sustainability

MDPI

Article

Developing a Risk Analysis Strategy Framework for Impact Assessment in Information Security Management Systems: A Case Study in IT Consulting Industry

Fotis Kitsios *, Elpiniki Chatzidimitriou and Maria Kamariotou

Department of Applied Informatics, University of Macedonia, GR54636 Thessaloniki, Greece; elpinikichatz@gmail.com (E.C.); mkamariotou@uom.edu.gr (M.K.)
* Correspondence: kitsios@uom.gr

Abstract: Organizations must be committed to ensuring the confidentiality, availability, and integrity of the information in their possession to manage legal and regulatory obligations and to maintain trusted business relationships. Information security management systems (ISMSs) support companies to better deal with information security risks and cyber-attacks. Although there are many different approaches to successfully implementing an ISMS in a company, the most important and time-consuming part of establishing an ISMS is a risk assessment. The purpose of this paper was to develop a risk assessment framework that a company followed in the information technology sector to conduct the risk assessment process to comply with International Organization for Standardization (ISO) 27001. The findings analyze the conditions that force organizations to invest in protecting information and the benefits they can derive from this process. In particular, the paper delves into a multinational IT consulting services company that undertakes and implements large business support installation and customization projects. It explains the risk assessment process and the management of the necessary configurations so that its functions are acceptable and in line with information security standards. Finally, it presents the difficulties and challenges encountered.

Keywords: information security management system (ISMS); ISO 27001; software consulting company; risk analysis; impact assessment

Citation: Kitsios, F.; Chatzidimitriou, E.; Kamariotou, M. Developing a Risk Analysis Strategy Framework for Impact Assessment in Information Security Management Systems: A Case Study in IT Consulting Industry. *Sustainability* **2022**, *14*, 1269. https://doi.org/10.3390/su14031269

Academic Editors: Panagiotis K. Marhavilas, George Boustras, Dimitrios E. Koulouriotis and Francesco Tajani

Received: 19 November 2021
Accepted: 15 January 2022
Published: 24 January 2022

1. Introduction

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 digitally 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 [1,2]. Cyber-attacks on confidential or sensitive information have increased over the years. 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 [3–5]. 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. Every client needs to know that the shared information is safely and correctly managed.

International Organization for Standardization (ISO) 27001 is a management system 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 its needs. The implementation of an ISMS 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. The standard does not specify specific procedures for realizing conditions, but instead, they must be installed and executed on a company-specific basis [6,7].

Various approaches to developing and implementing an ISMS in a company are presented in the literature. Putra et al. (2017) [8] presented a case study for "Institute XYZ" to

establish the essential risk criteria. They used the National Institute of Standards and Technology Special Publication (NIST SP) 800-30 revision while using ISO 27005 as a 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" [8]. Furthermore, to recognize information objects that are concerned with risk management tasks in an establishment, Agrawal (2017) [9] proposed a framework for ISO 27005 that can be employed. A case study of a health clinic was developed to group the information. Syreyshchikova et al. (2019) [10] presented how to design, create, and master an information security procedure under the prerequisites of ISO 27001 for the conditions of the industrial enterprise JSC "K." In the mentioned article, the method followed to establish an ISMS to comply with ISO 27001 was presented.

Although there are many different approaches on how to implement an ISMS in a company successfully, the desired outcome is the same: to keep information safe and to find the optimal solution that covers the company's needs [11–13]. 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 [14].

For that reason, it is essential to provide more case studies and more theoretical background regarding 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. The purpose of this paper is to develop a risk assessment framework that a company has followed in the information technology sector to conduct a risk assessment process to comply with ISO 27001.

The company's policy ensured the information it handled in both electronic and hard copy is adequately protected to guard against the outcomes of violations of privacy, failures of integrity, or disruptions to the accessibility 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 and thus not considered.

The company's rapid growth revealed that a 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. This became a goal for the company to proceed with a more detailed and enhanced information security policy. The conventional way of processing information security was not sustainable in a high-growth company. Risks emanating from human error multiplied as the company's workforce grew. Finally, the company kept receiving the same question from numerous clients: "Why should we trust our information with you?" Through the years, it became more and more challenging to get back to the clients with well-documented proof. Moreover, clients became less tolerant of information security uncertainty, and the information security team could no longer respond to the clients' need.

2. Theoretical Background

2.1. Information Security Management Systems and Benefits

According to Haufe et al. (2016) [15], 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. A company can process or maintain different kinds of data 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 a company should select and apply the appropriate shields to safeguard its physical and financial assets, reputation, legal standing, staff, and other physical and non-physical assets [12]. This is where an ISMS comes in handy. However, what is the purpose of an ISMS?

In the literature, there are several discussions on the purpose of ISMS. Diesch et al. (2020) [11] and Paananen et al. (2020) [16] point out that the primary aim of information security is to safeguard an organization's information, software, and hardware, which are its valuable resources. According to Von Solms and Van Niekerk (2013) [17], the plan, application, and process of ISMS should be able to stop and protect the hardware, software, and users' information from being endangered externally and internally, even when the company or organization is under threat.

In light of the above, we can understand that an ISMS is vital since it can protect its critical assets. However, implementing an ISMS is not an easy task, and poor planning can negatively affect a company. More specifically, it is possible to adopt processes or policies that create barriers in its functions while implementing an ISMS. 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. Furthermore, the workload will be increased due to the restrictions in information access. Moreover, it may not be possible to maintain work standards before adopting an ISMS, and the work quality may be lower. Finally, either the existing staff will need to dedicate time to processing additional checks regarding information security, or another team will be required to take over these tasks [16,18–20].

For the above reasons, regulation and cost-effectiveness are essential components of an effective ISMS. The procedure of ISMS as an essential component of every ISMS must be in agreement with an organization's goals and its mission [15,21]. 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 confidentiality, integrity, and availability of all information and data. Confidentiality refers to the idea that information and data should not be accessed by unauthorized people [22,23]. Companies work with financial records, know-how, proprietary code, client data, personal information, etc. Integrity refers to unauthorized changes in data and information. Although an ISMS cannot assure the accuracy of information and data stored, it embeds processes and tools that verify that changes are intended and correctly applied and are not fraudulent events [24]. Availability refers to information and systems that should be available upon request, at all times. The most common threats are denial-of-service and loss of data processing capabilities. Denial-of-service refers to user or intruder actions that clog computing services. In contrast, loss of data processing capabilities refers to the destruction of computing hardware or software resources, either physically (due to natural disasters or human actions) or through software unavailability (due to malevolent system access or operator error).

