UNIVERSITY OF MACEDONIA
MASTER OF SCIENCE IN APPLIED INFORMATICS
DEPARTMENT OF APPLIED INFORMATICS

THE IMPLEMENTATION OF INFORMATION SECURITY POLICY USING ISO 27001: A CASE STUDY IN A SOFTWARE COMPANY

MSc Dissertation

By

Elpiniki Chatzidimitriou

Thessaloniki, October 2019

ΥΛΟΠΟΙΗΣΗ ΠΟΛΙΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ ΧΡΗΣΙΜΟΠΟΙΩΝΤΑΣ ΤΟ ΔΙΕΘΝΕΣ ΠΡΟΤΥΠΟ ISO 27001: Η ΜΕΛΕΤΗ ΜΙΑΣ ΕΤΑΙΡΙΑΣ ΛΟΓΙΣΜΙΚΟΥ

Χατζηδημητρίου Ελπινίκη
Ανατολικών, Βαλκανικών και Σλαβικών σπουδών, ΠΑΜΑΚ, 2012

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΗΝ ΕΦΑΡΜΟΣΜΕΝΗ ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων Καθηγητής
Κίτσιος Φώτιος

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 30/10/2019

Κίτσιος Φώτιος	Στειακάκης Εμμανουήλ	Μαντάς Μιχαήλ
....	....	....

Χατζηδημητρίου Ελπινίκη

....

Περίληψη

Η εργασία αυτή περιγράφει τα κύρια χαρακτηριστικά των διεθνών συστημάτων διαχείρισης ασφάλειας πληροφοριών και του προτύπου προστασίας πληροφοριών 27001, τη δομή του και τις απαιτήσεις για την εφαρμογή του σε εταιρίες και οργανισμούς.

Οι οργανισμοί πρέπει να δεσμεύονται στη διασφάλιση της εμπιστευτικότητας, της διαθεσιμότητας και της ακεραιότας των πληροφοριών που έχουν στην κατοχή τους προκειμένου να διαχειριστούν νομικές και κανονιστικές υποχρεώσεις και να διατηρήσουν επιχειρησιακές σχέσεις εμπιστοσύνης. Αναλύουμε τις συνθήκες που αναγκάζουν οργανισμούς να επενδύσουν στην προστασία των πληροφοριών όπως επίσης και τα οφέλη που μπορούν να αποκομίσουν από αυτή τη διαδικασία. Παρουσιάζονται οι ρόλοι που εμφανίζονται σε έναν οργανισμό για την αποτελεσματική υλοποίηση ενός συστήματός διαχείρισης πληροφοριών καθώς και το θεωρητικό υπόβαθρο της διαχείρισης ρίσκου.

Ειδικότερα εξετάζουμε την περίπτωση μίας πολυεθνικής εταιρίας παροχής υπηρεσιών λογισμικού η οποία αναλαμβάνει και υλοποιεί έργα εγκατάστασης και προσαρμογής λογισμικού υποστήριξης μεγάλων επιχειρήσεων. Αναλύονται οι κύριες λειτουργικές δομές της, οι λόγοι που την οδήγησαν στην εφαρμογή μεθοδολογίας προστασίας πληροφοριών. Εξηγείται η διαδικασία αξιολόγησης ρίσκου και της διαχείρισης των απαραίτητων παραμετροποιήσεων ώστε οι λειτουργίες της να είναι αποδεκτές και σύμφωνες με τα πρότυπα ασφαλείας των πληροφοριών και τέλος παρουσιάζονται οι δυσκολίες και οι προκλήσεις που αντιμετωπίστηκαν.

Λέξεις Κλειδιά:

Σύστημα διαχείρισης ασφάλειας πληροφοριών, ISO 27001, εταιρία παροχής υπηρεσιών λογισμικού, αξιολόγηση ρίσκου, διαχείριση ρίσκου, στρατηγική εφαρμογής ISMS

Abstract

This paper describes the key features of international information security management systems, the information security management standard 27001, its structure, and requirements for its application to companies and organizations.

Organizations must be committed to ensuring the confidentiality, availability, and integrity of the information in their possession in order to manage legal and regulatory obligations and to maintain trusted business relationships. We analyze the conditions that force organizations to invest in the protection of information as well as the benefits they can derive from this process. The roles presented in an organization for the effective implementation of an information management system, as well as the theoretical background of risk management, are presented.

In particular, the paper delves into a multinational IT consulting services company that undertakes and implements large business support installation and customization projects. It analyzes its main operating structures, the reasons that led it to implement an information protection methodology. It explains the process of risk assessment and the management of the necessary configurations so that its functions are acceptable and in line with information security standards and finally presents the difficulties and challenges encountered.

Keywords:

Information Security Management System (ISMS), ISO 27001, software consulting company, Risk Assessment, Risk Treatment,

Acknowledgments

I am grateful to express my sincere gratitude to my supervisor, Associate Professor Kitsios Fotios for the continuous support of my thesis, for his patience, motivation, and immense knowledge. His guidance and encouragement helped me in all the time of research and writing of this thesis significantly.

I wish to give my heartfelt thanks to my family, friends, and colleagues whose support was determining to deliver this thesis.

Table of Contents

List of tables

Symbols

ISO: International Standards Organization

ISMS: Information Security Management System

CISO: Chief Information Security Officer

ISM: Information Security Manager

1 Introduction

1.1 Problem description – the importance

The information has always been an essential asset to every company, and this asset needs to be protected. In the modern world, most information is stored in a digital format and accessible online to ease access and minimize archiving time. However, this has one disadvantage: all this information can be exposed to various risks and threats depending on its importance (Posthumus and von Solms, 2004)

Throughout the years, cyber-attacks targeting confidential/sensitive information are on the rise. A company's growth can make it a more attractive target for cyber-attacks, and the leak of information can damage its reputation, revenue, and reliability (von Solms and von Solms, 2006).

For all of the above reasons, the establishment of an Information Security Management System (ISMS) is imperative to attract more customers and keep the existing ones. It is essential for every client to know that the shared information is safely and properly managed.

An ISO 27001 certificate is a framework to identify, assess, and find coping mechanisms for any imminent risk. It can provide a company with guidance to develop an effective ISMS based on the company's needs. The fact that the implementation of ISMS is company-specific means that every company needs to develop its strategy to better deal with information security risks and threats and, eventually, establish an ISMS that complies with ISO 27001. "Concrete measures for the fulfillment of requirements are not be stipulated by the standard but rather must be developed and implemented on a company-specific basis" (Disterer, 2013).

In literature, we encountered different approaches to develop and implement an ISMS in a company. Putra, Setiawan and Pradana (2017) presented a case study for the "Institute XYZ." In order to establish the basic risk criteria, they used the NIST SP 800-30 revision while using ISO 27005 as reference. They concluded that other guidelines could be used along with ISO 27005 and with one that includes, what they describe as "incident risk scenario" Putra, Setiawan and Pradana (2017).

Furthermore, Agrawal (2017) proposes "a framework for ISO 27005 [...] that can be used to identify information objects involved in a risk management task in an organization". They developed a case study of a health clinic to "classify the information based on the guideline provided by the UNINETT scheme."

Finally, Syreyshchikova et al., (2019) present a way of designing, developing, and mastering the information security process under the requirements of ISO 27001 for the conditions of the industrial enterprise JSC "K." In the above article, they present the method they followed to establish an ISMS to comply with ISO 27001.

Although there are many different approaches on how to successfully implement an ISMS in a company, the desired outcome is the same: to keep information safe and to find the optimal solution that covers the company's needs.

Moreover, one of the most important and time-consuming parts of establishing an ISMS in a company is a risk assessment. All possible risks should be identified, assessed, and classified. Since every company is different, the risks can also vary, and, there is not only one approach that every company can use for risk assessment.

For that reason, it is essential to provide more case studies and more theoretical background regarding the process of implementing an ISMS in a company so that every company or interested party can have access to all this information and use it for its purpose. As stated by Cavusoglu et al., (2015) there is a general belief among companies that in order to successfully confront security issues, is "by investing in technical and socio-organizational resources", however, Cavusoglu et al., (2015) believe that there is a gap in both theory and the empirical cases "for what constitutes a coherent set of organizational resources for information security controls and why variations exist in the number of such resources among organizations…."

1.2 The objective of this study – Main goals

The purpose of this study was twofold: On the one hand, to provide the theoretical background of the research and, on the other hand, to present a case study of a successful company of the Information Technology sector and the process followed to comply with ISO 27001.

