A Reference Risk Register for Information Security According to ISO/IEC 27005

Gonçalo Bernardo Mateus

Thesis to obtain the Master of Science Degree in

Engenharia de Telecomunicações e Informática

Supervisor(s): Prof. José Luís Brinquete Borbinha

Examination Committee

Chairperson: Prof. Paulo Jorge Pires Ferreira

Supervisor: Prof. José Luís Brinquete Borbinha

Member of the Committee: Prof. André Ferreira Ferrão e Couto Vasconcelos

November 2016

Acknowledgments

I would like to thank Professor José Borbinha and Ricardo Vieira for the amazing support during this project. Without their help, I believe I wouldn’t have finished it.

I would also like to thank my friends and coworkers at Muzzley.

Ultimately, I would like to dedicate the work done to my friends and family. A very special thank you to my parents, João and Anabela, to my brother Hugo and to my grandparents and uncles. I would also like to thank Elisa Simion, for the great support on these last few months.

Resumo

Nos dias de hoje, uma das maiores preocupações é garantir que a informação é mantida em segurança, sem colocar os ativos de organizações em risco. A gestão de risco tornou-se uma atividade essencial, permitindo organizações avaliarem os riscos e identificar os devidos procedimentos para a sua mitigação. Apesar da existência de um corpo consolidado de conhecimento, as organizações e os gestores de risco, em particular, ainda lutam para identificar o modelo de gestão de risco em segurança de informação mais adequado que deve ser usado no processo de gestão de riscos. O objectivo do presente documento é analisar o corpo de conhecimento de segurança de informação, a fim de estabelecer um modelo de gestão de risco em segurança de informação de referência. Este modelo proposto será aplicado no caso de uma organização real, seguindo um processo proposto, terminando com o desenvolvimento de um registo de riscos de referência, que mais organizações podem potencialmente usar para registar informações num processo de gestão de riscos em segurança de informação.

Palavras-Chave: Risco, Mitigar, Gestão, Informação, Registo, Segurança.

Abstract

Nowadays, one of the biggest concerns is to ensure that information is kept secure, without putting at risk organization’s assets. Risk management has become an essential activity, allowing organizations to assess risks and identify procedures to mitigate risks. Despite the existence of a consolidated body of knowledge, organizations and risk managers in particular still struggle to identify the most suitable information security risk management model that should be used in the risk management process. The purpose of this document to analyse the information security body of knowledge in order to establish a reference information security risk management model. This proposed model will be applied on a real life organization, following a proposed process, ending with the development of a reference risk register, which more organizations can potentially use to record information in a information security risk management process.

Keywords: Risk, Mitigate, Management, Information, Register, Security.

Table of Contents

List of Figures

List of Tables

List of Acronyms

IS	Information System(s)
IT	Information Technology
RM	Risk Management
ISM	Information Security Management
ISMS	Information Security Management System(s)
ISSRM	Information Systems Security Risk Management
ISRM	Information Security Risk Management
DSRM	Design Science Research Methodology
ISACA	Information Systems Audit and Control Association
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
NIST	National Institute of Standards and Technology
FAIR	Factor Analysis of Information Risk

1. Introduction

Headlines all over the world about stolen or missing data have become a frequent occurrence, increasing the importance of information security – the process to protect and preserve the availability, confidentiality and integrity of information. In the scope of information security, risk management is considered an essential activity in order protect and preserve information. Risk management allows the assessment of threats to information and consequently assures that those threats are controlled. When the subject is information security, ISO/IEC 27001 [8] is one of the most known references and defines the requirements for "establishing, implementing, maintain and continually improving an information security management system" [8]. within the context of the organization. The reference is part of the ISO 27000 family of standards that also contains ISO/IEC 27005 [7], providing guidelines for information security risk management (ISRM).

