International Journal on Advanced Science Engineering Information Technology

Vol.10 (2020) No. 3
ISSN: 2088-5334

# Adopting an ISO/IEC 27005:2011-based Risk Treatment Plan to Prevent Patients from Data Theft

Laura Cassandra Hamit[a], Haslina Md. Sarkan[b,1], Nurulhuda Firdaus Mohd Azmi[b,2], Mohd Naz'ri Mahrin[b,3], Suriayati Chuprat[b,4], Yazriwati Yahya[b,5]

[a] *Novocraft Technologies Sdn Bhd, C-23A-05, 3 Two Square, Seksyen 19, 46300 Petaling Jaya, Malaysia*
*E-mail: laura@novocraft.com*

[b] *Advanced Informatics Department, Razak Faculty of Technology & Informatics, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia*
*E-mail: [1]haslinams@utm.my; [2]huda@utm.my; [3]mdnazrim@utm.my; [4]suriayati.kl@utm.my; [5]yazriwati.kl@utm.my*

***Abstract*— The concern raised in late 2017 regarding 46.2 million mobile device subscriber's data breach had the Malaysian police started an investigation looking for the source of the leak. Data security is very important to protect the assets or information by providing its confidentiality, integrity, and availability not only in the telecommunication industry but also in other sectors. This paper attempts to protect the data of a patient-based clinical system by producing a risk treatment plan for its software products. The existing system is vulnerable to information theft, insecure databases, poor audit login, and password management. The information security risk assessment consisting of identifying risks, analyzing, and evaluating them were conducted before a risk assessment report is written down. A risk management framework was applied to the software development unit of the organization to countermeasure these risks. ISO/IEC 27005:2011 standard was used as the basis for the information security risk management framework. The controls from Annex A of ISO/IEC 27001:2013 were used to reduce the risks. Thirty risks have been identified, and seven high-level risks for the product have been recognized. A risk treatment plan focusing on the risks and controls has been developed for the system to reduce these risks to secure the patient's data. This will eventually enhance the information security in the software development unit and, at the same time, increase awareness among the team members concerning risks and the means to handle them.**

***Keywords*— data security; risk management; information security; ISO/IEC 27005; risk assessment plan.**

## I. INTRODUCTION

There was an uproar in late 2017 concerning the leak of 46.2 million mobile device subscriber's data. It was alleged that the data breach included more than 80,000 personal information coming from the Malaysian Medical Council, the Malaysian Medical Association, and the Malaysian Dental Association, according to Lowyat.net. Jobstreet.com also reported that private information had been compromised for subscribers who had their accounts created before 2012 [1].

The loss of such confidential information is damaging to the organization, and it can put that organization into a huge risk. Thus, information security risk management should be implemented into the organization to protect and to achieve the confidentiality, integrity, and availability (CIA) of the assets [2].

The ISO/IEC 27005:2011[3]–[7] information security risk management standard is an example of a standard that provides guidelines for information security risk management. In ISO/IEC 27005 standard, there are six risk management processes listed. They are context establishment, risk assessment, risk treatment, risk acceptance, risk communication, and risk monitoring and review.

A product at a local bioinformatics software company consists of a patient-centric system. It is vital to secure the patient's information against unauthorized disclosure of information. This information will be encrypted to protect its confidentiality and to maintain patient's information integrity, where the content of the data is guaranteed against any tampering attempts. For example, a patient report can only be signed off by an authorized physician. Having a system that is compliant to an international standard will uphold the market value of the product. Users can be assured that their data are safe and that they can use the product confidently.

The controls from Annex A of ISO/IEC 27001:2013 [8], [9] are useful in handling and helping to reduce the risks encountered. Risk treatment will reduce the risks which are not acceptable by using the controls from Annex A in ISO/IEC 27001. Another document named the Statement of Applicability (SoA), which listing all the controls needed, will be produced. It will specify which controls are applicable and which are not, plus the reason they are applicable or not applicable, the objectives to be achieved with the controls, and the description on how the controls will be implemented.

Once the SoA is done, a risk treatment plan will be produced. It contains detailed information on how the controls in the SoA are to be implemented, who will be doing what, and when. The risk treatment plan will only focus on the controls. After all the documents are ready, it is then time to implement the controls to the system.

