sustainability

MDPI

Article

The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector

Fotis Kitsios *, Elpiniki Chatzidimitriou and Maria Kamariotou

Department of Applied Informatics, University of Macedonia, 54636 Thessaloniki, Greece; elpinikichatz@gmail.com (E.C.); mkamariotou@uom.edu.gr (M.K.)
* Correspondence: kitsios@uom.gr

Abstract: In order to handle their regulatory and legal responsibilities and to retain trustworthy strategic partnerships, enterprises need to be dedicated to guaranteeing the privacy, accessibility, and authenticity of the data at their disposal. Companies can become more resilient in the face of information security threats and cyberattacks by effectively integrating security strategies. The goal of this article is to describe a plan that a corporation has implemented in the information technology industry in order to ensure compliance with International Organization for Standardization (ISO) 27001. This research demonstrates an examination of the reasons that force enterprises to make a investment in ISO 27001 in addition to the incentives that might be acquired from having undergone this process. In addition, the research examines the reasons that push firms to make an investment in ISO 27001. More particularly, the research investigates an international IT consulting services institution that is responsible for the implementation of large-scale business assistance insertion and projects. It demonstrates the risk management framework and the administrative structure of the appropriate situations so that its procedures are adequate and also in line with the guidelines founded by ISO 27001. In conclusion, it discusses the problems and difficulties that were experienced.

Keywords: strategy; ISO 27001; information security; IT sector; impact assessment

Citation: Kitsios, F.; Chatzidimitriou, E.; Kamariotou, M. The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. *Sustainability* **2023**, *15*, 5828. https://doi.org/10.3390/su15075828

Academic Editors: Zubair Baig and Fabrizio D'Ascenzo

Received: 30 November 2022
Revised: 1 March 2023
Accepted: 27 March 2023
Published: 27 March 2023

1. Introduction

Information has always been one of the most valuable assets for any firm, and it is imperative that this asset be safeguarded. To facilitate retrieval and reduce the amount of time spent on preservation, the majority of the world's information is now kept in electronic form and can be seen online. Nevertheless, this does have drawbacks; based on how important the information is, it may be vulnerable to a variety of hazards and threats [1,2]. Over the course of recent years, there has been an uptick in the number of cyberattacks targeting sensitive or confidential information. The expansion of a firm might make it a more desirable target for cyberattacks, and the accidental disclosure of confidential material can be detrimental to the company's image, income, and dependability [3–5]. In light of everything that has been discussed thus far, formulating strategies for data security is absolutely necessary in order to both bring in new clients and maintain relationships with existing ones.

The International Organization for Standardization (ISO) 27001 is a managerial system that identifies, evaluates, and locates coping strategies for any immediate danger. It can offer direction to a corporation so that it can effectively create an information security strategy depending on the specifications of the company. When a corporation decides to execute an information security strategy, it must first build its own strategy to better deal with information security risks and threats, and it must also ensure the stability of an information security strategy that conforms to ISO 27001. The specification does not detail any particular processes that must be followed in order to realize the conditions; rather, these procedures must be installed and carried out in accordance with company-specific guidelines [6,7].

The body of academic research on the subject presents a number of distinct methodologies that can be utilized by businesses to create and carry out an information security plan. A conceptual model of "Institute XYZ" was presented by Putra et al. (2017) [8] to help identify key risk factors. By referencing ISO 27005, they implemented the NIST SP 800-30 version. The group concluded that ISO 27005 could perhaps be used in conjunction with alternative recommendations, such as one that includes an "incident risk scenario" [8]. Agrawal (2017) [9] also presented a framework for ISO 27005 that may be used to locate records that pertain to risky organizational processes. A case study of a health clinic served as the basis for classifying the data. Syreyshchikova et al. (2019) [10] demonstrated how to establish, implement, and execute the information security method in accordance with the requirements of ISO 27001 for the conditions of the industrial firm JSC "K". The procedure that was utilized to create an information security plan that was in accordance with ISO 27001 was detailed in the article that was cited before.

Even if there are many various strategies that may be used to successfully integrate an information security strategy in a company, the end goal remains the same: to maintain data protection and find the ideal solution that meets the requirements of the firm [11–13]. In addition, conducting a risk assessment is one of the aspects of the process of developing a strategy for the protection of sensitive firm information that takes up the most time. It is necessary to recognize, evaluate, and categorize all of the potential dangers. Since each business is unique, the dangers that it faces are likely to be diverse as well, and there is not a single method of risk assessment that can be applied to all businesses [14].

Nowadays knowledge has evolved into a highly valuable asset for businesses, and as such, it must be protected in a manner similar to that of other essential assets. In point of fact, information ought to be sufficiently safeguarded in a manner independent of its layout and the mode in which it is transmitted. The predominant objective of information security is to adequately protect information from unsanctioned entry, utilization, disclaimer, disturbance, amendment, and obliteration. This is accomplished by encrypting, authenticating, and authorizing access to the information [15–17].

Companies place a high priority on the integration of information security controls such as those outlined in ISO/IEC 27002 in order to ensure the consistency of their operations, minimize the risk of possible danger, and achieve the maximum investment return and number of business possibilities. Particularly important to businesses that deal in information technology is the protection of sensitive data. The integration of ISO/IEC 27000 as a security standard is being demanded by a sizeable portion of the information technology businesses that have participated in or are currently taking part in a process enhancement scheme in accordance with ISO/IEC 15504 [15–17].

It is essential to appropriately designate and proficiently incorporate the requisite security controls among all of the controls proffered by the ISO/IEC 27002 benchmark in order to guide IT organizations implicated in procedure quality improvement as per ISO/IEC 15504 in the implementation of the ISO/IEC 27000 benchmark, even acquiring a credential against ISO/IEC 27001 [15–17]. In order to do this, it is necessary to adequately specify and proficiently enforce the suitable security controls.

To achieve this goal, it is essential to incorporate extensive research studies as well as supplemental propositions regarding the integration of an information security program in a company. This is necessary so that each corporation or relevant party can have direct exposure to all of this data and use it for its objectives. This article will develop a plan that a corporation in the information technology industry has been implementing in order to ensure compliance with ISO 27001, and its goal is to accomplish this purpose.

