6th International Scientific Conference ITEMA 2022 – Proceedings
DOI: https://doi.org/10.31410/ITEMA.2022.117

Impact of Risk Management in an Organizational Context

João Santos[1]
Leonilde Reis[2]
Manuel Landum[3]

Received: November 9, 2022
Revised: January 23, 2023
Accepted: February 6, 2023
Published: June 12, 2023

Keywords:
Information security;
Risk management;
Cybersecurity

Abstract: *In Portugal, the Council's Minister Resolution 41/2018, presents a complement to the General Data Protection Regulation (GDPR), which, in order to comply with it, defines technical guidelines for the Public Administration concerning the security architecture of networks and information systems. The objective of the paper is to present risk management in an organizational context. The adopted methodology is focused on the presentation of the research and obligations that the organizations have to take into account before the law and the regulatory authorities. International standards and how they can be applied in the context of the organization under study were analyzed, and the main results reached, aim to raise awareness within the organizations assertively, for the existing vulnerabilities and threats. Risk management was based on asset management and professional experience acquired over the years, as well as knowledge of internal procedures.*

1. INTRODUCTION

The Decree-Law 65/2021 applies to operators of critical infrastructure; operators of essential services and Public Administration entities, such as the organization under study, and defines the security requirements of network and information systems as well as the rules for incident notification. According to article 10º of Decree-Law 65/2021, entities that fall within the cited groups must consider all assets that ensure the functioning of the Information Systems and should carry out, at least once a year, an analysis of the risks associated with them.

Organizations have lately been targets of attacks, namely cyberattacks. This shows that there is a need, on the organization's part, to take action to avoid constraints on their operations. Therefore, it is preponderant that there is an understanding of the problem and finding ways to protect the organization and its assets (Santos, 2022).

All organizations must have security measures implemented; some of them imposed by legislation and others imposed internally, by knowledge of the cause and the need for protection. Security measures, especially legislated ones, may vary depending on the business area of the organization.

In that sense, this risk analysis should consider the Identification of threats; System failures; Natural phenomena; Human error; Malicious attacks; Failure to provide goods or services by a third party; Impact and probability of occurrence of the identified threats.

[1] Instituto Politécnico de Setúbal, Setúbal - Portugal
[2] Instituto Politécnico de Setúbal, Setúbal - Portugal
[3] Câmara Municipal do Barreiro, Barreiro - Portugal

2. RISK MANAGEMENT

According to the International Organization for Standardization (ISO), the norm aims to create standards for various activities of the organizations. ISO/IEC 27001:2018 enables organizations to implement an Information Security Management System (ISMS) through requirements suggested by the standard. The ISMS together with a risk management process increases the trust of stakeholders while preserving the confidentiality, integrity, and availability of information (ISO/IEC 27001, 2018).

Also, the norm ISO/IEC 27002:2022 - Information security, cybersecurity, and privacy protection - Information security controls, provides a set of generic controls in an ISMS scope, (ISO/IEC 27002, 2022). According to ISMS.ONLINE (2022) and compared to the previous version, it has a smaller number of controls, which are divided into four groups: People, Organization, Technology and Physical. The latest version of ISO considers compliance with regulations such as GDPR.

Supported by ISO/IEC 27001:2018 and ISO/IEC 27002:2013, ISO/IEC 27005:2018 was created to sustain an information security risk management platform, (ISO/IEC 27005, 2018). In this sense, ISO 31000:2018 also provides generic guidelines and a framework for risk management in organizations, independently of its sector. This standard aims to help organizations to identify opportunities, threats and how to treat risks. ISO 31000:2018 provides guidance for audit processes, whether internal or external. According to norm ISO 31000:2018, risk management must be considered in decision-making processes, as well as in all other organizational processes.

Risk criteria can be defined based on the internal and external contexts of the organization, such as the rules and existing laws. ISO 55000:2014 can be applied to all assets of an organization and all organizations, regardless of their nature. The guidelines of (ISO 55000, 2014) provide an overview of asset management.