Even though a company will implement controls to ensure the physical, technical, and administrative environment, the importance of the balance between confidentiality, integrity, and availability should not be overlooked [25–30]. The golden ratio is difficult to be achieved, and it appears to be the Achilles' heel to external attacks. For example, to ensure high availability, confidentiality might be in danger. On the other hand, if the company enforces confidentiality, availability might become too complicated.

Companies' dependency on Internet connectivity is increasing more and more. In contrast, 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 [31]. Cyber-attacks on a company can lead to severe damage to the affected company's reputation and investments. Even though the number of attacks is growing, the economic impact of security incidents are less clear. Still, it is doubtless that a single security infringement can give rise to irretrievable damage to a firm concerning corporate liability, loss of trustworthiness, and reduced income [3,5,32–35].

Although all participants are affected by security incidents, at the same time, to rephrase [10], 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 corpo-

rations, organizations, and companies recognize the importance of analyzing, evaluating, and effectively mitigating risks, duties and plans for dealing with information security threats, are generally not comprehensively established. Implementing an information security information system such as ISO 27001 is an effective and vital way to confront these threats and handle data safely and securely.

According to Velasco et al. (2018) [7], Diesch et al. (2020) [11], Hsu et al. (2016) [36], and Shojaie et al. (2016) [37], the benefits of ISO 27001 are as follows: ISO 27001 can provide numerous 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 handling process for information access, controls, and handling. To achieve this, the data handling process should be unambiguous and constantly 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 such as the General Data Protection Regulation (GDPR) and compliance with legal requirements. Legal penalties due to leakage of confidential information can result in long-lasting legal battles and enormous financial loss.

An ISO 27001 certified company can avoid all the adverse effects of 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 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 were identified sooner, the amount of data leaked would have been less, affecting fewer customers. An information security incident response system could have helped identify and tackle the attack at an earlier stage [6,7,18,36,37].

Moreover, an ISO certified company will analyze the root causes of similar attacks or incidents regularly through tests that will expose any system weaknesses before an actual attack takes place. Identifying vulnerabilities before an actual attack happens gives valuable time to the company to prepare itself for any data breach scenario. Finally, an ISO 27001 certified company should have an established disaster recovery plan. This would be activated in the event of an emergency—in other words, when an attack has already happened. It is vital to have a plan to follow to recover after an attack. If a company manages to proceed with its usual functions as soon as possible, the losses due to the attack will be minor. Every day that a company is not operating costs a significant amount of money, which is connected to the income and activities of the company [14,23,24,38].

2.2. ISO 27000: 27001, 27002

ISO/IEC 27001:2013 presents itself as the standard that stipulates the conditions for setting up, applying, sustaining, and constantly developing an ISMS within a company's framework. It also comprises prerequisites for the evaluation and handling of information security dangers designed to meet the organization's desires. The conditions set out in ISO/IEC 27001:2013 are non-specific and are expected to apply to all organizations, irrespective of type, size, or nature. It is a well-respected and internationally recognized security standard [6,7,18,36,37].

The ISO 27000 standards provide guidelines for fair practice for a complete ISMS. ISO 27000 provides a summary and terminology, whereas ISO 27002 provides overall guidance for information security actions and controls by extending the rules of practice for an ISMS. In early 2007, ISO 17799 was renamed as ISO 27002, which comprises of management-level suggestions for IT security handling. Toward implementing ISMS, ISO 27002 is a reference point for choosing generally acknowledged controls centered on the particular information security risk conditions of a company or organization [6,7,18,36,37].

To become certified for ISO 27001, a company needs to have implemented all security controls as they are mentioned in ISO 27002. The authorities in ISO 27002 are named the same way as in Annex A of ISO 27001—for example, for ISO 27002, control 6.1.2 is called "Segregation of duties", while for ISO 27001, it is termed "A.6.1.2 Segregation of duties". The dissimilarity is found in the level of detail. Segregation of duties refers to generic guidelines on how employees' duties should be distinguished to achieve greater responsibility. More specifically, ISO 27002 explains the controls that must be implemented in the organization (e.g., clear distinction of responsibilities through clear job descriptions of employees), providing the necessary tools for companies to embrace ISO 27001 more efficiently and with widely accepted means [6,7,18,36,37].

Without the details presented in ISO 27002, the controls outlined in Annex A of ISO 27001 cannot be carried out. However, without the management structure from ISO 27001, ISO 27002 would remain the remote effort of a few information security experts, with no recognition from the board of directors and no actual impact on the organization. These two standards exist separately because if they existed as a single standard it would have been too complicated and broad for practical application.

2.3. ISO 27001: Risk Assessment

According to Cavusoglu et al. (2015) [31], within the framework of information security, a well-structured security investment intent offers top executives a set of conditions to rationalize corporate financing of information security. Organizations could consider both the economic and non-economic consequences of investment decisions. Financial requirements, such as return on investment (ROI), permit evaluations of the economic viability of control concerning the value of properties to be safeguarded by the control and the value of the investment. Non-economic conditions are customer cooperation and emphasize organizational and operational viability. The organizational and management literature also proposes that a well-outlined strategic investment purpose is an essential component of the development processes, giving rise to organizational acceptance and change [31,33,38,39].

Risk is the keyword and the answer to the concerns above, while risk management defines prioritization. As contained in ISO 27000:2013, an ISMS maintains the privacy, integrity, and accessibility of information by using a risk management process that gives assurance to concerned parties that risks are effectively handled. Risk assessment is a tool for analyzing and interpreting risk. It refers to recognizing and evaluating the organization's susceptibilities [40–43]. It requires defining an evaluation scope and procedure, gathering and data analysis, and going through risk evaluation reports. The implementation team should collect and analyze the risk data. To accomplish this, all assets, risks, susceptibilities, safeguards and their importance, residue, and the probability of successful attacks must be identified [32,44,45].

Risk assessment should not be limited only to existing challenges but also to future ones by considering novel systems and inventions that are already in existence and those yet to come [46–49]. Implementing the risk assessment also leads to in-depth knowledge of the organization and its operations. The risk assessment team tries to understand how systems and procedures interact [32,50–52], allowing the company to identify gaps in its processes. It needs to be noted here, though, that the people who will run the risk assessment process 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 [44,45]. Just like the rest of the ISO 27001 aspects, there is no intensifier or mandatory template to follow when it comes to risk assessment. An information security team can perform a risk assessment that makes sense for the organization's structure.

