LAPPEENRANTA-LAHTI UNIVERSITY OF TECHNOLOGY LUT
School of Engineering Science
Software Engineering

ISO 27001 Standardization of the existing ISMS in a Software Industry SME

Examiners: Professor Jari Porras
Associate Professor Ari Happonen

Supervisors: Associate Professor Ari Happonen
Chief Information Security Officer Tuomas Rapo

TIIVISTELMÄ

Lappeenrannan-Lahden teknillinen yliopisto LUT
School of Engineering Science
Tietotekniikan koulutusohjelma
Varpu Huhtinen

Olemassa olevan tietoturvallisuuden hallintajärjestelmän ISO 27001 standardointi Ohjelmistoalan pk-yrityksessä

Diplomityö 2021

65 sivua, 12 kuvaa, 2 taulukkoa, 2 liitettä

Työn tarkastajat: Professori Jari Porras
Associate Professor Ari Happonen

Hakusanat: ISO 27001, ISO Standardointi, Tietoturvallisuuden hallintajärjestelmä, Tietoturva, ISO Sertifiointi

Keywords: ISO 27001, ISO Standardization, ISMS, Information Security, ISO Certification

Liikekumppanien huoli omien tietojen turvallisuudesta ja tietoturvauhkien määrän kasvu ovat kasvattaneet yrityksien tarvetta toteuttaa järjestelmiä, jotka mahdollistavat tietoturvallisen tiedon hallinnan. Tässä diplomityössä, kirjallisuus katsaus on tehty, jotta ymmärrettäisiin Tietoturvallisuuden Hallintajärjestelmän tärkeys ja mitä haasteita voi tulla vastaan järjestelmän standardoimisessa. Metodologia olemassa olevan järjestelmän ISO 27001 standardoimiseksi on määritetty kirjallisuuteen perustuen. Kyseinen metodologia otetaan käyttöön esimerkki Ohjelmistoalan pk-yrityksessä, jonka tavoite on ISO 27001 standardointi. Kirjallisuudesta havaittiin, että standardoinnin haasteita ovat muun muassa työntekijöiden haluttomuus muuttaa toimintatapojaan, yhdenmukaisuuden puute dokumentaatiossa, johdon välinpitämättömyys ja vaikeus määritellä tietoa sisältävät suojattavat omaisuudet. Vaiheet standardoimiseen seuraavat PDCA-sykliä kehittämismenetelmänä, jonka suunnittelu vaiheessa ISO 27001 vaatimukset ryhmitellään, puute analyysi nykyisestä järjestelmästä tehdään, vaadittu dokumentaatio päivitetään tai luodaan ja toteutetaan riskien hallinta iteraatio. Riskien hallinta suunnitelma toteutetaan mallin toteutus vaiheessa, auditointi ja hallinnon katselmointi suoritetaan tarkastus vaiheessa ja lopuksi parannuksia tehdään kehittämisen vaiheessa. Esimerkki yrityksessä, vaiheet toteutettiin toteutusvaiheelle asti tämän diplomityön puitteissa.

ABSTRACT

Lappeenranta-Lahti University of Technology LUT

School of Engineering Science

Software Engineering

Varpu Huhtinen

ISO 27001 Standardization of the existing ISMS in a Software Industry SME
Master's Thesis 2021

65 pages, 12 figures, 2 tables, 2 appendices

Examiners: Professor Jari Porras

Associate Professor Ari Happonen

Keywords: ISO 27001, ISO Standardization, ISMS, Information Security, ISO Certification

With the increasing number of threats to information security and the rising concern of business partners towards the security of their information, it is crucial for organizations to implement systems to manage appropriately information. In this thesis, a literature review is conducted to identify the importance of an effective Information Security Management System (ISMS), challenges that can occur when proceeding to standardize one and to define a methodology to ISO 27001 standardize the existing ISMS of an organization. The methodology is then applied to the existing ISMS of a software engineering SME seeking to standardize their ISMS with respect to the internationally recognized ISO 27001 standard. Among the identified challenges from literature there are the reluctance to change from employees, lack of consistency in documentation, lack of top management involvement and difficulties in identifying information assets. The steps to standardize the ISMS follow a Plan-Do-Check-Act (PDCA) process where ISO 27001 requirements are grouped, a gap analysis is conducted, all required documentation updated or created and risk management conducted in the planning phase, risk treatment implemented in Do-phase, auditing and reviewing the ISMS in the Check-phase and finally improving the ISMS in the Act-phase. The steps are implemented for the case company in this thesis only until the Do-phase.

ACKNOWLEDGEMENTS

I tend to believe that the greatest things in life are achieved with support and help from others, as no one can really travel the world entirely alone. It is the case for this thesis as well, and not only this but my entire studies in Finland. I want to thank LUT University for providing such great teaching that I went from a teenager who used to hate calculator algorithms and was not able to fill a simple form on the internet without help in high school to a young woman who loves spending hours coding on a computer and to whom friends turn for technological advice. Not only did this university provide me with great education, but it also helped me really find my own path in life.

My thanks also go to my family (including cats) and friends in France, Finland and Switzerland who all supported me in their own ways through the hard times we all face at some points, especially during studies. It was nice to share memes, cat pictures, play games, drink tea, call, swim, whatever we all did together to draw our minds away from studies for a little while.

As for this thesis especially, a big thanks goes to my academic supervisor, Ari Happonen, for his flexibility and always answering my emails fast with more than great advice on how to improve my thesis. Another great thank goes to my supervisor in the case company, Tuomas Rapo, without whom I would have never been able to understand the company's information security practices and processes so fast, and who helped the ISO 27001 project to go in the right direction, despite the various challenges we faced.

Last but not least, I thank the entire case company for providing me the chance to do my thesis on such an interesting and useful subject and for welcoming me so warmly in their team.

My academic studies may come to an end with this thesis, but as we all know, especially in technology, studies never end, which is a thing I am grateful for.

In Lappeenranta, on the 26th of August 2021
Varpu Huhtinen

TABLE OF CONTENTS

LIST OF SYMBOLS AND ABBREVIATIONS

AWS	Amazon Web Services
BSI (1)	Bundesamt für Sicherheit in der Informationstechnik
BSI (2)	British Standards Institution
B2B	Business-to-Business
CI	Continuous Improvement
CIA	Confidentiality, Integrity and Availability
CISO	Chief Information Security Officer
CMM	Capability Maturity Model
CVE	Cybersecurity Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
DDoS	Distributed Denial Of Access
DoS	Denial of Access
GDPR	General Data Protection Regulation
HTTP	Hypertext Transfer Protocol
ICT	Information Communication Technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IoT	Internet of Things
IS	Information Security
IT	Information Technology
ISMS	Information Security Management System
ISO	International Organization for Standardization
OPP	Obligatory Passage Point
OWASP	Open Web Application Security Project
PDCA	Plan Do Check Act
PII	Personally Identifiable Information
QA	Quality Assurance
RAC	Risk Acceptance Criteria
SME	Small & Medium-sized Enterprise
SoA	Statement of Applicability
SSL	Secure Sockets Layer
Tbps	Terabits per second
TC	Technical Committee

1 INTRODUCTION

Software industry is among the most vulnerable industries to attacks that could compromise the security of information, and it is the role of the organizations managing the information to keep it secure [1]. In the modern day, organizations do not only manage personal data from individuals but also information from customer organizations, sometimes critical business information which must be secured to avoid leaks to competitors, for instance. Information security management is not a trivial matter and needs to be addressed appropriately in order to ensure business continuity for the organizations and their customers benefit. To achieve this purpose, a variety of standard exists to support organizations in building efficient and effective Information Security Management Systems (ISMS).

In this thesis, the focus is brought on the ISO 27001 standard to which a case company working in the software industry is standardizing their ISMS against. However, before going in more details into the standardization itself and the importance of proper information management, it is important to understand the motivators that can bring a company to comply with different standards. Identifying these motivators will help in understanding on a case basis which is the main reason for an organization to comply to a standard and thus help in identifying the most important areas of the organization that need to be made compliant.

1.1 Standardization in the Software industry

In the modern society, standards are omnipresent as they range for example, from the medical field with the international DICOM standard regulating the storage and processing of medical digital images [2], to the electrical field with standards such as the Finnish SFS 6001 regulating the safety of high-voltage electrical installations [3]. The software industry field makes no exception to this standard omnipresence and working with standards in the field is unavoidable. Actually, standards in software engineering define a set of codified knowledge which has been documented through successes and failures in the discipline [4]. This codified knowledge needs to be learned and known by professionals in the field, as, unlike other engineering fields, software engineering does not rely on the laws of nature and consequently in order to build quality, interoperability and avoid common errors, having standards is crucial [4]. Standardization has been a key for the growth and power of

Information Communication Technology (ICT) that have allowed interoperability of different systems through universally accepted technologies [5]. For instance, web standards such as the Hypertext Transfer Protocol (HTTP) and Secure Socket Layer (SSL) help web services in exchanging information securely on the internet [6]. This need for interoperability of systems is explained by, inter alia, the rising need for smart cities as urbanization grows and the rising importance of the Internet of Things (IoT), in which information sharing is at the core [5].

ISO & IEC provide a wide number of standards for ICT ranging from information security to artificial intelligence, and standards covering the entire life-cycle of software and systems engineering activities [5]. For instance, ISO/IEC/IEEE 12207:2017 defines activities, processes, and tasks to perform throughout the different software life cycle processes [7]. Moreover, the quality of a software product can be assessed by using the guidelines provided by multiples software industry specific standards like ISO/IEC 25010 which defines the eight quality characteristics in a quality model for a software product [8], or the IEEE 730-2014 standard, from the Institute of Electrical and Electronic Engineers (IEEE), which is used as guidelines for the software quality assurance processes and which is harmonized with the previously mentioned ISO/IEC/IEEE 12207:2017 [9].

The standards listed above are, however, only a few examples of software industry specific standards. In fact, in 2017 on their research on software standards and software failures, Khan & Malik identified 32 active and relevant software industry specific standards from the IEEE database only, that cover different phases of software production in industry, such as documentation, Quality Assurance (QA) or software maintenance [10]. In their study, they also identified the twelve factors, with their 52 sub-factors in total, that can lead to software failures based on these standards [10]. With comparison, the ISO/IEC JTC 1 Technical Committee (TC), which is a joint committee of the International Organization for Standardization (ISO) and International Electrotechnical Committee (IEC), in charge of Information Technology (IT) standards has direct responsibility of 492 currently published standards with 22 subcommittees of which, for example, ISO/IEC JTC 1/SC7 is responsible of 205 standards related to Software and systems engineering, ISO/IEC JTC 1/SC 38 is responsible of 22 standards for cloud computing and distributed platforms and ISO/IEC JTC

1/SC 22 is responsible of 108 standards related to programming languages, their environments and systems software interfaces [11].

These numbers show that Khan & Malik have identified only a small portion of software industry specific standards and that practitioners in IT industry are guided or regulated by a multitude of standards. Furthermore, it is important to note that the Information Technology Joint Technical Committee (JTC) is the TC of ISO that has, by far, the most published standards with 3 276 standards against 950 published standards by ISO/TC 22, the TC for Road Vehicles, which is the second highest number by TC [12]. In addition, the IT committee has 613 standards under development against 259 for Road Vehicles, which shows that, like information technologies themselves, the standards for IT are constantly evolving and new standards are being developed at a high pace [12].

In addition to these sector specific standards, there also exists a multitude of standards that can be implemented in any organizations, no matter what business they operate in. Many standards are, for example, intended for system management in organizations such as the ISO 27001 and its ISO 27000 family on the information management, described in more details in 3.2. Another example of a non-industry specific standard is the widely implemented ISO 9000 standard family which is intended for quality management with the ISO 9001 standard that can be, as the ISO 27001 standard, certified against [13]. A third standard family that is not industry specific and to which some organizations seek certification is the ISO 14000 family that provides rules for environmental responsibility management of organizations [14].

These standards, ISO 9001, ISO 27001 & ISO 14001 have the highest certification numbers among the ISO standards [15]. In fact, by the 31st of December 2019, 883 521 organizations were issued a valid ISO 9001 certification, 312 580 a valid ISO 14001 certification and 36 362 a valid ISO 27001 certification [15]. When considering the spread among different sectors, if the number for not known sector is not considered, Information Technology is the field with the highest number of ISO 27001 certificates, 8562 against the category “Other Services” which has the second highest number, 1 435 and 989 for the transport, storage and communication sector, which is the third highest number [15]. This high number of certificates in ICT can be explained by the growing need for interconnected and interoperational information systems discussed earlier that increases the amount of

processed information and consequently increases the need for proper information management [5]. It is however important to note that, even though thousands of organizations are certified against various ISO standards, none of the certificates listed above are mandatory and organizations seek certification for various reasons of which some are documented in the following subsection.

1.2 Why organizations standardize?

Literature has extensively studied the reasons alongside the benefits organizations gain from certification to specific standards. First, when considering the software industry specifically, a study conducted by Ankur & Gupta in India, with a sample of 424 questionnaire responses from various Indian software engineers from different software firms, assessed the significance of quality certification through the CMM (Capability Maturity Model) and ISO 9001 certification [16]. The study found that certified organizations developed better software than non-certified ones, that the business excellence was improved and that better Total Quality Management were in place in the certified organizations [16]. The study shows that certification helps organizations in software industry to achieve better performance by following and implementing the standards in their organization.

Walrad, on their publication about the standards for the Enterprise IT profession, highlights the importance of standards in IT field as a sign of professionalism [17]. However, based on their paper, certification is not sufficient to prove this professionalism and it requires rigorous knowledge of the followed standards and well-implemented principles in practice. They also endorse the fact that the implementation of standards helps in building trust, as the standards and certifications associated with them give confirmation of good practices being implemented and taken in practice in an organization [17].

On a more general level, one motivator for organizations to seek certification relies in gaining a competitive advantage in their market. In fact, according to Uwizeyemungu & Poba-Nzaou, an organization does not only need resources that will allow it to build the products for its intended market to achieve success, but acceptance is also a requirement for it [18]. Acceptance can come from the customer but also from any stakeholder involved in formal or informal networks that the organization is embedded in and in order to reach this

acceptance, organizations need to adapt their products and processes to, for instance, different common practices and regulations that are used in these networks [18].
In the same study, three types of isomorphisms have been identified that influence the decision to standardize in organizations: coercive, when the pressure comes from business partners; normative when it comes from professional training and mimetic when it is induced by common practice in the field [18]. The coercive isomorphism that brings the need for an organization to standardize some of their product or processes to gain new customers, business partners or to respond to government regulations is the most relevant when thinking of gaining a competitive advantage by standardization. This is enhanced by Guler et al. in their study on the international spread of ISO 9000 Quality certificate in which they have identified coercive isomorphism as a strong mean to get the certification [19]. In fact, government organizations and multinationals have been identified as having a big effect on the implementation of the standard and certification seeking in organizations, as getting the certification was a competitive factor [19].

On the same idea of coercive isomorphism, Backhouse et Al., in their study on shaping an international Information Systems (IS) security standard, have identified that for standards to become an Obligatory Passage Point (OPP) for organizations, the pressure to get a certification often comes from power relationships [20]. Such relationship is one where an important customer or business partner sets getting a certification as a requirement, before going further in the contractual agreement with a company [20]. The adoption of specific standards can indeed be required to show a customer or business partner that good practices are in place and it helps in building an aura of trust and confidence in the business relationship [20].

Many studies have shown, over a large timespan, that organizations gain various benefits and mainly external ones from adopting standards as demonstrated by the literature cited above. In addition to these, in 1999, more than twenty years ago, Anderson et al. conducted a research to find the main reason for firms in getting the ISO 9000 certification [21]. The outcome of the study, conducted on over five hundred ISO 9000 certified manufacturing firms, showed that the primary reasons for companies to adopt the standard is in gaining competitive advantage by building trust and showing that good quality management and assurance practices are in place in the organization [21]. The same result was reached by

Prado-Román et al. in 2015 on their research on the benefits of certifying to ISO 9001 in the Spanish Construction Industry; in the research they analyzed responses of over a hundred quality managers of certified organizations and 86.6% of the responses yielded that certification was seen as a main reason for gaining a better competitive advantage, 74.4% agreed with the fact that certification improved internal processes in the organization and 62.2 % agreed on the fact that customer management was improved [22].

