organizational cybersecurity infrastructure. CISO will be supported by Cyber Resilience Team, which consists of employees with a proven interest in cybersecurity. These appointed employees would be the main persons to identify any vulnerabilities before they occur by using security overview function, which was described in chapter 8.1.2. Security overview function can identify all inactive or outdated cybersecurity protection software and would avoid 2nd cause when outdated software resulted in system vulnerability.

The first cause could be potentially avoided by training materials offered by SMESEC framework. Cybersecurity training within SMESEC framework is a must for any employee working in SME. Training materials are showing examples of various types of attacks and teaching how to protect against them and include ransomware in its patterns. Employees would be provided by a general overview of ransomware attacks and will be able to identify and report suspicious emails/links/software. Phishing emails and lack of cybersecurity training are top causes of ransomware attacks in 2019.

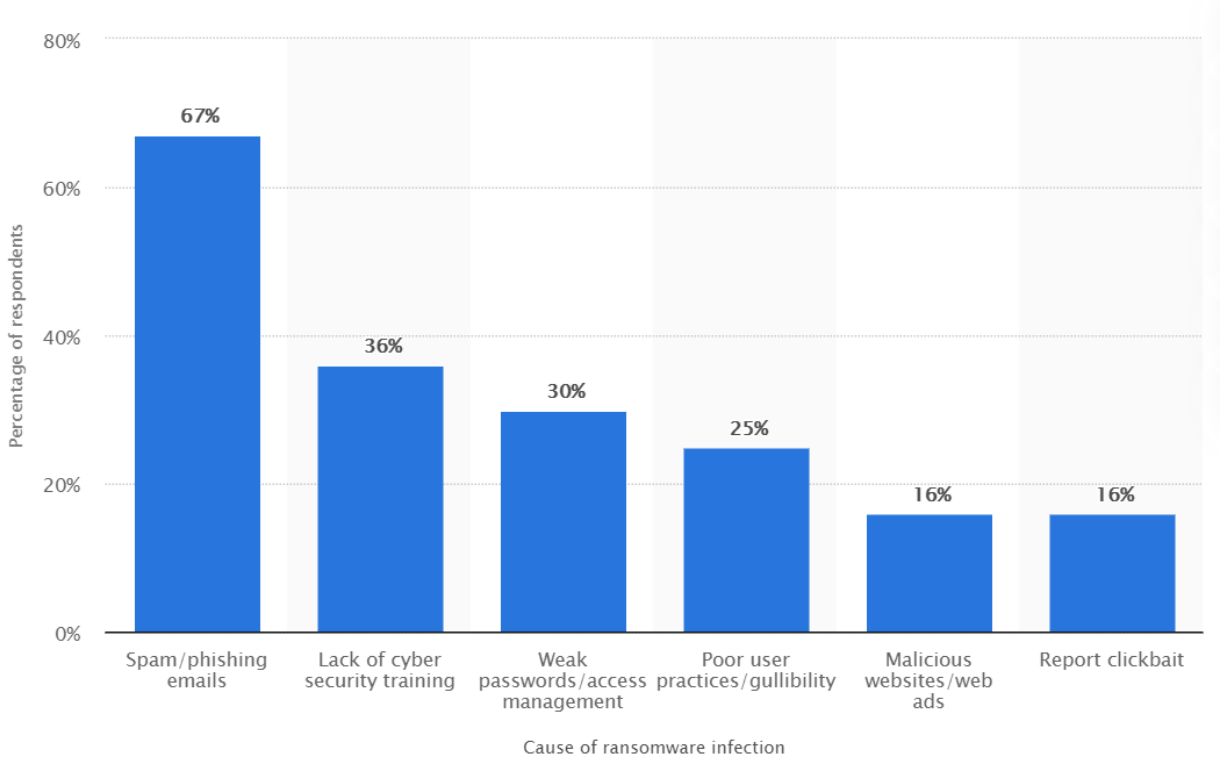

Figure 12: Cause of ransomware infection. Source: (Statista, 2019)