A risk assessment, as described in ISO 27001 under the clause 6.1.2, establishes and maintains information security risk criteria; produces consistent, accurate, and relative

results; identifies the risks in collaboration with the risk owners; and analyzes and evaluates those risks. During the risk assessment, the following activities can be implemented: identification of the assets that are at risk and definition of the status of importance according to value, sensitivity, and criticality; identification of potential threats; labeling of how possible it is for a threat to occur to a specific asset; definition of the impact, which usually includes the expected losses, damage, and recovery cost; reduction in risk by embedding risk management into the design of the asset; and limiting controls that are accepted by the company concerning the budget, such as introducing new policies and procedures, exporting the conclusions, and developing an action plan [8].

2.4. ISO 31000: Risk Management

The ISO 31000 Risk Management Standard is one of the risk management standards that is a series of international standards for applying risk management guidelines issued by the International Organization for Standardization. As is the case with the majority of other ISO management standards, ISO 31000 establishes a structured framework that is intended to suit the demands of companies of all sizes and types [53]. Additionally, it has been suggested that the ISO 31000:2018 standard be used as an appropriate basis for dealing with uncertainties when assessing risks in industrial activities. The ISO 31000:2018 risk management framework has recently been presented as a viable foundation for a thorough risk management examination. Although the standard is primarily used by industry participants, it is adaptable and not industry or sector specific. The ISO 31000:2018 definition of risk is distinct from other risk definitions used in traditional risk assessments in that risk is not defined solely in terms of the probability of bad or undesirable outcomes; rather, the emphasis is on risk management [54].

ISO 31000:2018 risk management is an iterative process that entails the following steps: (1) scope, context, and criteria definition; (2) risk assessment (including risk identification, risk analysis, and risk evaluation); (3) risk treatment; (4) data collection and reporting; (5) monitoring and review; and (6) communication and consultation [53,54]. ISO 31000 establishes a distinction between the risk management framework and two other components of an organization's risk management system—namely, risk management principles and risk management process. The risk management architecture is composed of these three components. The risk management framework is a collection of components that serve as the foundations and organizational structures for developing, implementing, monitoring, reviewing, and continuously improving risk management across the company. Certain risk management frameworks—for example, ISO 31000—are also referred to as risk management standards. Organizations frequently use these two names interchangeably. Risk management is a process that focuses on risk management—namely, communicating, consulting, establishing context, and identifying, assessing, evaluating, treating, monitoring, and reviewing risk [55].

ISO 31000 establishes fundamental principles, a structure, and methods. It is not intended to impose uniformity on risk management systems, but to define the risk management process in any given business, including security. It provides organizations with risk management standards that may be utilized to create and achieve their objectives, regardless of their size or type of business. The ideas, framework, and processes are applicable to both public and private organizations, as well as to all types of groups, associations, and enterprises. It establishes a uniform approach to risk management that is neither industry- nor sector-specific. Any form of risk can be managed using the risk management approach. It is applicable across the organization's lifespan and to any activity, including decision-making at all levels [55–57].

Risk reduction, risk anticipation, and risk management are all components of managing an organization that has risk management integrated into its business plan. As a result, enterprises frequently turn to ISO 31000 for assistance with this task. ISO 31000 can be utilized to make strategic decisions at the organizational level, as well as to manage processes, operations, projects, programs, goods, services, and assets [55,56].

3. Case Study Description

3.1. Case Study: Implementation of ISO 27001 in an IT Company

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

Venus specialists have deep industry knowledge across various establishments and verticals. The company understands the difficulty of executing new systems into a business and carefully works with its customer's business and IT specialists to assist them in recognizing prospects and goals. Venus then partners with them to provide entire project life-cycle services, effectively orchestrating all aspects of the project, from process reengineering through system design, development, and optimization. Venus is available to evaluate the change management desires for the organization and come up with the most efficient training to make sure there is complete acceptance of the new procedures and technology. Finally, the company transitions into committed, long-term support for production.

Venus combines know-how with robust science and problem solving to provide efficient software solutions to computerize and improve business procedures on time and budget. Technology experts in the company have multiple qualifications in science and engineering. Venus' Solution Center is certified as a European Union Research Organization and has won several European Union research programs. Scientists and engineers from the company have designed several improved problem-solving tools for accurate and daily company problems. Of great significance, Venus has tried and run these solutions on vast volumes of precise data from some of the world's biggest companies and has realized substantial and quantifiable business profits.

Venus is a company that is "project based". The company's technology consultants are assigned to each project for each client. The teams are dynamic; people are transferred in 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 consists of a centralized code repository. This code file archive allows 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 development and testing; a project issue tracker; and a separate entry to a time management tool. The tools and infrastructure described above provide the team with the appropriate framework to create, manage, and deliver the project, collaboration base, metrics, and analytics for quality assurance.

3.2. The Company's Status before ISO Implementation

Venus policy ensures the information it handles in both electronic and hard copy is adequately protected to guard against the outcomes of violations of privacy, failures of integrity, or disruptions to the accessibility 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 and thus not considered. Annual and on-boarding pieces of training regarding information security were held 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 already had some established processes that would make complying with ISO 27001 easier. However, many threats and vulnerabilities were not identified.

The company's rapid growth revealed that a 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. This became a goal for the company to proceed with a more detailed and enhanced information security policy. The

conventional way of processing information security was not sustainable in a high-growth company. Risks emanating from human error multiplied as the company's workforce grew. Finally, the company kept receiving the same question from numerous clients: "Why should we trust our information with you?". Through the years, it became more and more challenging to get back to the clients with well-documented proof. Moreover, clients became less tolerant of information security uncertainty, and the information security team could no longer respond to the clients' need.

4. Methodology

A strategic framework was developed to support Venus in developing an ISMS [13,18,58,59]. Figure 1 presents the process used by Venus to implement and evaluate an ISMS. During the first stage, the company established a security rule and relevant measures and controls. It then drew up a statement of the scope of its usage, explaining why the authorities were preferred over others. The company identified assets and requirements, assessed risks, and selected the evaluation method. In the second stage, the company implemented the security policy and relevant procedures, implemented controls and managed operations. During the implementation of the third stage of this process, the company assessed and measured the performance and reported the results to management. In the last stage, the company took appropriate preventive, predictive, and improvement actions to maintain and improve the ISMS [13,18].