1.3 Contribution

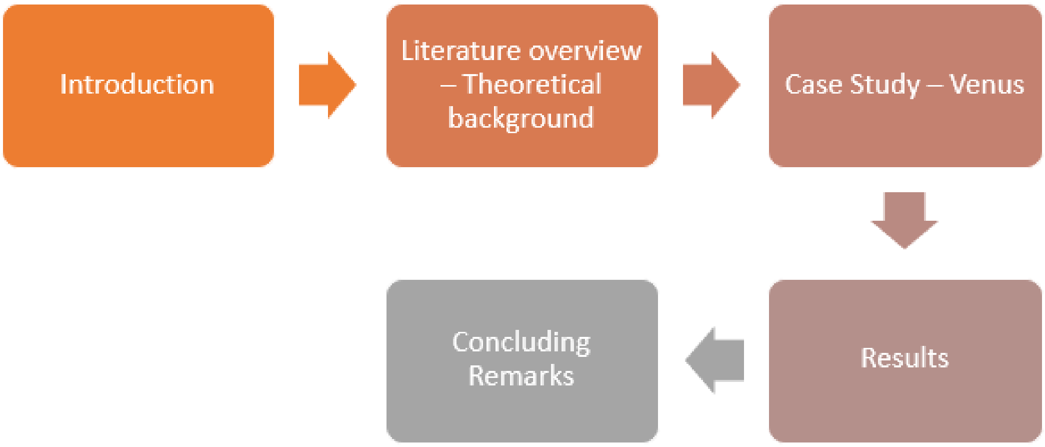
During the implementation of the selected ISMS, the ISO27001, in the company mentioned above, a company of the Information Technology sector, the key roles of this company, as they will be described in chapter 2.5, who needed to develop a strategy, realize that there is a luck of apposite structured, theoretical material to support their way to implementation. What is realized is that despite the fact that numerous books, papers, researches have been conducted, the nature of an ISMS that compels the fulfillment of requirements to be produced and executed per company, creates the need for a sector specific break down. There is a need to investigate the structure and thus the strategy of the implementation at the less possible collective category of companies.

Implementing an ISMS, requires a deep analysis, deep restructure and alignment of almost every aspect of a company’s departments, policies and procedures. There is a considerable uncertainty on the wide range of different paths which supposedly lead to same goal and a need for more case studies to look at actual paths that a company in scope can follow to achieve a successful implementation. Here should be mentioned that the term successful has in itself the object of the time that the implementation team needed to achieve compliance and also the rest of the company easily applied the changes.

Implementing an ISMS, is creating, applying and enforcing a set of changes and strategy to achieve and maintain them. An ISMS team needs to make sure that the selected set of the above are the optimal for the company. This thesis presents a case study and provides a “best-practice” in an IT consulting services company.

1.4 Structure

In Chapter 1, the problem is described, its importance is highlighted, and the objective of this thesis is presented while the chapter 2 is focused on presenting the main features of Information Security Management Systems and ISO 27001. More specific, it is focused on the main reasons companies invest time and money into implementing an ISMS; the leading roles that should be established in a company for the effective implementation of an ISMS and the theoretical background for risk management are presented. In Chapter 3, a case study of an IT consulting services company is introduced and is followed by a short description of the company, providing the company’s status before ISO implementation, and the reasons that triggered the company’s interest to invest resources in complying with ISO 27001. Finally, is provided an analysis of the company’s process to comply with ISO 27001. In Chapter 4 are presented the outcome and the conclusions of the research along with the difficulties encountered and some proposals for future research.



2 Literature overview – Theoretical background

In Chapter 1, we presented the main goals of this thesis, the reason we chose to investigate the implementation of ISO 27001 in a company, and we outlined the contribution of this work.

In this chapter, we will examine the Information Security Management Systems; we will present the main reasons the companies invest time and money into complying with ISO 27001, we will continue with the presentation of ISO 27001 and, consequently, 27002.

Furthermore, we will present the responsibilities of the new roles that need to be established in a company to implement and monitor compliance with ISO 27001 (Chief Information Security Officer and Information Security Manager) and, finally, we chose to focus on what we consider the most critical element of ISO 27001: Risk assessment.

2.1 About Information Security Management Systems (ISMS)

According to Haufe et al. (2016), “Information Security is considered a subset of IT governance.” Based on this statement, we can understand the importance of Information Security in the business strategy of a modern and competitive company.

Moreover, information is one of the critical assets for every company. Information can vary based on the company’s main activities, critical focus, or type; however, one thing remains the same: all this information should be kept safe.

A company can process or maintain different kinds of data that can be classified under different categories of information. From the client’s and staff’s records to accounting-related data, all this information should be available and accessible for the proper functioning of a company.

All this information should be protected and, quoting Hansche, Berti and Hare (2004) “A company should select and apply the appropriate shields in order to protect its physical and/or financial resources, reputation, legal position, employees, and other tangible and intangible assets.” This is where an ISMS comes to help. However, what is the purpose of an ISMS?

In literature, we came across many discussions regarding the purpose of Information Security Management Systems. Peltier (2017) points out that “The purpose of information security is to protect an organization’s information, software, hardware, which are its valuable resources”. According to Farn, Lin, and Fung (2004) “The design, implementation and operation of ISMS should prevent the hardware, software and users' data from being threatened externally and internally even while the company or organization is under threat.”

In light of the above, we can understand that an ISMS is vital since it can protect a company’s critical assets. However, the implementation of an ISMS is not an easy task, and poor planning can even negatively affect a company.

More specifically, in the process of implementing an ISMS in a company, it is possible to adopt processes or policies that create barriers in the company’s function:

- It may be more difficult or time-consuming for the staff to perform everyday tasks since more time will be required for the Information Security checks
- The workload will be increased due to the restrictions in information access
- It may not be possible to keep work standards as they were before the adoption of an ISMS and the work quality can be lower
- Either the already existing staff will need to dedicate time to process additional checks regarding Information Security or additional staff will be required in order to take over these tasks

For the above reasons, “adjustment and cost-effectiveness are key elements of a successful Information Security Management System (ISMS). ISMS-Processes, as basic elements of every ISMS, need to be aligned to the organization and its mission” (Haufe et al., 2016). This should be taken into consideration in the process of designing a successful ISMS and not at a later stage in order to avoid additional costs, increased workload, or lower quality.

The fundamental concept of an ISMS is to ensure the “CIA”:

- Confidentiality
- Integrity
- Availability

of all information and data.

- *Confidentiality*: Information and data should not be accessed by unauthorized people (Tipton and Nozaki, 2007) Companies treat as confidential the financial records, the know-how, the proprietary code, the client data, personal information, etc.

- *Integrity*: it refers to unauthorized changes in data and information. Although an ISMS cannot reassure the accuracy of information and data stored, it embeds processes and tools that verify that changes are intended and correctly applied and also are not a fraud event. (Tipton, 2010)

- *Availability*: information and systems should be available, upon request, at all times. Most common threats are mainly analyzed:
    - Denial-of-service which refers to user or intruder actions that tie up computing services
    - Loss of data processing capabilities, which refers to the destruction of computing hardware/software resources either by physical destructions (which may occur due to natural disasters or human actions) or software unavailability, which may occur due to malevolent system access or operator error.

So even though the company will incorporate controls to ensure the physical, technical, and administrative environment, what needs to be noted here is the importance of the balance between Confidentiality, Integrity, and Availability. The golden ratio is not that easy to be achieved, and this seems to be the Achilles' heel when it comes to external attacks. For example, in order to ensure high Availability, Confidentiality might be in danger. On the other hand, if the company enforces Confidentiality, then Availability might get too complicated.

After having examined the fundamental principles of an ISMS, we will now proceed with the main reasons that motivate companies to implement an ISMS.

2.2 Benefits-why companies care?

Companies’ dependency on Internet connectivity is increasing more and more while simultaneously, companies operate within a highly complicated and advanced security threat landscape that exposes their information infrastructure to a spectrum of security risks.

This leads to the appearance of unprecedented challenges and finally leads companies to establish more secure information technology (IT) infrastructure (Cavusoglu et al., 2015)

Cyber-attacks can cause significant damage to the reputation and finances of affected companies. Even though the number of attacks is growing, the economic impacts of security incidents are less clear, but it is doubtless that “even a single security breach may result in irreparable damage to firms in terms of corporate liability, loss of credibility, and reduced revenues” (Cavusoglu, Mishra and Raghunathan, 2004).

Although all participants are affected by security incidents, at the same time, to rephrase (Syreyshchikova et al., 2019), employees do not realize the importance of a company’s data confidentiality, and they do not take actions needed to reassure that no breach will occur.

Although corporations/organizations and companies identify the need to analyze, evaluate, and effectively reduce the risks, however, duties and plans regarding information security threats confrontation, are in general, not comprehensively established. Implementing an Information Security Information system, like ISO 27001, is an effective and vital way to confront these threats and be sure that data are handled safely and securely.

Whiting, Grazer (2018) present the benefits of ISO 27001 as follows:

“Adopting ISO 27001 can create several significant benefits for a company or an organization. By implementing ISO 27001, companies protect and manage their confidential data consistently by setting up a transparent management process for data access, controls, and management. In order to achieve this, the process of data management should be well defined and consistently managed”.

Furthermore, with ISO 27001, a company’s reputation is increased since clients are more willing to trust their data with an ISO 27001 certified company. This is also interpreted as increased profits and market share. Thus, the company becomes more confident and competitive to grow and attract more clients.

Another factor worth mentioning is alignment with international regulations like GDPR[1] as well as compliance with legal requirements[2]. Legal penalties due to leakage of confidential information can result in long-lasting legal battles as well as enormous money loss[3].

An ISO 27001 certified company can avoid all the adverse effects that derive from data breaches. Based on ISO 27001 provisions, a mature information security incident response system should be set up. This means that there is a system in place that will report and tackle any information security threats as early as possible.