Final 3rd cause would be avoided by pre-installed Unified Threat Management security tools that integrate multiple solutions, such as antivirus, VPN, firewalls and email filtering running separately or simultaneously. Example of such device is Fortinet next-generation firewall, VPN, web filtering etc. controlled in one console. Advantage of Unified Threat Management tools for SME's is that all security tools are offered as one package and do not require multiple protection tools from different software vendors, often unaffordable and hard to integrate for organizations. However, running all these security tools simultaneously on organizational computers can result in a decrease in computational power. It would require at least 8 GB of RAM space, which not every enterprise can meet. A decision which tools to run on an organizational computer should be based on its computational capabilities and vulnerability analysis.

Other SMESEC framework actions against ransomware attacks include the following:

- The detection of malware by the WAF ("CITRIX ADC") or local virus scanner ("Bitdefender");

- Malware detection through Forth "Cloud-IDS" or "IPS/IRS";

- Use the on-demand and on-access opportunities from the virus scanners;
- Check Bitdefender status;
- Check CITRIX ADC status;
- Check Forth Cloud-IDS status;
- Check that the firewall protects unwished data streams;
- The control of the application's administration right controls (SMESEC, 2020).

9.2. Company Y Description

Company Y is based in Vienna, Austria. Their main scope of business is 3D modelling for the gaming industry. They offer graphic modelling for big game developing studios such as Treyarch and Square Enix, in case large organizations require external assistance. Since their business is based on 3D illustration, almost 90% of their 40 employees are graphic designers. Rest employees are involved in Marketing and Finance. Company Y reported its annual turnover in 2019 as 6 million euros, which fits the European specification of a small enterprise. Company Y is highly dependent on its IT infrastructure, and any interruption of business processes can cause irreversible consequences.