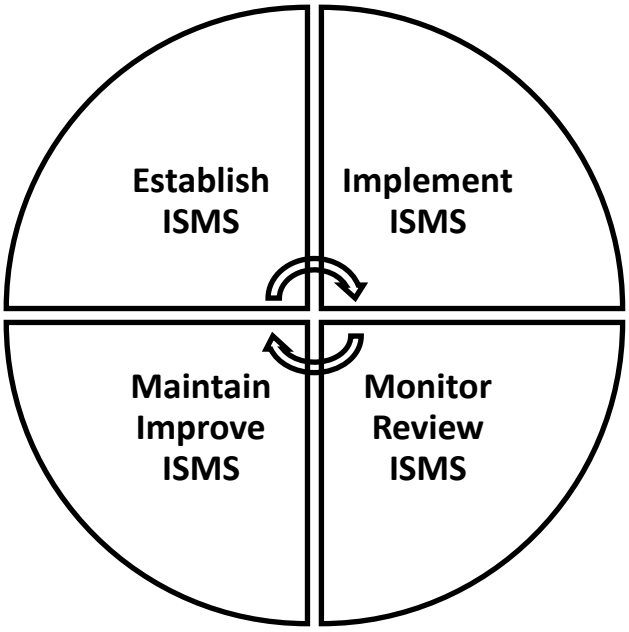

Figure 1. ISMS process.

Risk is the negative impact of any vulnerability and threat that might arise in Venus' information systems and assets. Risk management is the systematic identification, assessment, and implementation of steps and actions to reduce risks to an acceptable level. In the following few paragraphs, we determine and evaluate the methodology for assessment and treatment of information risks to define an adequate risk level following appropriate security standards (ISO/IEC 27001: 2013) and also provide the guidelines for the development of an effective risk management program within Venus' infrastructure.

Risk assessment, risk treatment, and their supporting controls and processes are applied to the entire Venus premises, concerning all informational and operational risks to all assets that could be used within the company and could impact Venus' information security. The controls and processes apply to all information security risk assessments conducted in the scope of Venus' ISMS, including all Venus' business processes and assets. The risk

assessment and risk treatment policy apply to all Venus business entities (e.g., employees, partners, contractors, local delivery partners, suppliers, members of the public).

Risk management is a process in Venus' ISMS framework intended 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 the following: development of clear assignment of responsibilities, development of consistent risk-identification methods, risk identification, 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; designing physical, procedural, and technical rules agreed with the information asset owners; and efficient treatment of risks.

Venus established the business and technical background of the information system being evaluated and made sure that the business aims were covered with all internal and external aspects that controlled the recognized risks. Regarding the business context, the identification of Venus' business owner of the information system was reviewed, including information classification, business processes supported, users of the system, security and compliance requirements. Regarding the technical context, the identification of Venus as the service owner of the information system was reviewed, as were Venus' users' ability to support and maintain the information system, logical architecture, and system components.

A risk assessment examined the importance of Venus' information systems and assets. A comprehensive risk evaluation was conducted for this particular information asset if its purposes were vital to Venus' business desires or if the assets were recognized to be at high risk. This included in-depth documentation and verification of assets, which provided for business effect evaluation of vulnerabilities and risks to those assets.

The risk assessment identified, quantified, and prioritized the risks following the Venus objectives and defined the criteria for the acceptable level of risk. The results of the risk assessment guided 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 proper control mechanisms to protect against these risks.

The risk assessment procedure included the systematic assessment of the risk scale (risk analysis) and the method of contrasting the risk against the risk conditions to determine the importance of the risks (risk assessment). The risk evaluation was conducted occasionally to deal with changes in safety precondition and risk conditions (e.g., assets, threats, susceptibilities, effects, and other essential changes). It was carried out systematically and capable of yielding similar and recurring results, several times depending on the part and criticality of Venus or the information systems under examination.

A risk assessment must be conducted with access to and 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, and 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, and following modifications to systems or processes. Modifications that might change the nature of threats and vulnerabilities could be required 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 included the implementation of proper control mechanisms to reduce risks, the acceptance of the risks of the conditions and criteria for risk acceptance are met, the avoidance of risks by not allowing actions that would cause threats, and the transfer of related risks to other parts (e.g., insurers or suppliers).

The risk decision with appropriate control mechanisms involved selecting and implementing control mechanisms in line with the requirements resulting from the risk assessment. The control mechanisms chosen should make sure the risks are reduced to

the barest minimum, taking into consideration the conditions and restrictions of national and international law and policies, contractual obligations with customers and suppliers, business requirements and objectives of Venus as described above, operational needs and regulations, the costs of applying and operating controls concerning the risks that are diminished and the remaining risks, depending on the conditions and limitations of Venus, the importance of balancing investment in the execution and operation of controls, and damage that may arise in the event of security failure and best practices.

Identifying all Venus' assets was the initial phase in the risk assessment process under ISMS scope (assets' impact on confidentiality, integrity, availability of the company's information). Assets included documents in physical or electronic form, applications and databases, IT equipment, infrastructure, people, and external and outsourced services. Furthermore, asset identification consisted of the owners of each asset (responsible personnel, organizational unit). Identifying vulnerabilities and threats for each asset was the next step in risk methodology. Several vulnerabilities and threats might be associated with each asset.

5. Results

5.1. Risk Assessment Process

Venus considered all potential vulnerabilities and risks relevant to a specific system, whether intrinsic or extrinsic, natural or human, accidental or intentional. Vulnerability and threat information was obtained from appropriate Venus' users and in some cases from professional security consultants, local and national law enforcement bodies, security facilities, and contacts. Table 1 shows the threat categories identified for Venus.

Table 1. Threat categories as identified for Venus.

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

Risks related to Venus' information systems, information, and operations could be identified in the following categories; any Venus user could identify threats relevant to the assets under examination. A comprehensive list of events that might prevent or delay Venus' business objectives was documented. Risk not included in this list might

not be assessed and mitigated. Threats from existing repositories might be added after related searches. A clear risk description was implemented to be considered and evaluated. Finally, risk identification included the potential impact on Venus' information systems and assets. Any potential risk that could affect the confidentiality, integrity, and availability of Venus' information systems, information, operations, and assets was documented in the risk assessment process. Risk evaluation criteria were established to provide a common understanding of these security measures, which minimized the potential impact to an acceptable level. The damage level and the cost caused by a threat determined the impact criteria. Table 2 presents the impact criteria that were defined.

Table 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

To determine the probability of future events and risks that might cause potential harm to Venus' information systems and assets, an analysis was conducted with the identified vulnerabilities and security controls in place. The impact of the loss of confidentiality, integrity, and availability was assessed following the impact criteria. The likelihood of occurrence was a risk factor based on an analysis of the probability that a particular threat could exploit a specific (or a set of) vulnerabilities. Risk is the outcome of the likelihood of a specific threat from potential vulnerability and the resulting impact (probability) on Venus' information systems and assets. Risk assessment activities provided the necessary information to design appropriate security controls and measures that would reduce or eliminate risks during the mitigation process (risk treatment).

