kriativ.tech

Edição Nº 9 – 22-01-2023
ISSN Print: 1646-9976 | ISSN Online: 2184-223X |

DOI: 10.31112/kriativ-tech-2022-06-81

Application tool for information security and cybersecurity risk management in an organization

Sérgio Pinto
Assistant Professor at ISTEC – sergioluz.pinto@my.istec.pt

Abstract: *Currently organizations are increasingly exposed to information security and cybersecurity attacks. Therefore, this article intends to describe a process for analyzing/auditing potential risks to be able to assist an organization in choosing the security measures and controls to define and implement an adequate level of security. Additionally, this article also intends to be a reference for the development of an application tool to implement this process.*

Keywords: *Cybersecurity, Impact, Organization, Probability, Risk, Threat, Vulnerability*.

I. Introduction

The purpose of this article is to briefly describe a process for analyzing/auditing potential information security and cybersecurity risks of a given organization and, therefore, to be able to assist the organization in choosing the security measures and controls to define and implement an adequate level of security.

The presented process is based on the reference document "Guide for Risk Management" of the CNSC (National Center for Cybersecurity) [1], which incorporates guidelines from the QNRCS (National Reference Framework for Cybersecurity) [2] and RJSC (Legal Regime for Cyberspace Security) [3]. This reference document suggests the need for the risk process management to be composed of the following phases: context establishment, risk assessment, risk treatment, risk acceptance and, finally, risk communication and monitoring.

Additionally, it is intended that this article also serves as a basis for the proposal of an application tool development in Istec to analyze/audit potential information security and cybersecurity risks of a given organization. Therefore, the tool must support an adaptable interactive questionnaire about settings used in components/assets to be analyzed (context), followed by the respective identification, analysis, and evaluation of the risks found (survey), which will give rise to recommendations for the treatment of these risks, based on the security reference recommendations.

II. Risk Management

An organization's risk management can be understood as managing uncertainty and determining the necessary actions so that it can be minimized to levels considered acceptable by the organization [1] [5] [6] [7] [8].

For a better understanding of risk management, below are some of the basic concepts applied to it:

- Threat: a potential cause of an unwanted incident which can cause damage to a system, individual, or organization;
- Vulnerability: weakness of an asset or control that one or more threats can exploit;
- Impact: the result from the occurrence of a certain security event on one or more resources that normally originates direct or indirect consequences on the impacted resources;
- Risk: a reasonably identifiable circumstance or event with a potentially adverse effect on the networks and information systems security.

The risk management process should be a structured exercise within which the organization identifies possible threats that might exploit vulnerabilities of its assets and the associated risk levels, assessing the probability of occurrence and possible impacts of the same. Therefore, this process must consist of the following phases, described in Figure 1 [5]:

- Establishing the Context (specific to each organization);
- Risk Assessment (which includes risk identification, analysis, and evaluation);
- Risk Treatment;
- Risk Acceptance;
- Risk Communication and Consultation, and Risk Monitoring and Review.

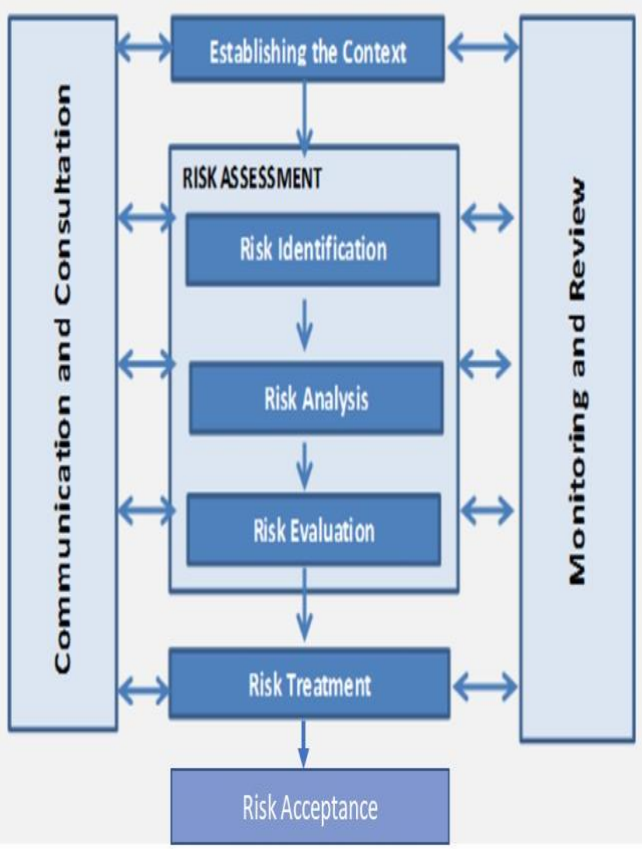

Figure 1: Risk management process

In the following sub-sections, a description of these various phases will be made, accompanied by a theoretical/practical example to complement and help understand them.