9.2.1. Company Y Organizational Chart

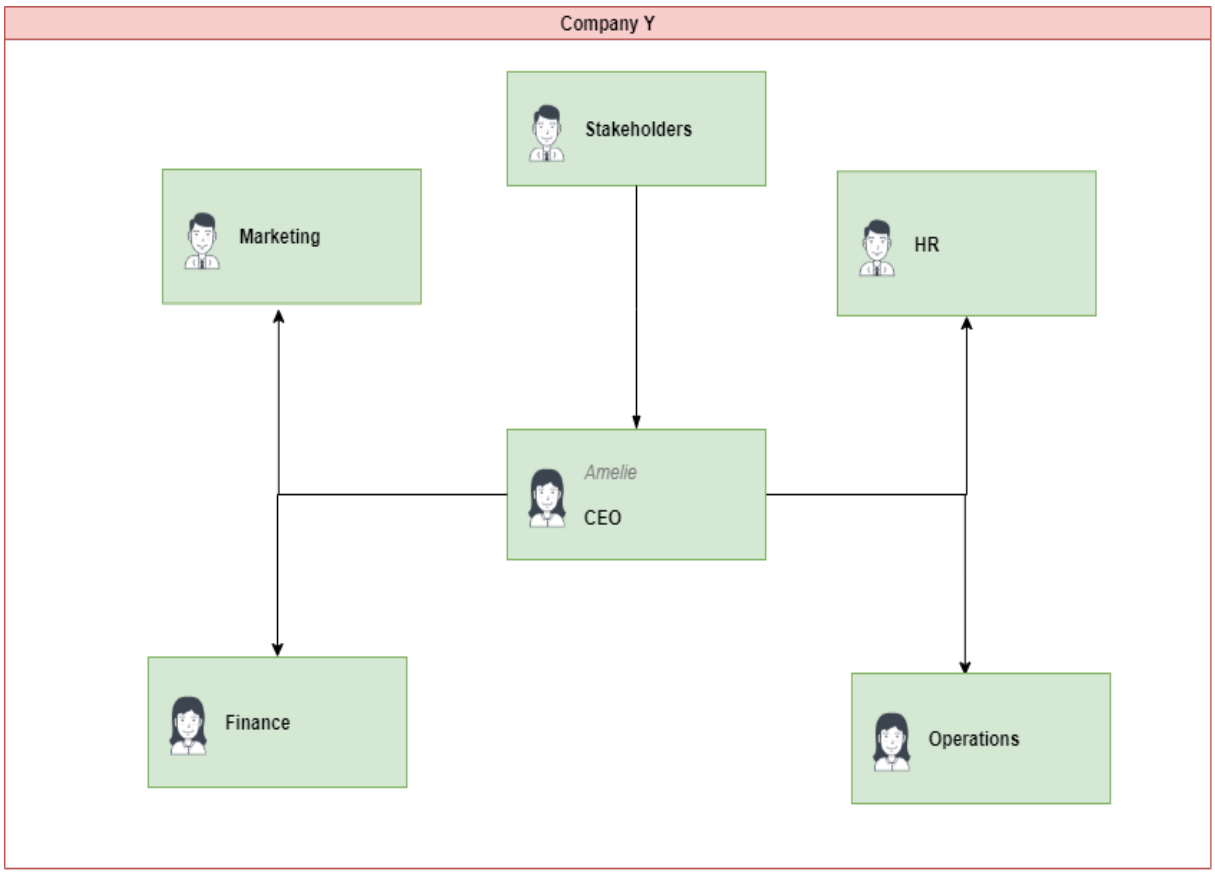

Figure 13: Company Y organizational chart. Source: own data

Unlike company X, company Y following a horizontal/flat functional-based organizational structure. This organizational chart is typical for small organizations at their initial stage. The benefit of this organizational structure is that employees are involved in the decision-making process. On the other hand, by opening the opportunity to decide for employees at all levels, decisions could be made wrongly by employees who lack experience or knowledge (Henrics, 2006).

9.2.2. Company Y Current State of Cybersecurity

In its current state company is using primitive cybersecurity tools for its protection: Antivirus and Firewall. However, the only IT specialist within the company had a previous cybersecurity background and using Kali Linux operating system as a security audit tool to prevent internal and external attacks. Simple penetration tests, and gathered data allowed an IT specialist to identify vulnerabilities and holes in the systems. He created a report and identified key areas, which are most vulnerable:

- SQL injection: SQLMAP tool in Kali Linux allowed to detect possible SQL injection codes, which can critically impact Company Y's web page

- XSS: XSSer tool in Kali Linux identified that there is a possibility to inject javascript code to bypass web page admin control:

9.2.3. Company Y SMESEC Implementation

By using freely distributed Kali Linux operating system, company Y was able to identify its weak points internally. However, the organization was lacking security tools used to protect itself. They were trying to adopt the NIST framework to increase its resistance against digital threats. Still, the framework seemed to complex and required significant time and financial resources for its adoption. To adopt the NIST framework company Y simply did not have a team member who had previous experience with NIST compliance. Subsequently, they found that there is a framework named SMESEC, which does not require prior experience and existing employees can deploy the framework single-handedly. Company Y already knew its weak point and wanted to focus on its current vulnerabilities since they were critical. SQL injection could lead to database data loss/damage while JavaScrypt code bypass could lead to web page admin control. By accessing admin user rights, cybercriminals could wipe their entire web portfolio and leak sensitive information.

In order to prevent these unwanted scenarios, SMESEC framework can offer such solutions:

- Built-in security dashboard that keeps track of outdated libraries, plugins, security tool etc. and to be up to date with the latest security patches.

- SMESEC practice to not share database accounts between various web applications.to potentially isolate the attacked area

- SMESEC good practices on code review, pair programming etc. Moreover, code should not be visible and reachable externally, which would decrease the risk of injection or bypass attacks.