Cyberattacks can happen every day, and it is crucial to be able to spot them at an early stage. For example, in the case of Target stores data breach, it took the company more than a week to spot the attack. If the attack was identified sooner, the data leaked would be less, and it would affect fewer customers[4]. An Information Security incident response system could help a lot to identify and tackle the attack at an early stage.

Moreover, an ISO certified company will analyze the root causes of similar attacks/incidents on a regular basis through tests that will expose any system weaknesses before an actual attack takes place. Identifying and vulnerabilities, before an actual attack

[1] The enforcement of General Data Protection Regulation of the EU on 25.05.2018 put Information Security at the forefront since it changed the way data is handled in every sector. Enforcement of GDPR motivated even more companies in the EU to implement Information Security Management Systems in order to comply with its new provisions. Further discussions regarding GDPR and its importance in ISMS is out of scope in the present thesis. You can find more information on https://eugdpr.org/ accessed 1.09.2019 and (Tankard, 2016).

[2] We would like to point out that when a company has clients from different countries / continents, it is even more difficult to implement an ISMS. Laws and regulations regarding Data Protection are different in every country and this should also be taken into consideration upon planning and implementation of an ISMS.

[3] We will indicatively refer to Capital One data breach of 2019 where personal information of nearly 106 million customers were exposed, Target Stores data breach (2013) where data of more than 110 million people were compromised (card and personal information). In the second case, CIO and CEO resigned and the estimated costs of this breach are approximately 162 million dollars.

[4] It is not uncommon companies not to identify threats at an early stage. This is most probably due to the fact that, quoting Bartnes Line, Anne Tøndel and Jaatun, (2019), “Companies do not see themselves as targets of attacks”.

happens, gives valuable time to the company to prepare itself for any data breach scenario.

Finally, an ISO 27001 should have an established disaster recovery plan. This would be activated in case of an emergency, in other words, when an attack has already happened. It is vital to have a plan to follow in order to be able to recover after the attack. If a company manages to proceed with its usual functions as soon as possible, the losses due to the attack will be less. Every day that a company is not functional costs a significant amount of money, and this is connected to the income and activities of the company.

To sum up, an ISO certified company has in place practices to cope with all three stages of an attack:

- Information Security Incident report system can help with identifying any vulnerabilities before an attack actually happens
- Root cause analysis and regular tests can provide more information regarding any threats and vulnerabilities, and this gives the company more time to find effective ways to deal with any attacks before they happen
- A disaster plan is in place to help the company recover and resume its usual functions as soon as possible after an actual attack

Having established practices to cope with threats or attacks even before they happen, is a potent weapon against cyberattacks that can result in money or reputation loss. Nowadays, these attacks are more and more often, and the companies need to adapt has this new situation. Therefore, ISO 27001 certification can help a company protect data, one of its most valuable assets.

After having outlined the main reasons that motivate companies to comply with ISO 27001, we will now proceed with the presentation of ISO 27001 and, consequently, 27002.

2.3 Historical overview of ISMS

The ISO 27001 and 27002 standards originate from UK DTI (Department of Trade and Industry of the United Kingdom) and BSI (British Standard Institution). “BSI is a non-profit distributing organization and offers global services in the linked fields of standardization, systems assessment, product certification, training, and advisory services" (ISO, 2019).

In 1989, UK DTI distributed a Code of Practice (CoP) for information security. In 1993, the Code of Practice was developed further with the support of industry under the name BS PD 003. In 1995, the British Standard 7799 (BS7799-1 standard) was introduced, which was based on BS PD 003. In 1999, the BS7799-1 standard was reconsidered to include certification and accreditation components, and this resulted in the introduction of BS7799-2 standard. In 2000, the BS7799-1 was transformed to ISO17799:2000 under the name 'Information Technology – Code of Practice for Information Security Management' and is considered the first international information security management standard by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). In 2002, BS7799-2 was revised to incorporate the Plan-Do-Check-Act cycle to be aligned with ISO 9001 and is considered to be the standard against which an ISMS could be certified. In 2005 (June), ISO17799 was revised again, and in October of the same year, ISO 27001 was introduced as ISO Certification Standard for an Information Security Management System. In 2007, ISO17799 was renamed to ISO 27002 which is considered a code of practice for the implementation of security controls in a system (Krause, Tipton, 2006).

Initially, BS7799 did not determine how to select the appropriate security controls which were related to a concrete set of circumstances. After its revision in 1999, BS7799 provides "examples of common approaches" to accomplish specific security goals (Pounde, 1999). BS7799 is organized into the following categories: (Tong, Fung, Huang, Chang, 2003)

(a) Business Continuity Planning
(b) System Access Control
(c) System Development and Maintenance
(d) Physical and Environmental Security
(e) Compliance
(f) Personnel Security
(g) Security Organization

(h) Computer and Network Management

(i) Asset Classification and Control

(j) Security Policy

2.4 ISO 27000 family- ISO 27001, 27002

The ISO/IEC 27001:2013 presents itself as the standard that "specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to apply to all organizations, regardless of type, size or nature." It is a well-respected and internationally recognized Security Standard (Everett, 2011).

The ISO 27000 series provides a guide to best practice for the overall information security management system. ISO 27000 provides an overview and vocabulary, while ISO 27002, extending the code of practice for an ISMS, includes general guidance for information security activities and controls (ISO, 2019). At the beginning of 2007, ISO 17799 was renamed as ISO 27002, which consists of management level recommendations for IT security management. ISO 27002 is a reference for selecting commonly accepted controls in the process of implementing an ISMS, based on the specific information security risk conditions of each company or organization.

In order to get certified for ISO27001, a company needs to have implemented all security controls as they are mentioned in ISO27002.

The controls in ISO 27002 has the same categories and name in Annex A of ISO 27001 – for instance, in ISO 27002, control 6.1.2 is named "Segregation of duties," while in ISO 27001 it is "A.6.1.2 Segregation of duties." The ISO 27002 provides details of the ISO 27001. The control objectives of Annex A of 27001 are directly derived from and aligned with those listed in ISO 27002 (ISO, 2019). ISO 27001 reference to Segregation of duties refers to generic guidelines on how duties of employees should be distinguished in order for further clarity of responsibility to be achieved within the organization. ISO 27002 in more depth, explains the controls that need to be applied in the organization (e.g. clear distinction of responsibilities through clear job descriptions of employees) providing thus the necessary tools for the companies to embrace ISO 27001 more efficiently and with largely accepted means (technetsolutions.net, 2019).

Controls defined in Annex A of ISO 27001 could not be implemented without the guidance and framework provided in ISO 27002; however, without the management framework from ISO 27001, ISO 27002 would remain just an isolated effort, “with no acceptance from the top management and therefore with no real impact on the organization” (technetsolutions.net, 2019).

2.5 Roles of ISMS

Implementing ISO 27001 in an organization requires new roles to be established in order to be more effective. A company must dedicate resources for management and operations. In this way, the company becomes more organized in terms of information security management since it benefits the clear delegation of information security responsibilities as everyone knows who is responsible for managing specific information assets. “This prevents confusion, simplifies processes and improves structure and focus." (Whiting and Grazer, 2018).

Chief Information Security Officer (CISO) and Information Security Manager (ISM) are the most important ones.

“The CISO is a strategic level position, responsible for ensuring that the information assets and IT systems are protected and secure and that such protection is in line with the strategic direction of the organization” (Hooper and McKissack, 2016) (p. 586). A CISO is positioned to manage the organization’s information security processes and to ensure that the board members are correctly informed of the organization’s security state so as to be able to make optimal decisions. The CISO should also be an excellent communicator with business knowledge and interpersonal skills. Among other, a CISO is responsible for:

- Coordinating all information security activities and staff involved in these
- Developing IT security governance mechanisms
- Implementing security awareness programs for employees through mentoring and training sessions

“An ISM (Information Security Manager) oversees the protection of hardware and software assets, networks and data against any threats including breaches and criminal acts" (Linton, 2013). An ISM should possess skills from the following categories:

- Advanced Technical skills
- Managerial skills
- Incidence response skills
- Business skills
- Core Information security skills

The following vital skills for ISMs are ranked from the most important to the least important (Haqaf and Koyuncu, 2018):

- "Understanding of information security issues from a management point-of-view (Project/process management skill)
- Identifying the best information security practices for risk management (Risk management skill)
- Designing information security systems (Core information security skill)
- Understanding of information security standards such as IEEE, IETF and ISO standards (27001), as well as frameworks such as NIST, COBIT, and ISACA (Core information security skill)
- Engaging in security governance and liaison with executive management (Core information security skill)
- Assessing team performance in regard to information security efficiency (Core information security skill)
- Scoping and planning a project, and understanding of project lifecycle (Project/process management skill)
- Assessing incident management (Core information security skill)
- Preparing risk assessment, monitoring and controlling procedures (Risk management skill)
- Developing and implementing IT security policies (Core information security skill)
- Assessing data security auditing activities (Core information security skill)

- Developing and implementing risk mitigation strategies (Risk management skill)
- Understanding of IT security architecture (Technical skill)
- Developing business cases (Project/process management skill)
- Aligning the objectives of information security and the organization (Business skill)
- Understanding of network security (Technical skill)"

However, the management of Information Security is about, "more than just locks and keys and must relate to the social grouping and behavior" (Dhillon and Backhouse, 2001). An ISM usually makes decisions with no involvement or discussions with employees, and that often results in a situation where employees misunderstand the concepts of Information Security.