III. Establishing the context

This first phase of the risk management process aims to define the scope and basic criteria to be considered for an organization's information security and cybersecurity risk management and the consequent implementation of procedures aimed at risk management. Therefore, the following procedures must be defined [1] [5]:

1) Definition of risk management criteria:
   - Risk assessment criteria:
     - Criticality of the assets involved:
       - Importance from an operational and business point of view of its confidentiality, availability, and integrity;
       - Stakeholder expectations and perceptions and the negative consequences for the organization's market value and reputation.
   - Risk impact criteria:
     - Assets classification:
     - Occurrence of attacks:
       - Compromised operations;
       - Loss of business opportunities and financial value;
       - Organization damaged reputation.
   - Risk acceptance criteria:
     - Definition of risk acceptance scale based on its impact:
       - Accept: become aware of the risk without adopting controls;
       - Mitigate: implement measures to reduce risk exposure;
       - Transfer: direct responsibility for consequences to third parties;
       - Avoid: eliminate the cause of the risk.

2) Definition of risk management scope and boundaries:

- Definition of the scope of risk management:
  - Ensure that all relevant assets are considered in the risk assessment process.
- Definition of risk management boundaries:
  - Recognition of the assets perimeter under the organization's responsibility to be considered in the risk management process.

3) Definition of risk management roles and responsibilities (e.g. usage of RACI matrix, defined in Table 1):
   - Identification of roles and responsibilities of the various stakeholders:
     - Top Management: leadership of the organization responsible for superior decisions;
     - Risk Manager: intermediate manager who manages risk across the organization;
     - Risk Owner: person or contracting organization that directly manages each of the assets subject to the risk management process.
   - Establishment of necessary relationships between stakeholders.

RACI Matrix - Example			
Tasks	Top Management	Risk Manager	Risk Owner
Task A	I	R,A	R.C
Task B	I	C	R
Task C	R	C	I

Table 1: RACI Matrix (*Responsible, Accountable, Consulted, and Informed*)

In our theoretical/practical example, let's consider that the employee, Mr. X, the organization project manager, was assigned the risk management project (role "Risk Manager" in the RACI table).

To start the project, Mr. X must start by establishing the context of the organization, where he must define the procedures described above: risk criteria to be used, the definition of risk management scope and boundaries, and the identification of the roles and responsibilities of the interested parties.

IV. Risk Assessment

This second phase seeks to identify, recognize, quantify, and describe risks to enable organizations to assess and prioritize them according to their perceived severity and other previously established criteria. The risk assessment process is broken down into the following activities/steps: 1) risk identification, 2) risk analysis, and 3) risk assessment.

In our example, after establishing the context, Mr. X must carry out the risk assessment process, for which he must follow the following steps [1] [4] [5]:

Step 1 – Risk identification

To identify risks, an organization's information security and cybersecurity risk assessment must be carried out. Therefore, assets, respective threats, controls and possible vulnerabilities must be identified. Afterwards, catalogs with lists of threats and common vulnerabilities should be consulted for subsequent identification of possible threats and associated vulnerabilities [1] [5].

In our example, Mr. X identified the following asset and characteristics which potentiate security risks:

- Asset: documentation file management platform for the organization's projects;
- Threats: possible external malicious attack;
- Existing controls: password policy;
- Vulnerability: weak password policy, jeopardizing the confidentiality and integrity of the information stored in this asset.

Therefore, Mr. X identified the following associated risk: the high possibility of user's

passwords stealing from the file management platform hosted in a cloud computing service, which the organization uses to make available all the documentation generated within the scope of the execution of its projects.