- Simultaneous usage of Bitdefender antivirus and firewalls/IDS (CITRIX ADC, FORTH) must be able to detect the above mentioned exploit attacks (SMESEC, 2020)

By using these good practices and software tools, company Y could solve its most critical issues. Yet, after framework adoption, if organizational employees know penetration testing - the best solution would be to test the efficiency of these methods as SMESEC does not cover ethical hacking methods.

Chapter 10: Desired State of SMESEC Framework

In its current testing phase, SMESEC consortium providing all cybersecurity tools as one installation package available for two operating systems: Window and Linux. However, all devices are currently unavailable for MacOS users, which is another popular desktop operating system after Windows (88.29 %), with a market share of 9.33 % (Operating System Market Share, 2020). By adding compatibility with the second most popular operating system in their next framework state, they have the opportunity to increase the number of potential users of their framework.

Current training materials are not segmented by the framework user type, which can lead to insufficient or irrelevant training for organizational employees. As an example, the framework does not cover the security overview dashboard at all in their materials, which is a crucial part of threat analysis. One of the options for SMESEC to improve the quality of training materials is within framework train tech-savvy employees, who will be monitoring and analyzing the cybersecurity status of the organization, and train rest outside of the framework platform. For instance, LinkedIn learning has dedicated high-quality video materials for basic cybersecurity principles. By implementation of this solution, SMESEC consortium will not waste their time and financial resources and focus on high-quality training materials for CISO and Cyber Resilience users, which are at the forefront of cybersecurity.

Another downside of the framework is that list of cybersecurity tools recommended by SMESEC is very limited. For instance, SMESEC suggesting only to use BitDefender against malware attack, since BitDefender is one of the castoreum’s close partners. However, in the case of SMEs, often, they already have a long-term contractual agreement with software providers. And for instance, if it is not BitDefender, and they are using Avast or McAffee solutions already for their organization, change of a software provider might stretch them financially. On the other

hand, if SMESEC would suggest a few alternative options per cybersecurity tool they rely on, it will give the desired flexibility of the framework for the organizations.

Chapter 11: Research Limitations and Conclusion

The current trend globally is evolving into virtual space and digitizing every aspect of human interaction to retailers, education, and business. Given the current situation even in the Czech Republic after SARS-CoV-2 , most of the companies, universities, and schools have developed a trend to use the services of virtual offices and applications, and life keeps moving forward by enabling the digital presence.

The main focus of this thesis and its goal it has reached is the protection of information from fraudulent, criminal digital activities. The SMESEC framework is new to the business world, and it adopts most or all the current trends covering gaps from cybersecurity to business continuity. Nonetheless, these results must be interpreted with caution as some limitations should be borne in mind. There was limited access to the data regarding the SMESEC framework implementation process in EU SMEs. As an external figure, there was no opportunity to test this process from the admin or user point of view; thus, there are no results or conclusions regarding the usability or efficiency of the framework. There were made several unsuccessful attempts to get insider information from the consortium members of SMESEC by email, LinkedIn, and Facebook. Moreover, publicly available SMESEC documents did not consist of enough information to conduct a more in-depth analysis of the framework and to assess its implementation in different kinds of SMEs. These types of data are essential to get better and more clear results on the practical part.

For the further study of this issue, it is recommended to identify possible ways to obtain more specific, subject-related data from the trusted parties. In the future, the next research activity held by experienced audit specialists who had experience working with the SMESEC framework would provide better results and significant findings.
Current research work also covered the desired state where the SMEs can use the SMESEC framework without making any significant changes, such as letting go of any contractual obligations and security measures that they have already purchased. It can considerably impact on the financial aspects of small business owners. If the companies already have an antivirus with the features of the SMESEC framework requirement, I suggest alignment with the rest of

the compliance. But it must be mentioned to the auditors that the current strengths of the tools they use comply with the SMESEC framework.