The policy of the organization makes certain that the information it manages, whether in physical or digital copy form, is appropriately protected to defend against the repercussions of breaches of privacy, failures of authenticity, or impediments to the usability of that data. The business had already established a significant number of procedures. Nevertheless, the vast majority of them were not recorded on a consistent basis or at all.

To put it another way, a significant portion of the dangers were not located, and hence, they were not taken into account. The lightning-fast expansion of the company made it clear that a uniform information security model has the potential to improve the functionality of some parts of the business. In addition to this, it turned out to be obvious that the firm's rapid expansion would make it a target. In light of this, the company decided to make the development of a more comprehensive and stringent information security policy one of its primary priorities. In a rapidly expanding company, the traditional approach to processing information security could not be maintained. As the number of employees at the company increases, the potential for errors caused by humans also increases. At the end of the day, clients from all walks of life continued asking the same query: "Why should we trust our information with you?" Offering clients well-documented data has become more challenging over time. Additionally, customers' tolerance for risk in data security declined, making it difficult for the information security team to match customers' expectations.

2. Theoretical Background

2.1. ISO 27000: 27001, 27002

Within the context of the organization, ISO/IEC 27001:2013 presents itself as the standard that specifies the requirements for establishing, implementing, maintaining, and continually developing an information security strategy. In addition to that, it incorporates necessary circumstances that are customized to meet the expectations of the company for the evaluation and management of data security threats. These prerequisites are essential for ensuring that information security risks are effectively mitigated. The conditions that are outlined in ISO/IEC 27001:2013 are non-specific, which means that it is expected that they will apply to all organizations, regardless of the type, size, or nature of the business. It is a security standard that is held in high regard and is acknowledged on a global scale [6,7,15–17].

The guidelines for ethical behavior that are provided by the ISO 27000 standards can be used as part of an all-encompassing information security strategy. ISO 27000 contains a description and nomenclature, whereas ISO 27002 offers appropriate direction for cybersecurity actions and control mechanisms by elongating the regulations of practice for a cybersecurity program. ISO 27000 was created to provide a phraseology and synopsis of ISO 27000. ISO 17799 was rebranded as ISO 27002 at the beginning of 2007, and it is now a set of recommendations for management-level IT security administration. ISO 27002 is a benchmark for choosing universally acknowledged restrictions centered on the specific information security risk circumstances of a business or organization [6,7,15–17]. This is an important step in the process of establishing a data security strategy.

In order for a business to be awarded the ISO 27001 certification, it must first have put into place all of the protection measures specified in the standard. The names of the officials in ISO 27002 are identical to those used in Annex A of ISO 27001. For instance, control 6.1.2 in ISO 27002 is referred to as "Segregation of Duties", while in ISO 27001 it is referred to as "A.6.1.2 Segregation of Duties". The difference can be seen in the amount of specific information provided. The term "segregation of duties" encompasses a wide range of guidelines that outline how the duties of different employees should be differentiated in order to achieve higher levels of responsibility. ISO 27002 provides the tools for enterprises to embrace ISO 27001 more efficiently and with a world-wide recognized method [6–8,15–17]. It explains the constraints that need to be utilized throughout the corporation (such as clear determining factors of commitments via explicitly delineated job assertions of employees).

The controls that are highlighted in Annex A of ISO 27001 cannot be executed unless the details that are proffered in ISO 27002 are also implemented. Nevertheless, even without the organizational hierarchy provided by ISO 270001, ISO 27002 would continue to be the distant exertion of a few data intelligence officials, with no acknowledgement from the board members and no real effect on the company. These two indicators are kept apart from one another since, if they were combined into a single standard, it would have been impossible to put them into practical use due to their excessive complexity and breadth.

2.2. Benefits of ISO 27001

Velasco et al. (2018) [7], Diesch et al. (2020) [11], Hsu et al. (2016) [15], and Shojaie et al. (2016) [16] cite the following advantages of implementing ISO 27001: A company or organization that implements ISO 27001 can realize a variety of important and significant benefits. Companies are able to protect and manage their confidential data in a consistent manner by implementing ISO 27001. This is accomplished by setting up a transparent handling process for information access, control, and handling. In order to accomplish this goal, the process of handling data must be clear and managed continuously. In addition to this benefit, obtaining ISO 27001 can help a company's reputation. This can be interpreted as increased profits and market share due to the fact that customers are more likely to trust an ISO 27001-certified business with their personal information. As a result, the company gains the self-assurance and competitive edge necessary to expand their customer base. It is also important to ensure that you are in compliance with national and international regulations, such as the General Data Protection Regulation (GDPR), as well as any other applicable laws. The risk of incurring legal penalties for disclosing confidential information can lead to drawn-out legal battles as well as significant financial loss.

Any and all negative effects of data breaches are completely avoidable for a business that has achieved ISO 27001 certification. An information security incident response system that is mature and up to date should be established in accordance with the provisions of ISO 27001. This indicates that there is a system in place that will report and address any information security threats as soon as they become apparent. It is essential to identify potential cyberattacks at an early stage because they can occur on a daily basis. For instance, in the case of the data breach that occurred at Target stores, the company did not discover the breach for more than a week. If the attack had been identified earlier, it would have been less severe, and fewer customers would have been affected. An information security incident response system might be able to assist in locating the attack and countering it at an earlier stage [6,7,15–17].

In addition, a business that has been awarded the ISO certification will conduct tests on a regular basis in order to identify any potential vulnerabilities in the system in advance of an actual attack. Finding security flaws in a system in advance of an actual attack gives the company valuable time to get itself ready for any possible data breach scenario. Last but not least, an organization seeking ISO 27001 certification needs to have a disaster recovery plan in place. This would be activated in the event of an emergency, which is another way of saying after an assault has already taken place. It is essential to have a strategy in place to follow in order to recover after an assault. If a company is able to continue operating as usual as soon as it is safe to do so, the losses that were sustained as a result of the attack will be minimal. Each day that a corporation is not functioning costs a substantial amount of money, which is linked to its revenue and operations [14,18–20].