Apart from technical considerations, Information Security processes also depend on people and how they perceive Information Security, which sometimes differs from the way ISMSs recognize it. As Adams and Sasse point out, insufficient communication with employees, "causes them to construct their model of possible security threats and the importance of security and these are often wildly inaccurate" (Adams and Sasse, 1999). This is the reason that Lee imports a new role, the role "change manager" or "change warrior" (Lee, 2005) who will hold business, communication, negotiation and political skills to achieve the change and conversion of the organizational culture in a way that it will be aligned to Information Security principles. Changing the organizational culture is a crucial element for the success of an ISMS. Changes in processes, roles, communication practices, business practices will inevitably occur and "change manager" or "change warrior" will be responsible for accomplishing this challenge. Thus, these three roles will ensure the implementation and effectiveness of the ISMS in the company.

2.6 The key elements of ISO 27001

Having analyzed why the organization needs to invest in security controls at the strategic level and before determining how to deploy security controls at the implementation level, given that the budget and time to protect the data is pre-decided, in which sector, the company, will focus its time and budget? In a hostile and dangerous environment, which are the priorities?

According to (Cavusoglu et al., 2015), “Within the context of information security, a well-developed security investment rationale provides senior managers with a set of criteria to justify organizational investment in information security. Firms could take into account the economic as well as the non-economic consequences of investment decisions. Economic criteria, such as return on investment (ROI), permit evaluations of the economic feasibility of control in terms of the value of assets to be protected by the control and the cost of the investment. Non-economic criteria, such as retention of customer goodwill, emphasize organizational and operational feasibility. The organizational and management literature also suggests that a well-defined strategic investment rationale is an integral part of the formation of processes leading to organizational adoption and change” (Cavusoglu et al., 2015).

Risk is the keyword and the answer to the questions above, while *risk management* will define the prioritization. More specific and according to Guttman and Roback (1995): Risk is the possibility of something adverse happening. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk. (Guttman and Roback, 1995)

2.6.1 Risk Assessment, Risk Management

As in ISO 27000:2013 is originally stated “The information security management system preserves the confidentiality, integrity, and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed”.

Risk assessment is a tool to analyze and interpret risk. It is the process of identifying and assessing the organization's vulnerabilities. It requires defining an assessment’s scope and methodology, gathering and analyzing data, and go through the risk analysis results. The implementation team should collect and analyze the risk data. To do that they should identify all assets, threats, vulnerabilities, safeguards, importance, residue, and the probability of a successful attack (Kent, Jansen and Tracy, 2008).

Risk assessment should not be delimited only to the existing challenges, but also to the future ones by considering the new systems and innovations that have already arrived in our lives and that are coming ahead. (Zio, 2018

Implementing the risk assessment also leads to in-depth knowledge about the organization and the operations within as the team who performs the risk assessment tries to understand how systems and operations are associated and interact with each other (Guttman and Roback, 1995) which eventually helps the company to identify gaps in its processes. Needs to be noted here, though, that the people who will run the process of the risk assessment need to have a clear, expanded view and extensive knowledge of the whole company.

Risk management is the next step and is the selection and implementation of the appropriate controls to mitigate risk to a level acceptable to the organization. (Kent, Jansen and Tracy, 2008). Just like the rest of the ISO27001 aspects, there is not an intensifier, mandatory template to follow when it comes to Risk Assessment.

An Information Security Team can perform a Risk Assessment the way it makes sense for the organization’s structure.

In this thesis, will be presented two different series of activities of performing a Risk Assessment. The first one will be according to ISO 27000:2013 as originally stated and will be presented in the next paragraph and the second one will be the one used by the company of the case study and will be presented in the respectful chapter.

As described under the clause 6.1.2 of ISO 27001, a risk assessment a. sets and sustains information security risk criteria, b. produces consistent, accurate and relative results, c. identifies the risks along with the risk owners, d. analyzes, and e. evaluates those risks.

We can break risk assessment to the following activities

1. Identification of the assets that are at risk and definitions of the status of importance according to the value, sensitivity, and criticality.

2. Identify potential threats.

3. Identify how possible is a threat to occur to a specific asset.

4. Define the impact. This usually includes the expected losses, damage and recovery cost.

5. Reduce risk by embedding risk-limiting controls that are accepted by the company as regards to the budget like introducing new policies and procedures.

6. Export the conclusions and organize an action plan.

Risk assessment can be quantitative or qualitative, according to Liu, Kuhn and Rossman, (2009) and can be quantitative, semi-quantitative, and qualitative according to Macdonald, (2004).

Quantitative analysis assigns a value to each risk component and the residual risk is calculated providing the loss expectancy. This type of analysis is trying to evaluate the cost of the risk, taking into consideration factors like the likelihood, the costs of potential damage and the cost of possible controls. According to Liu, Kuhn and Rossman, (2009) in quantitative analysis, "risk = probability of loss × cost of loss; managers must balance the expense of reducing vulnerabilities against the calculated risk". However, the quantitative approach "isn't always feasible due to the lack of reliable data (although it can be useful in comparing expected loss under various assumptions)." (Liu, Kuhn and Rossman, 2009)

Qualitative, on the other hand, combines elements from quantitative, in order to assess the level of risk, likelihood and the impact of possible incidents should be estimated and at this point is imported to the analysis the experience and personal judgment of the team that performs the risk assessment; (Liu, Kuhn and Rossman, 2009).

“Semi-quantitative assessment examines threats according to the consequences and probabilities of occurrence. This approach is based on the opinion of the people making assessment.” For example, probabilities can be divided into five classes: 0 – very unlikely, 1 – unlikely, 2 – rather unlikely, 3 – rather likely, 4 – likely (Nikolic and Ruzic-Dimitrijevic, 2009).

Since every event has various and probably multiple consequences, the estimation of incidental occurrences can be based on experience, standards, experiments or an expert advice (Nikolic and Ruzic-Dimitrijevic, 2009).

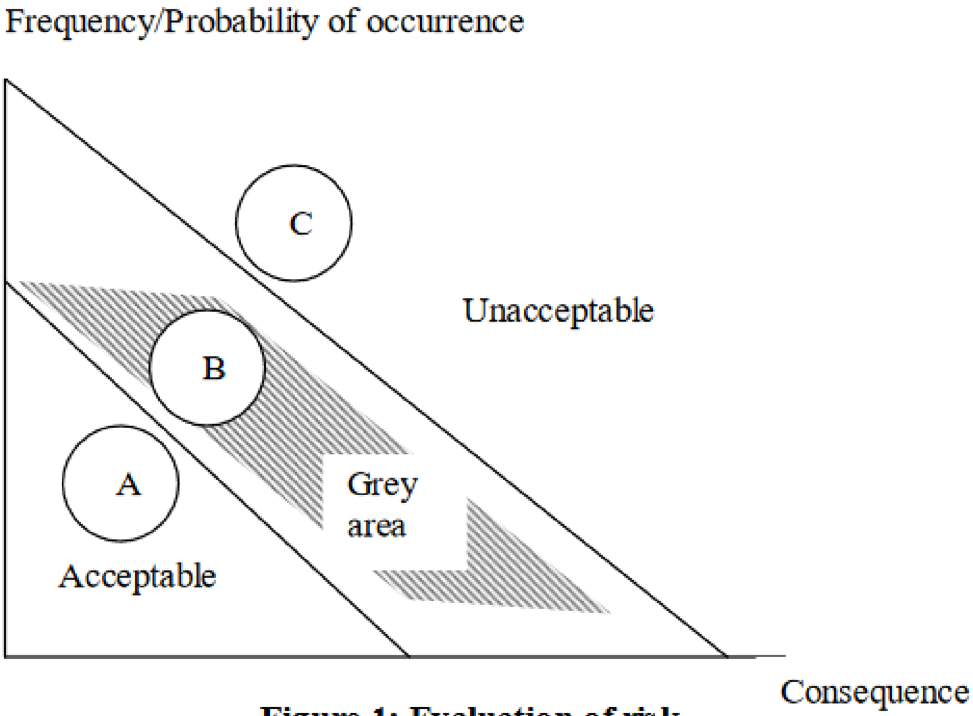


Figure 1: Evaluation of risk

3 Case Study – Venus

After having presented the ISO standards along with the key roles and responsibilities of CISO and ISM, we will now proceed with our case study. We will examine the company's status before implementing ISO 27001, the reason that lead the company to the decision to initiate the process to comply with the above ISO standard and the strategy the company followed to meet the requirements of ISO 27001.

3.1 Short description of the company

The company's name will be concealed for security reasons. In order to keep the text brief, the company will be given the name "Venus". Venus automates and optimizes data-driven business processes with software and services. Venus' consulting practices are well-known worldwide and are the global market leader for a famous platform.