Finally, in a recent paper published in January 2021, Culot et Al. conducted a literature review to find the current state of research on the ISO 27001 standardization topic, in which they found that, in 48% of the 96 articles selected for their review, the topic of motivations of organizations to voluntary standardize has been addressed [23]. It was found that for the majority the motivator was an institutional one with 19 studies stressing the motivator to be the improvement of the image of the organization, 11 articles stressing the motivator to be a governmental, regulatory or promotion activity, another 11 stressing the motivator to be demands of the market and finally 9 studies stressing the motivator to be isomorphism [23]. Based on these numbers, the motivators to standardize, which are identified earlier in this section, are also applicable to ISO 27001 standardization specifically. Additionally, they also identified functional reasons such as achieving higher levels of information security management and better efficiency in the related processes [23] which endorses the same idea as Prado-Román et al. of certification improving internal processes and management.

These papers help to understand some of the reasons motivating organizations to standardize or more precisely to seek a certification. It was indeed seen that certification can bring a competitive advantage compared to other non-certified competitors and better acceptance from the customer, as certifications prove that good practices are in place in the organization. In addition to the competitive advantage, the motivators can be a requirement from interested parties or mimetic nature in the field, which translates to different types of isomorphism. Moreover, standardization in an organization was found as improving efficiency and reducing business risks, as the different processes and activities are standardized and consequently uniformized which helps in avoiding, for instance, unawareness on how to conduct an activity as operations are standardized. The importance of standards specifically in the software industry was also discussed in this section, as the purpose of the empirical work of this thesis is to seek ISO 27001 certification for a software industry SME and

understanding the importance of standardization is crucial to achieve this goal, even though ISO 27001 is not a software industry specific standard. The existence of these non-sector specific standards was also discussed, and it can be argued that, as they are implementable in a more various number of fields, their meaning is better understood especially when an organization works in a Business-to-Business (B2B) environment with customers operating in other fields as they are more likely familiar with this type of standards than sector specific ones and consequently understand better the brought value.

1.3 Goals and delimitations

This thesis is done for an SME which operates in the software industry field. The company seeks to standardize their ISMS based on ISO 27001 requirements and the goal of this thesis is to (1) find the steps to undertake for an existing ISMS to get ISO 27001 certified, (2) identify the issues and challenges that may arise in the standardization process of an ISMS, (3) make corrective actions for the ISMS to comply with ISO 27001 standard's requirements.

The core of the paper relies on comparing the issues and challenges identified during (2) based on existing literature against new or similar issues that arose during the empirical work done in (3). The outcome of (1) is used to define the framework for the implementation of the ISO 27001 standard in the case organization. The outcomes of (2) are not used only for comparison but also to acknowledge the potential challenges and issues already existing and to proceed to the standardization implementation.

This work is not intended to provide guidance in implementing an ISMS in an organization that does not have any ISMS in place at the time of starting the process as the case organization has already one which is changed and improved to meet ISO 27001 requirements. It is also not in the scope of this work to find a certification body nor to initiate the certification audits in the case organization for which the ISO 27001 standardization methodology is implemented.

1.4 Structure of the thesis

This thesis is structured, first, with the introduction which provides, based on literature, an overview of the importance of standardization especially in the software engineering field.

In the second subsection, the reader is also made aware of the multiple reasons that could motivate an organization to seek certification so that the purpose of the ISO 27001 project of the case organization is better understood.

The second section is started with the background of information security standards, followed by a literature review to identify the risks related to information security to better understand why a properly implemented ISMS is important. The review is covered in a way that the commonly identified human-induced information security risks that enhance the importance to implement an efficient ISMS are identified in addition to some technical risks, mainly applicable to software development. In the same section, the most relevant challenges which have been encountered in ISMS standardization have been documented in a sub-section, based on another literature review which was conducted by searching for literature documenting potential failures or challenges faced by organizations in the standardization of their ISMS. This insight is sought in order to be able to pay special attention to these issues when proceeding to the standardization in the case organization.

The third section of the paper brings the focus on the ISO 27001 standard specifically by, first, identifying the advantages that the standardization against it can bring based on literature and second, providing an overview of the entire ISO 27000 standard family for the management of information security. After that, we conduct another literature review to identify the steps that are needed for implementing the standard on a general level and more precisely in SMEs.

The fourth section of the paper concerns the documentation of the ISO 27001 ISMS standardization in the case company. It is started by introducing more precisely the context of the company so that the motivators that lead them to seek the standardization of their ISMS are better understood. After that, the plan for the standardization is documented, which is built based on the literature of previous sections, followed by the implementation in practice in the case organization alongside discussion on the challenges that have been encountered during the process.

2 STANDARDIZING AN ISMS

To effectively standardize an ISMS, it is crucial to understand what makes proper information security so important and why it needs to be managed. Consequently, in this section the background to the creation of guidelines and standards for managing information security is documented. As information is vulnerable to various threats, common technical and human induced threats are documented in 2.2 so that the importance of managing these threats is better understood which endorses the importance of implementing an efficient and effective ISMS. However, even if by standardizing an ISMS an organization may gain different benefits as seen in 1.2, from improved processes to a higher confidence from customers, the standardization is not straightforward, and some challenges may be met during the process. Therefore, in 2.3 a literature review is conducted to understand these different challenges that may occur during the standardization based on the experience of other companies. This will provide insight on what could go wrong in the standardization and consequently be prepared for the challenges.

2.1 Background to the management of information security

In the current world, with the growing digitization of data, information security is no longer just the concern of organization's Security departments but of everyone, as every individual has some personal information stored on software systems [24]. The concern of information security has risen even more with the introduction of the General Data Protection Regulation (GDPR) in the European Union (EU) in 2018 which has significantly impacted the information security management of big and small Organizations which are doing business in the EU. In fact, even if not all information stored by organizations concerns personal data, all information that contains it must be secured against loss and damage and consequently the ISMSs of organizations have been revised to comply with the regulation to avoid administrative fines going up to 20 million euros or 4% of annual global turnover depending on which is higher for the organization [25], [26].

Moreover, the number of cyber threats has risen over the years with the globalization of connected IT, cloud-services, and a rising need for software with more and more valuable information being used and stored on different types of software solutions. It is the responsibility of the organizations to secure all the processed and stored information while

keeping the infrastructures running [24], [27], consequently, the organization is responsible for staying up-to-date on the threats and find ways to avoid the materialization of the risks presented by these. The variety of cyber threats is best illustrated with the number of publicly identified Cybersecurity Vulnerabilities and Exposures (CVE) which, at the time of starting this paper in mid-March 2021 was at 150 378, at the beginning of July 2021 at 156 334 and mid-August of the same year at 158 851 [28]. As a consequence, it can be stressed that information security management, especially in organizations developing web-based software or using them, should be paid great care to, as the number of cybersecurity vulnerabilities only keeps increasing.

In addition to that, it is important to note that for smaller companies, information breaches may induce costs so high that the company will not sustain them as it has been found on a survey commissioned by National Cyber Security Alliance (NCSA) in 2019 [29]. In fact, out of 1006 surveyed small businesses, 10% went completely out of business, 25 % filed for bankruptcy and 37% suffered financial losses as consequences of cyber-attacks on their business [29]. Another study stresses that most of cyberattacks are targeted towards SMEs as they tend to have less robust information security infrastructure than bigger companies and can be used as gateways to bigger companies [30]. Hence the importance of implementing a good ISMS, especially in SME organizations, which reputations and future are at risk in case of a bigger data breach or cyber-attack.

The ever-rising number of threats to information and the concern of people on how their information is stored and processed, has led to the need for properly implemented ISMSs. In fact, a well-thought ISMS can allow an organization to stay ahead of cyber-attacks and other threats to information security, significantly mitigate related risks and to show how all retained information is stored and handled [31]. However, some guidelines are needed to implement such ISMS which induced the creation of multiple frameworks that provide guidance and formal standardization related to information security for organizations. For instance, ISO/IEC 15408:2020 is an IT specific, three-part standard, which provides guidance for developing, evaluating or acquiring IT products that provide security functionality by addressing things such as information asset protection [32]. Another example of security related standard is the German IT-Grundshutz that provides Bundesamt für Sicherheit in der Informationstechnik (BSI (1)) Standards, namely BSI (1) Standards

200-X that give guidance on the requirements of an ISMS, on how an ISMS can be built and how risk management can be pursued [33]. In this paper, the focus is on the globally recognized ISO 27001 standard, which defines a framework to follow for organizations so that they remain up to date against risks related to information security. By complying with this latter standard, an organization can get ISO 27001 certified, which shows, inter alia, to external interested parties that the organization has good information security practices in place that conform with an internationally recognized standard.

This ISO 27001 standard is part of the large ISO/IEC 27000 standard family that covers different aspects of the information security management, this standard family was created in December 2000 by the collaboration of the International Electrotechnical Commission (IEC) and the International Organization for Standardization (ISO) to give an internationally recognized framework for good practices in information security management [34]. The initial version of the ISO 27001 standard was published in the United Kingdom by the British Standards Institution (BSI (2)) group as the second part of the multiple-part standard BS7799 in 1999 and named Information Security Management System [1]. This standard was revised in 2005 to cover risk analysis and management and was also renamed as ISO/IEC 27001:2005 [1]. After being renamed, the standard had one significant revision in 2013 The most recent version published of the ISO 27001 standard is the ISO/IEC 27001:2017 which did not bring any new requirements to the 2013 and made only minor aesthetic or wording changes [35].

2.2 Risks related to information security

Concern towards information security has risen over the years and organizations have grown more aware of its importance. However, the information security risks keep evolving as seen with, for instance, the CVE number [28]. In the case company, the increase in information security risks was seen when the company decided to move to web services instead of having exclusively internal servers in use, of which the accesses were manageable more easily than on the web, with the growing number of cyberattacks.

In order to avoid, inter alia, financial or reputational losses, an organization needs to stay up to date with these risks. In addition to the number of CVE, the current COVID-19 pandemic

illustrates well how the threats against information security evolve at a high-pace. In fact, organization have had to adapt overnight to new work practices and consequently opened doors for new security vulnerabilities due to, for instance, unpreparedness of some organizations to work securely remotely [36].

In order to properly address information security risks in their ISMS, an organization needs to understand that risks come from the entire environment, whether it is from an employee through social engineering, a malware or unsecure building [37]. The security breaches in an organization can have several consequences going from high costs to timely operating problems if the security breaches happen on critical parts of an organization [37]. Consequently, in this subsection, common human and technical threats to information security are identified.

2.2.1 Human-induced risks

Based on the 2021 Data Breach Investigation Report (DBIR) by Verizon, as seen in ***Figure 1***, information breaches occurred by more than 30% via social engineering and over 25% via Basic Web Application Attacks during the reviewed year [38]. In addition to these statistics, Verizon's report shows that "83% of breaches involved a human element" and that "61% of breaches involved credentials" [38]. Thus, it can be argued that human factors should be especially considered when managing information security.

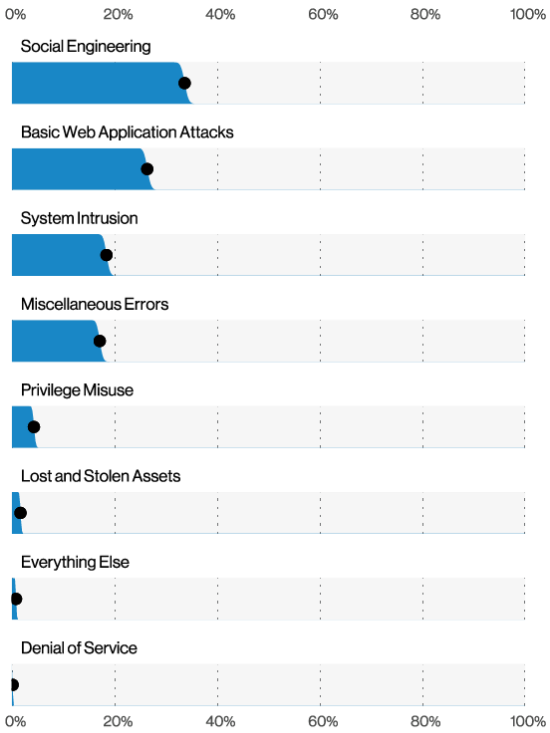

Figure 1. Patterns in breaches (n=5,275), from Verizon 2021 Data Breach Investigation Report [38]

Along the same idea of human induced information security threats, in their paper on the challenges and factors influencing information security policies in organizations, Alotaibi et al. stress that a big concern in organizations regarding information security relies in the threat that employees represent [39]. In fact, carelessness, unawareness or lack of instructions may create employee-induced information breaches [39]. It was also highlighted that even when security policies are in place, some employees are not aware of them [39], which shows the importance on implementing strict policies with respect to information security which are easily accessible and understandable . The lack of awareness that results in human-induced information security risks is often caused by a lack of training of employees or too much information provided at a time which is not assimilated correctly [39].

Alahamari and Duncan, on their systematic review of management of cybersecurity in SMEs, stress that smaller companies often have less robust information security processes in place due to a lack of expertise, of awareness or underestimation of their likeliness to fall victim to attacks [40]. In addition, it has been highlighted that even though employees are aware and know about security policies and practices that are implemented in the

organization, they may not follow them in their daily work which induces risks to information security [40]. Consequently, in addition to making employees aware of the policies in place, an organization needs to enforce the use in practice of these policies and consider the monitoring of the information security practices of employees in the ISMS.

2.2.2 Technical risks to information Security in Software development

In his book on Engineering Safe and Secure Software systems, Axelrod goes in details on the importance of considering all aspects of information security in the development of software systems [41]. Namely, the risks that can relate to information Confidentiality, Integrity and Availability of information, also called the CIA triad [42].

Even though, based on Verizon's report on security breaches, vulnerability exploitation are less common causes for information breaches with an incidence of only 3% [38], it is crucial for a software development company to consider such vulnerabilities when managing information security in order to avoid potential incidents and subsequent breaches. In fact, vulnerability exploitation refers to the action of successfully exploiting a vulnerability in software which may lead to significant information security breaches. Some catalogues are available for developers to be aware of these vulnerabilities and to help in risk treatment such as the Open Web Application Security Project's (OWASP) Top Ten Security issues [43] and Common Weakness Enumeration's (CWE) top 25 of most dangerous software weaknesses [44]. However, developers must keep in mind other risks and not only the top most severe in order to create and maintain secured software systems [41].

The Top Ten Security Risks related to information Security by OWASP were first published in 2003 [41] and revised multiple times until 2017 [43], when the latest version got available. The goal of OWASP is to support and improve the development of more secured software systems, especially web applications, and consequently they provide reports on the common vulnerabilities as open-source documentation in order for all software developers to have access and use of them [43]. The top ten vulnerabilities and descriptions in the most recent version published at the time of writing this thesis are documented in ***Appendix 1. OWASP Top 10 Security Vulnerabilities*** alongside their descriptions. As for CWE, it provides a list of the most common and severe issues that have been experienced by software engineers

from the past two years based on the date of publication [44]. These weaknesses represent a high risk to information security due to their easiness to be found and to be exploited, as such this list is provided publicly to allow all engineers who may be concerned by them, from developers to testers, insight on these weaknesses in order to consider them in their work [44]. The CWE list and the description of the weaknesses are available in ***Appendix 2. The CWE top 25***.