2.3. ISO 27001: Risk Assessment

According to Cavusoglu et al. (2015) [21], within the context of information security, a well-structured, insured, and bonded intent provides corporate executives with a set of guidelines under which they can justify the funding of data security within their corporations. When making decisions regarding investments, companies should take into account both the financial and the non-financial repercussions. It is feasible to carry out evaluations of the commercial feasibility of regulation with reference both to the valuation of the assets that will be shielded by the regulation and the value of the assets when financial requirements are met, along with a return on investment (ROI). Circumstances that are not associated with economics include a prominence on the operational and organizational feasibility of the company as well as collaboration from the target market. The research that has been conducted on organizations and management also indicates that having a clearly defined purpose for investment appraisal is an essential component of the progression processes that result in overall organizational conformity and change. This view can be found in a number of different articles [20–23].

The word "risk" is both the focus of this discussion and the solution to the aforementioned problems, and risk management is the process that determines which concerns take priority. In accordance with the requirements of ISO/IEC 27001:2013, an information security strategy protects the confidentiality, authenticity, and availability of data through the implementation of a risk management process that demonstrates to all parties involved that potential dangers are being adequately addressed. The analysis and interpretation of risk are performed with the help of a tool called risk assessment. It is the process of being aware of and assessing the vulnerabilities that exist within the organization [24–27]. In order to accomplish this, defining an assessment scope and protocol, conducting data collection and analysis, and reading through a contingency assessment are all necessary steps. The data concerning the risks should be gathered and analyzed by the implementation team. In order to accomplish this, it is necessary to identify all assets, risks, vulnerabilities, guarantees, significance, remnants, and the possibility of malicious activities [28–30].

When conducting a risk assessment, it is important not to just focus on the problems that already exist but to also think about the problems that might arise in the future by taking into account innovative systems and inventions, both those that already exist and those that have not been invented yet [31–34]. In-depth knowledge of the organization and its functions can also be gained through the process of implementing the risk assessment. The risk assessment team endeavors to gain an understanding of the ways in which systems and procedures interact [28,35–37], which enables the company to identify any loopholes in its procedures. It is worth noting, however, that the participants who will be in violation of operating the process of risk assessment need to have an extensive understanding of the entire company in addition to a concise, wider perspective on it. This is one of the most crucial elements of these roles.

The next step is risk management, which involves the classification and provision of effective controls to ameliorate risk to a level that is acceptable to the organization [29,30]. This step comes after the step of risk assessment, which is the initial step. When it comes to risk assessment, ISO 27001 does not include an exclamatory point or a mandatory framework that must be adhered to in the same way that it does for the other aspects of the standard. An impact assessment that is appropriate for the structure of the organization can be carried out by personnel that specialize in data security.

According to clause 6.1.2 of ISO 27001, a risk assessment is what sets up and retains information security risk requirements, generates consistent, precise, and positional results, and designates, interprets, and appraises risks in cooperation with the risk owners.

The following procedures may be performed as part of the risk assessment: identification of potential dangers, categorization of how likely it is that a threat will materialize with respect to a given entity, confirmation of the impact, which usually includes upcoming expenditures, structural failure, and recovery expenses, and reduction in losses by combining risk management into preexisting business processes [8].

2.4. ISO 31000: Risk Management

The International Organization for Standardization (ISO) has established a range of global standards for the application of strategic practice guidelines, one of which is the ISO 31000 Risk Management Standard. These risk management standards are a series of global standards. ISO 31000, like the vast majority of other ISO management standards, creates a systematic approach with the goal of meeting the requirements of businesses ranging in size and nature [38]. In addition, it has been recommended that the standard ISO 31000:2018 be utilized as an appropriate basis for interacting with ambiguity when identifying hazards in industrial activities. This is one of the suggestions that have been put forward. Recently, the ISO 31000:2018 risk management framework has been proposed as a viable establishment for the goal of conducting an in-depth inquiry into risk management. This investigation is intended to take place in order to better understand risk management. In spite of the fact that respondents in the industry are the primary users of the benchmark, the fact that it is adaptable and has no business or industry specificity makes it an appealing option. In

ISO 31000:2018, the concept of risk differs from the variety of adverse classifications used in conventional predisposing evaluation in the sense that risk is not simply characterized in light of the probability of adverse or disfavored effects; rather, the emphasis is put on risk management. This is because risk is not simply characterized in light of the likelihood of negative or unfavorable impacts. This is a significant distinction between the ISO 31000:2018 risk definition and other risk definitions [39].

In accordance with the recommendations of ISO 31000:2018, risk management is a progressive procedure that includes the following actions: (1) the classification of the purview, connotation, and requirements; (2) the risk assessment, which includes the identification, analysis, and assessment of the risks; (3) the treatment of risks; (4) the collection and reporting of data; (5) the reviewing and monitoring of risks; and (6) communication and collaboration [38,39]. The ISO 31000 benchmark separates the risk management program from the risk management principles and guiding principles used by an organization to manage its risks. The framework of the risk management system consists of these three parts. The foundations and institutional arrangements for developing, integrating, measuring, evaluating, and improving risk management across the enterprise are laid by the full suite of elements in risk management. ISO 31000 is a risk management framework that is sometimes referred to as a risk management standard. ISO 31000 is one example of such a framework. The terms "risk management" and "risk assessment" are often used interchangeably when discussing the process of communicating, consulting, establishing context, and identifying, assessing, evaluating, treating, monitoring, and reviewing risk inside an organization. What is commonly referred to as "risk management" [40] is actually a procedure whose primary goal is to deal with dangers.

The International Organization for Standardization (ISO) 31000 lays out the fundamental principles, a framework, and methods. Its goal is to define the risk management process in any specific firm, including security, rather than to enforce uniformity on risk management systems. Regardless of the size or nature of the organization, it provides businesses with risk management standards that can be put to use in the process of formulating and achieving their goals. The concepts, framework, and procedures can be applied to public as well as private organizations, as well as any and all varieties of groups, associations, and businesses. It lays the groundwork for a standardized method of risk management that is not specific to either the industry or the sector. The approach known as "risk management" can be utilized to mitigate virtually any type of risk. It is applicable throughout the entirety of an organization's existence and to any activity, including decision-making at all levels [40–42].