Venus consultants possess deep industry expertise across a diverse range of organizations and verticals. The company understands the challenges of implementing new systems into a business and work closely with its client's Business and IT experts to help them identify opportunities and goals. Venus then partners with them to provide full project life-cycle services, effectively orchestrating all aspects of the project, from process reengineering through system design, development and optimization. Venus is on hand to assess the change management needs of the organization and develop the most effective training to ensure full adoption of the new processes and technology. And finally, the company transitions into dedicated long-term support in production.

Venus combines expertise with strong science and analytics to provide effective software solutions that can automate and optimize business processes on time and on budget. The company's technology consultants have multiple science and engineering degrees. Venus' Solution Center is accredited as a European Union Research Organization and have won multiple EU research programs. The company's scientists and engineers have developed several value-added analytics tools for real, every-day company problems. More importantly, Venus has tested and run these solutions on massive amounts of real data from some of the world's top companies and has achieved tangible and measurable business benefits.

3.1.1 Organizational structure

Venus is a company which is “project based”. Company’s technology consultants are assigned to each project of each client. The teams are dynamic- people are assigned or moved out of the team according to the phase and workload of the project. A team might consist of 4-30 members.

For each client a separate, concrete infrastructure is created. This infrastructure includes:

- a centralized code repository, a code file archive which allows to multi-developer projects to handle various versions
- a centralized document library
- a dedicated directory in a project management tool
- dedicated distribution lists
- dedicated containers for the development and testing
- an issue-tracker for the project
- a separate entry to a time management tool

The tools and infrastructure as described above, provide the team with the appropriate framework to create, manage and deliver the project, collaboration base, metrics and analytics for the quality assurance.

3.2 Company’s status before ISO implementation

It was a Venus policy that the information it manages, in both electronic and hard copy, was appropriately secured to protect against the consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of that information

The company had a lot of processes already in place. However, most of them were not recorded regularly or at all. In other words, many of the threats were not identified, thus, not taken into consideration.

Annual and on-boarding pieces of training regarding Information Security were held in order to make employees aware of the company’s perceived policy regarding information security. An information security team was already established. The members were trained, and all staff members could address any concerns regarding Information Security.

In light of the above, the company had already some established processes that would make the process of complying with ISO 27001 easier; however, there were also many threats and vulnerabilities that were not identified.

3.3 What triggered the company's interest to comply with ISO (change title)

The rapid growth of the company revealed that standardized information security model could make certain business aspects more functional. Moreover, it became clear that rapid growth would make the company a target of cyber threats and this became a goal on its own for the company to proceed with more detailed and enhanced Information Security policy.

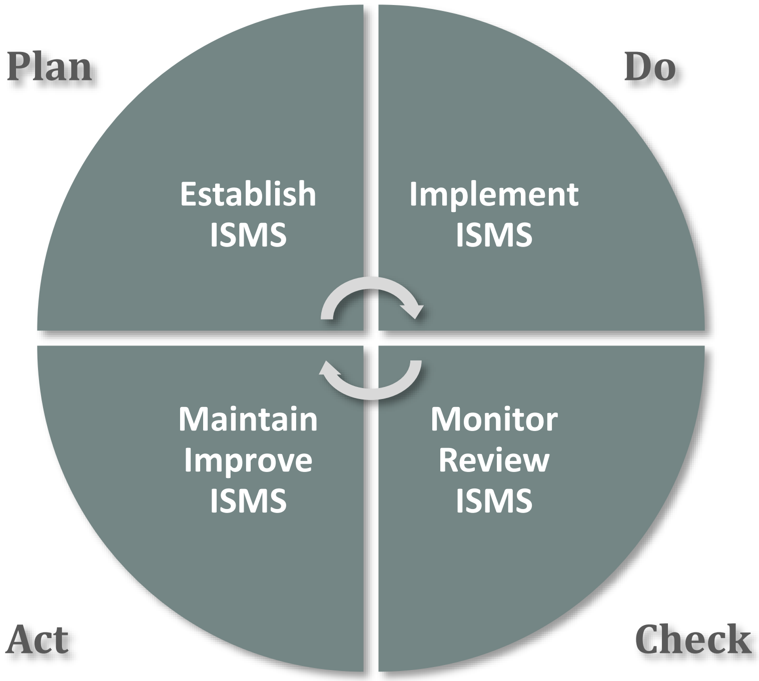
The established way of processing information security was not sustainable in a high factor growing company.

Risks emanating from human error multiply as the company's workforce grows.

Finally, the company kept receiving the same question from numerous clients: "Why should we trust our information with you?". Throughout the years, it became more and more challenging to get back to the clients with a well-documented proof. Moreover, clients became less and less tolerant towards information security uncertainty and the information security team could no longer respond to the clients' need.

The above situation can be identified in (Whiting and Grazer, 2018): ISO 27001 "reassures existing clients that the company will take any necessary security measures to protect their confidential data and attracts new customers who appreciate working with an organization that proactively secures their data."

3.4 Strategy to comply with ISO 27001



Venus followed the guideline, known as the ‘‘Plan–Do–Check–Act’’ process:

1. Plan – Establish ISMS: “establish a security policy and relevant procedures and controls; then prepare a statement of the scope of its application, justifying why the controls were selected and why others were not;” (Siponen and Willison, 2009)

   Establish the ISMS

   - Identify assets, requirements
   - Assess risks, control selection

2. Do – Implement ISMS): “implement the security policy and relevant procedures;” (Siponen and Willison, 2009)

   Implement the ISMS

   - Implement controls
   - Manage operations

3. Check – Monitor and Review ISMS: “assess and measure the process performance, and report the results to management;” (Siponen and Willison, 2009)

   Monitor and review the ISMS
   - Monitor performance
   - Assess performance

4. Act - Maintain and Improve ISMS) “take appropriate corrective actions.” (Siponen and Willison, 2009)

   Maintain and improve the ISMS
   - Corrective actions
   - Preventive actions

3.5 Risk assessment and risk treatment

Risk is the negative impact of any vulnerability and threat that might arise in Venus’ information systems and assets. Risk management enables the systematically identifying, assessing and taking necessary steps and actions to reduce risks to an acceptable level.

In the next paragraphs we will determine and evaluate the methodology for assessment and treatment of information risks, in order to define the acceptable risk level in accordance with appropriate security standards (ISO/IEC 27001: 2013) and also will provide the guidelines for development of an effective risk management program within Venus’ infrastructure.

Risk assessment, risk treatment and its supporting controls and processes are applied to entire Venus’ premises, in respect to all informational and operational risks to all assets which could be used within the company and/or could have an impact on Venus’ information security. It is applicable to all information security risk assessment conducted in the scope of Venus’ Information Security Management System (ISMS), including all Venus’ business processes and assets. The Risk Assessment and Risk Treatment policy applies to all Venus’ business entities (e.g. employees, partners, contractors, local delivery partners, suppliers, members of the public).

3.5.1 Objectives

Risk management is a process in Venus' Information Security Management System (ISMS) framework intending to contribute to the systematic identification, assessment and treatment of risks and to ensure an acceptable level of information security within the scope of the ISMS.

The objectives of risk assessment and risk treatment in the context of information security are:

- Early identification, management and treatment of risks in an acceptable tolerate manner
- Establishment consistent methods for risk identification
- Clear assignment of responsibilities when risks are identified
- Clear documentation of risks with their assessment
- Implementation of better security controls in Venus' information systems
- Better risk assessment decisions, providing information for cost effective security controls
- Design physical, procedural, technical controls agreed with the information asset owners
- Efficient treatment of risks

3.5.2 Business and Technical Context

Venus established the *business* and *technical* context of the information system being assessed and ensured that the business objectives are captured, with all internal and external factors that influence the identified risks.

- **Business Context**
  Identification of Venus' business owner of the information system being reviewed, Information classification, Business processes supported, Users of the system, Security and compliance requirements.
- **Technical Context**

Identification of Venus’ service owner of the information system being reviewed, Venus’ users to support and maintain the information system, Logical architecture, System components.

3.5.3 Risk Assessment Process

Risk assessment considers the value of Venus’ information systems and assets. If the objectives of an asset are critical to Venus’ business needs or if the assets are known to be at high risk, then a detailed risk assessment was conducted for this specific information asset. This involves in-depth identification and validation of assets, including business impact assessment of vulnerabilities and threats to those assets.

The risk assessment identifies, quantifies, and prioritizes the risks following the Venus’ objectives and defines the criteria of the acceptable level of risk. The results of the risk assessment guide Venus’ management in choosing the appropriate actions and the corresponding priority order for the administration of the information security risks and for the implementation of appropriate control mechanisms to protect against these risks.

The risk assessment includes the systematic assessment of the scale of the risks (Risk Analysis) and the process of comparing the risk against the risk criteria to the determination of the importance of the risks (risk assessment). The risk assessment process is conducted periodically to address changes in safety requirements and risk conditions, (e.g. assets, threats, vulnerabilities, impacts and other significant changes) and is carried out in a methodical manner capable of producing comparable and recurring results, several times depending on the part and criticality of Venus or information systems under examination.

A risk assessment must be conducted with access and an understanding of:

- Venus’ business processes.
- The risk-related impact on Venus’ business assets.
- The technical systems in place, supporting the business needs.
- The legislation and regulations to which Venus is subject.
- Up to date vulnerability and threat assessments.