Despite the existence of a consolidated body of knowledge, organizations and risk managers in particular still struggle to identify the ontology of risk concepts and relationships that should be used in the risk management process (i.e., struggle in finding a suitable ISRM model). The risk register (also known as risk log) is the concept that supports the recording of information relevant for the all phases of the risk management process. The risk register should be developed according to the pre-defined risk management model. An evidence of the diversity of information security risk management models is the different information security risk registers that exist in the literature [1] [6] [7] [12] [16] [19]. The multiple risk registers prevent the communication and sharing of information security risks between and within organizations, and the quality of the risk management information that consequently impacts the evaluation and mitigation of the identified risks. Note that although ISO/IEC 27005 provides the guidelines for information security risk management it does not fully prescribe a risk management model. Instead it defines a set of concepts that can be relevant to ISRM. This flexibility is justified by the diversity of contexts where ISRM can be applied but it also leads to multiple interpretations of what a proper ISRM model should be.

This document proposes to establish a reference ISRM model, based on the research done on the information security domain. Having established this model, the purpose will be to support the development of a reference risk register, following a proposed process that organizations can use to record information in a ISRM process.

1.1. Information Security

The main reference for ISRM for this document is the ISO 27000 family of standards, containing standards that "can be used to prepare organizations for an independent assessment of their ISMS applied to the protection of information" [2]. All information held by an organization is subject to both threat attacks and vulnerabilities, inherent of its use. Information security should be a central concern for the organization, and it should be applied in order to implement and ensure an adequate functioning of the management system for information security [23]. Information should therefore be seen as one of the most important assets of an organization, as as such, requiring protection against the loss of availability, integrity and confidentiality [2].

Satisfying security requirements within an organization is a real challenge and a structured and systematic approach of the security management risk is a useful way to identify the organizational requirements for the information security as well as for the creation of an efficient ISMS. [23]

During the course of this document, an in depth analysis is made regarding information security inside the risk management domain.

1.2. Risk Management

Before establishing its own objectives and focuses, an organization knows it will have both external and internal factors that can condition whether they will be achieved or not. The word “Risk” can be defined as the effect uncertainty has on an organization’s objectives. [3]

Organizations perform risk management by identifying risks, analyzing them and then evaluating whether the risk should be altered on a risk treatment phase, in order to satisfy their requirements [3].

The risk management process can be applied to multiple sized organizations, and to as many areas and levels as possible, as well as to specific projects and activities. [3]

The ISO/IEC 31000 standard describes the systematic and logical process of risk management in detail, and is this document’s main reference for risk management inside an organization.

1.3. Research Problem and Proposed Solution

It is essential that organizations follow a method for implementing guidelines that can ensure the safety of their information assets, treating vulnerabilities and protecting them against unwanted threats.

The problem identified, is that organizations and risk managers in particular still struggle to identify the ontology of risk concepts and relationships that should be used in the risk management process.

Based on the information security risk management body of knowledge (presented on chapter 2 of this document) the proposed solution consists on a reference ISRM model (presented at the end of chapter 3 of this document), for supporting a proposed reference risk register, that organizations can use in their risk assessment processes.

The reference risk register's multiple versions were implemented using a risk management software tool, called Holirisk[1], developed by INESC-ID. This tool was used to model the information security risk management processes inside a real organization. The real case was a Portuguese state owned company, operating worldwide, and from now on designated as "Case Study".

The next section will describe in detail the methodology used to build the proposed solution.

1.4. Research Methodology

The method used to build this proposal for a reference ISRM model, for supporting a reference risk register, was based on the Design Science Research Methodology [17] [18]. This methodology was used as base to build our proposed solution due to incorporating principles, practices and procedures to carry out a consistent model for presenting and evaluating Design Science research in IS.

Note that the methodology adopted was only based on DSRM, since there was no time for a formal assessment of the work done by a panel of experts, as initially intended. However, an "Application" phase did take place instead, in which the proposed ISRM model was applied to a real life Case Study, that resulted in our final proposal.

These were the steps taken to arrive to our proposed solution:

- **Identify Problem and Motivation; Define Objectives of a Solution:** The state of the art was gathered and the problem identified and analysed, concluding with the need to establish a reference ISRM model;
- **Design and Development:** The ISRM domain model proposal is developed based on the information security risk management body of knowledge;
- **Application:** The proposed ISRM domain model is used to develop a risk register proposal, which after suffering a process of adding continuous improvements, will be presented as the final reference risk register solution;
- **Communication:** After the project's end, the final conclusions and solution proposal were used to write the present document.