The steps that led to implementing a risk assessment included the following activities: threat identification, vulnerability identification, control analysis, likelihood determination, impact analysis, risk determination, control recommendation, and results from documentation. In the first activity, the likelihood of a potential threat occurring was evaluated. The threat probability (threat level) was described as the probable appearance of an occurrence. In establishing the probability of a threat, Venus had to consider threat causes, possible susceptibilities, and existing controls. In the second activity, analyzing a threat to an information system comprised an analysis of the vulnerabilities connected with Venus' environment—assessment of the vulnerability levels to a threat scenario. Venus' applied controls were tested. Next, Venus' implemented controls were considered, and they tried to minimize or eliminate the likelihood and probability of a threat that might arise from a system vulnerability. During the fourth activity, Venus considered the following essential factors: exposure (nature's) threat source, existence, and effectiveness of current controls. The probability of a threat occurrence was input, and the threat level and the susceptibility level were outputs of the probability of an event for a specific threat. In the fifth activity, the impact of a security event was described in terms of loss of confidentiality, integrity, and availability. Then, the likelihood of occurrence and the impact values were combined to estimate the risk level of each asset for an identified threat. The adequacy of Venus' planned and existing security controls were also included to assess the risk level. During the seventh activity, security controls that could mitigate and eliminate the identified risks were aligned with Venus' operations. The recommended controls had to ensure that the risk level was kept at a manageable level. Finally, after the risk assessment was completed, the results were documented in an official report. The risk levels were assessed with

established criteria, and appropriate measures were taken. Figure 2 presents a flowchart of the activities carried out during the risk assessment process.

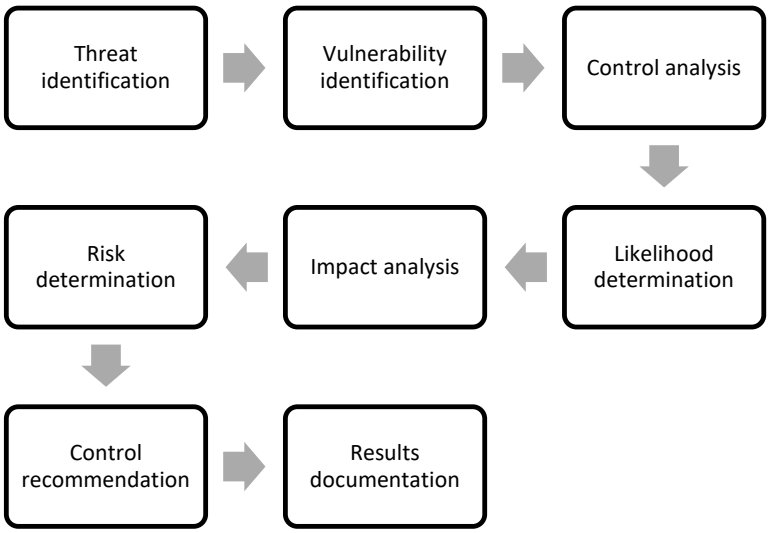

Figure 2. A flowchart of the activities carried out during the risk assessment process.

In the case of a risk, it was necessary to assess the relevant consequences for each vulnerability and threat individually for an individual asset. The likelihood of such a risk was required to be evaluated for each of Venus' assets. The severity of a risk was an overall assessment of both how likely it was to happen (likelihood) and the impact it would have if it did happen (impact occurrence). A potential vulnerability and/or threat was described as (Almost Certain, Probable, Possible, Unlikely, Rare). The effect of a security incident was defined in terms of loss of privacy, integrity, and accessibility. The quantification of impact was based on NIST SP 800-30 revision 1. Level risk was based on NIST SP 800-30 revision 1. Table 3 presents the likelihood probability and frequency levels and Table 4 shows impact levels.

Table 3. Likelihood probability and 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 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.

To measure recognized risk, a risk scale and a risk-level matrix were developed by Venus. The final risk measurement is obtained by multiplying the rating allotted for threat probability and threat effect. The complete risk ratings might be ascertained based on inputs from threat probability and threat effect groups.

The risk level matrix (Table 5) is a 5 × 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 basis for this explanation can be expressed in terms of the probability assigned to each threat probability level and the value assigned to each effect level. For every Venus asset, every possible threat was assigned.

Table 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	04.	0.8	1.2	1.6	2
	L1	1	0.2	0.4	0.6	0.8	1

The rating scale for impact levels (in terms of confidentiality, integrity, and availability) was 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. These criteria are based on ISO27005 [8]. The rating scale for likelihood levels is set as a 5-point rating scale: 0.20 is considered rare, 0.40 is unlikely, 0.60 is considered possible, 0.80 is probable, and 1.00 is considered almost certain. The risk limit is set at 2.9.

Table 5 presents the risk level matrix. 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 in the presence of a known susceptibility and threat. Table 6 shows the consequences and Table 7 presents consequence levels.

Table 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 7. Consequence levels.

Consequence Level	Description
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

5.2. Risk Treatment Plan

A response must be determined for each identified risk. The probability and impact of the risk is the basis of recommending which actions should be taken to mitigate the risk. A treatment option (security controls) shall be identified per cost–benefit analysis and the relevant impact criteria. Venus' risk treatment consisted of the following four levels: accept, reduction, transfer, and removal. At the first level, risk acceptance was reserved for low-priority risks where other treatment options would cost more than the potential impact. To mitigate the identified risk, all risks must include a recommendation of control(s) and alternative solutions. Venus will accept the identified risk. At the second level, risk mitigation entailed minimizing the likelihood and/or the effect of risk threats and vulnerabilities. Pro-active measures against risk are always more efficient than restoring the damage an identified risk has generated. Venus will plan and design future controls to address the identified risk. At the third level, risk transference entailed transferring the negative effect of a threat or vulnerability. Transferring the risk to a third-party (suppliers) will not eradicate a threat or vulnerability. Another party will be in charge of handling the related risk. Venus will list all options for the identified risks to be transferred to other entities (e.g., insurance). At the last level, risk avoidance involved changing aspects of the overall business processes or system architecture to eliminate the threat—avoiding the risk by discontinuing the related business activity.

Appropriate control objectives were selected in order to mitigate the identified risks and minimize the potential impact on Venus' information systems. Security controls were selected and/or designed following rules from the Annex of ISO/IEC 27001:2013 to ensure none were missed. The rules chosen for their respective threats were documented.

A risk treatment plan was established to manage and mitigate the necessary remediation actions. A risk treatment plan was designed to reduce the risks to critical Venus assets. Any potential risk that might arise from identified vulnerabilities and threats was addressed per its consequence level.