As it will be seen in 3.3.1, risk assessment is at the heart of the ISMS and thus understanding most of the vulnerabilities that could result in risks to information security in an organization is essential, no matter the field the organization operates in. For the scope of this thesis and the standardization of a software industry organization's ISMS, it is crucial to consider the common vulnerabilities identified in OWASP when proceeding to assess the information security risks, as the case company in this thesis develops software for customer companies which make it critical to avoid the higher risks that could put the customer's information at risk of unauthorized processing or access and permanently impact the customer relationship by affecting the trust they put in the products developed by the company. When considering these vulnerabilities in the risk assessment of a software industry, it is important to assess each one based on how likely the vulnerability is to exist in the developed software.

In Verizon's report, they also communicate the common causes for information security incidents shown in ***Figure 2***, in which it can be seen that the most common causes are Denial of Service (DoS), Basic Web Application Attacks, Social Engineering and System Intrusion, even though the latter one has significantly decreased since 2019 [45]. Social Engineering falls into human-induced threats discussed in the previous paragraph, all others are technical risks.

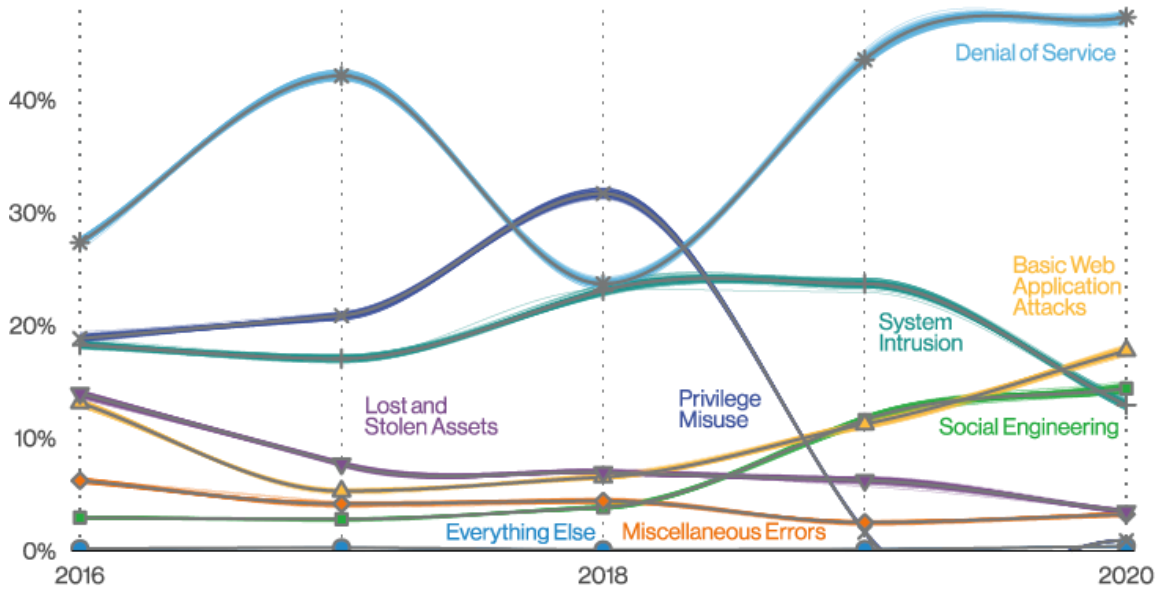

Figure 2. Patterns over time in incidents, from Verizon 2021 Data Breach Investigation Report [45]

A DoS attack is a threat in which it is impossible for users to access an IT resource due to traffic flooding performed by a malicious actor on a server, system or network which overloads the resources of the target [46], thus, this type of attack is a threat to information availability. However, even if DoS is the most occurring cause of information incidents, it is the lowest cause for information breaches, as it can be seen in **Figure *1*** from previous section, as it is easily mitigated using different network controls [47]. There still have been some notable DoS or Distributed DoS (DDoS) attacks with, for example, GitHub being offline for 10 minutes in 2018 due to a DDoS peaking at 1.35 terabits per second (Tbps) or Amazon Web Services (AWS) which encountered a DDoS peaking at 2.3 Tbps in 2020 which was mitigated using AWS shield [46].

Basic Web Application Attacks (BWAA) include attacks such as use of stolen credentials, which have been stolen through unnoticed social engineering or through credential stuffing where the user used credentials on the attacked system that were compromised elsewhere [48]. Other attacks included in BWAA are brute force or vulnerability exploiting which was already mentioned at the beginning of this section [48]. Brute force consists of an attack where the malicious actor makes request to a server by using a set of values that are premeditated by them; this type of attack is easily performed when there are no lockout policies in place on a website and consequently an infinite amount of requests can be sent to

a server [49]. For more details on vulnerability exploitation, the description of common weaknesses and vulnerabilities of ***Appendix 1. OWASP Top 10 Security Vulnerabilities*** and ***Appendix 2. The CWE top 25*** can be useful as they provide information on the most common vulnerabilities and related common exploits.

2.3 Challenges in ISMS standardization

As it was seen in section 2.2, there is a wide number of risks related to the CIA triad of information and consequently it is undeniable that information security management needs to be effectively and efficiently implemented in an organization. This topic of proper Information Security management has risen the interest of many scholars. Consequently, a wide number of challenges have been identified by them that could have occurred and could occur during ISMS standardization processes. These challenges may sometimes lead to inability to implement good practices in an organization. Consequently, when starting an ISMS standardization project, it is critical to become aware of potential challenges that may arise during the process so that they can be avoided, when possible, otherwise prepared for.

When creating their engineering environment based on ISO/IEC 27000 series to support organizations that use ISMS, Suhaimi et al. identified several challenges that can occur in organizations that have an ISMS in place [50]. First, threats and risks related to information security keep evolving, which requires continuous involvement from the organization to identify the new risks to update mitigation techniques that are in place in the ISMSs [50]. A second important challenge are the employee's different backgrounds, going to their familiarity with ISMSs to their work experience [50]. In fact, the different tasks related to ISMSs come with a number of documents that are inter-related, a lack of experience in performing such tasks may induce a lack of consistency in the documentation. The lack of consistency can also be affected by multiple people revising a same document at different time and places, or when sufficient quality is not achieved due to lack of requirement to produce these documents [50]. A last challenge that has been identified in the paper is the overlooking of some tasks, when people only focus on the tasks that are directly related to ISMS certification [50].

Abusaad et al., in their study on the implementation of ISO 27001 standard in Saudi Arabia have identified several obstacles to the implementation of the standard [51]. The study was conducted by interviewing the employees of eight different ISO 27001 certified organizations in Saudi Arabia, who were the supervisors of the certification process and the standard implementation in their company [51]. The first and major identified obstacle for the organizations was the identification of their valuable assets that had some risks related to information security, often due to limited scope [51]. The limited scope is closely related with the challenge mentioned in the previous paragraph, about limiting the scope to a specific service or area and not the entire organizations in order to get the certification. Another identified obstacle was the lack of experience [51], mentioned as well in the study by Suhaimi et al [50]. The reluctance to change from employees in the organizations was also seen as an obstacle to the ISO 27001 certification [51]. Finally, the involvement of top management in the process was a secondary obstacle as well as difficulties in understanding the ISO 27001 standard [51].

Tjirare & Shava, in their study on the implementation of ISO 27000 in Namibian organizations have identified several challenges during the surveys they had with employees of organizations that do not have the standard implementation in place [52]. Their study focused on the implementation of standards ISO 27000, 27001, 27002, 27003 and 27004 which purposes are detailed in 3.2 of this thesis, as they are part of the ISO 27000 standard family for information security management. The identified challenges were the lack of training of employees or weak experience in teams, improperly document policies and poor enforcement of these policies by management or co-workers [52].

The acceptance of standards by employees in Organizations is another challenge in the standardization of ISMSs that has been studied by Mueller et al. in their study on understanding what positively and negatively affects the adoption of IT standards [53]. Their study relies on literature and empirical data from interviewees, and even though the final result needs refining it gives a good preliminary idea of why some organizations fail in the implementation of IT standards [53]. Based on the study, new policies related to standards are more likely to be adopted by employees if they benefit from it, for instance if the adoption of the standard is seen as more useful than the former behavior or if they or the organization gains some visible benefits from the adoption of the standard [53]. Another motivating factor

for employees is from social influence, either from co-workers or from superior management in the organization adopting the standard [53]. However, the change of work routines can influence, as stated in the study by Abussad et al. discussed earlier, the willingness of employees to adopt standards and consequently change their work routines [51]. Thus, based on this study, to overcome the employee-acceptance challenge in that standardization process, it is important to define clear governance and management mechanisms that will enforce the usage of IT standards among employees of an organization [53].

Fenz et al. have conducted a study in 2013 to identify the main challenges in information security risk management [54]. Many of the identified challenges were closely related to challenges already mentioned in this section, found by other researchers. For instance, the difficulty in identifying the assets is identified as a challenge by Fenz et al. and Abusaad et al [51], [54]. An asset in this context refers to anything, physical or not that is connected at some level to information and consequently poses a risk for information security and needs to be secured by different means such as physical locks, technical firewalls or organizational policies [54]. Another challenge related to these assets is in determining their value and the losses that may arise from a breach in them, some losses may be of such impact that the organization will not be able to completely recover from them, for example when a loss of image happens in the eyes of the customers which will no longer be willing to use the provided service/product [54]. Moreover, Fenz et al. identified a challenge in the risk estimation, which is due to the evolving nature of risks noted by Suhaimi et al. as well [50], [54]. Due to this changing nature, a risk estimation at some point in time may not be valid at another time as the asset will have gained value in the eyes of potential attackers. Finally, directly related to this risks, overconfidence of organizations in risk assessments may make the assessments too optimistic and biased, which will increase the likelihood of information breaches [54].

When considering standardization to ISO 27001 specifically, the literature review conducted by Culot et al. finds that 68% of the studies included in their review provide the reader with challenges and opportunities that have been met during the implementation of the standard [23]. One recurring challenge being the difficulty in finding methods and tools to implement the standard, as it is, as it will be seen in 3.3.1, not a prescriptive standards and requires organizations to determine by themselves by what means the requirement will be achieved

[23]. Due to lack of expertise in ISO 27001 of the people in charge of the standardization, the selection of proper tools and methods has been found challenging and to sometimes results in not properly identified information assets and consequently lack of precision or accuracy in risk assessments [23].

In this section, major challenges that have occurred in ISMS standardization processes in different organizations have been identified. These challenges need to be considered when proceeding to the ISMS standardization in the case organization in the scope of this thesis. The identified challenges ranged from internal factors with employees reluctant to change and lack of involvement of top management, for instance, to external factors with, inter alia, evolving risks and interest of attackers in the information assets. Additionally, scholars stress that lack of expertise may induce difficulties in selecting appropriate tools and methods and consequently result in lack of precision in results required by standards. Thus, in order to achieve ISO 27001 certification, it is crucial to acquire some level of expertise and to find a clear methodology to follow in order to avoid or overcome the challenges that are identified in this section of the thesis.

3 ISO/IEC STANDARDIZATION PROCESS

In this section of the paper, the steps that are needed to standardize an ISMS with respect to ISO 27001 standard are defined, starting by understanding the benefits brought by the ISO 27001 standardization of an ISMS. Then, the ISO 27001 standard family is familiarized with in order to understand which ISMS related standards are important in the standardization process in addition to ISO 27001. Related works are then documented to see how the standardization process can be done in practice. Finally, the steps to take in the standardization and certification process are documented.

3.1 Advantages of ISO 27001 certified ISMS

In ISO/IEC 27000:2020, an ISMS is defined as consisting of set of "policies, procedures, guidelines, and associated resources and activities" that are managed by an organization with the goal to protect the assets that are related to information security [55]. The ISMS also represents a systematic approach in organizations that is undertaken for "establishing, implementing, operating, monitoring, reviewing, maintaining and improving" the information security of the organization with the perspective of achieving the set business goals [55]. In order to successfully implement an ISMS, the risk assessment and risk acceptance of an organization must be done [55]. A contributing factor to the success of an ISMS lies in the analysis of the requirements to protect the information security assets and implementing appropriate controls in the organization based on these requirements in order to keep the assets secure.

As mentioned previously in 2.2, the risks keep evolving due to new cyber-threats and changing values of information assets. By seeking the ISO 27001 certification, an organization must comply with the requirements of the standard among which are the need for a defined risk assessment process that defines the risk acceptance and the risk identification and analysis [56]. The ISMS should also include a risk treatment process that defines how the risks will be mitigating and treated [56]. Thus, it can be argued that an organization with an ISO 27001 certified ISMS in place is better aware of information security risks and knows how to treat them and maintains the risks assessment up to date to keep the certification. Moreover, the ISO/IEC 27001 standard is constantly evolving, with revisions occurring on three and five years cycle [34], to stay up to date with the continuously

evolving threats to information security, which makes organizations that follow the standard also up to date with these risks [31].

According to Higgins, ISO/IEC 27001 certifying the ISMS of an organization brings a great number of benefits, namely, it helps in ensuring that the ISMS is fit for purpose as it follows an internationally recognized standard [57]. Furthermore, in the standardization process risks related to information security shall be identified and their mitigation and management happens in a planned manner [56], [57]. Processes and procedures, in order to maintain and pursue information security, will also be defined with clear documentation and implemented in the policies and practices of the organization [56], [57]. In addition, when proceeding to the certification, an organization should also prove commitment to information security by implementing appropriate training of employees and clearly identifying roles and responsibilities with respect to information security [56], [57] which will automatically mitigate the threat represented by the organization's employees to information security. Finally, the certification serves as proof that the information has good information security practices in place, which brings value in the eyes of the customer [57].

3.2 Overview of ISO 27000 Series

The ISO/IEC 27001:2017 standard [56], as mentioned in the introduction, is part of the larger ISO/IEC 27000 standard family [55] that covers the entirety of information security and related Information Security Management Systems and which is developed by SC 27 of ISO/IEC JTC 1 for IT [58]. It is important to understand the connection of the different standards in this family to be able to certify an organization's ISMS according to ISO 27001 requirements. In fact, many of the standards in the family serve as guidelines for implementing and adopting the requirements defined in ISO 27001 and all the standards of the ISMS family are inter-related on some level, even when some are not yet published [55]. The categorization of the ISMS related standards, based on the four categories: vocabulary, general requirements, general guidelines and sector-specific guidelines, is visible in ***Figure 3*** .

As seen in ***Figure 3***, there is only one standard that covers the vocabulary which is the ISO/IEC 27000:2020 standard. It is crucial for organizations seeking ISO/IEC 27001

certification to study this standard as well so that they understand what the purpose of an ISMS and what connection there is between the different ISMS related standards. Furthermore, the standard defines all the vocabulary that needs to be understood when studying the ISO/IEC 27001 standard and related standards.