Based on the frameworks, the auditors create guidelines, and the company has to prove that the current procedures and processes are in the best interest in protecting the information. After that, business stakeholders are accountable for giving the correct information to the auditors so that the auditors may perform their assessment and come to a conclusion to create awareness of any potential breaches. And future recommendations that the business may follow with requirements of extensive validation techniques that the company might carry forward in achieving the final goal of SMESEC compliance.

This work has answered to the question “What is the role of cybersecurity in modern SMEs?” in the second and third chapters and it was found that cybersecurity became a vital part of any modern organization. Analysis of the last threats in the cyber area shows that modern SMEs, regardless of its capital and size, cannot be competitive without the adoption of concrete cybersecurity measures. Neglection of cybersecurity measures puts companies at the risk of contraction or shut-down. Chapters 7, 8 and 9 presented the answers for the research question “What are the benefits of adopting SMESEC cybersecurity framework for European SMEs?”. According to the findings, the main advantage of SMESEC compared to traditional frameworks is its narrow-focused orientation on the European SMEs. It allows adopting current framework in the different types of organization. Even the companies without substantial financial resources or prior knowledge about cybersecurity can implement SMESEC.

In conclusion, the purpose of the research has been achieved, although there were some limitations in data availability. Results identified that it is necessary to take timely actions to prevent possible threats in computer security of all divisions in the organizations. Moreover, it suggested the adoption of the SMESEC cybersecurity framework as a preventive action again cybercrimes.

Chapter 12: References

(n.d.). Retrieved from https://www.pcisecuritystandards.org/pdfs/Mapping-PCI-DSS-to-NIST-Framework.pdf

(n.d.). Retrieved from www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cybersecurity-Based-on-the-NIST-Cybersecurity-Framework.aspx

Auditing and Assurance. (2016). Retrieved from The Institute Of Chartered Accountants of India: https://www.icai.org/post.html?post_id=13814

Ramamoorti, S. (2003). Chapter 1 Internal Auditing: History, Evolution, And Prospects . The Institute of Internal Auditors .

(2007). In L. De Nardis, *The History of Information Security : A Comprehensive Handbook.*

(2019). In V. Oorschot, *Computer Security and the Internet.*

A., F. (2016). The basics of information security when working on a computer. INTUIT.

Abernathy, R., & McMillan, T. (2018). In *CISSP Cert Guide (3rd Edition) (Certification Guide)* (p. 314). Pearson IT Certification; 3 edition.

Ackerman, P. (2017). In *Industrial Cybersecurity. Efficiently secure critical infrastructure systems* (p. 174).

ACT. (2014). Retrieved from GOVCERT.CZ: https://www.govcert.cz/download/kii-vis/preklady/Act_181_2014_EN_v1.0_final.pdf

Amrin, N. (2014). *The Impact of Cyber Security on SME's*. Retrieved from https://essay.utwente.nl/65851/1/Amrin_MA_EEMCS.pdf

Atos Research. (2020). *SMESEC*. Retrieved from Atos Research % Innovation : http://booklet.atosresearch.eu/content/smesec

Auditing Multiple Public Clients, Partner-Client Tenure and Audit Quality. . (2012). Rochester: Social Science Electronic Publishing.

Avast. (2020). *Avast*. Retrieved from https://www.avast.com/cs-cz/c-wannacry

B, P., Simon, J., & Hatherly, D. (2005). Principles of external auditing.

Bilal, Z. O., & Nawal Said , A. (2015). *World Journal of Entrepreneurship Management and Sustainable Development*, 120.