6. Discussion

After conducting the risk assessment, 309 unique threats were identified. A total of 309 sets 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 to mitigate the identified risks and minimize the potential impact on Venus' information systems). A total of 269 risks were mitigated to an acceptable level by applying a set of controls to each threat. A total of 198 threats were mitigated to an acceptable level by the controls already in place, before the risk assessment, and 71 threats needed further treatment by applying new controls or upgrading the pre-existing ones. For 45 out of 71, we had to run a third round of control implementation since the second one was not enough. The CEO accepted 32 risks since we could not apply, 5 risks were transferred, and 3 risks were removed.

Various obstacles were faced during the implementation. The company had to assign the task of an ISMS implementation to its resources. The resources were to handle the management and implementation of the ISMS, and they were to be skilled employees with deep knowledge of the company's structure and operations. The role of the Chief Information Security Officer (CISO) was assigned to the Director of Development, and the role of the ISM was assigned to the Operations Manager. The problem was that these two resources already had tasks assigned to them, so a whole new restructuring had to take

place, with new employees hired to support the functions that were left behind. This added an extra cost to the company.

As mentioned above, Venus is a project-based company. Consultants and developers join or leave a team according to its needs. It should be noted that infrastructure is created for each project, including a code repository, a document library, a directory in a project management tool, mailing lists, containers for development and testing, an issue tracker, and an entry into a time management tool.

When the company started to implement the changes to secure information and allow access to it only to the project members, a significant level of complexity was created each time a resource needed to join or leave a team. The process became time-consuming and left room for mistakes. To deal with this challenge, the company assigned a dedicated development team to build a new product that automated all steps related to access management. This added an additional cost to the company.

Successful implementation of ISO 27001 requires employees' full support and contribution. During the execution 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 had stepped outside their comfort zones because they believed their work was being investigated under a microscope. They were worried about the time and effort it would take to follow all the policies and procedures that were related to the ISMS. Employees were also uncomfortable with the deadlines set to study the relevant documentation of these new policies and procedures. Employees thought the implementation of ISO 27001 was unnecessary and typical because only a small number of people were involved from the start. Awareness and realization of the importance of the ISMS were achieved after many training sessions and informal conversations.

As mentioned above, the circle of the ISO implementation did not close since the internal audit had not taken place yet. We strongly believe that it would be interesting to have an update on how this journey to ISO 27001 ends. What will be the findings of the audit? Will there be any nonconformities? Nonconformities are considered failures to meet specific requirements, failure to prevent a loss, failures to follow a process, and failures to successfully confront a security incident. What would be the reactions of the company?

The risk assessment and risk treatment took more than 11 months and 16 versions to be completed. This added complexity and delay to the company's processes, and the audit was postponed. In addition, pointing toward compliance with ISO 27001, the process is a constant source of change within an organization; thus, it affects the change management in a company. Future research could face all the difficulties and complexities of this separate section of a company's life.

7. Conclusions

The purpose of this paper was to develop a risk assessment framework that a company could follow in the information technology sector to conduct a risk assessment process to comply with ISO 27001. This paper analyzed how a company certified by ISO 27001 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.

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. The risks vary from other companies, but the desired outcome is to keep information safe and to find an optimal solution that covers the company's needs. 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 and thus were not considered.

Furthermore, the company's rapid growth revealed that a 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. This became a

goal for the company to proceed with a more detailed and enhanced information security policy. The conventional way of processing information security was not sustainable in a high-growth company. Risks emanating from human error multiply as a company's workforce grows. Finally, the company kept receiving the same question from numerous clients: "Why should we trust our information with you?" Through the years, it became more and more challenging to get back to the clients with well-documented proof. Moreover, clients became less tolerant of information security uncertainty, and the information security team could no longer respond to the clients' need. Thus, this paper was the outcome of the long journey of the implementation of ISO 27001 in the company. However, the risk assessment process is not static, and it will need to be repeated.

The practical contribution of this paper is that it provides a framework for practitioners to implement the risk assessment process in the information technology sector. Companies in the information technology sector are entirely devoted to their productive work and solving their day-to-day survival problems. They are often unable and unwilling to spend time and effort defining new processes or improving existing ones. Software engineers are more oriented towards products, services, or management than establishing new working practices.

Another contribution of this paper is that the implementation of ISO 27001 will have an impact in the medium-term on the day-to-day operation of the business, resulting in a reduction in workload and duplication of effort, and an optimization of the tasks related to the implementation and maintenance of the recommended best practices will help carry them out. Companies not only need to know what to do in order to improve their processes, but they need to have specific procedures describing in detail the work they have to perform, with a clear set of best practices that will help to carry them out. These procedures should be simple and applicable to the types of projects that they usually undertake.

A limitation of this paper is that the risk assessment and treatment took more than 11 months and 16 versions to be completed. As a result, future researchers can evaluate the impact and likelihood levels of each asset per threat. When the risk level is above the risk limit, Venus will examine all controls in place. A new risk level review will be conducted, and a risk treatment action will be evaluated based on the new risk level. For each identified risk, the treatment option must be documented.

Furthermore, future researchers can collect more information objects for Figure 2 by conducting literature reviews and discussions with information security risk practitioners. Some information objects based on ISO 27005 may be missing in this paper. The description of risks can support companies in developing an evaluation of the likelihood and impact of risks to ISMS. Furthermore, other tools can be used to expand a company's threats and vulnerabilities with the conditions that exist in ISMS. However, this paper can be considered as a starting point for the people who participate in the assessment process of ISMS and decision-making in an organization.

Another limitation is that it only includes one case study; selecting cases from various industries may have provided more robust support for the definition of specific recommendations contained in the ISMS. Considering the lessons learned from its application by more software development companies will provide valuable guidelines for practitioners in the information technology sector.