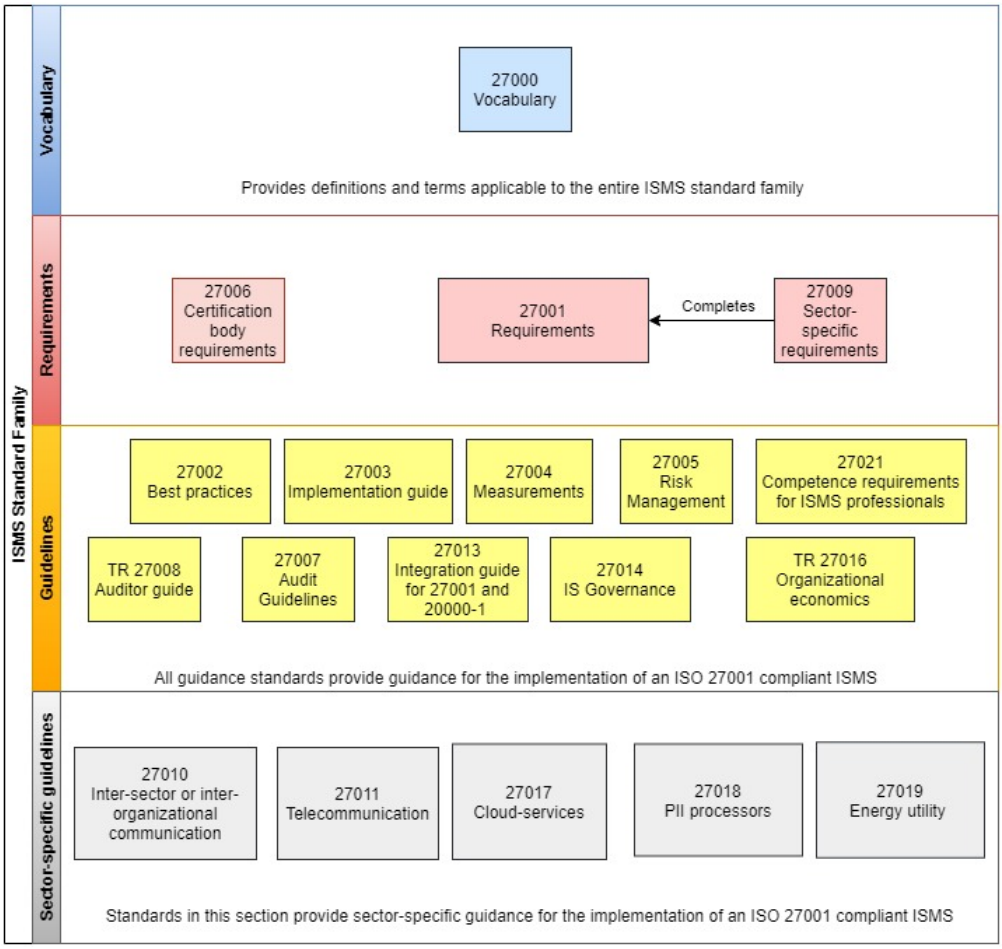

Figure 3. Structure of the ISMS standard family. [55]

When an organization seeks ISO 27001 certification, it is not possible to rely only on the specification standard nor the vocabulary standard. In fact, in the standardization process, the organization needs at least to get familiar with the code of practice documented in ISO/IEC 27002. This standard, as described in ISO/IEC 27000:2020, gives guidelines and best practices in the implementation of the security controls specified in ISO/IEC 27001:2017 [55]. The controls that are presented in the annex A for ISO/IEC 27001:2017 are aligned with the ones in ISO/IEC 27002 with the same numbering system and same objectives [59]. To achieve a successful implementation of their ISMS, an organization

needs to study both ISO 27001 and ISO 27002 to achieve proper control selection and implementation [34].

In addition, other standards of the family may be seen as useful on a case basis which makes it important for organizations to be aware of the different standards' purpose as many provide guidance that may help in complying with the ISO 27001 requirements. In ***Table* 1** the purpose and scope of the standard of ISO 27000 are defined. This table can provide guidance for the selection of standards that can help in the implementation of the ISO 27001 in an organization. ISO 27000, ISO 27001 and ISO 27002 are voluntarily left out of the table, as their purpose is defined in this section of the paper separately. With respect to the sector-specific standards, it was decided not to cover them all in the table but to focus on those which are specific to the software industry. Namely ISO/IEC 27017 for cloud services and ISO/IEC 27018 for Personally identifiable information (PII) processors in the cloud.

3.3 Implementation of ISO/IEC 27001

Being more familiar with the ISO 27000 standard family on ISMSs, in this section of the paper a process that can be followed for ISO/IEC certification based on literature is followed. Starting by studying literature on the general level of ISO/IEC 27001 implementation and then bring the focus on the point-of-view of SMEs, as this work's scope relies on the standard implementation in a software industry SME.

3.3.1 ISO/IEC 27001 certification process

Ganji et al. have conducted a literature review in 2019 on the approaches that have been made in literature to develop and implement the ISO/IEC 27001 standard in the ISMSs of organizations [60]. Based on the result of their review performed on 21 papers, most research were incomplete and had an average of only five requirements fulfilled out of twenty-two specified in the standard [60]. The analyzed studies spanned from 2005 to 2018 [60] and consequently covered different, and all, versions of the ISO/IEC 27001 standard. However, even with such an extensive timespan, no concept or methodology has been identified that clearly facilitates the work of organizations in designing, implementing or modifying their ISMS to comply with the ISO 27001 standard [60].

Table 1. ISMS standards and their purpose and scope. *[55]*

STD	PURPOSE AND SCOPE
27006	Defines the requirements that are needed for certification bodies to be accredited to give ISO/IEC 27001 certifications
27009	Defines sector-specific requirements additional to ISO/IEC 27001 requirements and ensures that there is no conflict between the requirements
27003	Standard to provide guidance on ISO/IEC 27001:2017 by providing guidelines for requirement implementation.
27004	Defines a framework that helps in the assessment of the effectiveness of ISMS following the ISO/IEC 27001 standard
27005	Provides guidelines for successful implementation of a process-oriented risk management with respect to ISO/IEC 27001
27007	Provides guidelines for performing internal or external audits related to ISMS with respect to ISO/IEC 27001
TR 27008	Provides guidelines for auditors that perform audits on information security control, is not intended to use as guidelines for performing audits on management systems
27013	Provides guidelines for organizations to integrate standards ISO/IEC 20000-1 and ISO/IEC 27001 when one of the two standards is already implemented in the management system or when the organization wants to implement both

STD	PURPOSE AND SCOPE
27014	Provides guidelines for governance of information security to ensure that an organization's security objectives are met
TR 27016	Provides an economical perspective in the assessment of the value of information security assets in an ISMS
27021	Defines the requirements for ISMS professionals that lead or are involved in the establishment, maintenance, and improvement of an ISMS in accordance with ISO/IEC 27001. Is intended mainly to demonstrate competence for professionals, to define needed competences when seeking an ISMS professional or for training and education
27017	Provides guidelines and additional controls that are specific to cloud services, intended to be used by service providers and customers
27018	Provides guidelines, controls and control objectives that are intended to protect PII with respect to ISO/IEC 29100 standard for public cloud environment

This difficulty in finding a universally working method for the implementation of the standard can be explained by the flexibility of the standard itself. In fact, ISO/IEC 27001 is a standard that is applicable to organizations of all sizes, types and nature [56]. Moreover, it

is not a prescriptive standard, and even though it specifies precise requirements for organizations to fulfill, it is up to the organization to determine the appropriate manner to meet a specific requirement based on their size, type and nature [1].

Even though there is no predefined clear and universal method for the ISO 27001 standardization, literature gives guidance on different things to consider and successfully implement the standard. Regarding the standardization process itself, one of the most important things to consider at the beginning of the process is the clear definition of the scope, which is closely related to the context of the organization. With respect to scoping and context establishment, Beckers et. Al. present a solution for establishing the context and identifying security assets of Cloud Computing companies [61] and based on the literature review by Ganji et. Al., the most covered criteria in literature about ISMS standardization were indeed the organizational context, the interested parties and determining the scope of the ISMS [60]. Establishing the context of the organization is one of the requirements of ISO 27001 as it helps in defining the external and internal factors influencing information security, the documented scope is a way to indicate to all interested parties, such as customers or employees, to what extend the ISMS is applied in the organization [1]. Furthermore, scoping is one of the nine keys to success defined by Calder in his book on the implementation of ISO 27001 [62]. The goal of scoping is to define the information assets of an organization by considering the business, the location, the used technology and overall environment of the organization; it is a crucial step as it is the first step in establishing what assets will need protection and which will be left out of the scope of the ISMS [62].

Based on the book mentioned above, Nine steps to success: an ISO 27001:2013 implementation overview, there are nine steps that are to be taken in order to achieve successful ISO 27001 certification [62]. First, in the project mandate step, it is crucial to get the support from top management [62], which is a clear requirement of the standard [56], setting up a budget and resources for the project and acquiring the needed competences for implementing the standard in the organization [62]. Support of top management must be acquired as it is a crucial step in order to get the needed support and commitment from all employees, if the top management is not sufficiently committed to make the project work and sets it as a low priority, it is likely that the certification will not be achieved [1]. In addition, top management is responsible for establishing a documented Information Security

policy which complies with the purpose of the organization and ensuring that related objectives are defined, documented and appropriate [56]. Acquiring the needed competences refers to hiring a consultant or training someone in understanding the ISO 27001 standard in depth in order to proceed to a gap analysis of current security practices in place in the organization [62]. Doing the gap analysis of the current security practices is useful in order to define a high-level plan on the entire project.

Once this high-level plan has been determined, the project initiation step can start in which roles and responsibilities are defined and in which the project plan is detailed [62]. It is important to keep the CEO involved throughout the process and consider having members of different departments of the organization as members of the steering group of the project, especially people more reluctant to change in order to achieve the intended outcome [62]. Good project planning and proper role assignation are part of the keys to success in the certification, as it will be ensured that everyone knows their responsibilities and are aware of what to expect from the project.

The third step defined in the book is the initiation of the ISMS and includes the definition of a process to approach the ISMS implementation. Continual improvement is key when thinking of processes to secure information, and consequently the approach to the implementation of the ISMS must follow a continual improvement approach such as COBIT Continual Improvement Life Cycle or the Plan-Do-Check-Act (PDCA) model [62]. This model used to be promoted directly by the standard [63] and is among the most used approaches when implementing management systems [62]. In this ISMS initiation phase, a process to create all the needed documentation for the ISMS is also suggested, as the documentation creation is the most time-consuming task to undertake in the implementation [62].

Then comes the step of setting the management framework for the implementation, in which the scope, which purpose was described at the beginning of this section, is defined, the information security objectives are refined and all internal and external issues are considered with respect to information security [62]. In this context, issues factors from the internal and external environment of the organization that could affect in some way the information security [64]. Understanding the needs and requirements of interested parties is mandatory,

as is the awareness of all internal and external issues; all these must indeed be considered in the definition of the ISMS scope based on clause 4 of ISO 27001 [56]. It is also required when scoping to consider all internal and external dependencies and interfaces related to information that are required in the business of the organization [56], [62].

The fifth step as defined by Calder, is in defining the baseline security criteria, meaning assessing currently used controls in the organization with respect to compliance requirements, contractual agreements, business goals, security objectives, etc [62]. A good way to approach this is, according to Calder, by building an inventory of all contracts and compliance requirements so that it can be assessed which controls are missing, if any, with respect to these requirements [62].

The sixth step and which is at the heart of an ISMS, is the risk management which begins with the definition of the risk-acceptance criteria of the organization [62]. The risk acceptance criteria (RAC), based on ISO 27005, can for instance be expressed as the ratio of benefit gained against the cost of the risk materializing, it can also be different for separate risk classes [65]. Then all risks to valuable information assets are identified alongside their vulnerabilities and the impact on information integrity, availability and confidentiality is estimated in case of successful exploit of a vulnerability by a threat [62]. Once the risks are assessed, the appropriate controls should be defined to treat these risks based on the prioritization of the risks; treatment options and controls should be defined by keeping in mind the RAC [62]. Many of the required documented information from the ISO 27001 are produced in activities related to risk management, meaning a documented methodology for assessing and treating risks, the risk assessment report, the Statement of Applicability (SoA) and the risk treatment plan [56].

The risk management process defined in ISO 27005 is illustrated in ***Figure 4***, this standard provides guidelines to implement a risk management process into the ISMS of an organization and it can be used to document risk assessment and treatment methodologies in an organization which will be ISO 27001 compliant. In fact, ISO 27001 requires the methodologies to be consistent, reproducible and repeatable [56]. The illustrated process is iterative, meaning that the scope of each iteration or risk management is defined separately instead of having to cover the entire ISMS scope each time a risk management is conducted.

Approaching the risk management iteratively helps in putting less time and effort into the risk management process while still assessing effectively high risks [65]. When the risk management iteration context is established, the risk assessment is done in which the risks are identified, analyzed and evaluated which results in the required risk assessment report, a report containing all relevant details on the assessed risk. If enough information is provided in order to determine the risk treatment options at the end of the assessment, risk treatment options can be chosen [65].

In the risk treatment phase, illustrated on ***Figure 5***, it is decided whether the risk is retained, modified, avoided or shared and when modified appropriate controls are defined to mitigate the risks [65]. As an outcome, the risk treatment produces the Statement of Applicability (SoA), where the applicability of the controls in Annex A of ISO 27001 are documented alongside the justification for their inclusion or exclusion and the status of implementation [56]. Once all controls are defined, if they are not yet implemented, they are included in the risks treatment plan in which the schedule and responsibilities for treating the risks are defined.