When risk management is incorporated into an organization's business plan, managing the company requires a multi-faceted approach that includes risk reduction, risk anticipation, and risk management. As a consequence of this, businesses frequently consult the ISO 31000 standard for guidance when completing this endeavor. It is possible to use ISO 31000 in order to make strategic decisions at the organizational level, as well as in order to manage procedures, transactions, initiatives, schemes, commodities, facilities, and investments [40,41].

3. Case Study Description

3.1. A Case Study Illustrating the Implementation of ISO 27001 in an Information Technology Company

The name of the company is abbreviated to XYZ to avoid any security breaches. By utilizing software and services, XYZ is able to both automate and optimize data-driven business processes. Its consulting practices are among the most well-known in the entire world, and it holds the position of global market leader for a well-known platform.

The XYZ industry experts have comprehensive knowledge of the industry across a wide range of companies and verticals. The company is aware of how challenging it can be to implement new systems into an existing business, and as a result, it collaborates carefully with the customers' business and IT specialists in order to assist those customers in recognizing their prospects and goals. After that, XYZ forms a partnership with them in order to

provide services covering the entirety of the life cycle of the project. In this capacity, XYZ effectively orchestrates all aspects of the project, beginning with the process reengineering and continuing on through the system design, development, and optimization phases. XYZ is available to evaluate the change management needs of the organization and devise the method of training that will be most effective in ensuring that the organization's employees fully accept the new processes and technologies. In the end, the company makes the shift to providing committed and long-term support for the production.

XYZ is able to provide effective software solutions for the computerization and improvement of business procedures on time and within budget because of its unique combination of know-how, solid science, and problem solving. The company's technology experts hold multiple degrees and certifications in related fields, including science and engineering. Its Solution Center has been acknowledged by the European Union as a Research and Innovation Center which has been successful in obtaining a number of research grants from the European Union. The industry's scientists and engineers have developed a number of advanced problem-solving tools that are specifically tailored to the day-to-day challenges faced by the company. Significantly, XYZ has tested and implemented these solutions on massive amounts of accurate data provided by some of the largest corporations, and as a result, the company has realized considerable and countable increases in its corporate profits. This is a very important development.

The XYZ Corporation is what is known as a "project-based" business. Technology advisers from the company are delegated to work on each project for their respective clients. The teams are fluid, and members are added to or removed from the group based on the current phase of the project and the amount of work that needs to be done. The number of people on a team can range anywhere from four to thirty.

A one-of-a-kind, custom-made concrete infrastructure is developed for every individual customer. The core of this connectivity is a comprehensive database for the source code. This code file archive enables multi-developer projects to maintain different iterations, a centralized document library, a dedicated database in a project management software, committed directories, diligent containers for both development and testing, an endeavor native app, and a differentiated admission to a time management method. The instruments and facilities that were described in the previous paragraph provide the squad with a suitable structure that supports, monitors, and delivers the project, as well as a collaborative effort base, metrics, and predictive analysis for quality assurance.

3.2. The Company's Status Prior to the Implementation of ISO

The XYZ strategy assures that the data it handles, whether in electronic or tangible copy form, is properly secured to guard against the consequences of data breaches, breakdowns of authenticity, or instabilities to the connectivity of that information. The organization already had a significant number of its processes operational. On the other hand, the vast majority of them were not recorded on a consistent basis or at all. To put it another way, a significant proportion of the dangers were not recognized, and consequently, they were not taken into account. Employees were made aware of the company's perceived policy regarding information security through the delivery of training on an annual and on-boarding basis in the subject of information security. Already, a group dedicated to the protection of sensitive information had been assembled. All of the staff members had received training, so they were able to address any questions or concerns that arose regarding the confidentiality of the information. In light of what has been stated above, the business already possessed a number of well-established procedures that would make it simpler to comply with the requirements of ISO 27001. On the other hand, a significant number of dangers and holes in security were not found.

The speedy expansion of the company made it clear that a standardized information security model has the potential to improve the functionality of certain facets of the business. In addition to this, it became abundantly clear that the company's rapid expansion would make it a target for various cyber threats. Because of this, the company set a new objective

for itself, which was to move forward with an information security policy that was more comprehensive and comprehensively enhanced. A company that was experiencing rapid expansion found that the traditional approach to processing security information was no longer viable. The increasing size of the company's workforce brings with it an increase in the likelihood of mistakes being made by employees. In the end, the business was continuously confronted with the same query from a variety of customers: "Why should we trust our information with you?" It became progressively more difficult over the course of the years to get back to the customers with evidence that was adequately documented. In addition, customers' tolerance for unpredictability in information security decreased, and the information security team was unable to satisfy customers' requirements after this development.

4. Methodology

XYZ has made the decision to implement a strategy that will bring them into compliance with ISO/IEC 27001:2013 [13,17,43,44]. Figure 1 presents the steps of the ISO/IEC 27001:2013 process. The first step in the process involves the establishment by the company of a security rule along with the pertinent measures and controls. After that, it composes a statement describing the range of its application and elaborating on the reasons why the authorities were favored over other candidates. The company is responsible for determining the assets and requirements, conducting a risk assessment, and selecting the evaluation method. The second phase involves the company actually enforcing its security policy, along with its associated procedures, controls, and management structures. The third stage of this procedure is the organization conducting an evaluation, setting initiatives, and then providing the results of these evaluations to managers. Information security is kept up and improved upon by using the final stage's preventative, prognostic, and enhancement measures [13–17].