Boynton, W., Johnson, R., & Kell, W. (2006). In *Assurance and the integrity of financial reporting (8th ed.).*

BSI. (2018). *BSI Standard 100-1*. Retrieved from BSI: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-1_e_pdf.pdf?__blob=publicationFile&v=1

BSI. (2018). *BSI Standard 100-2.* Retrieved from BSI: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-2_e_pdf.pdf?__blob=publicationFile&v=1

Carrigan, M. (2020). *2019 Small Business Failure Rate: Startup Statistics by Industry*. Retrieved from National Business Capital & Services : https://www.national.biz/2019-small-business-failure-rate-startup-statistics-industry/

Chen, Q. (2017). Retrieved from https://www.osti.gov/servlets/purl/1423027

Coll., D. N. (2018). Retrieved from GOVCERT.CZ: https://www.govcert.cz/download/kii-vis/preklady/5517enVyhl%C3%A1%C5%A1ka_o_kybernetick%C3%A9_bezpe%C4%8Dnosti_2018_v1.3_final_vodoznak.pdf

Comission, E. (2017). *Small and Medium-Sized Enterprises'Access To Finance.* Retrieved from https://ec.europa.eu/info/sites/info/files/file_import/european-semester_thematic-factsheet_small-medium-enterprises-access-finance_en.pdf

Cosserat , G., Leung, P., & Cooper, B. (2004). Modern auditing & assurance service (2nd ed.). John Wiley & Sons. Australia.

CSA. (2019). *How much does a security audit cost?* Retrieved from CSA: https://cybersecadvisor.org/blog/how-much-does-a-security-audit-cost/

Decree No. 82/2018. (2020). Retrieved from polverini strnad: https://www.ak-ps.eu/en/the-aim-of-the-new-cyber-security-decree-is-to-increase-the-effectiveness-of-solutions-of-cyber-security-incidents.html

Deloitte. (2018). *Adopting robotic process automation in Internal Audit.* Retrieved from https://www2.deloitte.com/us/en/pages/risk/articles/internal-audit-robotic-process-automation-adoption.html?icid=internalsearch_promo_rpa-in-ia

Deloitte. (2019). *"Internal audit future trends and innovation".* Retrieved from https://www2.deloitte.com/us/en/pages/risk/articles/internal-audit-future-trends.html

Donald, W., & Turney, P. (1990). In *Auditing EDP Systems: Second edition* (p. 108).

Donaldson, S., Sigel, S., & Williams, C. (2018). In S. Donaldson, *Enterprise Cybersecurity Study Guide: How to Build a Successful Cyberdefense Program Against Advanced Threats.*

Edward Snowden: Leaks that exposed US spy programme. (2014). Retrieved from BBC: https://www.bbc.com/news/world-us-canada-23123964

EU recommendation 2003/361. (2003). Retrieved from European Comissiom: https://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_en

FBI. (2014). *A Byte Out of History $10 Million Hack, 1994-Style*. Retrieved from https://www.fbi.gov/news/stories/a-byte-out-of-history-10-million-hack

Gannon, P. (2014). *WW1: First World War technology: Room 40 secret intelligence unit*. Retrieved from https://eandt.theiet.org/content/articles/2014/06/ww1-first-world-war-technology-room-40-secret-intelligence-unit/

Gert, W. (2014). *SMEs and the credit crunch: Ciurrent financing difficulties, policy measures and a review of literature* . Retrieved from OECD: https://www.oecd.org/finance/SMEs-Credit-Crunch-Financing-Difficulties.pdf

Ghosh, A., & Moon, D. (2005). Auditor Tenure and Perceptions of Audit Quality. The Accounting Review.

Henrics, M. (2006). *Falling Flat?* Retrieved from Enterpreneur: https://www.entrepreneur.com/article/74836

Huang, L. (2019). *The Influence of Enterprise Management Risk on Audit Fees* . Retrieved from fhttps://www.scirp.org/html/13-1762321_90570.htm

Ingham, K., & Forrest, S. (2014). A History and Survey of Network Firewalls. *University of New Mexico*, 7.

Institute, M. G. (2017). Where machines could replace humans - and where they can't (yet).

Jonas, N. (2014). SME's life cycle - steps to failure or success? 1.

Katua, N. T. (2014). The Role of SMEs in Employment Creation and Economic Growth in. *International Journal of Education and Research* .

Kirti, P. (2016). Audit.