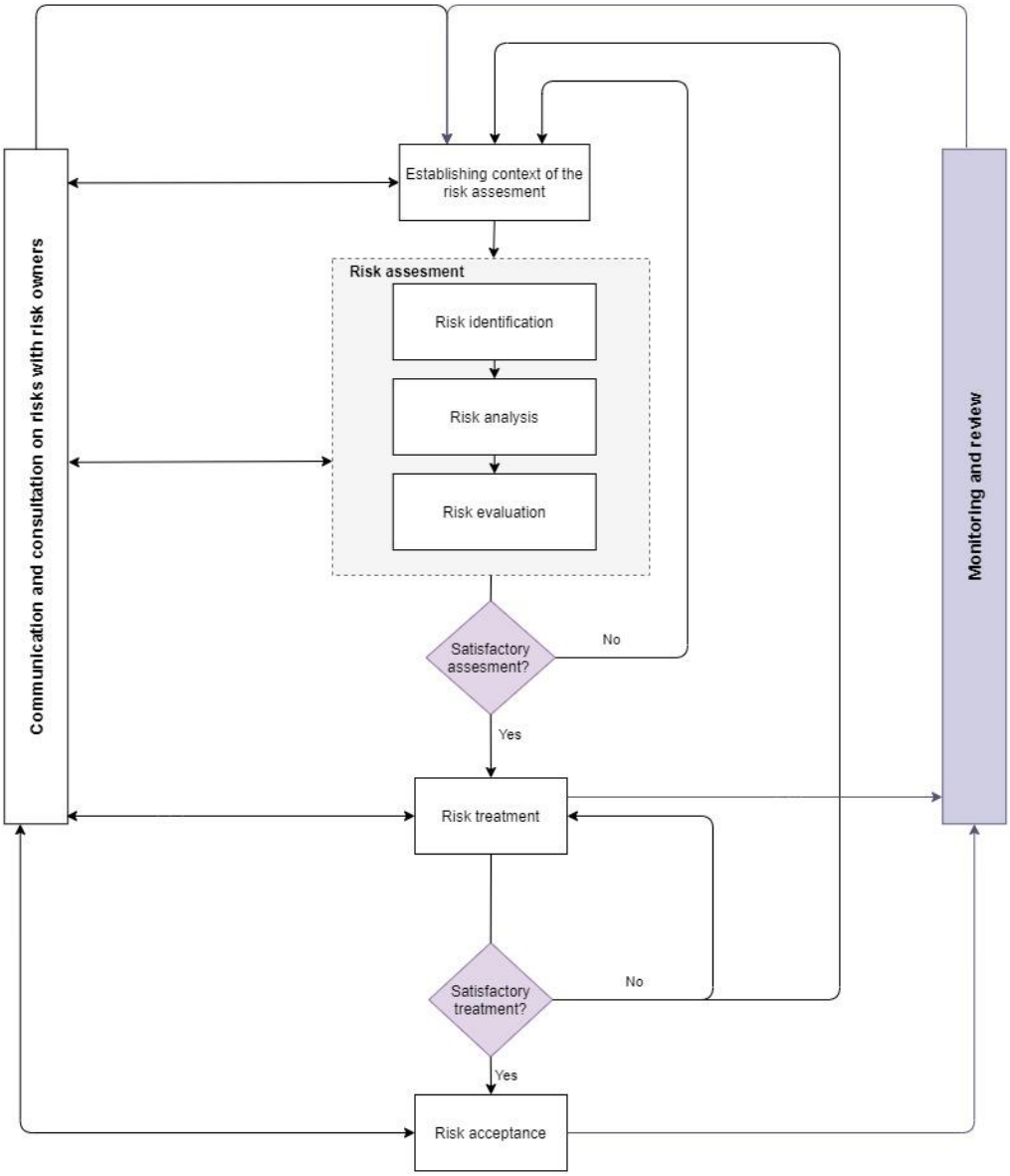

Figure 4. Risk management process based on ISO 27005 *[65]*

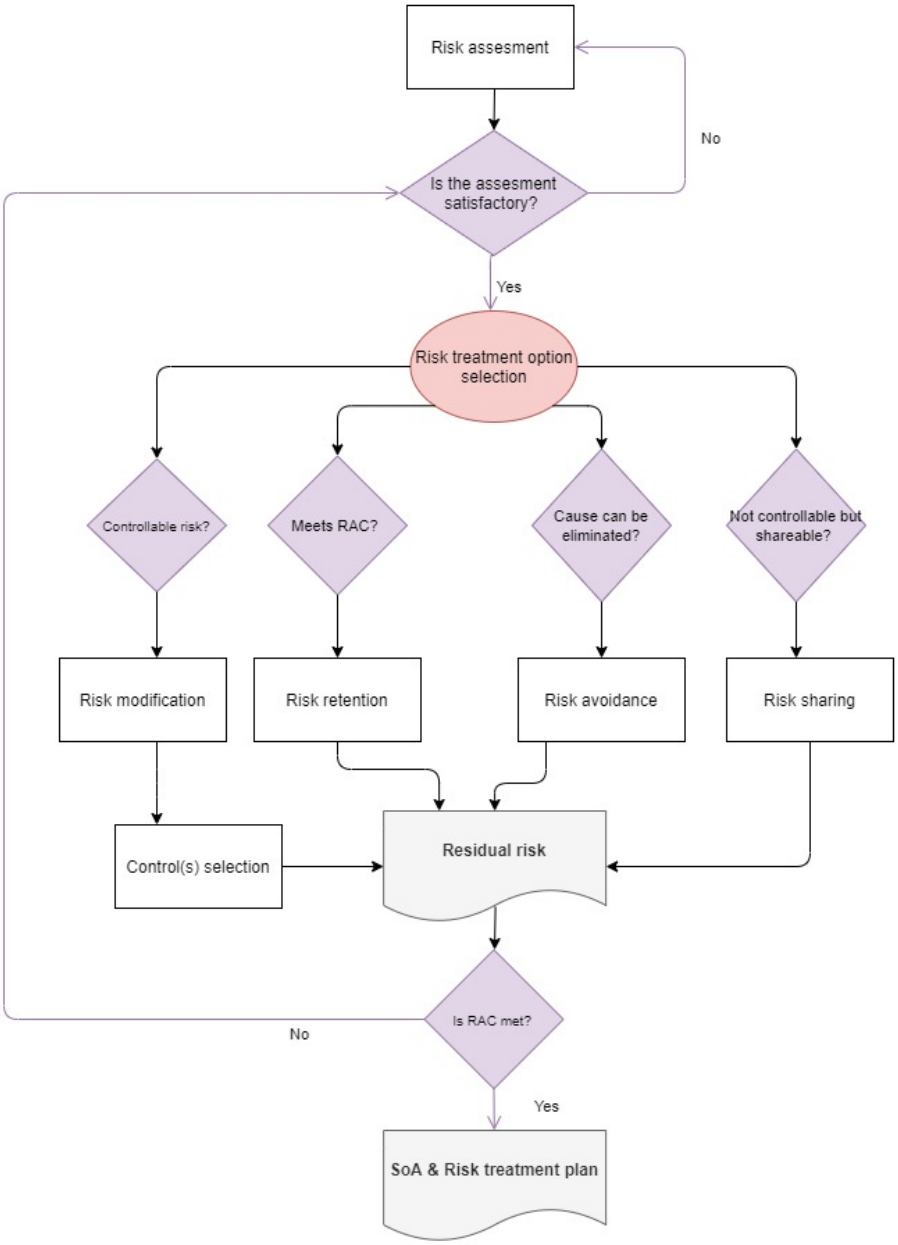

Figure 5. Risk treatment option selection *[65]*

The seventh step defined by Calder is the implementation, which means the implementation of all the work that has been done until now with document creation and assessments. For instance, risk treatment plans produced in the risk management phase are implemented and competences required for ISMS are acquired if they are missing [62].

As mentioned in a previous paragraph of this section, the ISO 27001 relies on an ISMS implementation approach that promotes continual improvement. As such, the eighth step to

success lies in the testing of the ISMS [62]. Testing of the ISMS includes definition of measurement and monitoring methods that define what, how and when things will be monitored, measured, analyzed, and evaluated [56], [62]. Testing also relies on proceeding to internal audits and management reviews to ensure that the ISMS is effective, appropriate and efficient [56]. Based on ISO 27001 and the guidelines in ISO 27003, the management review and audit processes are not required to be documented, but outcomes of the processes are required to be documented [56], [64]. In fact, the audit reports need to be reviewed and management review report need to be done to prove that, inter alia, changes in internal and external issues are considered alongside results from audit or monitoring and measurement activities [64].

Finally, the last step for ISO 27001 certification defined by Calder is the certification itself, meaning, first, the selection of a certification body that, preferably, is appropriate for the field the organization has business in [62]. To ensure successful certification, the organization should ensure that the required documentation is complete, comprehensive and available for auditors and that all employees of the organization are properly aware and implement correctly defined information security practices [62]. In addition, it is important to have conducted at least an iteration of audit and management review to be able to prove that the processes are known and that the organization is able to implement them in practice [63]. ***Table 2*** defines in a detailed manner the activities that must be taken in a PDCA approach to the ISMS implementation, based on the steps and descriptions defined by Calder.

3.3.2 ISO/IEC certification in an SME

In 2009, Valdevit et al., in their research project for developing an ISMS implementation guide for SMEs, identified how the ISO/IEC 27001 standard could be best adapted to the needs of an SME regarding their ISMS [66]. The objectives for the guide were identified by going through the certification process in an existing SME in Luxembourg from June 2006 to May 2008 and by identifying the issues that came during the experimentation [66]. Consequently, they identified six objectives for their guide including the downsizing of the requirements specified in ISO/IEC 27001 to meet with available resources in SMEs and providing tools for the implementation of the standard with tools for documentation and

templates [66]. The outcome results in scaling down the requirements to 32 major activities that were split into 5 separate set of activities to achieve the outcome progressively [66]. In their guide, they provide solutions for better understandability of the standard with clear examples for the structure of the processes required by the standard which include the name for the process, a description, the detailed steps of the process, the inputs, outputs and every stakeholder involved in the process [66]. The use of numerous templates and tools in the implementation of the ISMS in an SME is justified by downsizing the need for human resources. Their guide was assessed by experts in charge of IT standardization activities in Luxembourg [66].

Table 2. Phases in PDCA for ISO 27001 certification. [63]

	Description
Plan	a) Definition of the ISMS scope b) Definition of the IS policy & Objectives c) Definition of a risk management process d) Conduct risk management process e) Create SoA & risk treatment plan
Do	a) Implement risk treatment plan b) Implement training and awareness programmes for employees c) Manage operations and resources as defined in the ISMS d) Implement measurement & monitoring activities
Check	Test, audit and review the ISMS for appropriateness and effectiveness.
Act	Implement Continuous Improvement (CI) actions on the ISMS as defined after testing, auditing and reviewing.

Later, in 2010, Valdevit & Mayer developed a tool to provide a method for SMEs to perform more efficient gap analysis, which is a required step when an organization seeks ISO 27001 certification [67]. Their research was motivated by the successful certification they reached

for an SME in Luxembourg in 2008 [66], process which was documented in the paper of the previous paragraph. In their research, they noted the redundancy of some requirements in the standard and thus decided that this redundancy should be removed as a first step in the gap analysis [67]. After that, the suggestion is to categorize the requirements and controls based on, for instance, the roles that are related to different requirements instead of going through every requirement in order and one by one [67]. Finally, when asking questions to different roles identified in the previous phase, it is important to make simple questions to find the gaps, as not everyone is an ISMS specialist in the organization [67]. Proceeding in such a manner in SMEs has proven, based on their experiments, to be a more efficient manner to approach the gap-analysis [67].

Based on these papers, implemented an ISMS in an SME can be resource-consuming if not planned correctly and if proper tools are not taken into use. Consequently, it is important to start the ISO 27001 standardization process by getting familiar with the standard and defining steps that will be undertaken in order to achieve certification. A first step being the grouping of the ISO 27001 requirements to remove redundancy and to proceed smoothly to the following steps. After that, it is crucial to identify current gaps of the ISMS in place in an organization with respect to the previously grouped requirements. When all gaps are identified, corrective actions should be implemented. **Figure *6*** illustrates a PDCA approach derived from this part of literature and the previous subsection 3.3.1, the fixes to documentation such as information security policy or risk management methodologies is dependent on the gap analysis and are not required if there are no gaps. However, a new risk management iteration needs always to be conducted to ensure that new risks are also considered. The implementation actions of implementing risk treatment and measurement & monitoring activities can be done simultaneously and once changes are implemented the concerned employees need to be made aware of the changes and trained if necessary. Checking happens as defined in the ISMS when the different activities and procedures are implemented and when a management review is completed, the ISMS is improved if necessary.

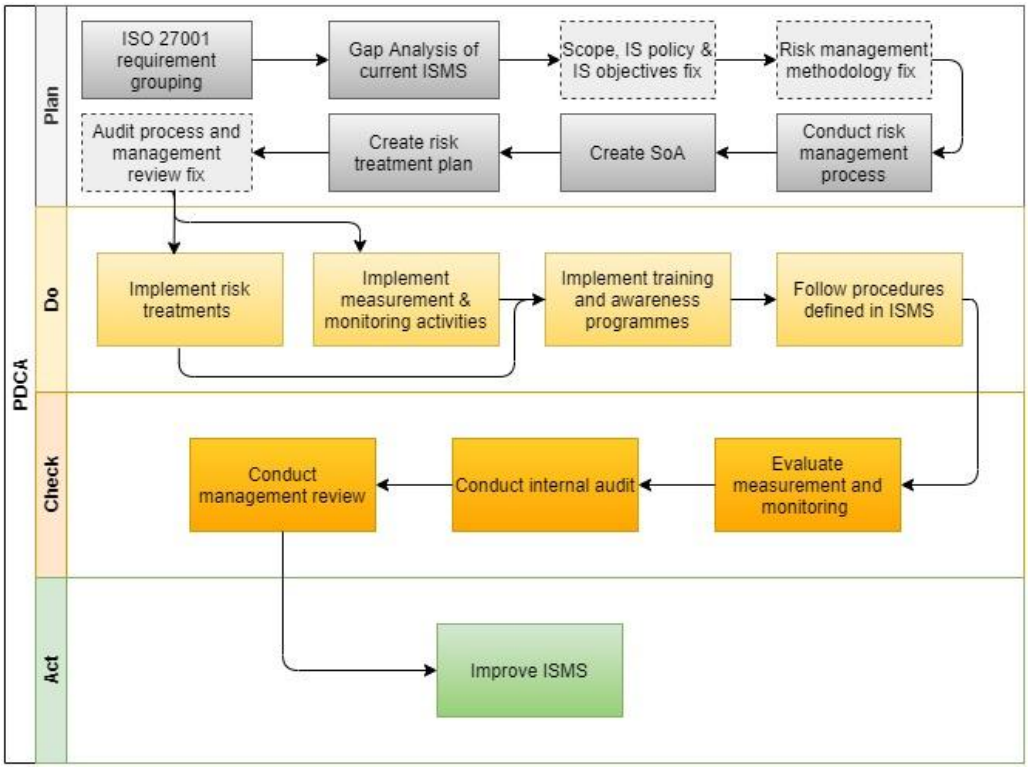

Figure 6. PDCA for ISO 27001 standardizing an existing ISMS

4 ISO 27001 STANDARDIZATION OF AN EXISTING ISMS IN A CASE COMPANY

In this section, the goal is to better understand the context in which the case company operates in and what motivates them to standardize their ISMS. Then, a methodology is defined based on the literature discussed in 3.3 that is followed in the ISO 27001 standardization of the ISMS of this case company. Finally, the implementation of the methodology in practice is documented.

4.1 The case company

The case company in which this ISMS standardization process is conducted is an SME operating in the software industry field, as mentioned earlier in the paper. They operate in an exclusively B2B environment where they develop software only for other businesses operating in a same field. This field is highly competitive and requires confidence in how the information they provide to the case organization is processed. In fact, it must be proven that the information is processed safely and that their competitors may not gain access to sensitive information on their processes and methods. Consequently, it can be stressed that the main motivator for this case company in seeking to standardize their ISMS with respect to ISO 27001 requirements relies in the coercive isomorphism induced by customers, as the main goal is to prove to the customers that they can be confident that the information they provide to the case company is processed securely.

In addition to this coercive isomorphism, by ISO 27001 standardizing, the company will ensure that it has a globally recognized certificate for its ISMS which will prove externally that good practices and processes are in place with respect to information security. Another important factor that makes the ISMS standardization important in this case is its high vulnerability to become a target to cyberattacks due to it developing web applications and being a small business, which category has been found to be more vulnerable to cyberattacks in section 2.1. By standardizing their ISMS, they would not only build better confidence in their Information Security Management, but they would also ensure that they have processes and activities in place to mitigate or to avoid risks that could cause severe information breaches and subsequently irreversible consequences for the company.

Most of the employees of the company work in the software production team, and as the information security is sought to be standardized especially in the developed software products to secure customer's information, the major focus in the standardization will rely in getting the ISMS efficient from the software development point-of-view and enforcing the importance of good practices in development for software developers. However, as it is an SME and all processes are related on some level, the standardization needs to cover the entire organization to implement good and standardized activities in all information management of the organization. In fact, customer information is not handled only in development but also in sales, so every employee and department are concerned by the ISMS standardization.

4.2 Planning the ISO 27001 standardization in the case Company

The approach to the standardization of the existing ISMS in the case company considers the related literature documented in the previous parts of this paper, especially the research by Valdevit et al. on their successful ISO 27001 certification in an SME in Luxembourg. Thus, the first step of the planning for the implementation relies on the grouping of the requirements defined in the standard. This grouping helps in familiarization with all the clauses more fully and to proceed to the implementation in a more efficient manner than proceeding in the order that the clauses are documented in the standard.

Once all the requirements are grouped, a spreadsheet is done in which every category identified during the grouping is documented. Each of these categories has the related clauses of the standard and the requirement that must be met on the rows below the category name. A part of this spreadsheet is visible as an example in ***Figure 7***. This Spreadsheet is used in identifying the gaps that exist in an existing ISMS against the requirements of the ISO 27001 standard. This comparison is a gap analysis, where the goal is to check at what level an existing system is against a specified objective. The tool is built in such a way that it could be used later and easily edited, so that during different internal or external audits, the auditor could see from there directly where all specific documentation is, when applicable. Moreover, as mentioned previously, continual improvement is crucial within an ISMS due to changing internal and external factors influencing the information security. Consequently, it is important when standardizing and acquiring tools to consider solutions that will help in the future maintenance of the management system.

Therefore, in addition to the related clause of the standard and the requirement itself, the gap analysis tool has a column to specify the link or path to the associated document or documents of a requirement. The tool also has a column for documenting the identified gaps and a column for other notes that is meant, for instance, to document already existing elements in the ISMS that could be used to fix the gaps. The most important columns in the spreadsheet, in addition to the requirements themselves, are, however, the status of the implementation and the level of documentation.