Figure 1 represents the followed work method to build the proposed solution.

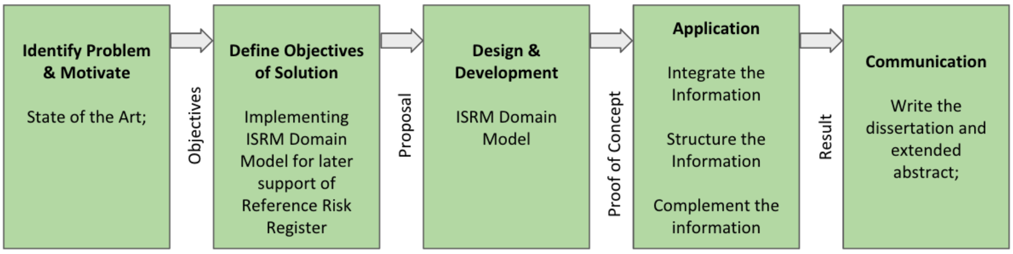

Identify Problem & Motivate
State of the Art;
Objectives
Define Objectives of Solution
Implementing ISRM Domain Model for later support of Reference Risk Register
Proposal
Design & Development
ISRM Domain Model
Proof of Concept
Application
Integrate the Information
Structure the Information
Complement the information
Result
Communication
Write the dissertation and extended abstract;

Figure 1 – Methodology used to build the proposed solution

[1] Holirisk Website: http://holirisk.sysresearch.org/.

1.5. Document Structure

This document is structured in the following way:

- **Chapter 1 – Introduction:** A introduction about the general context in which this document is placed, risk management, information security, the research problem, motivation, this document's main objectives and the research methodology used.
- **Chapter 2 – Related Work:** All the theoretical background and research are presented.
- **Chapter 3 – Problem Analysis:** In this chapter, the considered references are analysed, concluding with the core ISRM concepts needed to build our domain model proposal.
- **Chapter 4 – Application:** In this chapter, the proposed domain model is presented and applied to a real life case of an organization. The process of arriving to the final solution is described in three distinct steps, ending the chapter with the final reference risk register proposal.
- **Chapter 5 – Conclusions and Future Work:** The final conclusions regarding the work done are presented, as well as last reflections over lessons learned, and proposals regarding future work.

2. Related Work

On this chapter of the document, the state of the art gathered during research is presented, concluding with the problem identification, for which later in this document a solution is proposed.

2.1. Risk Management Fundamentals

This section describes the main concepts and principles present on the risk management domain.

The ISO Guide 73 [5] provides the vocabulary used in risk management. The following concepts, present throughout this document, were selected as the most important to discuss inside the ISO Guide 73, and were selected based on all the research done:

- **Risk**: effect of uncertainty on objectives. [5]
- **Risk register**: record of information about identified risks. [5]
- **Risk management**: coordinated activities to direct and control an organization with regard to risk. [5]
- **Risk management process**: systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk. [5]
- **Risk management framework**: set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization. [5]
- **Risk report**: form of communication with the intent to inform internally or externally person concerned, by providing the current state of risk and its management. [5]

A risk management framework can, therefore, be understood as a system whose purpose will be to ensure the fulfilment of the goal of risk management. It should also include a risk management process, and the resources and principles used in its implementation, as represented on Figure 2. These features can be the most varied, being, however, that the most important one in practice has been called risk register, which can result in multiple solutions depending on the technical and technological support available to the risk management.

In Figure 3, we have the informal structure of the risk management process, as originally defined in [3].

The risk assessment process inside the risk management process specifies the overall process of risk identification, risk analysis and risk evaluation.

The three stages that divide risk assessment, present in Figure 3, are:

- **Risk identification**: process of finding, recognizing and describing risks. [3]
- **Risk analysis**: process to comprehend the nature of risk and to determine the level of risk. [3]
- **Risk evaluation**: process of comparing the results of risk Analysis with risk criteria to determine

whether the risk and/or its magnitude is acceptable or tolerable. [3]

This process has been adopted by organizations over the course of time, however the need to implement it within a reliable framework might help to insure that risk is managed efficiently, effectively and coherently.