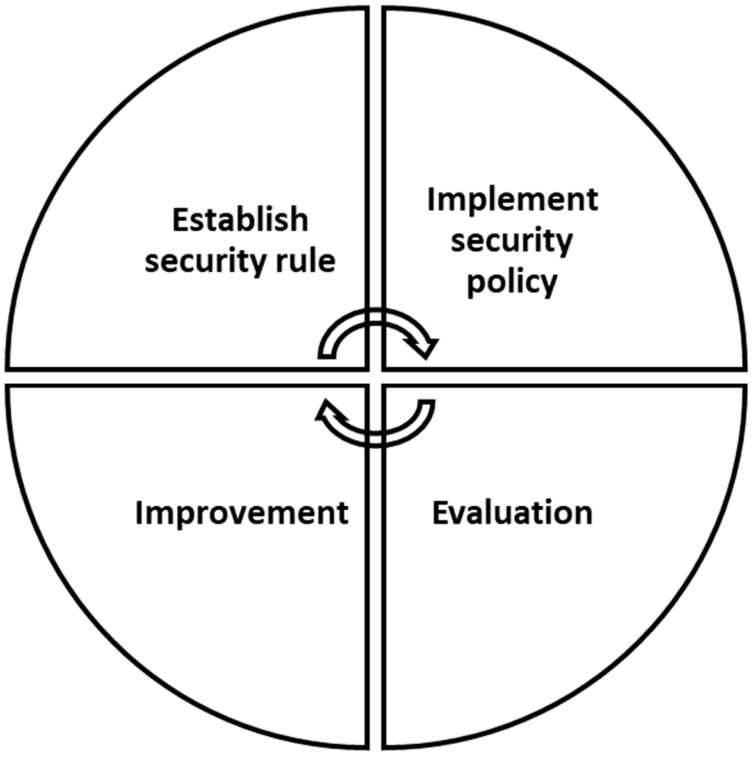

Figure 1. The process to implement ISO/IEC 27001:2013.

The potential for harm that could be caused by the exposure of weaknesses or the introduction of new dangers to the organization's information systems and assets is referred to as "risk". The process of systematically identifying, evaluating, and carrying out measures and activities with the goal of reducing levels of risk to an acceptable level is known as risk management. In the next section, we will ascertain and appraise the method of analysis for assessing and dealing with cybersecurity threats to identify a sufficient risk level regarding enhanced security benchmarks (ISO/IEC 27001:2013). Additionally, we will establish the specifications for the creation of an effective mitigation program within its connectivity.

Risk evaluation, hazard identification, and their respective assisting limits and procedures are implemented to the entirety of the XYZ establishments in regard to each and every explanatory and reputational risk to each and every investment that may be utilized inside the corporation and could have an effect on its data security. In addition, all of these procedures are supported by a set of policies and procedures. It is applicable to all data security risk evaluations carried out within the purview of its information security strategy, which includes all of its business processes and investments. The risk assessment and hazard analysis policy are applicable to all XYZ commercial enterprises (including, but not limited to, personnel, associates, consultants, the municipal delivery alliance, distributors, members of the general public, and others).

Risk analysis is a process that is included in its information security strategy. The goal of this step is to commit to the systematic monitoring, evaluation, and therapeutic interventions of risks as well as to guarantee an appropriate level of information security within the scope of the information security strategy. The goals of hazard assessment treatment modalities in the field of information technology include better risk assessment judgments, better risk evaluation, better record-keeping of threats and their evaluations, assimilation of elevated security restrictions in its data systems, and better risk assessment decisions.

XYZ provided the commercial and technological background of the data system that was being assessed, and they made sure that the business goals were obscured with all the internal and external facets that monitored the recognized risks. As part of the organizational environment, a review was conducted to determine who the owner of the information system was, the classification of the data, types of business processes that can be endorsed, types of users bolstered by the system, security protocols, and compliance regulations. In accordance with the defined context, an evaluation was undertaken on the characterization of XYZ as the relevant stakeholder in the information system. The capability of its users to perform and retain the information system, as well as the logical architecture and system elements, was also investigated.

The significance of a company's information systems and assets is investigated during a risk assessment. If the company recognizes that its assets are vulnerable to a high level of risk or if the purposes of this particular information asset are essential to the company's business desires, a thorough risk assessment will be carried out on the asset. This involves conducting exhaustive documentation and confirmation of assets, which enables an evaluation of the potential impact on the business of any security flaws or risks posed by those assets [45–48].

The hazard assessment designates, clarifies, and selects the risks that are associated with achieving the XYZ targets. It also sets out the requirements for what constitutes an effective risk management plan. The findings of the risk assessment are used to direct monitoring in the selection of suitable actions and the establishment of a suitable priority order for the management of information about potential threats and the enactment of the necessary control procedures to safeguard against these risks.

The procedure for evaluating risks involves conducting a comprehensive analysis of the risk scale (risk analysis), followed by a method that compares the risk to the risk conditions in order to establish the relative significance of the risks (risk assessment). The risk assessment is carried out on a regular basis so that adjustments can be made to account

for shifting safety preconditions and risk conditions (e.g., assets, threats, susceptibilities, effects, and other essential changes). It is carried out in a methodical manner and is capable of producing results that are comparable to one another and can be replicated multiple times, with the quantity of times depending on the component and degree of significance of XYZ or the information systems that are being investigated.

A risk assessment involves carrying out with connectivity to and a comprehension of its business operations, the hazards implications on its business assets, the technological structures in place to promote the business needs, the regulatory frameworks to which XYZ is subordinate, and up-to-date uncertainty and hazard evaluations. After the launch of a new information processing model, after the acquisition of a new information asset, and after any changes made to the systems or processes, a risk evaluation needs to be carried out at the very least. When there has been no review for a relatively long time, it is possible that adjustments that could alter the nature of the risks and security flaws will be necessary (e.g., after three years).

Following the completion of the risk assessment, the management of the organization was tasked with determining the most suitable risk treatment approach for each of the risks that were identified. Risks can be mitigated through the application of suitable risk control mechanisms, accepted if the circumstances and requirements for contingency planning are met, hidden by not enabling actions that could be construed as threats, or transferred from one area of the establishment to another (e.g., insurers or suppliers).

The risk judgment that includes adequate control signal transduction pathways entails selecting and putting into action control processes in a manner that is congruent with the prerequisites that are the direct result of the risk assessment. The control mechanisms that are chosen should ensure that the risks are whittled down to the bare minimum required, taking into account the restrictions of worldwide law and regulations, treaty arrangements with suppliers and customers, the business requirements and priorities of XYZ as defined above, operational requirements, regulatory requirements, and the expenses of implementing and functioning restrictions regarding the risks that are eroded and the residual risks. The identification of all of its assets is the first step in the process of risk assessment that falls under the purview of the information security strategy's scope (assets' impact on the company's information in terms of its confidentiality, integrity, and availability). Documents in either physical or electronic form, applications and databases, information technology equipment, and infrastructure are all included in the assets list.