The status of implementation of the requirement is defined in the status column in the table and is set as one of the five values below:

1. **Needs to be checked**: when it has not yet been assessed if the requirement is met or not
2. **Not yet implemented**: when the requirement is not implemented at any level in the ISMS currently
3. **Implemented but not entirely**: when the requirement is implemented but there are some gaps
4. **Implemented and complete**: when the requirement is fully implemented in the current ISMS
5. **Implemented and room for improvement, not mandatory**: when the requirement is fully implemented but that some minor changes could be made for more clarity for example

As for the level of documentation, it is defined in the column Document/record availability and is set on one of the six levels below:

1. **Not yet checked**: when the documentation for this requirement has not been checked yet
2. **Completely documented**: when the documentation related to this requirement is complete
3. **Not documented but needed**: when there is no available documentation but that the documentation is required by the standard
4. **Documented but not entirely**: when there is documentation that needs fixes with respect to the requirement
5. **Not mandatory**: when documentation is not required by the standard
6. **Room for improvement, not mandatory**: when some documentation could be added or updated for more clarity in the future during the auditing of the ISMS

	A	B	C	D	E	F	G
1	Related standard clause	Requirement	Status	Document/ Record availability	Associated document(s)	Identified gaps	Other notes
2	Scope and context of the Organization						
3	4.1	Are all external issues identified?	Needs to be checked	Not yet checked			
4	4.1	Are all internal issues identified?	Needs to be checked	Not yet checked			
5	4.2	Are all parties that can be affected or affect organization decisions identified?	Needs to be checked	Not yet checked			
6	4.2	Are requirement of all these parties identified?	Needs to be checked	Not yet checked			
7	4.3	Is the ISMS' scope clearly defined ?	Needs to be checked	Not yet checked			
8	4.3	Are the internal and external interfaces and dependencies identified?	Needs to be checked	Not yet checked			
9	Information security policy						
10	5.1	Is the policy compatible with strategic direction of the organization?	Needs to be checked	Not yet checked			
11	5.2	Is the policy appropriate for the purpose of the organization?	Needs to be checked	Not yet checked			
12	5.2	Is information on or a framework provided for IS objectives?	Needs to be checked	Not yet checked			
13	5.2	Is there commitment from management for CI? (i.e. statement)	Needs to be checked	Not yet checked			
14	5.2	Is there commitment from management to satisfy applicable IS requirements?	Needs to be checked	Not yet checked			
15	5.2	Is it available to all interested parties?	Needs to be checked	Not yet checked			
16	5.2	Is it easily understandable by all employees? (language and format)	Needs to be checked	Not yet checked			
17	Information security objectives						
18	6.2	Are the objectives consistent with security policy?	Needs to be checked	Not yet checked			
19	6.2	Are the objectives measurable? (are the objectives verifiable)	Needs to be checked	Not yet checked			
20	6.2	Are the objectives communicated?	Needs to be checked	Not yet checked			
21	6.2	Are there updates on the objectives when needed?	Needs to be checked	Not yet checked			
22	6.2	Is there a connection to applicable IS requirement and results from risk	Needs to be checked	Not yet checked			
23	6.2	Is there a defined plan in order to achieve the requirements? (what will be done, required resources, responsibles, completion date, how results will be evaluated)	Needs to be checked	Not yet checked			
24	5.1	Do the objectives meet with strategic direction of organization? (management	Needs to be checked	Not yet checked			
25	Resources						
26	7.1	Are all resources determined to establish, implement, maintain and continuously improve ISMS?	Needs to be checked	Not yet checked			

Figure 7. Gap analysis tool for ISO 27001 requirements.

The following step in the planning, after identifying all the gaps in the existing ISMS, is to define a clear plan to address these gaps. When proceeding to set a priority for the different gaps that need to be addressed, it is crucial to think of how the different documents and processes are inter-related. For instance, as it was seen in 3.3.1, establishing a proper scope for the ISMS is essential in the planning phase. Hence, if the scope is found as having gaps it is crucial to start by fixing the gaps in this before proceeding to address the other gaps. An approach to the prioritization technique to address all the gaps in an appropriate order relies in comparing the gaps with the different steps of the ISO 27001 implementation using the PDCA approach documented in ***Table*** . Based on this, the proposed order in which to address potential gaps is by following the phases that are followed when implementing an ISO 27001 standardized ISMS. This defined order for fixing the gaps is shown in ***Figure 8***. The goal is to take each ISO 27001 requirement category defined in the first stage of this process, and if gaps have been identified, the gaps are fixed before addressing the potential gaps in the following category.

All the categories are inter-dependent and takes as an input outputs from the previous categories which makes it crucial to proceed to gap fixing in the specified order, unless not doing so is well justified. If the order of the categories for fixing the gaps is not followed without a good justification, the entire standardization will be delayed or compromised. In fact, it was seen in 3.3 that good planning is crucial for successful standardization, and not proceeding to the plan will induce delays or even higher resource-use and a chain a chain-effect where a non-fixed gap in one of the categories leads to more gaps in the following categories.

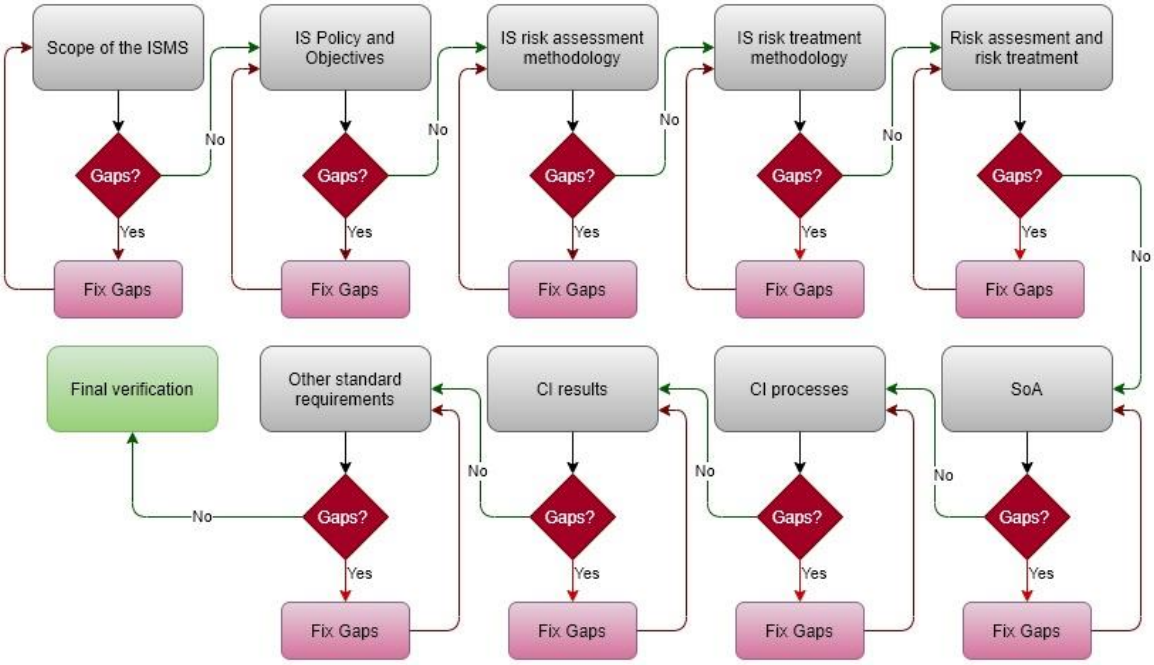

Figure 8. Gap fix priority.

An example of a chain-effect is illustrated on ***Figure 9***, which is derived from the literature reviewed in previous sections**Error! Reference source not found.** It starts with not p roperly determined information asset in the scoping phase, which has been identified as a challenge, leading to issues in information security objectives and risks assessments. As the risk assessment is not complete in this scenario due to issues in the scope, a risk that was overlooked materializes as the associated risk did not have any treatment. Depending on the severity of the risk, the outcome could result in loss of reputation, time or finances when dealing with the consequences. As such, this type of situation needs to be avoided which makes it crucial to follow appropriately the plan for standardizing the ISMS of the company.

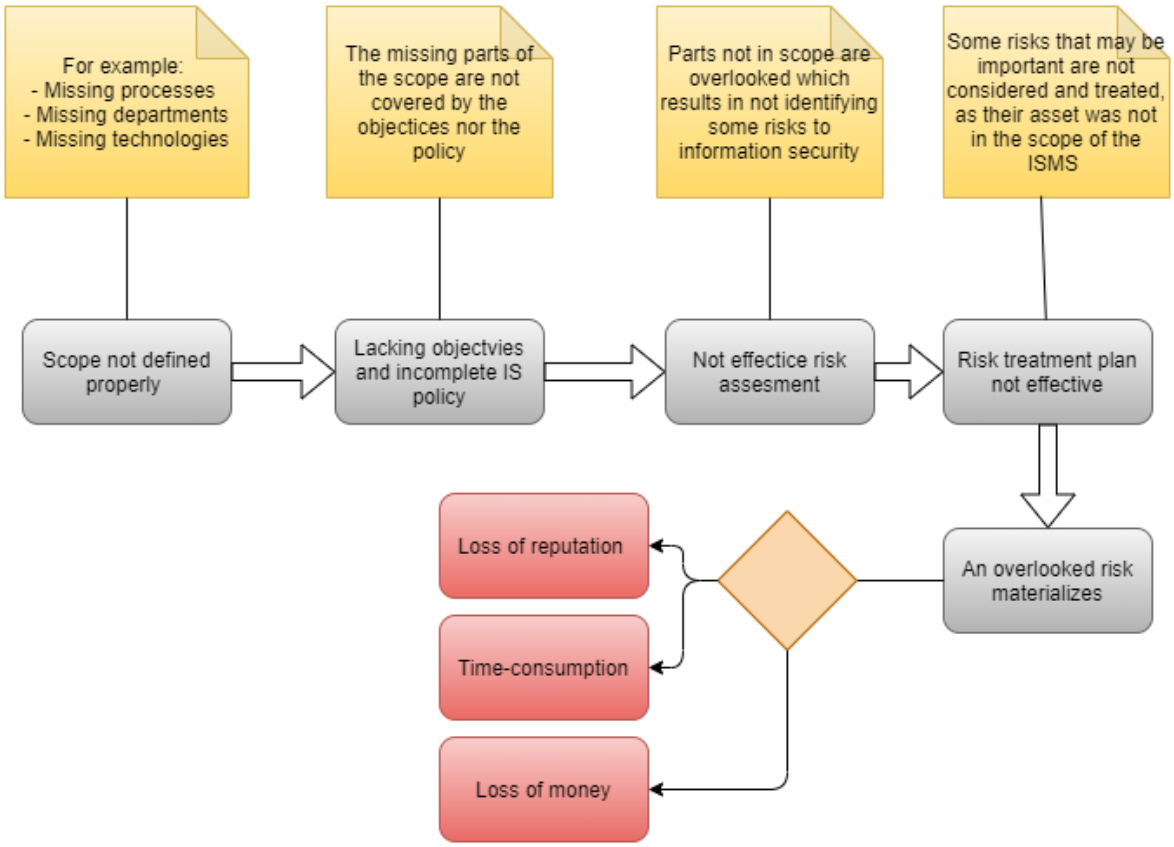

Figure 9. Chain-effect example when not following implementation plan

4.3 Implementation of the ISO 27001 standardization plan

The gap analysis described in the beginning of 4.2 was conducted in the case organization to define what was missing from the current ISMS and what needed updates. As a result, it was found that most documented information was available on some level, except from the Statement of Applicability which is specific to the ISO 27001 standard. However, gaps were identified in many documents and the documentation was not organized in the most appropriate way with respect to availability of documentation, and consistency of documentation was lacking which could have impacted the maintenance of the documentation.

To fix the found gaps, a meeting was held in which the author of this thesis, the Chief Information Security Officer (CISO) and the production manager got through the gaps and decided in which order to proceed and defined roles for the fixes on a general level. For the meeting to be more efficient, it was preceded with a grouping of the identified gaps based on the mandatory documents of ISO 27001. In each document category, the already existing

elements were also documented which helped in having a more global view of the state of implementation. In addition to documentation gaps, the ones in the required processes were also considered alongside the elements that are already existing in the organization's ISMS. As all gaps were clearly documented based on the requirement they rely on, defining the priority in which the gaps would be fixed was easier. After that, it was decided to fix the gaps in the order presented on ***Figure 3***, except for the information security policy as the changes to make it in were only minor and did not involve any new clauses in the policy that could have impacted following parts of the ISMS.

Consequently, the fixes started with the context of the organization and the scope of the ISMS. It was found that even though the existing ISMS's scope was documented on some level, it was not defined in the amount of details required by the standard and for the maintenance of the ISMS it was seen as more appropriate to make a new document entirely from start to ensure that all important areas were considered in the following steps of the standardization and that what needed to be left out was indeed left out. Based on ISO 27001, the context needs to be documented only at the extent seen appropriate by the organization and is not mandatory [56]. For maintainability and better understanding of the scope, it was decided to document all internal and external issues influencing information in security so that during CI activities it could be easily determined which were the considered issues and assess their appropriateness and up-to-dateness.

Contrarily to what was found in literature of section 2.3, it was not found as challenging to define the scope of the ISMS as the context of the organization was clearly known by the CISO and production manager, which made the process of defining precisely every external and internal issues that could influence the efficiency and effectiveness of the ISMS easier. In addition to that, the CEO's feedback on the scope was also acquired to ensure that the scope met the purpose of the organization, as required by ISO 27001.

Alongside scoping, an information asset inventory was also created in which all assets containing information used by the organization were documented. Each asset was associated with a unique ID and categorized based on its sensitivity and its access rights. Setting up this inventory in this early stage, even though it is a requirement only from controls in Annex A of ISO 27001 [56], helped in the step of risk identification and facing

and overcoming early-on challenges in identifying the valuable assets in the organization, which was found to be challenging in [19], [47] & [50]. However, the creation of this asset inventory was not straightforward and defining all the information assets that are valuable for the organization was indeed challenging as a variety of information systems are in use and it was especially difficult to find on what level to define the assets in order to keep the inventory understandable and maintainable. This issue was solved by eliciting all information connected to a product, service or system included in the ISMS scope and determining whether the information container could be considered as an individual asset or not.

The risk assessment was conducted after small improvements were made to the existing risk assessment process, to make it ISO 27001 compliant, meaning producing reproducible, consistent, and repeatable results [56]. The process was started by creating a risk assessment spreadsheet of which the different columns are illustrated in ***Figure 10*** & ***Figure 11***. The risk probability and severity are defined quantitatively using a scale predefined for the purpose of the organization and the risk level is defined as the product of these two values. This spreadsheet was filled by adding the already identified risks from existing risk management iterations reports, which were part of the already implemented ISMS, and adding new ones based on literature of paragraph 2.2 and the asset inventory that was created earlier. The decision to include all previously identified risks was made as the previous risk management iteration were old and the risks needed to be re-assessed due to changes in processes. In the documentation of the risk management process, the links to CWE's most dangerous programming errors [68], OWASP's top ten security risk [43] and Verizon's data breach reports [38] were provided and monitoring their change was added in things to monitor and measure. In this way, it was ensured that reviewing risks evolvement in the organization was considered, as it was found as challenging in [50] & [54].

As it was seen in 2.2.1, human-induced risks to information security are the most common risks as they arise from various sources such as lack of awareness of employees, their carelessness, or malicious actors. Most of the human factors applicable to the case company were already identified in previous risk management iterations of the organization, but some were still added, or the existing ones were described in more details in order to ease the analysis and evaluation processes and subsequently the selection of treatment options.

Regarding technically induced risks, literature from 2.2.2 was used to assess what type of vulnerabilities could exist in the software developed in the organization and in the development process itself. Mainly OWASP and CWE were used in this part of the risk assessment and once the existing vulnerabilities were identified they were added to the risk assessment spreadsheet.

A	B	C	D	E
Target	Asset ID & Name	Vulnerability	Threat	Risk description (Consequences)

Figure 10. Part 1/2 or risk assessment spreadsheet columns

F	G	H	I	J	K	L	M	N	O
Probability	Severity	Risk level	Risk treatment option	Current control(s)	Planned control(s)	Control implementation date	Probability after treatm	Severity after treatment	Risk level after treatment

Figure 11. Part 2/2 or risk assessment spreadsheet columns

When the risks related to the information assets of the organization were identified, the same team that worked on the scheduling of fixing the found gaps proceeded to the risk analysis and evaluation. Each risk was evaluated based on its probability and severity, then the risk treatment option was chosen, and the risk re-evaluated based on the selected treatment option, to ensure that the RAC was met. The entire risk management process followed closely the guidelines in ISO 27005 of the ISO 27000 standard family, which, as specified in 3.2, gives guidance for implementing a process-oriented risk management process and for selecting appropriate risk treatment options.