A risk assessment must be conducted at least:

- For every new information processing system.
- Following the introduction of a new information asset.
- Following modifications to systems or processes
- Modifications which might change the nature of threats and vulnerabilities.
- When there has been no review for a relatively long period (e.g., three years).

For each of the risks identified after the risk assessment, Venus' management had to decide on the appropriate risk treatment method. Possible risk treatment options include:

- Implementing appropriate control mechanisms to reduce risks.
- Acceptance of the risks if the conditions and criteria for risk acceptance are met.
- Avoiding risks by not allowing actions that would cause risks.
- Transfer of related risks to other parts, (e.g., insurers or suppliers).

The risk decision with appropriate control mechanisms involves the selection and implementation of control mechanisms in line with the requirements resulting from the risk assessment.

The control mechanisms chosen should ensure that the risks are reduced to an acceptable level taking into consideration:

- The requirements and limitations of national and international law and regulations
- Contractual obligations with customers and suppliers
- Business requirements and objectives of Venus as described above
- Operational requirements and constraints
- The costs of applying and operating control in relation to the risks that are diminished and the remaining risks, depending on the requirements and constraints of Venus
- The need to balance investment in the implementation and operation of controls and damage that may arise in the event of security failure
- Best practices

3.5.4 Assets, Vulnerabilities, Threats

Asset identification

The identification of all Venus' assets is the initial phase in risk assessment process, under ISMS scope (assets' impact on confidentiality, integrity, availability of company's information). Assets include documents in physical or electronic form,

Category	Threats
Theft	Theft, Vandalism
Software Error	Software Error
Software Error	Malware
Software Error	Unauthorized Access
Outage	Power Outage
Outage	Telecommunications Outage
Network Error	Network Attack
Natural Disaster	Earthquake
Natural Disaster	Flood
Natural Disaster	Fire
Legal	Breach of Contractual Relations
Legal	Breach of Legislation
Human Error	Information Misuse
Human Error	Operator Error
Human Error	Misuse of User Privileges
Human Error	Destruction of Records
Hardware Error	Hardware Error
Hardware Error	Damage to Cabling
Access Error	Locked Out
Software Error	Errors in Maintenance
Hardware Error	Malfunction of Equipment
Human Error	Unauthorized Installation of Software
Hardware Disposal	Non-safe Deletion of Media
Hardware Reuse	Non-safe Reassignment of Hardware
Removable Media	Use of Non-Encrypted Removable Media

applications and databases, IT equipment, infrastructure, people, external and outsourced services. Furthermore, asset identification shall include owners of each asset (responsible personnel, organizational unit). Vulnerabilities and threats identification of each asset is the next step in risk methodology. Several vulnerabilities and threats might be associated with each asset.

Vulnerabilities, Threats

Venus considers all protentional vulnerabilities, threats applicable to a specific system whether intrinsic or extrinsic, natural or human, accidental or malicious. Vulnerability and threat information is obtained from appropriate Venus' users and in some cases from specialist security consultancies, local, national law enforcement agencies, security services and contacts.

Table 3-1: Threat Categories as identified for Venus

3.5.5 Risk Identification

Risks related to Venus' information systems, information, and operations could be identified in the following categories:

- Any Venus' user identifies threats that are relevant to the assets under examination.
- A comprehensive list of events that might prevent, or delay Venus' business objectives shall be documented. Risk not included in this list might not be assessed and mitigated.
- Threats from existing repositories might be added after related searches.
- Clear risk description, in order to be assessed and evaluated.
- Risk identification shall include the potential impact on Venus' information systems, assets.

Any potential risk that could affect the confidentiality, integrity, and availability of Venus' information systems, information, operations and assets will be documented in the risk assessment process.

Risk evaluation criteria shall be established in order to provide a common understanding of these security measures, which will minimize the potential impact to an acceptable level.

The damage level and the costs caused by a threat will determine the impact criteria. The impact criteria could be considered as:

Table 3-2: Impact Criteria

Impact Criteria	
Loss of financial value	Consequences on correlated procedures
Direct financial consequences	Security incidents, attacks
Indirect, long-term financial consequences	Breaches of legal, regulatory requirements
Disruption of plans and deadlines	Private agreement issues
Enterprise procedures obstruction	Privacy issues
Loss of business value	Competition related issues
Opportunity loss	Sensitive and personal data, damage reputation
Malfunctions on commercial activities	Public confidentiality issues

3.5.6 Risk Assessment Activities

In order to determine the likelihood of a future event and/or threat that might cause potential harm to Venus' information systems and assets, an analysis is conducted with the identified vulnerabilities and security controls in place. The impact of the loss of confidentiality, integrity, and availability is assessed in accordance with the impact criteria. The likelihood of occurrence is a risk factor on an analysis of the probability that a certain threat is capable of exploiting a certain (or a set of) vulnerability. Risk is the outcome of the likelihood of a certain threat from a potential vulnerability and the resulting impact (probability) on Venus' information systems, assets.

Risk assessment activities will provide the necessary information for the design of appropriate security controls and measures which will reduce or eliminate risks, during the mitigation process (risk treatment).

The steps that leads to the implementations of a risk assessment includes the following activities:

- *Threat identification*: The probability of occurrence for each possible threat is assessed. The threat probability (threat level) is defined as the expected appearance frequency. In determining the likelihood of a threat, Venus shall take into consideration threat sources, potential vulnerabilities, and existing controls.
- *Vulnerability identification*: Analysis of a threat to an information system shall include an analysis of the vulnerabilities associated with Venus' environment. Assessment of the vulnerability levels against a threat scenario. Venus' applied controls will be tested.
- *Control analysis*: Venus' implemented controls shall be taken into consideration and tested in order to minimize and/or eliminate the likelihood, probability of a threat that arises from a system vulnerability.
- *Likelihood determination*: Venus shall consider the following important factors: vulnerability's (nature) threat source, existence, and effectiveness of current controls. The likelihood of occurrence of a threat takes as an input, the threat level, and the vulnerability level outputs the likelihood of occurrence for the specific threat.
- *Impact analysis*: The impact of a security event could be described in terms of - and/or a combination of any - loss of confidentiality, integrity, and availability.
- *Risk determination*: The likelihood of occurrence and the impact values are combined in order to estimate the risk level of each asset, for an identified threat. The adequacy of Venus' planned, existing security controls will also be included to assess the risk level.
- *Control recommendation*: Security controls that could mitigate and/or eliminate the identified risks, in alignment with Venus' operations. The recommended controls shall ensure that the risk level will be reduced to an acceptable level.
- *Results documentation*: After the risk assessment has been completed, the results shall be documented in an official report.

The risk levels are assessed with established criteria, and appropriate measures will be taken.

3.5.7 Likelihood and Impact Evaluation

In case of a risk, it is necessary to assess the relevant consequences for each vulnerability and threat, for an individual asset. The likelihood of the occurrence of such a risk is necessary to be assessed for each Venus' asset. The severity of a risk is an overall assessment of both how likely it is to happen (likelihood) and the impact if it does happen (impact occurrence).

The likelihood of a potential vulnerability and/or threat can be described as (Almost Certain, Probable, Possible, Unlikely, Rare). The impact of a security incident can be described in terms of loss of confidentiality, integrity, and availability.

Table 3-3: Likelihood Probability, Frequency Levels

Likelihood Level	Likelihood Description
Almost Certain	Expected to occur in most circumstances.
Probable	Will probably occur in most circumstances.
Possible	Might occur at some time.
Unlikely	Not expected but conceivable, could occur sometime.
Rare	Not expected and would only occur in specific circumstances.

Table 3-4: Impact Levels

Impact Level	Impact Description
High (H5, H4, H3, H2, H1)	Loss of availability, confidentiality or integrity has considerable, critical and/or immediate impact on the company's cash flow, operations, functionality, legal, contractual obligations, and/or its reputation.
Medium (M5, M4, M3, M2, M1)	Loss of confidentiality, availability or integrity might cause costs and has medium or low impact on legal, contractual obligations and/or the company's reputation.

Low (L5, L4, L3, L2, L1)	Loss of confidentiality, availability or integrity does not affect the company's cash flow, legal, contractual obligations and/or its reputation.

3.5.8 Risk-Level Matrix

Venus developed a risk scale and a risk-level matrix in order to measure an identified risk. The final risk determination is derived by multiplying the rating assigned for threat likelihood (probability) and threat impact. The overall risk ratings might be determined based on inputs from threat likelihood and threat impact categories.

The risk level matrix (table 5) is a 5 x 15 matrix of threat likelihood (Almost Certain, Probable, Possible, Unlikely, Rare) and threat impact (High 1-5, Medium 1-5, Low 1-5) and shows how the overall risk levels are derived. The determination of these risk levels or ratings may be subjective. The rationale for this justification can be explained in terms of the probability assigned for each threat likelihood level and a value assigned for each impact level. For every Venus' asset, every possible threat will be assigned.