5. Results

XYZ takes into account all of the prospective threats and risks that are pertinent to a particular system, regardless of whether they are extrinsically motivated, natural or human, unintentionally or maliciously. Information on vulnerabilities and threats is gathered from relevant users of the system, as well as, in some instances, from cybersecurity advisors, local and national law enforcement agencies, security facilities, and contacts.

The following classifications could be used to classify the risks that are associated with the organization's information systems, data, and operations: Any user of XYZ can prevent damage that is pertinent to the assets that are being examined. Documentation must be carried out on an exhaustive list of occurrences that have the potential to thwart or delay the company's business goals. It is possible that the risks that are not included in this list will not be evaluated or mitigated. After conducting related searches, potential dangers from previously discovered archives might be added. The implementation of a clear method for determining the validity was performed so that it could be regarded and analyzed. The possible effect on the association's data systems and assets must also be included in the identification of risks. During the assessment process, any possible threat that could compromise the confidentiality, authenticity, or affordability of its information systems, information, operations, or assets will be substantiated. In order to include a mutual understanding of these security precautions, which will mitigate the possible impact to

an adequate degree, assessments of risk shall be established. The impact criteria will be determined based on the damage level as well as the cost that is caused by the threat.

Activities such as hazard verification, security vulnerability classification, providing guidance, probability perseverance, performance measurement, contingency perseverance, regulating suggestions, and documenting results are the steps that lead up to the actual implementation of a risk assessment. The first activity involves determining how likely it is that a potential threat will actually materialize. The probability of an occurrence, also known as the threat level, is defined as the likelihood that an occurrence will take place. When determining the likelihood of a threat, XYZ needs to take into account the causes of the risk, potential vulnerabilities, and controls that are already in place. The second activity is an analysis of a threat to an information system, and part of that involves conducting a risk assessment of the vulnerabilities associated with the system's environment. Next, the controls that have been put in place on the system will be evaluated, and attempts will be made to reduce or eliminate the likelihood and probability of a threat that results from a vulnerability in the system. During the fourth activity, XYZ is required to take into consideration the following important aspects: visibility (to nature's malicious attacker), the existence of current controls, and the efficiency of those controls. The probability of a threat occurrence is input, and the threat level and the susceptibility level are outputs of the probability of an event for a specific threat. The implications of a security event could be defined in terms of a breach of data, decency, and accessibility in the fifth activity. After that, the values of the likelihood of an event occurring and its impact are combined in order to arrive at an estimate of the risk level posed by each asset in relation to an identified threat. When determining the level of risk associated with the project, we will also take into account how well its planned and existing security controls work. During the seventh activity, the security controls that could mitigate or even eliminate the risks that were identified were aligned with the operations of the company. The risk level ought to be maintained at a manageable level if the recommended controls are to be effective. When everything is said and done, a formal report will be compiled with the findings of the risk assessment after it has been completed. Figure 2 presents a flowchart of the activities carried out during the risk assessment process.

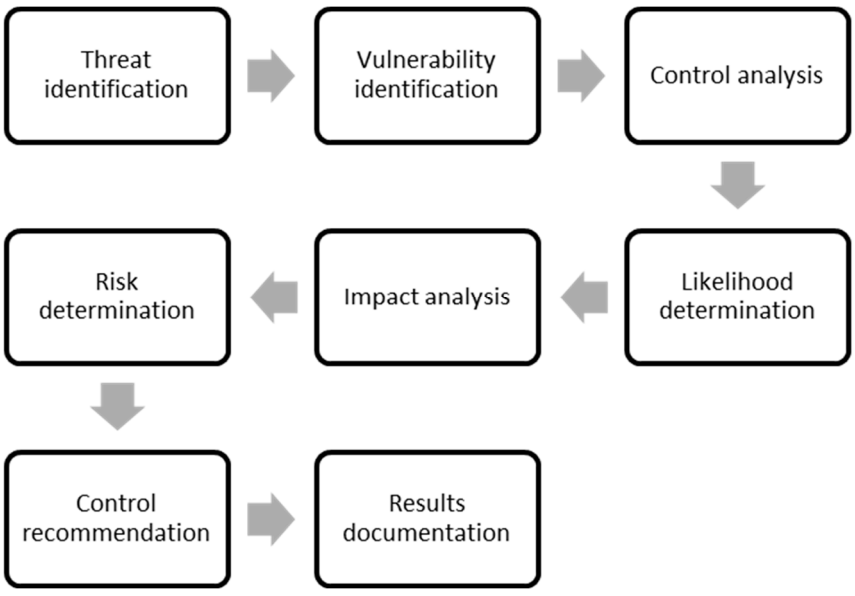

Figure 2. A flowchart of the activities carried out during the risk assessment process (source: the authors).

The levels of risk are being evaluated using the predefined criteria, and the appropriate actions are going to be taken. In the event that there is a risk, it is necessary to conduct an analysis of the pertinent consequences for each vulnerability and threat that pertains specifically to an individual asset. It is necessary to conduct an analysis of each of its assets to determine the likelihood of such a risk. The severity of a risk is a comprehensive evaluation that takes into account both the likelihood that an event will take place and the consequences that will result from that event if it does take place (impact occurrence). A potential vulnerability and/or threat can be described as "almost certain", "probable", "possible", "unlikely", or "rare", where "almost certain", "probable", and "possible" are the most likely outcomes. The impact of a security breach can be summed up as a loss of privacy, integrity, and accessibility. NIST SP 800-30 revision 1 was used to determine the quantification of the impact. NIST SP 800-30 Rev. 1 was also used to determine the level of risk.

A response must be determined for each identified risk. The probability of the risk occurring and its potential impact will serve as the basis for the recommendations that will be made regarding the actions that should be taken to mitigate the risk. It is necessary to determine a treatment option (security controls) in accordance with a cost-benefit analysis and the criteria that are pertinent to the impact. Its risk treatment is divided into the four levels listed below: accept, reduce, transfer, and remove. At the first level, risk acceptance ought to be reconsidered for low-priority risks for which other treatment options would incur costs that are greater than the potential impact. All risks need to include a recommendation of control(s) and alternative solutions in order to mitigate the risk that has been identified. XYZ has decided to take the risk that has been identified. At the second level, risk mitigation entails reducing the likelihood of risk threats and vulnerabilities, as well as the effects of those vulnerabilities and threats. It is always more efficient to take preventative measures against risk than to repair the damage that was caused by a risk that was identified. XYZ will be responsible for the planning and design of any future controls to address the identified issues. At the third level, factors that increase include reducing the detrimental impact of a hazard or frailty. The elimination of a risk by transmitting it to a third party, such as a supplier, will not eliminate the underlying vulnerability or threat. The management of the risk that is associated with this endeavor will be handled by a different entity. XYZ will compile a list of all possible avenues for transferring the risks that have been identified to other organizations (e.g., insurance). Changing components of the overall business processes or the architecture of the system is what is involved in the final stage of risk avoidance. This is performed in order to remove the threat. Eliminate the possibility of negative outcomes by putting a stop to the associated commercial activity.