Once the entire risk management iteration was conducted, the risk treatment controls, existing and planned, were compared with the controls in Annex A in order to create the SoA document. The SoA was made using a spreadsheet in which all controls from Annex A are documented and it is defined whether or not they are applicable, the justification for implementation or non-implementation, the current state of the control's implementation, date of assessment and the date of the planned implementation and the date of the actual implementation; ***Figure 12*** illustrates the structure of the SoA document. The ISO 27002 standard, which provides guidance in implementing controls, was useful in determining on what level the already existing controls were implemented and how to implement missing

but needed controls. In fact, the names of the controls that are listed in Annex A do not give enough details on what needs to be done which endorses what Calder stresses in [34], that at least ISO 27002 and ISO 27001 needed to be acquired in order to meet the standard requirements. Creating the SoA was a time-consuming task, which can be explained by the lack of experience of working with the standard and knowledge of the different controls by the ISO 27001 project team, which was an identified challenge in 2.3. as it required the team to check multiple times for the implementation guidance in ISO 27002. However, going individually through the different controls and their guidelines helped in finding omissions and means in which to improve already existing controls and their documentation, when applicable.

Control	Control description	Applicability	Justification	Current state	How control is applied and/or will be	Last assessed	Planned implementation (if applicable)	Full implementation date
A.5 Information security policies								
A.5.1 Management direction for information security								
Policies for information security	A5.1.1 A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant parties	Applicable		Implemented				
Review of the policies for information security	A.5.1.2 The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness	Applicable		Implemented				
A.6 Organization of information security								
A.6.1 Internal Organization								
Information security roles and responsibilities	A.6.1.1 All information security responsibilities shall be defined and allocated	Applicable		Implemented				

Figure 12. Statement of Applicability structure

When the SoA was complete and it was ensured that no omissions were made, it was used in a subsequent meeting to produce the risk treatment plan with the organization's CISO in which the responsibilities and timelines to implement all the needed but not yet implemented controls were defined alongside precise description of things to do. Only a few controls that were found to be applicable were not implemented at all. However, as ISO 27001 standardization relies on continual improvement, it was decided to check every control implementation when in doubt of its compliance which resulted in a risk treatment plan that spans until the following year in order to have enough resources for control implementation while ensuring the business continuity. In fact, as the members of the steering group of the ISO 27001 project in this case SME were also responsible of other tasks of high importance in the organization, at times resources to implement controls were low and the only way to overcome this without impacting business continuity was by expanding the risk treatment schedule.

The risk treatment plan contained mainly documentation updates for maintainability purposes and for continuous improvement. In order to avoid issues mentioned in 2.3 with

the documentation, namely the lack of consistency due to multiple people revisioning the documents at different time and places, it was decided to include a version control table to every document where the made modifications, the dates and the author are logged. To overcome this same issue, it was decided to include instructions to most templates so that, in addition to future training session on the documentation use, employees would be able to find quickly the instructions to the use of the templates which would enhance the consistency of these documents as well. For the same reasons of maintainability and continuous improvement, it was decided to create clear and more detailed documentation and policies for the company on some practices that were already in place in the organization, for instance regarding password management or mobile devices. In that way, it is ensured that there is available and detailed information on the means to maintain a high level of security in the information assets of the company. To ensure that employees are aware of the policies and practices related to information security, and as the lack of enforcement was identified as a challenge in 2.3, it was decided to conduct a training at least once a year and to measure the awareness by surveying the employees after each session.

With respect to maintainability and continuous improvement of the ISMS, measurement and monitoring activities were defined based on the identified risks and their treatment options and the information security objectives of the organization. All the measurement and monitoring activities determined for the ISMS of the case company were documented in a spreadsheet with the parameter being measured such as access rights or breach reports and the objective set for this parameter. Each parameter is also associated with a measurement or monitoring periodicity and an evaluation periodicity, alongside the needed resources, responsibilities and methods for conducting these activities. In that way, it is ensured that it is known how, when and by whom the activities are conducted as required by the standard. In addition to the monitoring and measurement activities, the existing audit process for the case company's ISMS was revised to be more appropriate with the other updated parts of the ISMS. As the lack of requirement for documentation has been identified as a challenge in 2.3, it was decided to create templates to fill for the audit initiation and reporting the outcomes so that all these documents remain consistent. A management review process was also written to review the effectiveness, efficiency, and appropriateness of the ISMS on a regular basis and to find opportunities for improvement.

5 DISCUSSION AND CONCLUSIONS

As stated in this thesis, the goals of this paper were to find the steps to undertake for an existing ISMS to get ISO 27001 standardized, to identify the challenges that may arise during the standardization process and finally to make corrective actions to the existing ISMS in a case company based on these findings. Identifying the steps to undertake has been done by conducting a literature review focusing on guidance for ISO 27001 certification and the ISO 27000 standard family. Based on this literature, it was decided to follow the PDCA approach in the implementation and start the planning by getting familiar with the ISO 27001 standard and proceeding to grouping the requirements in order to proceed to the gap analysis of the existing ISMS which was a crucial step to identify what processes and activities were already in place in the organization. The challenges were also identified based on previous experience of standardization implementation documented in existing work and considered throughout the standardization process.

A notable challenge that has been identified by scholars is the lack of knowledge and experience in ISO 27001 standardization. This challenge also materialized in the case company as the standard was unknown to the team working on the project and it required a lot of time to get familiar enough with the standard and the entire ISO 27000 family. However, starting the implementation by proceeding to the grouping of the requirements as defined in the methodology in 4.2 proved itself useful as it helped in getting familiar with all the requirements of ISO 27001 and to find clearly what needed to be done. In addition, using different standards of the family as guidelines helped in defining more clearly what needed to be done and in understanding ISO 27001, which was identified as a challenge in 2.3. The standards that were used, in addition to ISO 27001, were ISO 27000 to understand the vocabulary, ISO 27003 to understand what could be done to meet the requirements, ISO 27002 to understand how to implement controls from Annex A, ISO 27005 to determine how to implement a risk management plan that complies with ISO 27001 and finally ISO 27004 to define things to measure, monitor, evaluate and how to do it. A suggestion for companies that seek the certification and to consequently standardize their ISMS is to really get familiar with all the standards from ISO 27000 that could be useful for them, based on their own experience, knowledge and need.

Another challenge that arose significantly in literature is the difficulty in identifying the valuable information assets. This also occurred in the case company but was well managed by mapping together the information systems identified in the scope and finding related documents or systems. What really helped in overcoming this challenge was the appropriate documentation of the scope where external factors, internal factors and interfaces were documented and consequently it was ensured that everything was considered when proceeding to produce documentation for the ISMS.

Another important challenge that has been identified by scholars is the lack of consistency in the documentation, and this was seen as well in the case company. The existing ISMS was hard to maintain and update due to different people having been part of the initial process with low documentation on some choices that were made. It is important to keep in mind, when creating documentation for an ISMS, to keep it easily maintainable in order to avoid over-use of resources later on and most of all to keep the ISMS usable after potential changes occur in employees or roles in the company. This maintainability can be achieved by version control, for instance, and in the case of processes by documenting them and adding to places that are easily accessible by the people who need the information and are authorized to access it. In addition, the lack of consistency can be treated by setting clear requirements and guidelines for documentation, for instance by creating templates for reports, which was done in the case company. For these requirements and guidelines to be followed, it is important to make all employees of the organization who update these documents aware of the changes and train them in their practical implementation. Including clear instructions in templates for their use is also a good way to tackle problems of document consistency as clear guidelines would be defined.

It was not in the scope of this thesis to get the ISO 27001 certification process started and at the time of writing this conclusion the entire risk treatment plan was not yet implemented in the case company. Neither were the testing activities conducted, namely measurement and monitoring, audit and management review. Consequently, there may come some other changes to the updated ISMS based on these testing activities and the certification audit and some new challenges may occur. Thus, in the future steps of the ISO 27001 standardization process it would be interesting to give special attention to some challenges that were identified in literature, especially the reluctance to change from employees, as currently no

new training session were organized and the few procedural changes that were made were not yet completely communicated to other employees as they were not fully implemented.

6 SUMMARY

In this thesis, it was seen that standardizing an ISMS is important for different reasons going from competitive advantage for a company to a legal requirement. The heart of an ISMS is the risk management, and it was seen that threats to information security can come from the entire environment of the company which makes it even more crucial to standardize the ISMSs and keep them up to date.

However, different challenges can occur during the ISMS standardization process and the challenges identified based on literature in this thesis are the reluctancy to change from employees, the lack of experience in standardization, the difficulty in identifying valuable information assets, the difficulty to keep track of evolving risks, the lack of involvement of top management, poor enforcement of policies, not appropriate or consistent documentation, difficulty to find methods and tools to implement the standard, overlooking some tasks and the difficulty of understanding the standard.

The steps to ISO 27001 standardize an existing ISMS in an organization were also identified and implemented. An appropriate manner to proceed to this standardization is the PDCA approach in which planning phase the requirements of ISO 27001 are grouped and the gap analysis of the existing ISMS conducted. If the gap analysis finds gap in the documentation required by the standard or seen as important by the organization, namely the scope, information security policy & objectives, risk management methodologies and continuous improvement processes, these are updated. After that, a risk management is conducted to create the SoA and risk treatment plan which are implemented in the Do-phase. In addition, measurement & monitoring activities are also implemented in this phase alongside training and awareness programmes for employees. The process is finalized by proceeding to test the ISMS through measurement & monitoring, an internal audit and a management review.

The ISO 27001 project in the case company remained at the Do-phase when finalizing this thesis, but some of the challenges identified by scholars were encountered. Such challenges were the identification of valuable information assets, the lack of consistency in documentation, lack of experience with ISO 27001 and consequently difficulties to understand the standard. These challenges were overcome by setting up version control in

documentation, creating templates, defining a detailed scope to identify information assets and by getting familiar with standards of the ISO 27000 family providing guidelines for implementation. What remains to be seen and may be challenging is the acceptance of change from employees and the enforcement of policies, especially newly implemented ones.

REFERENCES

[1] A. Chopra and M. Chaudhary, *Implementing an Information Security Management System*. India: Apress, 2020.

[2] O. S. Pianykh, *Digital Imaging and Communications in Medicine (DICOM) - A practical Introduction and Survival Guide*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008. doi: 10.1007/978-3-540-74571-6

[3] SESKO ry, "SFS 6001:2018 Suurjännitesähköasennukset." Finnish Standards Association, 2018.

[4] C. Y. Laporte and M. Munoz, "Not Teaching Software Engineering Standards to Future Software Engineers-Malpractice?," *Computer*, vol. 54, no. 5, pp. 81–88, May 2021, doi: 10.1109/MC.2021.3064438

[5] IEC and ISO, "IEC, ISO and information communication technology," p. 9, Mar. 2019.

[6] S. Butler *et al.*, "Maintaining interoperability in open source software: A case study of the Apache PDFBox project," *Journal of Systems and Software*, vol. 159, p. 110452, Jan. 2020, doi: 10.1016/j.jss.2019.110452

[7] International Organization for Standardization, "ISO/IEC/IEEE 12207:2017," *ISO*, 2017. https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/37/63712.html (accessed Mar. 16, 2021).

[8] International Organization for Standardization, "ISO/IEC 25010:2011," *ISO*, 2011. https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/03/57/35733.html (accessed Mar. 16, 2021).

[9] IEEE SA, "IEEE 730-2014 - IEEE Standard for Software Quality Assurance Processes," 2014. https://standards.ieee.org/standard/730-2014.html (accessed Mar. 16, 2021).

[10] H. H. Khan and M. N. Malik, "Software Standards and Software Failures: A Review With the Perspective of Varying Situational Contexts," *IEEE Access*, vol. 5, pp. 17501–17513, 2017, doi: 10.1109/ACCESS.2017.2738622

[11] International Organization for Standardization, "ISO - ISO/IEC JTC 1 - Information technology," 2021a. https://www.iso.org/committee/45020/x/catalogue/p/1/u/0/w/0/d/0#projects (accessed Apr. 06, 2021).

[12] International Organization for Standardization, "ISO - Technical Committees," *ISO*, 2021b. https://www.iso.org/technical-committees.html (accessed Apr. 06, 2021).

[13] International Organization for Standardization, "ISO 9000 family — Quality management," *ISO*. https://www.iso.org/iso-9001-quality-management.html (accessed Mar. 16, 2021).

[14] International Organization for Standardization, "SFS-EN ISO 14001: en Environmental management systems. Requirements with guidance for user (ISO 14001:2015)." Finnish Standards Association, 2015.

[15] ISO, "1. ISO Survey 2019 results - Number of certificates and sites per country and number of sector overall," *ISO Survey of certifications to management system standards - Full results*, Mar. 30, 2021.

https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1 (accessed Jul. 22, 2021).
[16] A. Jain and S. L. Gupta, "Significance of Quality Certification Towards Business Excellence: Case of Indian software Industry," *International Journal of Innovation*, vol. 2, no. 3, p. 6, 2011.
[17] C. Walrad, "Standards for the Enterprise IT Profession," *Computer*, vol. 50, no. 3, pp. 70–73, Mar. 2017, doi: 10.1109/MC.2017.68
[18] S. Uwizeyemungu and P. Poba-Nzaou, "Understanding information technology security standards diffusion: An institutional perspective," in *2015 International Conference on Information Systems Security and Privacy (ICISSP)*, Feb. 2015, pp. 5–16.
[19] I. Guler, M. F. Guillén, and J. M. Macpherson, "Global Competition, Institutions, and the Diffusion of Organizational Practices: The International Spread of ISO 9000 Quality Certificates," *Administrative Science Quarterly*, vol. 47, no. 2, pp. 207–232, 2002, doi: 10.2307/3094804
[20] J. Backhouse, C. W. Hsu, and L. Silva, "Circuits of Power in Creating De Jure Standards: Shaping an International Information Systems Security Standard," *MIS Quarterly*, vol. 30, pp. 413–438, Aug. 2006, doi: 10.2307/25148767
[21] S. W. Anderson, J. D. Daly, and M. F. Johnson, "Why Firms Seek Iso 9000 Certification: Regulatory Compliance or Competitive Advantage?," *Production and Operations Management*, vol. 8, no. 1, pp. 28–43, 1999, doi: https://doi.org/10.1111/j.1937-5956.1999.tb00059.x
[22] C. Prado-Román, C. del Castillo-Peces, C. Mercado-Idoeta, and J. del Castillo-Peces, "Chapter 9 The ISO 9001 Standard in the Spanish Construction Industry," in *Achieving Competitive Advantage through Quality Management*, Springer, pp. 143–154.
[23] G. Culot, G. Nassimbeni, M. Podrecca, and M. Sartor, "The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda," *The TQM Journal*, vol. 33, no. 7, pp. 76–105, Jan. 2021, doi: 10.1108/TQM-09-2020-0202
[24] E. Ozkaya, "1. Importance of Cybersecurity - Knovel," in *Cybersecurity - The Beginner's Guide*, 2019, pp. 5–26.
[25] IT Governance Privacy Team, "Chapter 5: Information Security as part of Data Protection," in *EU General Data Protection Regulation (GDPR) - An Implementation and Compliance Guide*, 3rd ed., 2019, pp. 111–126.
[26] IT Governance Europe, "GDPR Penalties and Fines | IT Governance Finland." https://www.itgovernance.eu/fi-fi/dpa-and-gdpr-penalties-fi (accessed Mar. 12, 2021).
[27] P. K. Singh, *Combating Cyber Threat*. 2018. Accessed: Mar. 12, 2021. [Online]. Available: http://web.a.ebscohost.com.ezproxy.cc.lut.fi/ehost/ebookviewer/ebook/ZTAwMHh3d19fMTgzOTc0N19fQU41?sid=32b1fca0-d29f-4834-b6be-dbb06fe533ff@sessionmgr4008&vid=0&format=EK&lpid=l7&rid=0
[28] MITRE Corporation, "Total CVE records," *CVE*, Jul. 06, 2021. https://cve.mitre.org/cve/ (accessed Jul. 06, 2021).
[29] National Cyber Security Alliance (NCSA), "Small Business Cyber Target Survey Data," *Stay Safe Online*, 2019. https://staysafeonline.org/small-business-target-survey-data/ (accessed Jul. 23, 2021).