This paper starts with a review of information security risks. The following section will elaborate on the methodology of the work, followed by the discussion in the fourth section. We will end this paper by discussing the adoption done and present our conclusions.

Information security is a significant worry in various industries. There have been cases of privacy theft that led to massive economic damages [2]. To mitigate these critical information security risks, some standards are explored and investigated, such as ISO 27000, 27001, 27002, 27003, and 27004 [4], [10]–[13]. It is necessary to counter the aftereffect of any threats to an organization by implementing information security risk measures [14].

There are a few factors that are important for us to understand before implementing our work. The is a relationship among threat, asset, vulnerability, and risk as can be seen in Fig. 1, therefore, this section deals with their relationships. The following subsections describe each item in detail.

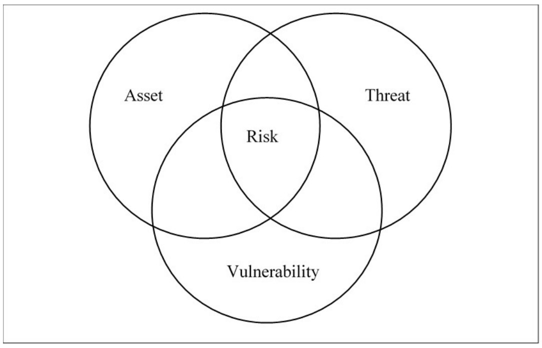

Fig. 1 The relationship among threat, asset, vulnerability and risk

### A. Threat

A threat is defined as any prospective action that can cause harm or loss to a service or product. Usually, to prevent any loss after the production phase, threats are being identified in the early stage of product development. The cost of threats removal or reducing threats late will be very high. It is a well-known fact that prevention is always better than cure [15].

It is seen as an action, a potential action, or no action which can cause harm and damage that can be divided into natural threats, human threats, and environmental threats [16], [17]. The number of human threats in security and privacy incidents is growing [18]. The human threats can be further categorized into malicious and non-malicious. The malicious act includes theft, unauthorized access to the system or network services, and loss of organization assets. Non-malicious acts refer to the employee that unintentionally exposed confidential data, which can be the biggest threat inside the organization itself. Few employees are aware that they have the responsibility to protect the organization's confidential data and fail to identify which data is confidential and which are not. Their lack of awareness can cause huge loss to the organization.

### B. Asset

An asset is a valuable thing, information, or anything that is important to an organization that they could not afford to lose in any means possible. The standard ISO/IEC 27001:2013 ensures the security of the assets [19] from any threats. Assets can be divided into tangible and intangible assets, measured in money. Identifying assets are important for risk management analysis. After identifying the assets, they are then ranked into different classes, for example, critical assets, moderate assets, and low asset classes. This will guide the organization to be more concerned about the most critical assets as a priority. Assets are exposed to various threats [15].

### C. Vulnerability

Vulnerability is defined as a weakness that is either accidentally or intentionally triggered. The weakness in the security or controls of asset may be exploited by threats [9], [15] Vulnerabilities usually is a technical issue, but sometimes the incidents were caused by human, for example, the employee uses weak password which is vulnerable to attack from an outsider. Sometimes, without notice or awareness, someone will download software, not knowing that it contains malicious code. Both organization and organization products are vulnerable to threats.

Identifying vulnerabilities is essential for the implementation of ISO/IEC 27005 standards by using controls to mitigate the identified vulnerability and to protect assets via preventative, corrective, or detective measures [7], [20]. Not all threats can be identified during the development, thus the product risks being delivered with some vulnerabilities to the users. From time to time, update or patch will be released to fix those flaws. The costs to have a good security into a product or software are huge, the budgets are limited and usually will not be able to cover additional security implementation. When there is no vulnerability being exercised, there is no risk from a threat source.

### D. Risk

Risk is defined as an uncertainty that could affect one or more objectives [15], [16]. For a risk to be present in the system, a threat must exploit a vulnerability through any potential action and cause assets damage or loss [10]. It is important to understand what risk mean in the information system security. To easily identify the security risks, one must know or identify the assets, the possible threats to the assets and the vulnerabilities exploited by these threats. The risk analysis is the most complex part in implementing

ISO/IEC 27005:2011. Examples of security risks are shown in Fig. 2.