For the purpose of mitigating the risks that have been identified and minimizing the potential impact on its information systems, appropriate control objectives have been selected. The selection and/or design of security controls is conducted in accordance with the guidelines found in the Annex of ISO/IEC 27001:2013. This is performed to guarantee that none of the controls have been overlooked. Documentation can be found pertaining to the rules that were chosen for each of the threats.

It is essential to handle and mitigate the risks associated with the requisite mitigation actions, so a risk treatment plan is developed. A risk treatment plan is devised with the intention of lessening the threats that critical XYZ assets are exposed to. Any possible threat that might emerge as a result of the risks and vulnerabilities that have been identified is dealt with according to the level of its consequence.

6. Discussion

During the stage of the implementation, a variety of challenges were encountered. The company had no choice but to delegate the responsibility of implementing an information security strategy to its available resources. Skilled employees who have an in-depth understanding of the organization's structure and operations should be the resources that manage and implement the information security strategy. This responsibility should fall to

the resources, not the company. It was decided that the Director of Development would take on the responsibilities of the Chief Information Security Officer (CISO), while the Operations Manager would be responsible for developing an information security strategy. The problem was that these two resources already had tasks assigned to them, which meant that an entirely new restructuring needed to take place and new employees needed to be hired to support the functions that were left behind. The company incurred an additional expense as a result of this.

After the organization began executing the adjustments to safeguard the information and enable access to it exclusively for the project team members, the process became significantly more complicated every time a resource was required to join or depart a team [49–52]. When the company first started executing the changes that would make the data more secure and facilitate only internal stakeholders' entry to it, that's when the diversification was developed. The procedure requires a lot of time and opens the door to the possibility of making mistakes. In order to overcome this obstacle, the company has tasked a separate development team with the task of creating a new product that is capable of fully automating all of the processes that are associated with access management. The company incurred an additional expense as a result of this.

For the implementation of ISO 27001 to be successful, it is necessary for employees to provide their full support and contributions [53–56]. There were some obstacles encountered while putting ISO 27001 into effect. To assure the success of the information security plan and to earn the support of the workforce, it was essential to tackle these obstacles. To be more specific, workers felt as though they had pushed themselves to the limit since they expected their work to be rigorously examined. They feared it would take too much time and effort to implement all of the information security policy and practice changes that were proposed. The deadlines that were set for employees to review the pertinent documentation of these new policies and procedures were another source of unease for workers. Because only a select few people were involved in the initial stages of the ISO 27001 implementation, employees had the impression that it was both pointless and standard procedure. After participating in a number of training sessions and having casual conversations, participants finally achieved awareness of the information security strategy as well as realization of its significance.

Because the internal audit had not yet taken place (as was mentioned above), the circle representing the ISO implementation could not be considered complete. It would be interesting to have an update on how this process of becoming ISO 27001 certified ultimately plays out. What sort of conclusions will the audit bring to light? Will there be any instances that do not comply with the standards? Failure to meet specific requirements, failure to prevent a loss, failure to follow a process, and the inability to effectively interrogate a security incident are all examples of nonconformities. Nonconformities can also be categorized as failures to follow a procedure. What kinds of responses do you anticipate coming from the company?

More than eleven months and sixteen different drafts were required to finish the risk assessment and treatment. As a result, the processes within the company became more complicated, which led to a delay in conducting the audit, which was ultimately postponed. In addition, the process is a consistent source of change within an organization; as a result, it has an effect on change management in a company. This is significant because compliance with ISO 27001 is a requirement of the process. It is possible that future research will encounter all of the challenges and complexities that are associated with this distinct phase of a company's life.

The practical contribution of this paper is that it offers a strategy that can be used by professionals in the information technology industry to devise a strategy for protecting sensitive data. The productive work of these corporations and the resolution of the day-to-day challenges they face in order to stay afloat are the sole focuses of those in the information technology sector. They are frequently unable and unwilling to invest time and effort into the definition of new processes or the improvement of existing procedures.

Software engineers focus more on the commodities, facilities, or strategic planning of their companies than they do on developing innovative methods of work.

In the medium term, the requirements of ISO 27001 will have an impact on the firm's day-to-day operations, resulting in less effort and less duplication and more responsibility for implementing and maintaining the best practices the organization has determined to be most effective. In addition, this paper contributes to the discussion by saying this. Corporations require not only to be mindful of the steps to take to enhance their processes but also to have conventional guidelines that describe the work that they are required to accomplish, as well as a well-specified set of quality standards to aid in the communication of such procedures. These policies and processes ought to be clear and applicable to the kinds of projects they generally work on.

It took more than 11 months and 16 different versions to finish the risk assessment and treatment for this paper, which is one of the paper's limitations. As a consequence of this, researchers in the future will be able to assess the level of impact and likelihood posed by each asset for each risk. When the risk level is greater than the risk limit, XYZ will review all of the controls that are in place. A new risk level review is going to be carried out, and a risk treatment action is going to be evaluated with reference to the new risk level. Documentation of the treatment choice needs to be performed for each identified risk.

In addition, future researchers can learn more by consulting with experts in the fields of information security and risk management, as well as by performing literature studies. There could be ISO 27005-based information objects that are not included in this work. The description of risks can help businesses determine the possibility and impact of threats to their information security plan. In addition, a company's information security policy may call for the implementation of supplementary technologies in light of the specific threats and vulnerabilities it faces. However, for those individuals who are a part of an organization's evaluation process for information security strategy and decision-making, this article can serve as a starting point for further research and discussion.