In conclusion, risk assessment is the part of risk management that provides a structured process that identifies how the organization's objectives may be affected (**Risk identification**), analysing the risk in terms of consequences (**Risk analysis**) and their probabilities before deciding on whether further treatment is required (**Risk evaluation**).

The **ISO/IEC 31010** standard specifies risk assessment techniques that attempt to answer the following fundamental questions [4]:

- What can happen and why (by risk Identification)?
- What are the consequences?
- What is the probability of their future occurrence?
- Are there any factors that mitigate the consequence of the risk or that reduce the probability of the risk?

Table 1, extracted from [4] contains such techniques.

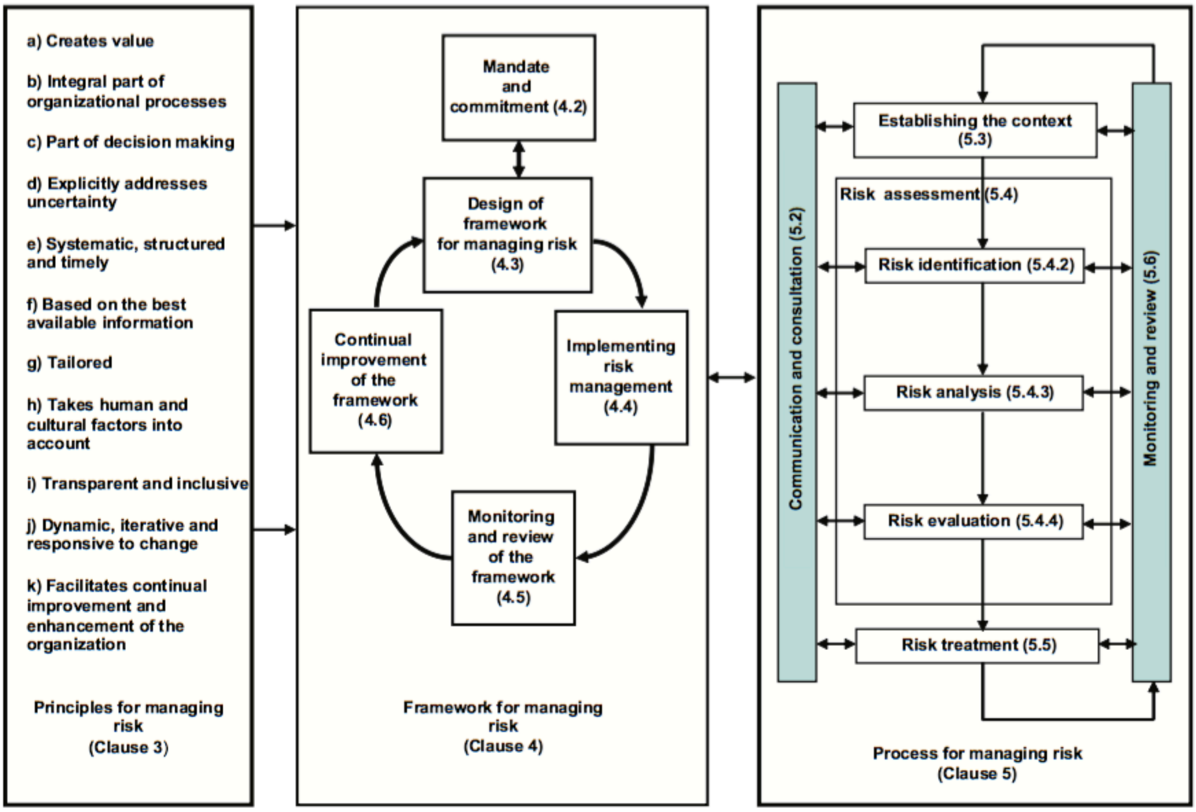

a) Creates value
b) Integral part of organizational processes
c) Part of decision making
d) Explicitly addresses uncertainty
e) Systematic, structured and timely
f) Based on the best available information
g) Tailored
h) Takes human and cultural factors into account
i) Transparent and inclusive
j) Dynamic, iterative and responsive to change
k) Facilitates continual improvement and enhancement of the organization
Principles for managing risk (Clause 3)
Mandate and commitment (4.2)
Design of framework for managing risk (4.3)
Continual improvement of the framework (4.6)
Implementing risk management (4.4)
Monitoring and review of the framework (4.5)
Framework for managing risk (Clause 4)
Communication and consultation (5.2)
Establishing the context (5.3)
Risk assessment (5.4)
Risk identification (5.4.2)
Risk analysis (5.4.3)
Risk evaluation (5.4.4)
Risk treatment (5.5)
Monitoring and review (5.6)
Process for managing risk (Clause 5)