Author Contributions: Conceptualization, F.K. and E.C.; methodology, M.K.; formal analysis, E.C.; resources, E.C.; data curation, F.K.; writing—original draft preparation, F.K., E.C. and M.K.; writing—review and editing, F.K., E.C. and M.K.; supervision, F.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Mishra, S. Organizational objectives for information security governance: A value focused assessment. *Inf. Comput. Secur.* **2015**, *23*, 122–142. [CrossRef]
2. Nicho, M. A process model for implementing information systems security governance. *Inf. Comput. Secur.* **2018**, *26*, 10–38. [CrossRef]
3. Deane, J.K.; Goldberg, D.M.; Rakes, T.R.; Rees, L.P. The effect of information security certification announcements on the market value of the firm. *Inf. Technol. Manag.* **2019**, *20*, 107–121. [CrossRef]
4. Joshi, C.; Singh, U.K. Information security risks management framework–A step towards mitigating security risks in university network. *J. Inf. Secur. Appl.* **2017**, *35*, 128–137. [CrossRef]
5. Sen, R.; Verma, A.; Heim, G.R. Impact of cyberattacks by malicious hackers on the competition in software markets. *J. Manag. Inf. Syst.* **2020**, *37*, 191–216. [CrossRef]
6. Disterer, G. ISO/IEC 27000, 27001 and 27002 for Information Security Management. *J. Inf. Secur.* **2013**, *4*, 92–100. [CrossRef]
7. Velasco, J.; Ullauri, R.; Pilicita, L.; Jácome, B.; Saa, P.; Moscoso-Zea, O. Benefits of implementing an isms according to the ISO 27001 standard in the Ecuadorian manufacturing industry. In Proceedings of the 2018 IEEE International Conference on Information Systems and Computer Science (INCISCOS), Quito, Ecuador, 13–15 November 2018; pp. 294–300.
8. Putra, F.; Setiawan, H.; Pradana, A. 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. In Proceedings of the 2017 International Conference on Information Technology Systems and Innovation (ICITSI), Bandung, Indonesia, 23–24 October 2017; pp. 251–256.
9. Agrawal, V. A Framework for the information classification in ISO 27005 standard. In Proceedings of the IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), New York, NY, USA, 26–28 June 2017; pp. 64–269.
10. Syreyshchikova, N.; Pimenov, D.; Mikolajczyk, T.; Moldovan, L. Information safety process development according to ISO 27001 for an industrial enterprise. *Procedia Manuf.* **2019**, *32*, 278–285. [CrossRef]
11. Diesch, R.; Pfaff, M.; Krcmar, H. A comprehensive model of information security factors for decision-makers. *Comput. Secur.* **2020**, *92*, 101747. [CrossRef]
12. Nasir, A.; Arshah, R.A.; Ab Hamid, M.R.; Fahmy, S. An analysis on the dimensions of information security culture concept: A review. *J. Inf. Secur. Appl.* **2019**, *44*, 12–22. [CrossRef]
13. Niemimaa, E.; Niemimaa, M. Information systems security policy implementation in practice: From best practices to situated practices. *Eur. J. Inf. Syst.* **2017**, *26*, 1–20. [CrossRef]
14. Diéguez, M.; Bustos, J.; Cares, C. Mapping the variations for implementing information security controls to their operational research solutions. *Inf. Syst. e-Bus. Manag.* **2020**, *18*, 157–186. [CrossRef]
15. Haufe, K.; Colomo-Palacios, R.; Dzombeta, S.; Brandis, K.; Stantchev, V. Security management standards: A mapping. *Procedia Comput. Sci.* **2016**, *100*, 755–761. [CrossRef]
16. Paananen, H.; Lapke, M.; Siponen, M. State of the art in information security policy development. *Comput. Secur.* **2020**, *88*, 101608. [CrossRef]
17. Von Solms, R.; Van Niekerk, J. From information security to cyber security. *Comput. Secur.* **2013**, *38*, 97–102. [CrossRef]
18. Mesquida, A.L.; Mas, A. Implementing information security best practices on software lifecycle processes: The ISO/IEC 15504 security extension. *Comput. Secur.* **2015**, *48*, 19–34. [CrossRef]
19. Pérez-González, D.; Preciado, S.T.; Solana-Gonzalez, P. Organizational practices as antecedents of the information security management performance. *Inf. Technol. People* **2019**, *32*, 1262–1275. [CrossRef]
20. Tsohou, A.; Karyda, M.; Kokolakis, S. Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Comput. Secur.* **2015**, *52*, 128–141. [CrossRef]
21. Tu, C.Z.; Yuan, Y.; Archer, N.; Connelly, C.E. Strategic value alignment for information security management: A critical success factor analysis. *Inf. Comput. Secur.* **2018**, *26*, 150–170. [CrossRef]
22. Koohang, A.; Anderson, J.; Nord, J.H.; Paliszkiewicz, J. Building an awareness-centered information security policy compliance model. *Ind. Manag. Data Syst.* **2019**, *120*, 231–247. [CrossRef]
23. Topa, I.; Karyda, M. From theory to practice: Guidelines for enhancing information security management. *Inf. Comput. Secur.* **2019**, *27*, 326–342. [CrossRef]
24. Leszczyna, R. A review of standards with cybersecurity requirements for smart grid. *Comput. Secur.* **2018**, *77*, 262–276. [CrossRef]
25. Kitsios, F.; Kamariotou, M.; Talias, M. corporate sustainability strategies and decision support methods: A bibliometric analysis. *Sustainability* **2020**, *12*, 521. [CrossRef]
26. Kitsios, F.; Grigoroudis, E.; Giannikopoulos, K.; Doumpos, M.; Zopounidis, C. Strategic decision making using multicriteria analysis: New service development in Greek hotels. *Int. J. Data Anal. Tech. Strateg.* **2015**, *7*, 187–202. [CrossRef]
27. Kitsios, F.; Kamariotou, M. Strategic IT alignment and business performance in SMES: An empirical investigation. In *Business Information Systems Workshops*; Abramowicz, W., Corchuelo, R., Eds.; Springer LNBIP 373; Springer Nature: Berlin/Heidelberg, Germany, 2019; pp. 113–123.
28. Kitsios, F.; Kamariotou, M. Information systems strategy and innovation: Analyzing perceptions using MCDA. *IEEE Trans. Eng. Manag.* 2021; *in press*. [CrossRef]