Step 2 - Risk analysis

In the next step, the risk analysis is carried out, which aims to verify the origins of the identified risks, their consequences and impacts, and the probability of their occurrence.
For a better understanding of the different concepts of this step, the following definitions should be considered [1] [5]:

- Causes: the risk factors, both internal and external to the organization, must be registered according to the threats and vulnerabilities previously identified and within the scope defined for this risk management process;
- Risk: should be expressed as the combination of the impact of an event and its probability of occurring. This risk is calculated without any treatment effect or application of existing controls and can be expressed in the following formula:

Risk = (probability of the threat exploiting the vulnerability) x (total impact cost of the exploited asset)

In our example, Mr. X used the following procedures for the identified risk analysis:

- Risk analysis methodology: quantitative risk analysis (other option would be "qualitative");
- Criteria for probability and impact of the identified risk (scale from 1: "Very unlikely" to 5: "Very likely"):
  - Generic Impact: 4 "Significant consequences";
  - Probability: 5 "Very likely to happen".
- Risk level calculation (Probability x Impact): 20 "Critical', taking into account his organization-defined 5x5 risk matrix in Table 2.

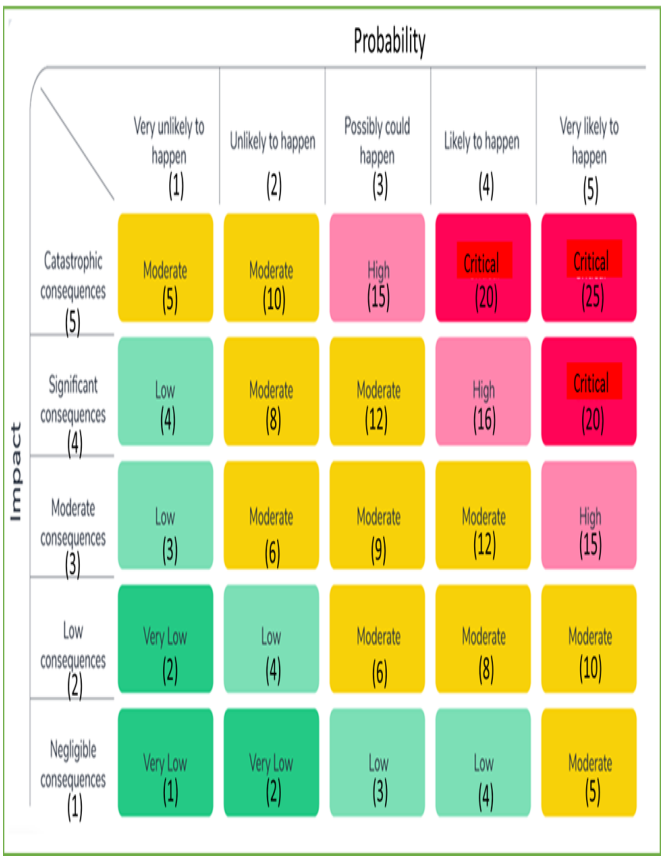

Table 2: 5x5 Risk matrix

Step 3 - Risk Evaluation

This third and final risk assessment step is intended to assist in decision-making on the appropriate treatment of previously identified and analyzed risks. Therefore, as described in Table 3, it must be decided which of the following possible treatments should be recommended for the assessed risks [1] [5]:

- Accept: accepting the risk without adopting controls. This option is used in situations where the risk is within the acceptance criteria defined by the organization. For example, only accepting low and very low-level risks;
- Mitigate: reduce risk exposure, drawing up action plans and applying specific or additional controls to mitigate the risk or reduce it to fit the risk acceptance criteria defined by the organization;
- Transfer: transfer responsibility for the risk consequences to third parties. Risk responsibility is transferred to an entity

other than the organization, for example, assigning to suppliers or other partners the management of organization assets or business activities;

- Avoid: eliminate the risk cause, eliminating the process that generates it. This option aims to discontinue business activities or support assets that can act as a source of risk for the organization to eliminate it definitively. This option is typically considered when the treatment plan is too costly, and the targeted business activity or asset is no longer relevant to the organization's business objectives.

Risk level and its treatment			
Level	Recommended treatment		
Critical		Mitigate/	Avoid
High		Mitigate/	Transfer
Moderate		Mitigate/	Transfer
Low	Accept/	Mitigate/	Transfer
Very Low	Accept		

Table 3: Risk levels treatment example

In our example, given the calculated level ("Critical": 20), the organization cannot accept it since all "Critical" risk levels should be mandatorily treated unless the organization's top management has formally accepted them.

V. Risk Treatment

This third phase involves, identifying, formalizing, and implementing one or more action plans, which aim to control or mitigate the risk causes identified in the previous phase [1] [5].