KPMG. (2016). Retrieved from https://assets.kpmg/content/dam/kpmg/pdf/2016/05/Cyber-Security-and-Board-Oversight-Whitepaper.pdf

KPMG, F. I. (2017). *Audit 2025. The future is now.* Retrieved from https://assets.kpmg/content/dam/kpmg/us/pdf/2017/03/us-audit-2025-final-report.pdf

Leung, P., & Cooper, P. (2004). In *Modern auditing & assurance service (2nd ed.).*

Leyden, J. (2012). *The 30-year-old prank that became the first computer virus*. Retrieved from The Register: https://www.theregister.co.uk/2012/12/14/first_virus_elk_cloner_creator_interviewed/

Maurer, R. (2015). *Human Error Cited as Top Cause of Data Breaches*. Retrieved from SHRM: https://www.shrm.org/ResourcesAndTools/hr-topics/risk-management/Pages/Human-Error-Top-Cause-Data-Breaches.aspx

Melanie, W. (2019). *Top 4 cybersecurity frameworks*. Retrieved from IT Governance Blog: PCI DSS (47%)

Mervin, K. (2018). *“Where is the audit profession going?”* . Retrieved from Accounting Today: https://www.accountingtoday.com/opinion/where-is-the-audit-profession-going

Millaire, P. (2017). What All Cyber Criminals Know:. 2-3.

Minárik, T. (2020). *National Cyber Security Organization: Czechia*. Retrieved from CCDCOE: https://ccdcoe.org/uploads/2019/12/CS_organisation_CZE-3.0_Revised_TJ_Final_PDF.pdf

Mutune. (2020). Retrieved from https://cyberexperts.com/cybersecurity-frameworks/

NIST. (2008). *NIST Special Publication 800-55.* Retrieved from National Institute of Standards and Technology: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55r1.pdf

NIST Special Publication 800-26. (2017). Retrieved from National Institute of Standards and Technology.

OECD. (2014). SME STATISTICS: TOWARDS A MORE SYSTEMATICSTATISTICAL MEASUREMENT OF SME BEHAVIOUR . *ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT* .

Operating System Market Share. (2020). Retrieved from Net Marketshare: https://netmarketshare.com/operating-system-market-share.aspx?options=%7B%22filter%22%3A%7B%22%24and%22%3A%5B%7B%22deviceType%22%3A%7B%22%24in%22%3A%5B%22Desktop%2Flaptop%22%5D%7D%7D%5D%7D%2C%22dateLabel%22%3A%22Trend%22%2C%22attributes%22%3A%22share%22%2

Paul, T. (2013). In *Critical Information Infrastructure Protection and Resilience in the ICT Sector* (pp. 305-306). Retrieved from https://books.google.cz/books?id=P8ueBQAAQBAJ&pg=PA305&lpg=PA305&dq=1960s:+Password+protection&source=bl&ots=RYjwNJM5aI&sig=ACfU3U2aOTlQSjlcJeAziTNA2gbr5Zz3qQ&hl=en&sa=X&ved=2ahUKEwjg79Kr64fmAhURkxQKHe6HBsAQ6AEwEXoECAYQAQ#v=onepage&q=1960s%3A%20Password%2

Perlroth, N. (2017). *All 3 Billion Yahoo Accounts Were Affected by 2013 Attack*. Retrieved from The New York Times: https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html

Peters, J. (2020). *What is ISO 27001 Compliance? Essential Tips and Insights*. Retrieved from Varonis : https://www.varonis.com/blog/iso-27001-compliance/

Ross, R., Katzke, S., & Johnson, A. (2015). NIST Special Publication 800-26. In *Security Self-Assessment Guide for Information Technology*.

Sarens, G., De Beelde, & Evaraert, P. (2009). Internal Audit: A Comfort Provider to the Audit Committee,. *The British Accounting Review, Vol. 41*, 90-106.