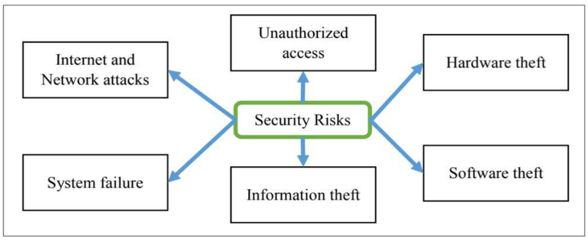

Fig. 2 Types of Security Risks

The origin of unauthorized access can be from external and internal threats; due to the improper access control, the organization exposed to unauthorized access to their important data. The insider threats such as authorized users can be a risk to the organization if not appropriately controlled. Whenever the network is compromised, intruders such as hackers can easily attack the system.

Risks from the external and internal threats are very costly, loss of credibility, the reputation of the organization is at risk, and loss of market share. Risks include unauthorized disclosure of confidential information, disruption of services, the loss of employee productivity, financial loss, legal implications from customers or public or investors, and blackmail may happen by threating to expose confidential information [21], [22].

ISO/IEC 27001 is the best-known standard in the family, providing requirements for an information security management system (ISMS). An ISMS [23] is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes, and IT systems by applying a risk management process.

## II. Material and Method

Information security assures all information assets are protected with confidentiality, integrity, and availability (CIA) [24]. It offers market assurance by protecting confidential data in a well-mannered method. ISO/IEC 27005 standard provides guidelines for information security risk management, which supports the ISO/IEC 27001 ISMS. Implementing ISO/IEC 27005:2011 to the system will be a huge advantage because it will help in the risk management process [25]. ISO/IEC 27001:2013 standard [26], on the other hand, provides an overview of risk management. ISO/IEC 27005:2011 risk management process is comprised of 6 activities, which are context establishment, risk assessment, risk treatment, risk acceptance, risk communication, and risk monitoring & review [25].

In this paper, we will focus on the creation of the risk treatment plan. The plan will detail out the security controls that need to be implemented, who is responsible for them and how the decision on risk treatment is made, and lastly, what are the necessary tools to be used. The risk management activities of ISO/IEC 27005:2011 are divided into the following sub-sections:

### A. *Context Establishment*

The first thing to do before doing the risk assessment is to define what methodology to be used. This is the most important parts of ISMS implementation. ISO/IEC 27001 standard do not specify what methodology to be used for the risk assessment, it is up to the organization to apply any methodology that suitable to their needs. Deliverable from this activity is the risk assessment and risk treatment methodology document.

The goal of this context establishment is to define the basic criteria, scope and boundaries and rules on how to perform the risk assessment and treatment. Basic criteria must be defined beforehand which include risk evaluation criteria, impact criteria, and risk acceptance criteria. The scope of the risk assessment is within the Software Development Unit.

### B. *Risk Assessment*

After the risk assessment methodology has been decided, it is time to do the risk assessment activity. Risk assessment (RA) is a systematic process to identify risk, evaluate risk, prioritized risk based on the risk evaluation criteria. The risk assessment activity can be further split into three distinct activities, which are risk identification, risk estimation, and risk evaluation [27]. The purpose of identifying the risk is to carry out a thorough and systematic process to find out everything that could endanger the confidentiality, integrity, and availability of the information. It includes the identification of assets, threats, existing controls, vulnerabilities, and consequences.

Assets can be divided into primary assets and supporting assets. Patient information and business processes have been identified as a primary asset. Supporting assets include the software, hardware, network, personnel, site, and organization. Threats identification has been made through discussion and with the help of threat catalog from Annex C of ISO/IEC 27005:2011[28]. Annex A ISO/IEC 27001:2013 [26], [29], [30] has a total of 114 controls that are available for use. By identifying existing controls, additional costs can be prevented, and only necessary controls are being implemented. There is a total of 23 existing controls identified. Table 1 shows several identified controls.

TABLE I
Several Existing Controls That Have Been Identified

| No. | Controls ID | Controls to be implemented |
|---|---|---|
| 1 | A.7.3.1 | Termination or change or employment responsibilities |
| 2 | A.9.2.1 | User registration and de-registration |
| 3 | A.9.2.2 | User access provisioning |
| 4 | A.9.2.3 | Management of privileged access rights |
| 5 | A.9.2.5 | Review of user access rights |
| 6 | A.9.2.6 | Removal of adjustment of access rights |

The threats and vulnerabilities have been identified through discussions and by referring to the catalog available from Annex C and D of ISO/IEC 27005:2011. Table 2 shows the different identification activities. The approach for risk analysis can be made qualitatively or quantitively. The loss of the CIA of the assets should be assessed too because different threats and vulnerabilities will have different impacts. Then, the business impact can be represented qualitatively or quantitatively. Besides, the incident probability of happening should be assessed qualitatively or quantitatively so that the probability of each incident and impact are able to be assessed.

