# Impact Assessment in Information Security Management Systems

Subjects: Computer Science, Information Systems
Contributor: Fotis Kitsios

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.

Keywords: information security management system (ISMS) ; ISO 27001 ; impact assessment

## 1. Information Security Management Systems and Benefits

According to Haufe et al. (2016) [1], information security is considered a subset of IT governance. Based on this statement, here 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 [2]. This is where an ISMS comes in handy. However, what is the purpose of an Information security management systems (ISMSs)?

In the literature, there are several discussions on the purpose of ISMS. Diesch et al. (2020) [3] and Paananen et al. (2020) [4] 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) [5], 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, 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 [4][6][7][8].

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 [1][9]. 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 [10][11]. 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 [12]. 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 [13][14][15][16][17][18]. 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 [19]. 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 [20][21][22][23][24][25].

Although all participants are affected by security incidents, at the same time, to rephrase [26], employees do not realize the importance of a company's data confidentiality, and they do not take actions needed to reassure that no breach will occur. Although corporations, organizations, and companies 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) [27], Diesch et al. (2020) [3], Hsu et al. (2016) [28], and Shojaie et al. (2016) [29], 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 [30][27][6][28][29].

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 [31][11][12][32].

## 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 [30][27][6][28][29].

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 [30][27][6][28][29].

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 [30][27][6][28][29].

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.

## 3. ISO 27001: Risk Assessment

According to Cavusoglu et al. (2015) [19], 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 [19][23][32][33].

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 [34][35][36][37]. 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 [22][38][39].

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 [40][41][42][43]. 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 [22][44][45][46], 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 [38][39]. 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 [47].

## 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 [48]. 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 [49].

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 [48][49]. 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 [50].

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 [50][51][52].

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 [50][51].

## References


1. Haufe, K.; Colomo-Palacios, R.; Dzombeta, S.; Brandis, K.; Stantchev, V. Security management standards: A mapping. Procedia Comput. Sci. 2016, 100, 755–761.
2. 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.
3. Diesch, R.; Pfaff, M.; Krcmar, H. A comprehensive model of information security factors for decision-makers. Comput. Secur. 2020, 92, 101747.
4. Paananen, H.; Lapke, M.; Siponen, M. State of the art in information security policy development. Comput. Secur. 2020, 88, 101608.

5. Von Solms, R.; Van Niekerk, J. From information security to cyber security. Comput. Secur. 2013, 38, 97–102.
6. 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.
7. 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.
8. 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.
9. 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.
10. 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.
11. Topa, I.; Karyda, M. From theory to practice: Guidelines for enhancing information security management. Inf. Comput. Secur. 2019, 27, 326–342.
12. Leszczyna, R. A review of standards with cybersecurity requirements for smart grid. Comput. Secur. 2018, 77, 262–276.
13. Kitsios, F.; Kamariotou, M.; Talias, M. corporate sustainability strategies and decision support methods: A bibliometric analysis. Sustainability 2020, 12, 521.
14. 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.
15. 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.
16. Kitsios, F.; Kamariotou, M. Information systems strategy and innovation: Analyzing perceptions using MCDA. IEEE Trans. Eng. Manag. 2021; in press.
17. Kitsios, F.; Kamariotou, M. Artificial intelligence and business strategy towards digital transformation: A research agenda. Sustainability 2021, 13, 2025.
18. 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.
19. 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.
20. 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.
21. 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.
22. Eling, M.; Wirfs, J. What are the actual costs of cyber risk events? Eur. J. Oper. Res. 2019, 272, 1109–1119.
23. 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.
24. Michel, A.; Oded, J.; Shaked, I. Do security breaches matter? The shareholder puzzle. Eur. Financ. Manag. 2020, 26, 288–315.
25. 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.
26. 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.
27. 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.
28. 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.

29. 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.
30. Disterer, G. ISO/IEC 27000, 27001 and 27002 for Information Security Management. J. Inf. Secur. 2013, 4, 92–100.
31. 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.
32. 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.
33. Haqaf, H.; Koyuncu, M. Understanding key skills for information security managers. Int. J. Inf. Manag. 2018, 43, 165–172.
34. 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.
35. 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.
36. 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.
37. 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.
38. 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.
39. Karanja, E. The role of the chief information security officer in the management of IT security. Inf. Comput. Secur. 2017, 25, 300–329.
40. 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.
41. 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.
42. 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.
43. Zio, E. The future of risk assessment. Reliab. Eng. Syst. Saf. 2018, 177, 176–190.
44. 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.
45. 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.
46. 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.
47. 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.
48. 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.
49. 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.

50. Govender, D. The use of the risk management model ISO 31000 by private security companies in South Africa. Secur. J. 2019, 32, 218–235.
51. 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.
52. 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.