The rating scale for impact levels (in terms of confidentiality, integrity, and availability) is set as a 15-point rating scale from L1 to H5: L1, L2, L3, L4, L5, M1, M2, M3, M4, M5, H1, H2, H3, H4, H5. The rating scale for likelihood levels is set as a 5-point rating scale: Rare: 0.20, Unlikely: 0.40, Possible: 0.60, Probable: 0.80, Almost Certain: 1.00. The risk limit is set at 2.9.

The risk level matrix with its ratings represents the level of risk to which the Venus information system, asset, and/or process might be exposed given an identified vulnerability, threat.

Table 3-5: Risk Level Matrix

			Likelihood				
			Rare	Unlikely	Possible	Probable	Almost Certain
		Value	0.20	0.40	0.60	0.80	1.00
Impact	H5	15	3	6	9	12	15
	H4	14	2.8	5.6	8.4	11.2	14
	H3	13	2.6	5.2	7.8	10.4	13
	H2	12	2.4	4.8	7.2	9.6	12
	H1	11	2.2	4.4	6.6	8.8	11
	M5	10	2	4	6	8	10
	M4	9	1.8	3.6	5.4	7.2	9
	M3	8	1.6	3.2	4.8	6.4	8
	M2	7	1.4	2.8	4.2	5.6	7
	M1	6	1.2	2.4	3.6	4.8	6
	L5	5	1	2	3	4	5
	L4	4	0.8	1.6	2.4	3.2	4
	L3	3	0.6	1.2	1.8	2.4	3
	L2	2	0.4	0.8	1.2	1.6	2
	L1	1	0.2	0.4	0.6	0.8	1

Table 3-6: Likelihood - Consequences

Likelihood Rating	Minor	Serious	Severe	Major	Catastrophic
Almost Certain	Medium	High	Critical	Critical	Critical
Probable	Medium	Significant	High	Critical	Critical
Possible	Medium	Medium	Significant	High	Critical
Unlikely	Low	Low	Medium	Significant	Critical
Rare	Low	Low	Medium	Medium	High

Table 3-7: Consequence Levels

Critical	Extreme risk – detailed research, management planning required
High	High risk – immediate attention needed
Significant	Significant Risk – management attention needed
Medium	Medium risk – management responsibility must be specified
Low	Low risk – routine procedures must be managed

3.5.9 Risk Treatment

For each identified risk, a response must be determined. The probability and impact of the risk will be the basis of recommending which actions shall be taken to mitigate the risk. A treatment option (security controls) shall be identified in accordance with cost-benefit analysis and the relevant impact criteria

3.5.10 Risk Treatment Actions

Venus' risk treatment consists of the following four levels:

- Accept: Risk acceptance shall typically only be taken for low-priority risks, in cases where other treatment options will cost more than the potential impact.

All risks shall have a recommendation of control(s) and alternative solutions to mitigate the identified risk. Venus will accept the identified risk.

- Reduction: Risk mitigation involves reducing the probability and/or the impact of risk threat/vulnerability to an acceptable level. Pro-active action against risk is often more effective than attempting to repair the damage an identified risk has caused. Venus will plan and design future controls in order to address the identified risk.
- Transfer: Risk transference involves shifting the negative impact of a threat, vulnerability. Transferring the risk to a third-party (suppliers) does not eliminate a threat, vulnerability. Another party will be responsible for managing the related risk. Venus will list all options for the identified risks in order to be transferred to other entities (e.g., insurance).
- Removal: Risk avoidance involves changing aspects of the overall business processes or system architecture to eliminate the threat, vulnerability. Avoiding the risk by discontinuing the related business activity. Venus will plan all appropriate actions for the removal of assets related to identified risks.

For every asset per threat, Venus will evaluate its impact and likelihood levels. When risk level is above the risk limit, Venus shall examine all controls in place. A new review of risk levels will be conducted, and according to the new risk level, a risk treatment action shall be evaluated. The treatment option(s) shall be documented for each identified risk(s).

3.5.11 Selection of Controls

Appropriate control objectives are selected in order to mitigate the identified risks and minimize the potential impact on Venus' information systems. Security controls are selected and /or designed in accordance with controls from Annex of ISO/IEC 27001:2013 to ensure that none have been missed. The selected controls for their respective threats will be documented.

3.5.12 Risk Treatment Plan

A risk treatment plan is established in order to manage and mitigate the necessary remediation actions. Risk treatment plan is designed to reduce the risks to critical Venus assets. Any potential risk which might arise from identified vulnerabilities and threats shall be addressed in accordance with its consequence level.

Venus' management, in consultation with the risk owners accepts all remaining risks, accordingly. The risk treatment plan will be prepared by the Chief Information Security Officer where the design and the implementation of controls will be scheduled.

3.5.13 Responsibilities

The Chief Information Security Officer will monitor the implementation progress of the risk treatment plan in a regular basis and the effectiveness of the information security framework in order to ensure that the related security controls are effective as designed. The results and the subsequent reviews of risk assessment and risk treatment will be documented. The Chief Information Security Officer shall update the risk assessment and the corresponding residual risk accordingly.

The Information Security Manager is responsible for carrying out risk assessments whenever they are required by Venus' ISMS and in coordination with the Chief Information Security Officer. Moreover, the Information Security Manager in collaboration with the Information Data Owners will review medium and low risks and recommend suitable actions. The Information Security Manager is also responsible to maintain channels of communication with appropriate specialists.

4 Results

The information in all forms, that the company holds, process, maintains and shares is an important business asset and need to be protected with appropriate measures, mechanisms and security controls.

In order to build confidence and ensure that the company preserves its competitive edge, commercial image, cash-flow, portability, legal, regulatory and contractual compliance, information security standards should be in place. Therefore, an information security team was conducted to design and implement all the appropriate policies to support these security standards and to build a structure that safeguards the security of company’s data and information systems.

Risk assessment was conducted. The risk assessment identifies, quantifies, and prioritizes the risks following the Venus’ objectives, defines the criteria of the acceptable level of risk and the results of the risk assessment guide Venus’ management in choosing the appropriate actions and the corresponding priority order for the administration of the information security risks and for the implementation of appropriate control mechanisms to protect against these risks.

4.1 Results in numbers

After conducting the risk assessment, 309 unique threats were identified
309 set of controls were in place at the end of the risk assessment (one set for each threat: a threat might need more than one control in order to mitigate the identified risks and minimize the potential impact on Venus’ information systems.

Risk Reduction:

- 269 risks were mitigated to an acceptable level by applying a set of controls to each threat
    - 198 threats were mitigated to an acceptable level from the controls that were already in place, before the risk assessment
    - 71 threats needed further treatment by applying new controls or upgrade the pre-existing ones
        - For the 45 out of 71 we had to run a third round of control implementation since the second one was not enough

Accept the Risk

- 32 risks were accepted by the CEO since we could not apply an appropriate control

Transfer the Risk

- 5 risks were transferred

Risks Removed

- 3 risks were removed

4.2 Problems during the implementation

Various obstacles were faced during the implementation.

4.2.1 Dedicated Security Team

The company had to assign the task of an ISMS implementation to its resources. The resources should handle the management and implementation of the ISMS and they should be skilled employees with deep knowledge of the company's structure and operations. The role of CISO was assigned to the Director of Development and the role of the ISM was assigned to the Operations Manager, the writer of this thesis. The problem was that these two resources had already tasks assigned to them so a whole new restructure should take place, new employees to be hired to support the tasks that left behind. This added extra cost to the company.

4.2.2 Security and complexity

As mentioned above, Venus is a company which is project based. Consultants and developers join or leave a team according to its needs. Let it be reminded that for each project an infrastructure is created which includes: code repository, document library, a directory in a project management tool, mailing lists, containers for the development and testing, an issue-tracker and an entry to a time management tool.

When the company started to implement the changes in order to secure information and allow access to it only to the project members, a significant complexity was created each time a resource needs to join or leave a team.

The process became time consuming and open up to mistakes. To deal with this challenge, the company assigned a dedicated development team to build a new product which automates all steps related to the *access management*. This added an additional cost to the company.

4.2.3 Security and change management

Successful implementation of ISO 27001 requires employees' full support and contribution. During the implementation of ISO 27001, a few difficulties arose. These difficulties had to be addressed to gain the trust and goodwill of employees and to ensure the effectiveness of the ISMS. Specifically, employees felt that they stepped outside their comfort zones because they considered their work was investigated under the microscope. They worried about the time and effort that would take to follow all the policies and procedures that were related to the ISMS. Employees were also uncomfortable with the deadlines that were set to study the relevant documentation of these new policies and procedures. Due to the fact that a small number of people were involved from the beginning, employees thought the implementation of ISO 27001 was unnecessary and typical. Awareness and realization of the importance of the ISMS were achieved after many training sessions and informal conversations.

5 Concluding remarks

Leakage of confidential information is a nightmare for every company and can have adverse effects that vary from severe damage to the company's reputation to time-consuming legal battles that result in losing a significant amount of money.

A security breach can happen intentionally (an employee from the company gives access to confidential information) or unintentionally (access to confidential information is granted after a cyber-attack). In both cases, the result is the same: access to confidential information is provided to unauthorized users, and the reputation of the company is at stake.

This thesis analyzed how a company certified by ISO 27001 has established practices to prevent similar incidents, to be able to assess the information security risks and cope with any threats or vulnerabilities and to ensure that things are fully and consistently documented and kept up to date.