TABLE II
IDENTIFICATION OF ASSETS, THREATS, CONTROLS, VULNERABILITIES, AND CONSEQUENCES

| Identification | Activity |
|---|---|
| Assets | Any asset that has value to the organization and requires protection must be identified. The asset owner also should be identified for each asset. The asset owner will determine the asset value. |
| Threats | The threats should be identified generically and by type. |
| Controls | The source of threats also needs to be identified. |
| Vulnerabilities | Identify the existing and planned controls. |
| Consequences | Identify the control implementation and usage status. |

To evaluate the risks, the estimated risks will be compared against the risk evaluation criteria and risk acceptance criteria. After risk estimation has been done, risk evaluation will be used to make decisions for future action. As there are multiple low and medium risks cases, ISO/IEC 27005:2011 suggested that the information security properties, and the importance of the business process that are supported by certain assets should be taken into consideration.

### *C. Risk Treatment*

The risk treatment option is based on the outcome of the risk assessment result. The priorities of each individual risk should be defined clearly for the implementation and their timeframes [8], [31]. The purpose of risk treatment activity is to specify which security controls need to implemented, who is responsible for it, what the deadlines are and which resources, for example, financial or human, are required for the implementation. This implementation means writing various policies and procedures, implementing some technical controls, and organizing processes differently. Several policies have been identified. There is a need for documentation to satisfy the control from Annex A of ISO 27001.

The deliverable from this activity is the risk treatment plan. A risk treatment plan will record all the implementation plan for the identified risks. Risk reduction is the only risk treatment entity selected for this project. The objective of this paper is to come up with the implementation plan. This plan is to be prepared before the real implementation is put in place. The deliverable for this activity is the risk treatment plan, which will be used for the real implementation at a later stage in the organization. This paper does not include the fourth activity of risk management, which is risk acceptance.

After the risk treatment plan has been defined, the residual risks must be determined. These residual risks will go through the risk assessment process again, and if the risk acceptance criteria are still not met, we will go through another iteration of risk treatment before proceeding into risk acceptance.

## III. RESULTS AND DISCUSSION

Risk evaluation was done to prioritize the risks identified. Risk levels should be compared against the risk evaluation and risk acceptance criteria to produce the risk ranking. After the risk assessment has been done, there are a total of 30 risks identified. And from the 30 identified risks, there are seven risks considered as high risk. The option that was used during the risk treatment is risk modification. The way this was done was through brainstorming with a few people responsible for the project. The output was written on Excel sheets.

The risk treatment activity was done to specify which security controls need to be implemented, who should be responsible for doing it, what the deadlines are and which resources are required to be implemented in the future. We gave priority to the higher level of risks from the list of identified risks

In the risk treatment plan, all controls that must be implemented must be listed, with details on how to implement those controls. The risk treatment plan must get approval from the risk owners because they are the ones who will ensure the effectiveness of the implemented controls and the risk treatment.

Table 3 shows a part of the risk treatment plan. The risk treatment plan produced will be used as guidelines for future implementation of controls into the organization. By implementing the risk management framework into the organization, the organization will have a proper procedure for identifying and mitigating the encountered risks.

TABLE III
A PART OF THE RISK TREATMENT PLAN

| No | Risk | Controls ID | Controls to be Implemented | Responsible Person | Resources | Results |
|---|---|---|---|---|---|---|
| 1 | Backup is not made regularly | A.12.3.1 | Information backup | Employee | 1 person 1 day | Not yet implemented |
| 2 | No 'logout' when leaving the workstation | A.11.2.8 | Unattended user equipment | Developer | 1 person1 day | Not yet implemented |
| 3 | Unprotected password tables, Unprotected database | A.10.1.1,<br>A.10.1.2,<br>A.18.1.5 | Policy on the use of cryptographic controls, Key management, Regulation of cryptographic controls | Developer | 1 person1 day | Not yet implemented |

There is a total of 30 risks identified during the process of risk identification. And out of 30 total risks, 7 risks are considered as a high-level risk. To treat these risks, controls from the Annex A of ISO 27001:2013 will be implemented to reduce them. After all the controls have been identified, the risk treatment plan is produced where the implementation method, the person responsible for the implementation, and the dateline are identified. The responsible manager must review this proposed plan to obtain higher management approval.