29. Kitsios, F.; Kamariotou, M. Artificial intelligence and business strategy towards digital transformation: A research agenda. *Sustainability* **2021**, *13*, 2025. [CrossRef]
30. Kitsios, F.; Kamariotou, M. Business strategy modelling based on enterprise architecture: A state of the art review. *Bus. Process Manag. J.* **2019**, *25*, 606–624. [CrossRef]
31. Cavusoglu, H.; Cavusoglu, H.; Son, J.; Benbasat, I. Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. *Inf. Manag.* **2015**, *52*, 385–400. [CrossRef]
32. Eling, M.; Wirfs, J. What are the actual costs of cyber risk events? *Eur. J. Oper. Res.* **2019**, *272*, 1109–1119. [CrossRef]
33. Jeong, C.Y.; Lee, S.Y.T.; Lim, J.H. Information security breaches and IT security investments: Impacts on competitors. *Inf. Manag.* **2019**, *56*, 681–695. [CrossRef]
34. Michel, A.; Oded, J.; Shaked, I. Do security breaches matter? The shareholder puzzle. *Eur. Financ. Manag.* **2020**, *26*, 288–315. [CrossRef]
35. Xu, H.; Guo, S.; Haislip, J.Z.; Pinsker, R.E. Earnings management in firms with data security breaches. *J. Inf. Syst.* **2019**, *33*, 267–284. [CrossRef]
36. Hsu, C.; Wang, T.; Lu, A. The impact of ISO 27001 certification on firm performance. In Proceedings of the IEEE 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, USA, 5–8 January 2016; pp. 4842–4848.
37. Shojaie, B.; Federrath, H.; Saberi, I. Getting the full benefits of the ISO 27001 to develop an ISMS based on organisations' InfoSec culture. In Proceedings of the 10th International Symposium on Human Aspects of Information Security and Assurance (HAISA), Frankfurt, Germany, 19–21 July 2016; pp. 88–100.
38. Weishäupl, E.; Yasasin, E.; Schryen, G. Information security investments: An exploratory multiple case study on decision-making, evaluation and learning. *Comput. Secur.* **2018**, *77*, 807–823. [CrossRef]
39. Haqaf, H.; Koyuncu, M. Understanding key skills for information security managers. *Int. J. Inf. Manag.* **2018**, *43*, 165–172. [CrossRef]
40. Marhavilas, P.K.; Koulouriotis, D.E. Developing a new alternative risk assessment framework in the work sites by including a stochastic and a deterministic process: A case study for the Greek Public Electric Power Provider. *Saf. Sci.* **2012**, *50*, 448–462. [CrossRef]
41. Koulinas, G.K.; Marhavilas, P.K.; Demesouka, O.E.; Vavatsikos, A.P.; Koulouriotis, D.E. Risk analysis and assessment in the worksites using the fuzzy-analytical hierarchy process and a quantitative technique—A case study for the Greek construction sector. *Saf. Sci.* **2019**, *112*, 96–104. [CrossRef]
42. Marhavilas, P.K.; Koulouriotis, D.; Gemeni, V. Risk analysis and assessment methodologies in the work sites: On a review, classification and comparative study of the scientific literature of the period 2000–2009. *J. Loss Prev. Process Ind.* **2011**, *24*, 477–523. [CrossRef]
43. Marhavilas, P.K.; Filippidis, M.; Koulinas, G.K.; Koulouriotis, D.E. A HAZOP with MCDM based risk-assessment approach: Focusing on the deviations with economic/health/environmental impacts in a process industry. *Sustainability* **2020**, *12*, 993. [CrossRef]
44. Barton, K.A.; Tejay, G.; Lane, M.; Terrell, S. Information system security commitment: A study of external influences on senior management. *Comput. Secur.* **2016**, *59*, 9–25. [CrossRef]
45. Karanja, E. The role of the chief information security officer in the management of IT security. *Inf. Comput. Secur.* **2017**, *25*, 300–329. [CrossRef]
46. Koulinas, G.K.; Demesouka, O.E.; Marhavilas, P.K.; Vavatsikos, A.P.; Koulouriotis, D.E. Risk assessment using fuzzy TOPSIS and PRAT for sustainable engineering projects. *Sustainability* **2019**, *11*, 615. [CrossRef]
47. Marhavilas, P.K.; Koulouriotis, D.E. A risk-estimation methodological framework using quantitative assessment techniques and real accidents' data: Application in an aluminum extrusion industry. *J. Loss Prev. Process Ind.* **2008**, *21*, 596–603. [CrossRef]
48. Marhavilas, P.K.; Filippidis, M.; Koulinas, G.K.; Koulouriotis, D.E. The integration of HAZOP study with risk-matrix and the analytical-hierarchy process for identifying critical control-points and prioritizing risks in industry—A case study. *J. Loss Prev. Process Ind.* **2019**, *62*, 103981. [CrossRef]
49. Zio, E. The future of risk assessment. *Reliab. Eng. Syst. Saf.* **2018**, *177*, 176–190. [CrossRef]
50. Marhavilas, P.K.; Koulouriotis, D.E. A combined usage of stochastic and quantitative risk assessment methods in the worksites: Application on an electric power provider. *Reliab. Eng. Syst. Saf.* **2012**, *97*, 36–46. [CrossRef]
51. Marhavilas, P.K.; Koulouriotis, D.E.; Spartalis, S.H. Harmonic analysis of occupational-accident time-series as a part of the quantified risk evaluation in worksites: Application on electric power industry and construction sector. *Reliab. Eng. Syst. Saf.* **2013**, *112*, 8–25. [CrossRef]
52. Marhavilas, P.K.; Tegas, M.G.; Koulinas, G.K.; Koulouriotis, D.E. A joint stochastic/deterministic process with multi-objective decision making risk-assessment framework for sustainable constructions engineering projects—A case study. *Sustainability* **2020**, *12*, 4280. [CrossRef]
53. Sanjaya, I.G.A.S.; Sasmita, G.M.A.; Arsa, D.M.S. Information technology risk management using ISO 31000 based on ISSAF framework penetration testing (case study: Election commission of X city). *Int. J. Comput. Netw. Inf. Secur.* **2020**, *12*, 30–40. [CrossRef]

54. Parviainen, T.; Goerlandt, F.; Helle, I.; Haapasaari, P.; Kuikka, S. Implementing Bayesian networks for ISO 31000: 2018-based maritime oil spill risk management: State-of-art, implementation benefits and challenges, and future research directions. *J. Environ. Manag.* **2021**, *278*, 111520. [CrossRef]
55. Govender, D. The use of the risk management model ISO 31000 by private security companies in South Africa. *Secur. J.* **2019**, *32*, 218–235. [CrossRef]
56. Rampini, G.H.S.; Takia, H.; Berssaneti, F.T. Critical success factors of risk management with the advent of ISO 31000 2018-Descriptive and content analyzes. *Procedia Manuf.* **2019**, *39*, 894–903. [CrossRef]
57. Barafort, B.; Mesquida, A.L.; Mas, A. ISO 31000-based integrated risk management process assessment model for IT organizations. *J. Softw. Evol. Process* **2019**, *31*, e1984. [CrossRef]
58. BahooToroody, F.; Khalaj, S.; Leoni, L.; De Carlo, F.; Di Bona, G.; Forcina, A. Reliability estimation of reinforced slopes to prioritize maintenance actions. *Int. J. Environ. Res. Public Health* **2021**, *18*, 373. [CrossRef] [PubMed]
59. Di Bona, G.; Forcina, A.; Falcone, D.; Silvestri, L. Critical risks method (CRM): A new safety allocation approach for a critical infrastructure. *Sustainability* **2020**, *12*, 4949. [CrossRef]