In our example, the organization must make the strategic decision to perform the following activities to mitigate the risk found and analyzed as a "Critical" level:

1) Ensure that the file management platform provider changes its password management policy in accordance with the best practices within a period to be defined;
2) Evaluate other platforms that provide the same service, with security conditions considered appropriate by the organization.

A person responsible for carrying out these risk treatment activities must also be identified ("Risk Owner" function in the RACI Table 1); in our example, the employee Mrs. Y Information Systems Director, and an estimated date for their resolution must also be agreed upon. The chosen date must be in conformance with the priorities assigned to the identified risks, taking into account the level of risk and the criticality of the assets involved.

After the successful execution of risk treatment activities, it can be considered that the risk found has been mitigated and can be accepted by the organization.

VI. Risk Communication and Consultation

This activity aims to define a consensual behavior on managing information security and cybersecurity risks through the exchange or sharing of information between those responsible for the process definition and the interested parties that must follow it. The information to be communicated should include the risks: existence, nature, form, probability, severity, treatment, and acceptability [1] [5].

Risk communication should ensure that those responsible for defining the risk management process and stakeholders are aligned on the reason for decisions and security actions taken. To this end, this communication must be bidirectional.

Therefore, the organization should establish a risk communication and consultation plan to ensure the commitment of those responsible for the risks. For example, in case of specific incidents to ensure a good response, according to the previous plan.

VII. Risk Monitoring and Review

This activity indicates that the department responsible for managing the organization's risks is responsible for regularly monitoring the organization's environment to identify in a timely manner any change that may have occurred in the context and that could originate a risk perception change. In this case, the entire risk analysis process for the detected changes must be repeated [1] [5].

As already referred, this article also intends to be a reference for the proposal of an application tool development to implement a risk management process in an organization. For this purpose, in Figure 2 is presented a brief description of the chaining and tasks of the various phases of our theoretical/practical example, namely, the three phases of the risk assessment process, followed by the respective risk treatment [1].