For the current organization, the ISO/IEC 27005:2011 is found to be a suitable standard to help the software development unit to implement information security risk management into the existing systems. This standard has guidelines that are detailed enough to cover the risk assessment and risk treatment process required by the organization. The implementation of the risk assessment did not require sophisticated nor expensive tools. We were able to implement the process by just using Excel spreadsheets, catalogs of vulnerabilities and threats together with a good risk assessment methodology.

## IV. Conclusion

The risk management methodology has been performed, and the result obtained is the risk treatment plan. This plan will be useful for future control implementation. Due to the short time frame to prepare this paper, only a risk treatment plan was produced without being implemented yet. In the next phase, this risk treatment plan will be used as a guideline to implement the controls into the organization. The implementation of ISO/IEC 27001 standard into the Development unit of the company will be very beneficial for everyone.

With the information security risk management process being implemented into the company Development Unit, the information assets will be secured. The organization will also have a proper procedure or process to identify risks, evaluate risks, and treat the risks with the security risk management part adopted from the ISO/IEC 27005 standard.

Several challenges were encountered in this project. Some people did not fully understand the importance of risk management, and they thought that this procedure was just another effort that was added to their workload. Therefore, there was a need to spend some time convincing them of how important this work is.

In this paper, 30 risks have been identified, and 7 of them were categorized as high-level risks for the product. A risk treatment plan has been developed for the system to reduce these risks to secure the patient data, thus preventing any data theft. This plan will describe which security controls need to be implemented, who is responsible for them, what the deadlines are, and which resources are required, and it will be the document that all will be referring to in the future implementation in the software development unit of the organization.

## Acknowledgment

Universiti Teknologi Malaysia financially supports the research under Research University Grant, Vote No: 14H76.

## References

[1] R. Latiff and J. Wagstaff, "Malaysia investigating reported leak of 46 million mobile users' data," *Thomson Reuters*, 2017.

[2] R. M. Alhajri, S. J. Alsunaidi, R. Zagrouba, A. M. Almuhaideb, and M. A. Alqahtani, "Dynamic interpretation approaches for information security risk assessment," *2019 Int. Conf. Comput. Inf. Sci. ICCIS 2019*, pp. 1–6, 2019.

[3] F. M. Dedolph, "The Neglected Management Activity: Software Risk Management," vol. 8, no. 3, pp. 91–95, 2003.

[4] K. Beckers, S. Faßbender, M. Heisel, J. C. Küster, and H. Schmidt, "Supporting the development and documentation of ISO 27001 information security management systems through security requirements engineering approaches," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 7159 LNCS, no. 256980, pp. 14–21, 2012.

[5] J. Breier and F. Schindler, "Assets Dependencies Model in Information Security Risk Management," pp. 405–412, 2014.

[6] A. Iqbal, H. Suhaimi, T. Manji, Y. Goto, and J. Cheng, "A Systematic Management Method of ISO Information Security Standards for Information Security Engineering Environments," pp. 370–384, 2011.

[7] S. Patino, E. F. Solis, S. G. Yoo, and R. Arroyo, "ICT Risk Management Methodology Proposal for Governmental Entities Based on ISO/IEC 27005," *2018 5th Int. Conf. eDemocracy eGovernment, ICEDEG 2018*, pp. 75–82, 2018.

[8] T. Kosub, "Components and challenges of integrated cyber risk management," pp. 615–634, 2015.

[9] A. Madhavi and S. Lincke, "Security Risk Assessment in Electronic Health Record System," *2018 IEEE Technol. Eng. Manag. Conf. TEMSCON 2018*, pp. 1–4, 2018.

[10] D. J. Tjirare and F. B. Shava, "A Gap Analysis of the ISO / IEC 27000 Standard Implementation in Namibia," pp. 1–10, 2017.