[30] L. A. Aguilar, “The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses,” *U.S. Securities and exchange commission*, Oct. 19, 2015. https://www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize-businesses.html (accessed Jul. 23, 2021).
[31] B. Lewis, “The cyber secrets,” *ISOfocus*, p. 27, 2019.
[32] International Organization for Standardization, “SFS-EN ISO/IEC 15408-1:2020 Information technology. Security techniques. Evaluation criteria for IT security. Part 1: Introduction and general model (ISO/IEC 15408-1:2009).” Finnish Standards Association, 2020.
[33] Federal Office For Information Security, “IT-Grundschutz,” *Federal Office for Information Security*. https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz.html;jsessionid=17362F235CFE8CB6F2D59433E7AC39C6.internet461?nn=409850 (accessed Mar. 31, 2021).
[34] A. Calder, *ISO27001/ISO27002 : A Pocket Guide*. United Kingdom: IT Governance Publishing, 2008.
[35] M. Mariano, “ISO 27001 Changes Between 2013 and 2017 | I.S. Partners, LLC,” *https://www.ispartnersllc.com/*, Feb. 04, 2019. https://www.ispartnersllc.com/blog/iso-27001-2013-2017/ (accessed Mar. 31, 2021).
[36] H. S. Lallie *et al.*, “Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic,” *Computers & Security*, vol. 105, p. 102248, Jun. 2021, doi: 10.1016/j.cose.2021.102248
[37] J. R. Vacca, *Computer and Information Security Handbook*, vol. 2nd. 2013. Accessed: Mar. 17, 2021. [Online]. Available: http://web.b.ebscohost.com.ezproxy.cc.lut.fi/ehost/ebookviewer/ebook/ZTAwMHh3d19fNDg1OTk3X19BTg2?sid=b9fbb555-1325-47cc-8825-459da8a4c52c@pdc-v-sessmgr02&vid=0&format=EB&lpid=lp_377&rid=0
[38] Verizon, “2021 Data Breach Investigations Report,” *Verizon Business*, 2021. https://www.verizon.com/business/resources/reports/dbir/ (accessed Jul. 26, 2021).
[39] M. Alotaibi, S. Frunell, and N. Clarke, “Information security policies: A review of challenges and influencing factors,” *International Conference for Internet Technology and Secured Transactions (ICITST)*, no. 11th, pp. 352–358, 2016, doi: 10.1109/ICITST.2016.7856729
[40] A. Alahmari and B. Duncan, “Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence,” in *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, Jun. 2020, pp. 1–5. doi: 10.1109/CyberSA49311.2020.9139638
[41] C. W. Axelrode, *Engineering Safe and Secure Software Systems*. Boston: Artech House, 2013. Accessed: May 06, 2021. [Online]. Available: http://web.a.ebscohost.com.ezproxy.cc.lut.fi/ehost/ebookviewer/ebook/ZTAwMHh3d19fNzUzNTgwX19BTg2?sid=2936672a-065e-4ccb-ada7-cdc7e018d06c@sessionmgr4007&vid=0&format=EB&lpid=lp_iii&rid=0
[42] J. Fruhlinger, “The CIA triad: Definition, components and examples,” *CSO Online*, Feb. 10, 2020. https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html (accessed May 07, 2021).
[43] OWASP, “2017 Top 10 | OWASP,” 2017. https://owasp.org/www-project-top-ten/2017/Top_10.html (accessed May 06, 2021).

[44] MITRE Corporation, “CWE - 2021 CWE Top 25 Most Dangerous Software Weaknesses,” Jul. 26, 2021. https://cwe.mitre.org/top25/archive/2021/2021_cwe_top25.html (accessed Aug. 26, 2021).
[45] Verizon, “2021 Data Breach Incident Classification Patterns,” *Verizon Business*, 2021. https://www.verizon.com/business/resources/reports/dbir/2021/incident-classification-patterns/ (accessed Jul. 27, 2021).
[46] K. Fergusson and P. Loshin, “What is a Denial-of-Service Attack?,” *SearchSecurity*, Apr. 2021. https://searchsecurity.techtarget.com/definition/denial-of-service (accessed Jul. 27, 2021).
[47] Verizon, “2021 DBIR Denial of Service Incidents,” *Verizon Business*, 2021. https://www.verizon.com/business/resources/reports/dbir/2021/incident-classification-patterns/denial-of-service/ (accessed Jul. 27, 2021).
[48] Verizon, “2021 DBIR Basic Web Application Attacks,” *Verizon Business*. https://www.verizon.com/business/resources/reports/dbir/2021/incident-classification-patterns/basic-web-application-attacks/ (accessed Jul. 27, 2021).
[49] “Brute Force Attack Software Attack | OWASP Foundation.” https://owasp.org/www-community/attacks/Brute_force_attack (accessed Aug. 10, 2021).
[50] A. I. H. Suhaimi, Y. Goto, and J. Cheng, “An Engineering Environment Based on ISO/IEC 27000 Series Standards for Supporting Organizations with ISMSs,” in *Future Information Technology*, Berlin, Heidelberg, 2014, pp. 195–201. doi: 10.1007/978-3-642-55038-6_30
[51] B. AbuSaad, F. Saeed, K. Alghathbar, and B. Khan, “Implementation of ISO 27001 in Saudi Arabia – obstacles, motivations, outcomes, and lessons learned,” Jan. 2011.
[52] D. J. Tjirare and F. B. Shava, “A gap analysis of the ISO/IEC 27000 standard implementation in Namibia,” in *2017 IST-Africa Week Conference (IST-Africa)*, May 2017, pp. 1–10. doi: 10.23919/ISTAFRICA.2017.8102376
[53] T. Mueller, S. Dittes, F. Ahlemann, N. Urbach, and S. Smolnik, “Because Everybody is Different: Towards Understanding the Acceptance of Organizational IT Standards,” in *2015 48th Hawaii International Conference on System Sciences*, Jan. 2015, pp. 4050–4058. doi: 10.1109/HICSS.2015.487
[54] S. Fenz, J. Heurix, T. Neubauer, and F. Pechstein, “Current challenges in information security risk management,” *Information Management & Computer Security*, vol. 22, no. 5, pp. 410–430, Jan. 2014, doi: 10.1108/IMCS-07-2013-0053
[55] International Organization for Standardization, “SFS-EN ISO/IEC 27000:2020 Information technology. Security techniques. Information security management systems. Overview and vocabulary (ISO/IEC 27000:2008).” Finnish Standards Association, 2020.
[56] International Organization for Standardization, “SFS-EN ISO/IEC 27001:2017 Information technology. Security techniques. Information security management systems.” Finnish Standards Association, 2017.
[57] S. Higgins, “Information Security Management: THE ISO 27000 (ISO 27K) SERIES | DCC,” Mar. 19, 2009. https://www.dcc.ac.uk/guidance/briefing-papers/standards-watch-papers/information-security-management-iso-27000-iso-27k-s (accessed Mar. 19, 2021).
[58] International Organization for Standardization, “ISO/IEC JTC 1/SC 27 - Information security, cybersecurity and privacy protection,” *ISO*.

https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/committee/04/53/45306.html (accessed Aug. 16, 2021).
[59] International Organization for Standardization, “SFS-EN ISO/IEC 27002:2017.” Finnish Standards Association, 2017.
[60] D. Ganji, C. Kalloniatis, H. Mouratidis, and S. M. Gheytassi, “Approaches to Develop and Implement ISO/IEC 27001 Standard - Information Security Management Systems: A Systematic Literature Review,” *Internation Journal on Advances in Software*, vol. 12, pp. 228–238, 2019.
[61] K. Beckers, H. Schmidt, J. Kuster, and S. Faßbender, “Pattern-Based Support for Context Establishment and Asset Identification of the ISO 27000 in the Field of Cloud Computing,” in *2011 Sixth International Conference on Availability, Reliability and Security*, Aug. 2011, pp. 327–333. doi: 10.1109/ARES.2011.55
[62] A. Calder, *Nine Steps to Success : An ISO 27001:2013 Implementation Overview*, Third Edition. Ely, Cambridgeshire, United Kingdom: IT Governance Publishing, 2016. Accessed: Mar. 22, 2021. [Online]. Available: http://web.a.ebscohost.com.ezproxy.cc.lut.fi/ehost/ebookviewer/ebook/ZTAwMHh3d19fMzkxMTA0X19BTg2?sid=e3f7d785-cc87-47da-b85b-3722686c7dbc@sessionmgr4006&vid=0&format=EB&lpid=lp_13&rid=0
[63] A. Calder, *Nine steps to success an ISO 27001 implementation overview*, 1st edition. Ely, U.K: IT Governance Pub, 2005.
[64] International Organization for Standardization, “SFS-ISO/IEC 27003:2017 Information technology. Security techniques. Information security management systems. Guidance.” Finnish Standards Association, 2017.
[65] International Organization for Standardization, “SFS-ISO/IEC 27005:2018 Information technology. Security techniques. Information security risk management.” Finnish Standards Association, 2018.
[66] T. Valdevit, N. Mayer, and B. Barafort, “Tailoring ISO/IEC 27001 for SMEs: A Guide to Implement an Information Security Management System in Small Settings,” *CCIS 42*, vol. CCIS 42, pp. 201–212, 2009.
[67] T. Valdevit and N. Mayer, “A Gap Analysis Tool for SMEs Targeting ISO/IEC 27001 Compliance,” 2010. doi: 10.5220/0002865504130416
[68] Common Weakness Enumeration, “CWE - 2020 CWE Top 25 Most Dangerous Software Weaknesses,” 2020. https://cwe.mitre.org/top25/archive/2020/2020_cwe_top25.html (accessed May 07, 2021).

APPENDIX 1. OWASP TOP 10 SECURITY VULNERABILITIES

The description provided here are only summaries, more detailed descriptions are available directly on OWASP'S website referenced in [43].

Vulnerability	Description
A1:2017 Injection	The interpreter can be tricked to execute not intended commands or access data without authorization as a response to untrusted data that is sent to it in the form of injection flaws in command or queries.
A2:2017 Broken Authentication	Incorrect implementation of functions related to authentication and session management, which gives room for attackers to exploit the vulnerabilities to access other user's identities either permanently or temporarily.
A3:2017 Sensitive Data Exposure	Attackers can steal or modify sensitive data that is not secured properly using encryption.
A4:2017 XML External Entities (XXE)	Internal files can be disclosed by attackers due to poorly configured or old XML processors that evaluate external entity references inside XML documents.
A5:2017 Broken Access Control	Poorly configured access rights on authenticated users account can provide attackers a way to access unauthorized data or/and functionality.
A6:2017 Security Misconfiguration	Common issue regarding security misconfiguration. Special attention must be paid to secure configuration, patching and upgrade of used frameworks, libraries, applications and operating systems.
A7:2017 Cross-Site Scripting (XSS)	Attacker can hijack user sessions, redirect the user to malicious sites or deface web sites due to unproper validation or escaping when an application includes untrusted data in a new web page. This issue can also occur when a web-page is updated with data supplied by the user by using a browser API creating HTML or Javascript.
A8:2017 Insecure Deserialization	Remote code execution, replay attacks, injection attacks and privilege escalation attacks are performed due to insecure deserialization
A9:2017 Using Components with Known Vulnerabilities	Attacks are possible due to the use of components (Libraries, frameworks, etc) with known vulnerabilities as the components run with the same privileges as the application itself.
A10:2017 Insufficient Logging & Monitoring	Attackers can attack systems and tamper, extract and destroy data due to insufficient logging and monitoring. Such attacks are, most of the time, detected after more than 200 days and by external parties.

APPENDIX 2. THE CWE TOP 25

The description provided here are only summaries, more detailed descriptions are available directly on CWE'S website referenced in [44].

Weakness	Description
Out-of-bounds Write	Due to the software writing data out of the boundaries of a buffer, data can be corrupted, or a crash can occur.
Cross-Site scripting (XSS)	Software does not or incorrectly neutralize input from user before placing it in the output of a webpage used by other users. This may result in untrusted data being send to the website with malicious script which will open the way for an attacker to perform different malicious activities impacting information security.
Out-of-bounds Read	The software reads data out of the boundaries of a buffer which can result in an attacker being able to read information from another location or in a crash of the software.
Improper Input Validation	Data that is sent to the application is not appropriately or not at all validated which may result on an attacker's ability to send input to the application which will lead to altered control flow, arbitrary code execution or arbitrary resource control by the application.
OS Command injection	Due to incorrect or inexistant neutralization of external input elements used in an Operating System command, an attacker can execute commands on the operating system.
SQL Injection	Due to incorrect or inexistant neutralization of external input element used in an SQL command, the security checks could be bypassed, statements to modify databases could be included or system commands could be executed.
Use After Free	Program may crash, use unexpected values or execute code when a place in memory is referenced after it has been freed.
Path Traversal	A pathname is constructed using external input and due to wrong neutralization of special elements, the pathname resolves to another path outside the intended restricted directory which allows an attacked to access other directories.
Cross-Site Request Forgery	Inability of a web application to check if a request was intentionally submitted by a user, which would allow an attacker to trick a client to make unintentional request which will be interpreted as authentic requests.
Unrestricted Upload of File with Dangerous Type	An attacker is able to upload or transfer dangerous file types inside a product's environment.
Missing Authentication for Critical Function	When there is no authentication mechanism for functionality of the software requiring provable user identity or which has a high resource-consumption. This could result in unauthorized data access, processing or corruption of data by an attacker.

(continues)

APPENDIX 2. (continues)

Integer Overflow or Wraparound	Calculation in the software that produces and overflow or wraparound that could cause the software to crash, data to be corrupted, arbitrary code executed.
Deserialization of Untrusted Data	Due to a lack of restriction during the deserialization process, an attacker may be able to perform unauthorized actions as the application deserializes untrusted data.
Improper Authentication	The software is not able to prove on a sufficient level that an actor has a claimed identity, which could allow attackers to access sensitive information.
NULL Pointer Dereference	Application crashes or exits due to it trying to dereference a pointer expected to be valid, but which is null.
Use of Hard-Coded Credentials	An attacker is able to bypass authentication due to passwords or cryptographic keys being hardcoded in the software.
Improper Restriction of Operations within the Bounds of a Memory Buffer	An attacker is able to cause a crash in the system, read information, alter the control flow or execute arbitrary code as the software reads or writes to a location outside the memory buffer on which operations are performed.
Missing Authorization	Actors are able to perform action they should not be able due to the software not performing authorization checks.
Incorrect Default Permissions	Anyone is allowed to modify files due to a misconfiguration in file permissions during installation.
Exposure of Sensitive Information to an Unauthorized Actor	The software displays information to an actor who has not been explicitly allowed to access this information.
Insufficiently Protected Credentials	Methods used to store and transmit authentication credentials are not secured enough and an attacked may intercept/retrieve them.
Incorrect Permission Assignment for Critical Resource	Permissions to access security-critical resources are misconfigured and can be read or modified by unintended actors.
Improper Restriction of XML External Entity Reference	Incorrect documents are embedded in the product's output due to URIs in XML entities that resolve to documents that are outside the sphere of control initially intended.
Server-Side Request Forgery	The web server retrieves the content of an URL without ensuring that the request is sent to the intended destination which would allow an attacker to access information or execute code.
Command Injection	The externally influenced input from an upstream component forming a command or parts of it are not, or not correctly, neutralized, which allows an attacker to inject commands into the application.