Portuguese Public Institution, the Câmara Municipal do Barreiro (CMB), is responsible for the management of the municipality of Barreiro and provides services to citizens in the areas of spatial planning, social action, housing, transport and communications, energy, environment and basic sanitation, health, education, sports, consumer protection, civil protection, culture, and heritage.

The risk treatment will be defined based on the strategies: avoid, assume, remove, probability, consequence, share and retain defined in ISO 31000:2018, which are added the strategies of mitigating or transferring the risk referred to in the Quadro Nacional de Referência para a Cibersegurança (QNRCS) of Centro Nacional de Cibersegurança (CNCS), as described in Table 1.

Table 1. presents the strategies that can be followed in the process of treating the risk, as well as a brief description of each and what its source is. The responsible for the treatment of the risk should define the best strategy to be followed, considering all the various variables influencing it.

In the study conducted in an organizational context, 16 risks were identified in Table 2. Risk 03 is presented as it is considered that in the context of the paper, it can constitute added value. Risk 03 was identified by the fact that the Local Area Network (LAN) consists of nine /16 subnets, allowing 64516 hosts per subnet, making a total of 580644 hosts on the LAN. The LAN is oversized, allowing too many hosts considering the CMB needs, which leaves a wide spectrum of Internet Protocols (IP) available, that can be used by intruders and given the size of the networks it becomes difficult to detect these intrusions.

Table 1. Risk treatment

Strategy	Description	Source
Avoid	Avoid the risk when deciding not to start or continue with the activity that origins the risk.	ISO 31000:2018 CNCS-QNRCS
Assume	Take on or increase the risk to pursue an opportunity	ISO 31000:2018 CNCS-QNRCS
Remove	Remove the source of risk	ISO 31000:2018
Probability	Change the odds	ISO 31000:2018
Consequence	Changing the consequences	ISO 31000:2018
Share	Share risk (e.g., through contracts, insurance purchases)	ISO 31000:2018
Retain	Retain risk by reasoned decision	ISO 31000:2018
Mitigating	Reduce the impact or likelihood of risk	CNCS-QNRCS
Transferring	Transfer impact to third parties	CNCS-QNRCS

Source: Santos, 2022.

Table 2. Possibility to connect external devices to the organization on the network

#03 – Possibility to connect external devices to the organization on the network	
Assets	Network
Responsible	GINT
Threat	Unauthorized access; Intrusion; Cyberespionage
Vulnerability	Insecure network architecture
Confidentiality	Yes
Integrity	Yes
Availability	Yes
Probability	3 - Average
Impact	5 – Very High
Risk Level	15
Treatment	Avoid
Action	Scale the LAN to CMB needs; Implement security by MAC Address
Responsible for the treatment	GINT
Cost	No

Source: Santos, 2022.

The impact defined as very high derives from the threats set into question the 3 principles of the triad of security, availability, integrity, and confidentiality. Given that connection of some non-CMB equipment has already been recorded in the internal network, it is understood that the probability of this happening is medium. This risk can be avoided by implementing security mechanisms, which validate the MAC address of equipment that is attempting to connect to the LAN and resizing the LAN to a subnet where the allowed IPs are adjusted to the real needs of the CMB.

It can be verified in Figure. 1 that 50% of the identified risks have a high impact and 19% of those are considered Very High impact. These levels of impact require action, as the result of their occurrence may be catastrophic.

It can also be verified that 31% of the remaining risks are of lower impact. The risk impact analysis is important, but its treatment must consider other variables, such as the probability of its occurrence, the activities in question, and the threats to which they are subject.