Figure 2 – Relationships between risk management principles, framework and process [3]

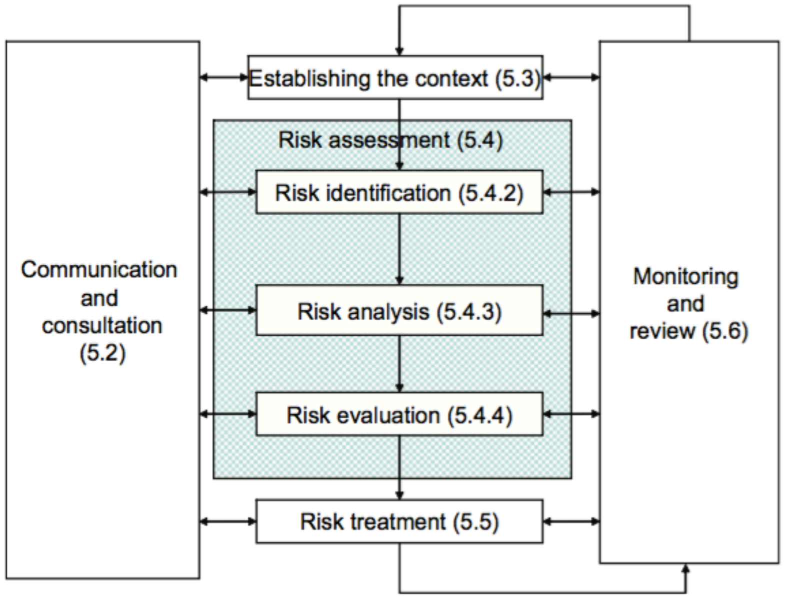
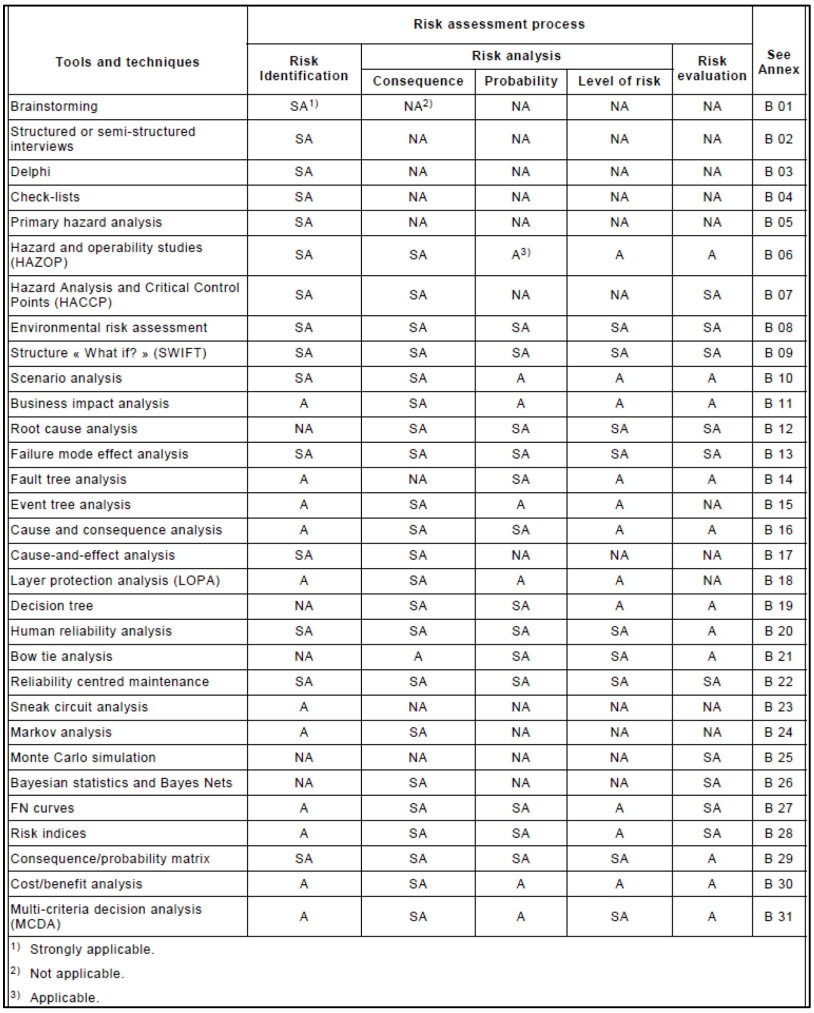