[11] T. Faculty, A. Susanto, T. Faculty, and T. Faculty, "Assessment of ISMS Based On Standard ISO / IEC 27001 : 2013 at Diskominfo Depok City," 2013.

[12] G. Wangen, "Information Security Risk Assessment: A Method Comparison," *Computer (Long. Beach. Calif).*, vol. 50, no. 4, pp. 52–61, 2017.

[13] L. Rukh and A. A. Malik, "Swiss Army Knife of Software Processes," in *2017 International Conference on Communication Technologies (ComTech) Swiss*, 2017, pp. 3–5.

[14] A. Alwi and K. A. Zainol Ariffin, "Information Security Risk Assessment for the Malaysian Aeronautical Information Management System," *Proc. 2018 Cyber Resil. Conf. CRC 2018*, pp. 1–4, 2019.

[15] O. O. Mwambe and I. Echizen, "Security oriented malicious activity diagrams to support information systems security," *Proc. - 31st IEEE Int. Conf. Adv. Inf. Netw. Appl. Work. WAINA 2017*, pp. 74–81, 2017.

[16] J. Bayne, "An Overview of Threat and Risk Assessment," 2002.

[17] G. Stoneurner, A. Goguen, A. Feringa, and N. S. Publication, *Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology*, vol. 30, no. July. 2002.

[18] R. Bojanc and B. Jerman-Blažič, "An economic modelling approach to information security risk management," *Int. J. Inf. Manage.*, vol. 28, no. 5, pp. 413–422, 2008.

[19] H. Susanto, F. Bin Muhaya, M. N. Almunawar, and Y. C. Tuan, "Refinement of Strategy and Technology Domains STOPE View on ISO 27001," *arXiv Prepr. arXiv1204.1385*, pp. 1–7, 2010.

[20] T. Neubauer, A. Ekelhart, and S. Fenz, "Interactive Selection of ISO 27001 Controls under Multiple Objectives," in *Proceedings of The Ifip Tc 11 23rd International Information Security Conference*, Boston, MA: Springer US, 2008, pp. 477–492.

[21] H. S. Group, "The Adoption of IT Security Standards in a Healthcare Environment," pp. 765–770, 2008.

[22] S. Tritilanunt and S. Ruaysungnoen, "Security Assessment of Information System in Hospital Environment," pp. 11–16, 2017.

[23] L. Astakhova and I. Zemtsov, "Situational approach to information security," *Proc. - 2018 Ural Symp. Biomed. Eng. Radioelectron. Inf. Technol. USBEREIT 2018*, pp. 136–139, 2018.

[24] H. Susanto and M. N. Almunawar, "Information Security Awareness : A Marketing Tools for Corporate ' s Business Processes," pp. 1–12, 2012.

[25] G. Wangen, C. Hallstensen, and E. Snekkenes, "A framework for estimating information security risk assessment method completeness: Core Unified Risk Framework, CURF," *Int. J. Inf. Secur.*, vol. 17, no. 6, pp. 681–699, 2018.

[26] B. Ţigănoaia, “Some Aspects Regarding the Information Security Management System within Organizations – Adopting the ISO/IEC 27001:2013 Standard,” *Stud. Informatics Control*, vol. 24, no. 2, pp. 201–210, 2015.

[27] M. McNeil, T. Llansó, and D. Pearson, “Application of capability-based cyber risk assessment methodology to a space system,” pp. 1–10, 2018.

[28] ISO, “International Standard ISO / IEC FDIS 27001,” vol. 2005. ISO, 2005.

[29] J. W. Candra, O. C. Briliyant, and S. R. Tamba, “ISMS planning based on ISO/IEC 27001:2013 using analytical hierarchy process at gap analysis phase (Case study: XYZ institute),” *Proceeding 2017 11th Int. Conf. Telecommun. Syst. Serv. Appl. TSSA 2017*, vol. 2018-Janua, no. 4, pp. 1–6, 2018.

[30] A. Longras, T. Pereira, P. Carneiro, and P. Pinto, “On the Track of ISO/IEC 27001:2013 Implementation Difficulties in Portuguese Organizations,” 2018, pp. 886–890.

[31] B. Barafort, A. L. Mesquida, and A. Mas, “Integrating risk management in IT settings from ISO standards and management systems perspectives,” *Comput. Stand. Interfaces*, vol. 54, no. November 2016, pp. 176–185, 2017.