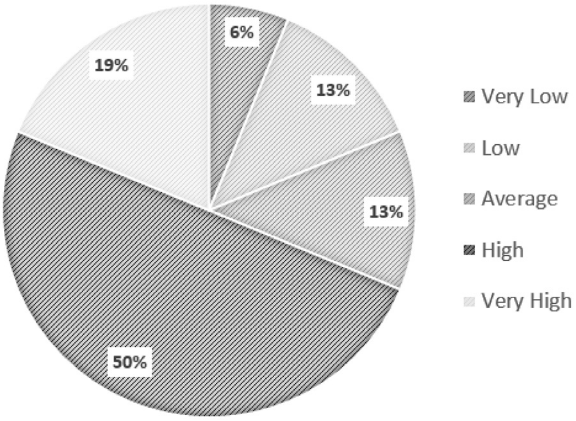

Figure 1. Risk Impact
Source: Santos, 2022.

The risks identified in this study were classified as well as analyzed to their impact on the organization. It was possible to conclude that some of these risks should be mitigated by finding solutions that can minimize the impact of their occurrence. Considering the specificity of the public organization under study, it was also verified that other risks should be assumed, and the risks that should be transferred to third parties were also identified.

3. FUTURE RESEARCH DIRECTIONS

The latest studies show us that vulnerability exploitation activities tend to increase in quantity, as well as should be increasingly sophisticated, and their impacts may have catastrophic consequences. As such, it is necessary to view Information Security Management as a continuing activity. In order to ensure high levels of security, it is necessary to define the steps to be taken in each process, which implies internal changes, such as transfers of employees, equipment, shared folders, or factors such as hiring employees and acquiring equipment.

These steps should include a detailed identification and analysis of each of these assets to identify which risks are associated with them and thus define how they should be treated. Risk mitigation can be facilitated by creating an internal security policy, based on ISO/IEC 27002:2022 controls and the recommendations of the Ministry Council Resolution 41/2018. The policy should be in place for the needs of the CMB, given that we are dealing with a public administration organization, with all its specificities.

4. CONCLUSION

The digital world and its benefits should continue to evolve, just as the threats will arise on a larger scale and in an increasingly elaborate way. It is necessary to monitor threats from all stakeholders, from security professionals to all other employees. There is a whole of laws in the sphere of information security and cybersecurity with which public administration organizations are not exempt from complying with them.

The compliance plan with these laws can be supported by the guidelines of the ISO standards studied and the QNRC of CNCS and can be adapted to real needs. Considering known threats, it is necessary to define strategies and act preventively before them. This means a deep knowledge of the organization, its processes, its assets, and its objectives.

In the definition of these strategies, it is essential to understand the impact of their implementation, because the sustainability of organizations may depend on the balance between the lack of investment in security mechanisms and how easily the organization can fall into the temptation to create rules in such a restricted way that makes it impossible to perform regular, daily tasks.

Risk management should be properly supported, and should indicate how those who have the task of making decisions about their treatment should act and manage it. However, in some cases, there is a need for critical analysis, and it may be necessary to put into practice the experience and know-how of the team, and the perception that it has about the organization and its functioning. Therefore, in conclusion, there is no exact way to perform the management of security information, it will always depend on the context in which it is inserted and who is treating and managing it.

References

ISMS.Online. (2022). *ISO 27002:2022 Changes, Updates & Comparison*. https://www.isms.online/iso-27002/iso-27002-revisions-updates-comparison/

ISO 31000. (2018). *Risk management — Guidelines*. https://www.iso.org/standard/65694.html

ISO 55000. (2014). *Asset management — Overview, principles and terminology*. https://www.iso.org/standard/55088.html

ISO/IEC 27001. (2018). *Information security management systems - Requirements*, 2018. www.iso.org/isoiec-27001-information-security.html

ISO/IEC 27002. (2022). *Information security, cybersecurity and privacy protection — Information security controls*. https://www.iso.org/standard/75652.html

ISO/IEC 27005. (2018). *Information technology — Security techniques — Information security risk management*. https://www.iso.org/standard/75281.html

Santos, J. (2022). *Gestão da Segurança da Informação.* Relatório de Estágio de Licenciatura, Instituto Politécnico de Setúbal.