Schreier, J. (2011). *Sony Estimates $171 Million Loss From PSN Hack*. Retrieved from Forbes: https://www.wired.com/2011/05/sony-psn-hack-losses/

Securityaware. (2019). *SMESEC framework - training courses*. Retrieved from https://securityaware.me/preview_course.php?course_id=192

Shane Richmond, & Williams, C. (2011). Retrieved from The Telegraph: https://www.telegraph.co.uk/technology/news/8475728/Millions-of-internet-users-hit-by-massive-Sony-PlayStation-data-theft.html

Singh, S. (2009). In *The code book.*

Small and Medium Enterprises (SMES) Finance. (2019). Retrieved from World Bank: https://www.worldbank.org/en/topic/smefinance

SMESEC. (2019). *About SMESEC*. Retrieved from https://www.smesec.eu/about.html

SMESEC. (2020). *D2.1 SMESEC security characteristics*. Retrieved from SMESEC: https://www.smesec.eu/doc/SMESEC_D2.1_SMESEC_security_characteristics_description_security_and_market_analysis_report_V1.1.pdf

SMESEC. (2020). *D2.3 Security Awareness Plan Report*. Retrieved from SMESEC: https://www.smesec.eu/doc/SMESEC_D2.3_Security_Awareness_Plan_Report_v1.0.pdf

SMESEC. (2020). *D3.3 Final Version of the SMESEC security*. Retrieved from SMESEC.

SMESEC. (2020). *D3.5 Preliminary SMESEC Security*. Retrieved from SMESEC: https://www.smesec.eu/doc/SMESEC_D3.5_preliminary_awareness_and_training_report_v1.0.pdf

SMESEC. (2020). *D5.1 Trial scenario definitions and evaluation methodology specification*. Retrieved from SMESEC: https://www.smesec.eu/doc/SMESEC_D5.1_Trial_scenario_definitions_and_evaluation_methodology_specification_v1.0.pdf

Statista. (2019). *Leading cause of ransomware infection 2019*. Retrieved from Statista: https://www.statista.com/statistics/700965/leading-cause-of-ransomware-infection/

Statistics on small and medium-sized enterprises. (2018). Retrieved from Eurostat: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Statistics_on_small_and_medium-sized_enterprises&oldid=451334#General_overview

Steller, H. (2011). Auditing Principles. The University of Michigan.

Swanson, M. (2001). Security Self-assessment Guide for Information Technology System. U.S. Department of Commerce, Computer Security Division, Information Technology, National Institute of Standards and Technology.

Symantec. (2018). *10 cyber security facts and statistics for 2018*. Retrieved from https://us.norton.com/internetsecurity-emerging-threats-10-facts-about-todays-cybersecurity-landscape-that-you-should-know.html

Symantec. (2019). *2019 Internet Security Threat Report*. Retrieved from https://www.symantec.com/en/uk/security-center/threat-report

Teck-heang, L., & Azham, A. (2008). *Accounting and Auditing*.

The History Of Computer Virus. (2008). Retrieved from https://thekill08.wordpress.com/2008/05/24/the-history-of-computer-virus-english-coding/

V.A., N. (2002). In *Short history of cryptography evolvement.* Moscow State University.

V.C., I. (2015). In *"Dark rooms ": the history of Russian censorship. XVIII - beginning of XX century* .

Verizon. (2019). *2019 Data Breach Investigations*. Retrieved from https://enterprise.verizon.com/resources/reports/dbir/

Wei, L., & Aiken, M. (2003). *Accounting history.* Retrieved from https://www.tandfonline.com/doi/abs/10.1080/09585200210164566a?journalCode=rabf20

Writer, S. (2018). *A Brief and Incomplete History of Cybersecurity*. Retrieved from United States Cybersecurity Magazine: https://www.uscybersecurity.net/history/

Wyk, A. l. (1989). The Lehigh virus. In *Computers & Security* (pp. 107-110).

Zou, J. (2019). On the Role of Internal Audit in Corporate Governance. *American Journal of Industrial and Business Management*, 63-71.