Establishing the context (5.3)
Risk assessment (5.4)
Risk identification (5.4.2)
Risk analysis (5.4.3)
Risk evaluation (5.4.4)
Risk treatment (5.5)
Communication and consultation (5.2)
Monitoring and review (5.6)

Figure 3 – Risk management process [3]



Tools and techniques	Risk assessment process					See Annex
	Risk Identification	Risk analysis			Risk evaluation	
		Consequence	Probability	Level of risk		
Brainstorming	SA[1]	NA[2]	NA	NA	NA	B 01
Structured or semi-structured interviews	SA	NA	NA	NA	NA	B 02
Delphi	SA	NA	NA	NA	NA	B 03
Check-lists	SA	NA	NA	NA	NA	B 04
Primary hazard analysis	SA	NA	NA	NA	NA	B 05
Hazard and operability studies (HAZOP)	SA	SA	A[3]	A	A	B 06
Hazard Analysis and Critical Control Points (HACCP)	SA	SA	NA	NA	SA	B 07
Environmental risk assessment	SA	SA	SA	SA	SA	B 08
Structure « What if? » (SWIFT)	SA	SA	SA	SA	SA	B 09
Scenario analysis	SA	SA	A	A	A	B 10
Business impact analysis	A	SA	A	A	A	B 11
Root cause analysis	NA	SA	SA	SA	SA	B 12
Failure mode effect analysis	SA	SA	SA	SA	SA	B 13
Fault tree analysis	A	NA	SA	A	A	B 14
Event tree analysis	A	SA	A	A	NA	B 15
Cause and consequence analysis	A	SA	SA	A	A	B 16
Cause-and-effect analysis	SA	SA	NA	NA	NA	B 17
Layer protection analysis (LOPA)	A	SA	A	A	NA	B 18
Decision tree	NA	SA	SA	A	A	B 19
Human reliability analysis	SA	SA	SA	SA	A	B 20
Bow tie analysis	NA	A	SA	SA	A	B 21
Reliability centred maintenance	SA	SA	SA	SA	SA	B 22
Sneak circuit analysis	A	NA	NA	NA	NA	B 23
Markov analysis	A	SA	NA	NA	NA	B 24
Monte Carlo simulation	NA	NA	NA	NA	SA	B 25
Bayesian statistics and Bayes Nets	NA	SA	NA	NA	SA	B 26
FN curves	A	SA	SA	A	SA	B 27
Risk indices	A	SA	SA	A	SA	B 28
Consequence/probability matrix	SA	SA	SA	SA	A	B 29
Cost/benefit analysis	A	SA	A	A	A	B 30
Multi-criteria decision analysis (MCDA)	A	SA	A	SA	A	B 31

[1] Strongly applicable.

[2] Not applicable.

[3] Applicable.

Table 1 – Relevant techniques for risk assessment [4]

2.2. Information Security Fundamentals

This section describes the main concepts, principles and methods used on the ISRM domain, starting with the most important references (ISO 27000 family of standards) and finally describing ISRM frameworks (ISO/IEC 27005, COBIT, OCTAVE, NIST and FAIR).

The ISO 27000 family of standards main objective is to allow organizations to develop and implement their own processes for managing the security of their information assets including financial information, intellectual property, and employee details, or information entrusted to them by customers or third parties. these standards can also be used to prepare for an independent assessment of their ISMS applied to the protection of information. [2]

To better understand the concept behind this family of standards, one must first explore the purpose of information security.