There is only one case study included, which is another limitation; selecting cases from a wider spectrum of companies may have supplied more compelling evidence for the classification of detailed guidance enclosed in the information security strategy. Taking into consideration the knowledge gained from its implementation by a greater number of software developers will provide professionals in the information technology sector with helpful regulations.

7. Conclusions

This paper described the approach taken by an IT firm to meet the requirements of ISO 27001. This article looked at how an ISO 27001-certified firm handles practices such as documenting everything, making certain that it is up-to-date, and assessing risks to information security.

Due to the fact that conducting a risk assessment is one of the most time-consuming and crucial steps involved in developing an information security strategy for a company, it is imperative that each and every potential risk be identified. The risks are unique to each company, but the end goal is the same: to safeguard the data and find the best possible solution that meets all of the requirements of the business. The corporation already had a significant number of its procedures operational. However, the vast majority of them were not documented on a regular basis or at all.

To put it another way, a significant portion of the dangers were not recognized, and consequently, they were not taken into account. In addition, the speedy expansion of the company made it clear that a streamlined information security model has the potential to improve the functionality of certain business operations. In addition, it turned out to be obvious that the company's rapid expansion would make it a target of cyberattacks. In light of this, the company decided to make the development of a more comprehensive and stringent information security policy one of its primary priorities. In a rapidly expanding company, the traditional approach to accessing information security could not be maintained. As

the number of employees at the company increases, the potential for errors caused by humans also increases. In the end, the business kept getting the same question from a variety of customers, and that question was, "Why should we trust our information with you?" Over the course of the years, providing clients with evidence that was adequately recorded became an increasingly difficult task. Additionally, customers developed a lower tolerance for ambiguity regarding information security, and the information security team was unable to meet the customers' demands as a result. As a result, the lengthy process of implementing ISO 27001 in the company finally culminated. Nevertheless, the process of risk assessment is not static, and it will need to be carried out multiple times.

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. 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.
16. 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.

17. 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]
18. Topa, I.; Karyda, M. From theory to practice: Guidelines for enhancing information security management. *Inf. Comput. Secur.* **2019**, *27*, 326–342. [CrossRef]
19. Leszczyna, R. A review of standards with cybersecurity requirements for smart grid. *Comput. Secur.* **2018**, *77*, 262–276. [CrossRef]
20. 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]
21. 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]
22. 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]
23. Haqaf, H.; Koyuncu, M. Understanding key skills for information security managers. *Int. J. Inf. Manag.* **2018**, *43*, 165–172. [CrossRef]
24. 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]
25. 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]
26. 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]
27. 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]
28. Eling, M.; Wirfs, J. What are the actual costs of cyber risk events? *Eur. J. Oper. Res.* **2019**, *272*, 1109–1119. [CrossRef]
29. 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]
30. Karanja, E. The role of the chief information security officer in the management of IT security. *Inf. Comput. Secur.* **2017**, *25*, 300–329. [CrossRef]
31. 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]
32. 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]
33. 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]
34. Zio, E. The future of risk assessment. *Reliab. Eng. Syst. Saf.* **2018**, *177*, 176–190. [CrossRef]
35. 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]
36. 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]
37. 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]
38. 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]
39. 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]
40. 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]
41. 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]
42. 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*, 1–15. [CrossRef]

43. 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]
44. 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]
45. Ali, R.F.; Dominic, P.D.D.; Ali, S.E.A.; Rehman, M.; Sohail, A. Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. *Appl. Sci.* **2021**, *11*, 3383. [CrossRef]
46. Chu, A.M.; So, M.K. Organizational information security management for sustainable information systems: An unethical employee information security behavior perspective. *Sustainability* **2020**, *12*, 3163. [CrossRef]
47. Dospinescu, O.; Dospinescu, N. The use of information technology toward the ethics of food safety. *Ecoforum J.* **2018**, *7*, 1–11.
48. Allhoff, F.; Henschke, A. The internet of things: Foundational ethical issues. *Internet Things* **2018**, *1*, 55–66. [CrossRef]
49. Kitsios, F.; Kamariotou, M. Information Systems Strategy and Strategy-as-Practice: Planning Evaluation in SMEs. In Proceedings of the Americas Conference on Information Systems (AMCIS2019), Cancun, Mexico, 15–17 August 2019; pp. 1–10.
50. Kitsios, F.; Kamariotou, M. Decision Support Systems and Strategic Information Systems Planning for Strategy Implementation. In *Strategic Innovative Marketing; Springer Proceedings in Business and Economics*; Kavoura, A., Sakas, D., Tomaras, P., Eds.; Springer: Cham, Switzerland, 2017; pp. 327–332.
51. Kamariotou, M.; Kitsios, F. Critical Factors of Strategic Information Systems Planning Phases in SMEs. In *Information Systems; EMCIS 2018; Springer LNBIP 341*; Themistocleous, M., Rupino da Cunha, P., Eds.; Springer Nature: Cham, Switzerland, 2019; pp. 503–517.
52. Kamariotou, M.; Kitsios, F. An empirical evaluation of strategic information systems planning phases in SMEs: Determinants of effectiveness. In Proceedings of the 6th International Symposium and 28th National Conference on Operational Research, Thessaloniki, Greece, 8–10 June 2017; pp. 67–72.
53. Podrecca, M.; Culot, G.; Nassimbeni, G.; Sartor, M. Information security and value creation: The performance implications of ISO/IEC 27001. *Comput. Ind.* **2022**, *142*, 103744. [CrossRef]
54. Legowo, N.; Juhartoyo, Y. Risk Management; Risk Assessment of Information Technology Security System at Bank Using ISO 27001. *J. Syst. Manag. Sci.* **2022**, *12*, 181–199.
55. Mirtsch, M.; Kinne, J.; Blind, K. Exploring the adoption of the international information security management system standard ISO/IEC 27001: A web mining-based analysis. *IEEE Trans. Eng. Manag.* **2021**, *68*, 87–100. [CrossRef]
56. Culot, G.; Nassimbeni, G.; Podrecca, M.; Sartor, M. The ISO/IEC 27001 information security management standard: Literature review and theory-based research agenda. *TQM J.* **2021**, *33*, 76–105. [CrossRef]