5.1 Summary and final remarks

Companies should be and verified to be committed to protecting the confidentiality, availability, and integrity of all types of information within their control in order to manage information risk and meet business, legal and regulatory obligations and to maintain trusted business relationships. A successful company is the one that manages to better suit the client's need and in this competitive corporate world, it is essential to keep up with all new trends in Information Technology. Adoption of an ISMS and risk management systems ensures that for all the above, appropriate actions and controls were put in place.

After all, a corporate risk register should include the information risk along with business operational, financial and safety risks (Everett, 2011).

During the writing of this thesis, the writer was part of the implementation team of the ISO 27001, the implementation of a strategy to prevent leakage of confidential information, that was vital for the Venus company.

A large number of threats needed the attention and care of the team. Many controls were applied to mitigate all threats and result to the risk treatment; which threats needed to be transferred, accepted, removed. This thesis was completed only after all the implementation was over and presented the outcomes in numbers. However, the company didn’t go through the external audit and thus the certification process until the time of this thesis was published.

5.2 Research restrictions and limitations

This thesis was the outcome of the long journey of the implementation of ISO 27001 of the Venus company. The risk assessment and risk treatment took more than 11 months and 16 versions to be completed. This added complexity and delay not only to the company’s processes but also to this thesis as well.

In addition, the initial plan was that this thesis would also include the results of the audit, but the initial structure eventually changed in order to match the current situation. The audit was postponed so the rest of the “story line” can be included in a next research.

5.3 Future research directions

As mentioned above, the circle of the ISO implementation did not close since the internal audit did not take place by day this thesis was published. We strongly believe that it would be interesting to have an update on how this journey to ISO27001 ends. What will be the findings of the audit? Will there be any nonconformities? Nonconformities are considered the failures to meet certain requirement, failure to prevent a loss, failure to follow a process, failure to successfully confront a security incident. What would be the reactions of the company?

In addition, pointing toward to compliance with ISO 27001, the process is a constant source of change within an organization thus, affects the change management in a company. A research could be conducted to face all the difficulties and the complexities to this separate section of a company’s life.

Bibliography

Adams, A. and Sasse, M. (1999). Users are not the enemy. *Communications of the ACM*, 42(12), pp.40-46.

Aggeliki Tsohou, Maria Karyda, Spyros Kokolakis, 2015, Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs, *Computers & Security*, 52, pp. 128-141.

Agrawal, V. (2017). A Framework for the Information Classification in ISO 27005 Standard. *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing* (CSCloud), pp.264-269.

Akhyari Nasir, Ruzaini Abdullah Arshahb, Mohd Rashid Ab Hamid, Syahrul Fahmy, 2019, An analysis on the dimensions of information security culture concept: A review, *Journal of Information Security and Applications*, 44, pp. 12–22.

Calder, A. (2005). A business guide to information security. London: Kogan Page.

Cavusoglu, H., Cavusoglu, H., Son, J. and Benbasat, I. (2015). Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. *Information & Management*, 52(4), pp.385-400.

Cavusoglu, H., Mishra, B. and Raghunathan, S. (2004). The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce*, 9(1), pp.70-104.

Chris Pounde, 1999, The Revised Version of BS7799 - So What’s New?, *Computers & Security*, 18, pp. 307-311.

Christina Whiting, David Grazer, 2018, How ISO 27001 Can Benefit Your Organization, [online] Available at: < https://www.tevora.com/iso-27001-can-benefit-organization/> [Last Accessed: 22/08/2019].

Debi Ashenden, 2008, Information Security management: A human challenge? *Information Security Technical Report*, 13, pp. 195–201.

Dhillon Gurpreet, Backhouse James, (2011), Current directions in IS security research: towards socio-technical perspectives’. *Information Systems Journal*, 11, pp. 127–153.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. Journal of Information Security, 04(02), pp.92-100

Eva Weishäupl, Emrah Yasasin, Guido Schryen, 2018, Information security investments: An exploratory multiple case study on decision-making, evaluation and learning, *Computers & Security*, 77, pp. 807-823.

Everett, C. (2011). Is ISO 27001 worth it? *Computer Fraud & Security*, 2011(1), pp.5-7.

Farn, K., Lin, S. and Fung, A. (2004). A study on information security management system evaluation—assets, threat and vulnerability. *Computer Standards & Interfaces*, 26(6), pp.501-513.

Guttman, B. and Roback, E. (1995). An introduction to computer security, the NIST handbook. Gaithersburg, MD: U.S. Dept. of Commerce, Technology Administration, National Institute of Standards and Technology.

Hansche, S., Berti, J. and Hare, C. (2004). *Official (Isc)2 guide to the CISSP exam*. Boca Raton: Auerbach Publications.

Haufe, K., Colomo-Palacios, R., Dzombeta, S., Brandis, K. and Stantchev, V. (2016). Security Management Standards: A Mapping. *Procedia Computer Science*, 100, pp.755-761.

Hooper, V. and McKissack, J. (2016). The emerging role of the CISO. *Business Horizons*, 59(6), pp.585-591.

Husam Haqaf, Murat Koyuncu, 2018, Understanding key skills for information security managers, *International Journal of Information Management*, 43, pp. 165-172.

ISO 27001 Implementer's Forum, 2009, Guideline for Roles & Responsibilities in Information Asset Management [pdf] Available at:<https://www.iso27001security.com/ISO27k_Roles__responsibilities_for_information_asset_management.pdf>.

ISO. (2019). BSI. [online] Available at: https://www.iso.org/member/2064.html [Accessed 5 Sep. 2019].

ISO 27001 benefits, 2019, *ISO 27001 benefits*, [online] Available at: https://www.itgovernance.co.uk/iso27001-benefits.

Kent, K., Jansen, W. and Tracy, M. (2008). Guide to general server security. Gaithersburg, Mar.: U.S. Dept. of Commerce, National Institute of Standards and Technology.

Krause, Tipton, 2006, Information Security Management Handbook, Sixth Edition, Auerback Publications.

Lee Des, (2005), CIOs can thrive as pace of change quickens. [online] Available at: https://www.computerweekly.com/opinion/CIOs-can-thrive-as-pace-of-change-quickens.

Linton, I. (2013). The job description for an information security manager. [online] Available at: <http://work.chron.com/job-description-information-securitymanager-17180.html.> [Accessed: 5 Aug. 2019].

Liu, S., Kuhn, R. and Rossman, H. (2009). Understanding Insecure IT: Practical Risk Assessment. *IT Professional*, 11(3), pp.57-59.

Line, M. B., Tøndel, I. A., & Jaatun, M. G. (2016), Current practices and challenges in industrial control organizations regarding information security incident management – Does size matter? Information security incident management in large and small industrial control organizations, *International Journal of Critical Infrastructure protection*, 12, pp. 12-26

Nikolic, B. and Ruzic-Dimitrijevic, L. (2009). Risk Assessment of Information Technology Systems. *Issues in Informing Science and Information Technology*, 6, pp.595-615

Peltier, T. (2017). Information security fundamentals, second edition.: CRC Press.

Posthumus, S. and von Solms, R. (2004). A framework for the governance of information security. Computers & Security, 23(8), pp.638-646.

Putra, F., Setiawan, H. and Pradana, A. (2017). *Design of Information Security Risk Management Using ISO/IEC 27005 and NIST SP 800-31 Revision 1: A Case Study at Communication Data Applications of XYZ Institute*. 2017 International Conference on Information Technology Systems and Innovation (ICITSI) Bandung, Indonesia, 23-24 October, pp.251-256.

Siponen, M. and Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management*, 46(5), pp.267-270.

Sławomir Wawak, 2010, The Importance of Information Security Management in Crisis Prevention in the Company, *Global Economic Crisis and Changes*, pp. 638-645

Syreyshchikova, N., Pimenov, D., Mikolajczyk, T. and Moldovan, L. (2019). Information Safety Process Development According to ISO 27001 for an Industrial Enterprise. Procedia Manufacturing, 32, pp.278-285.

Tankard, C. (2016). What the GDPR means for businesses. *Network Security*, 2016(6), pp.5-8.

technetsolutions.net. (2019). Difference Between ISO 27001 And 27002 Standard - technetsolutions.net. [online] Available at: http://technetsolutions.net/difference-between-iso-27001-and-27002-standard/ [Accessed 28 Aug. 2019].

Tipton, H. and Nozaki, M. (2007). Information security management handbook. Boca Raton, FL: Auerbach Publications.

Tipton, H. (2010). Information Security Management: Purpose. *Encyclopedia of Information Assurance*, pp.1556-1562.

Tong, C., Fung, K., Huang, H. and Chan, K. (2003). Implementation of ISO17799 and BS7799 in picture archiving and communication system: local experience in implementation of BS7799 standard. *International Congress Series*, 1256, pp.311-318

T. R. Peltier, 2013, Information security fundamentals. CRC Press, 2013

Von Solms, R. and von Solms, S. (2006). Information security governance: Due care. Computers & Security, 25(7), pp.494-497.

Zio, E. (2018). The future of risk assessment. *Reliability Engineering & System Safety*, 177, pp.176-190.