VIII. Application tool

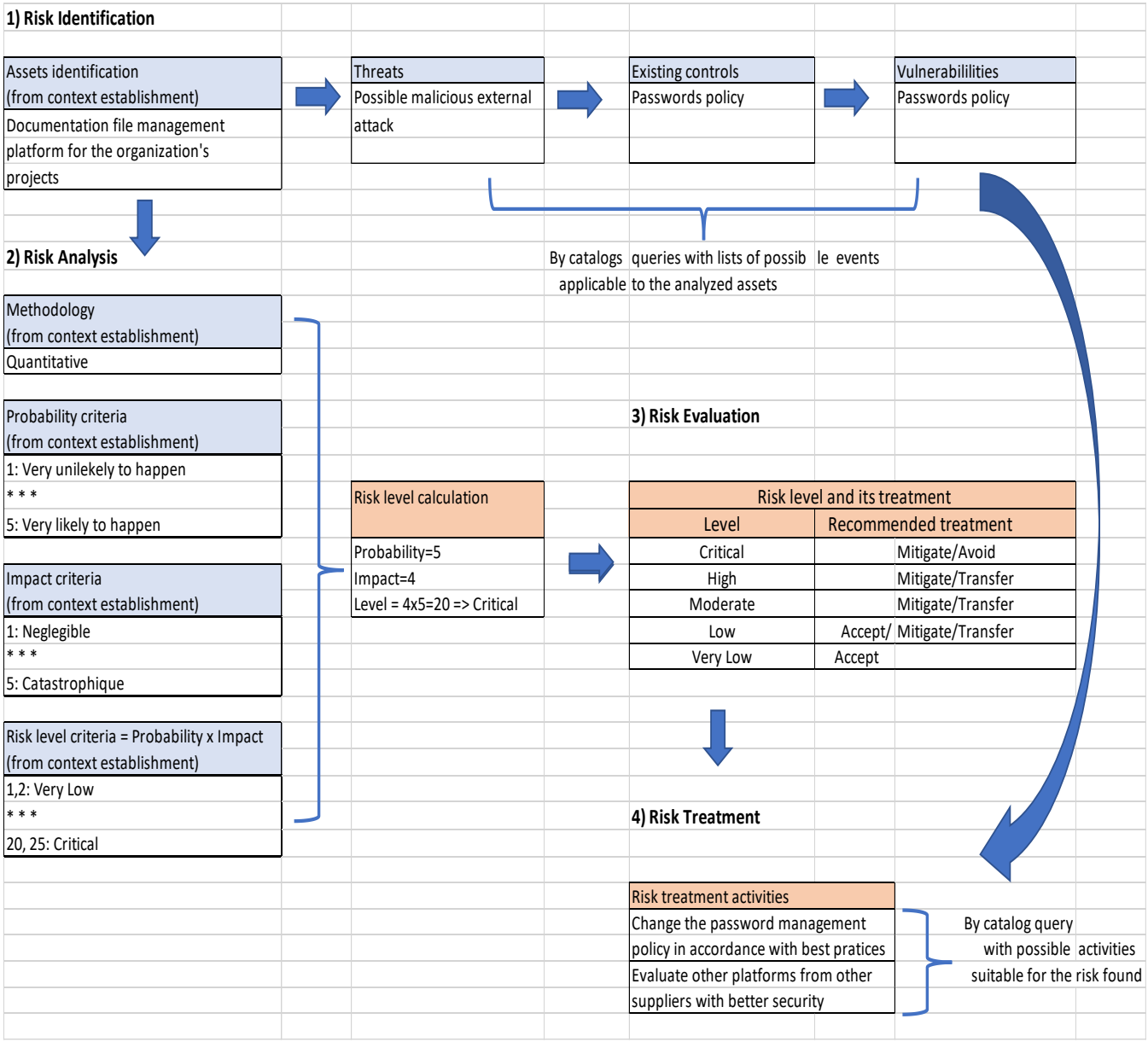

Figure 2: Phases of the theoretical/practical example

The tables with the blue top should correspond to a component of "manual" inputs, depending on the specific characteristics of the organization to be audited, corresponding to the establishment of the context and identification of assets and respective risks. The remaining tables with an orange top, used for assessing and treating the risk detected, should be able to have their values/activities calculated in the most "automated" possible mode, depending on the content specified in the tables with a blue top.

IX. Conclusion

The purpose of this document is, based on a reference document [1], not only to briefly describe an analysis/audit process of potential information security and cybersecurity risks of a given organization, but also to serve as a basis for developing an application tool with the same function.

It should be noted that this tool should have a component of "manual" inputs adaptable to the specific characteristics of the organization to be audited. This component should establish the context and be able to identify the assets and respective threats, security controls, and possible vulnerabilities existing in the organization. Afterwards, depending on the previously obtained information, a common component should be invoked, which is intended to be as "automated" as possible, for assessing the risks found, which should give rise to the recommendations for these risks treatment.

X. References

[1] CNCS (2022), "Guia para Gestão de Riscos em matérias de Segurança da Informação e Cibersegurança", retrieved from: https://www.cncs.gov.pt/docs/guia-de-gestao-dos-riscos.pdf

[2] CNCS (2019), "QNRCS: Quadro Nacional de Referência para a Cibersegurança", retrieved from: https://www.cncs.gov.pt/docs/cncs-qnrcs-2019.pdf

[3] Artigo 10º Decreto Lei nº 65/2021, 30 de julho, "Regime Jurídico da Segurança do Ciberespaço", retrieved from: https://www.cncs.gov.pt/pt/regime-juridico/

[4] CNCS (2020), "Quadro de Avaliação de Capacidades de Cibersegurança", retrieved from: https://www.cncs.gov.pt/docs/cncs-quadrodeavaliacao.pdf

[5] ISO/IEC 27005:2018, "Information technology -- Security techniques -- Information security risk management", retrieved from: https://www.standards-pdf-download.com/iso-iec-27005-2018-download-free.html

[6] NIST (2022), "Risk Management Framework: Security and Privacy Controls for Information Systems and Organizations, Revision 5", SP 800-53, retrieved from: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[7] NP ISO/IEC 31000, "Gestão do Risco – Linhas de orientação", retrieved from: http://qualitividade.pt/wp-content/uploads/2016/04/NPISO031000_2012.pdf

[8] ISO/IEC 27001:2022, "Information security, cybersecurity and privacy protection — Information security management systems — Requirements" , retrieved from: http://www.itref.ir/uploads/editor/2ef522.pdf

XI. Abbreviations

CNCS	Centro Nacional de CiberSegurança
ISO	International Organization for Standardization
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
Istec	Instituto Superior de Tecnologias Avançadas
QNRCS	Quadro Nacional de Referência para a Cibersegurança
NIST	National Institute of Standards and Technology
RACI	Responsible, Accountable, Consulted and Informed
RJSC	Regime Jurídico da Segurança do Ciberespaço