Besides involving the preservation of availability, confidentiality and integrity of information, the information security domain may also involve protecting and preserving the authenticity and reliability of information, also ensuring that entities can be held accountable. There are other very important concepts in the information security domain, selected according to research:

- **Threat**: potential cause of an unwanted incident, which may result in harm to a system or organization. [2]
- **Vulnerability**: weakness of an asset or control that can be exploited by one or more threats. [2]
- **Event**: occurence or change of a particular set of circumstances. [2]
- **Consequence**: outcome of an event affecting objects. [2]
- **Control**: measure that is modifying risk. [2]
- **Impact**: adverse change to the level of business objectives achieved. [7]
- **Asset**: anything that has value to the organization. [8]

Assets (in this case, information assets) need to be protected through defining, achieving, maintaining, and improving information security effectively, maintaining and enhancing its legal compliance and image. These coordinated activities directing the implementation of suitable controls and treating unacceptable information security risks are generally known as elements of information security management. [2]

According to each organizations strategic decisions and security requirements, the ISMS (information security management system) needs to be in accordance with all the stakeholders, including shareholders, business partners, customers and any other relevant parties.

In order to maintain a properly functional ISMS, an organization needs to undertake the following steps [2]:

- Identify information assets and their associated information security requirements;
- Assess information security risks and treat information security risks;
- Select and implement relevant controls to manage unacceptable risks;
- Monitor, maintain and improve the effectiveness of controls associated with the organization's

information assets;

It is important that the information security management system is part of, and integrated with the organization’s processes and overall management structure, and that information security is considered in the design of processes, information systems, and controls. To establish and implement the ISMS, is necessary to define the needs, objectives, security requirements and the organizational processes. [8]

The **ISO/IEC 27001** standard can be used by internal and external parties to assess the organization’s ability to meet its own information security requirements, also ensuring guidance through the selection of adequate and proportionate security controls that protect information assets and give confidence to the interested parties.

Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures, software and hardware functions. These controls, defined on this standard, need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met. [9]

The **ISO/IEC 27002** standard is designed to be used as a reference for selecting controls within the process of implementing an ISMS, based on ISO/IEC 27001 [8] or as a guidance document for organizations implementing commonly accepted IS (information security) controls. [9]

2.2.1.ISO/IEC 27005

The ISO/IEC 27005 standard is this document’s main reference for information security risk management in an organization, providing guidelines for the requirements of an ISMS according to ISO/IEC 27001.

According to this standard, the risk management process in information security can be applied either to a complete organization as a part of the organization (i.e. department, service, location), information system (existing or planned) as well as particular aspects of control (i.e. business continuity plan) [7].

An iterative approach in conducting the risk assessment process may increase depth and assessment detail in each iteration [7].

This standard defines a Plan, Do, Check, Act information security risk management process, consisting of the following steps [7]:

Plan

- Establish the context for information security risk management. This includes selecting criteria for evaluating risk, determining impact, and accepting risk; defining the asset scope and boundaries over which risk management will be conducted (for example, which applications will be assessed); and determining the organizational structure, roles, and responsibilities for performing risk management.

- Risk assessment involves conducting risk Analysis to identify risks in terms of assets and their value, threats, existing controls, vulnerabilities that could be exploited, and consequences due to impact and loss should risks be realized. The magnitude of potential consequences is estimated in qualitative terms, quantitative where possible, taking the likelihood of incident occurrence into account. risks are prioritized against evaluation criteria and organizational objectives.
- Develop a risk treatment plan that identifies the controls necessary to reduce, retain, avoid, or transfer identified risks. Controls are selected by per- forming a cost/benefit analysis, taking criteria into account. Residual risk falls within acceptable risk tolerances.
- The decision to accept identified risks and the responsibilities for each decision are formally documented. Responsible managers review and approve proposed risk treatment plans. risk information is shared between decision makers and key stakeholders to provide assurance and support ongoing decision making.

Do

- Implement the risk treatment plan.

Check

- Continually monitor and review risks including all relevant factors (including asset value, impacts, threats, vulnerabilities, and likelihood). Identify and act on any changes that add new assets, threats, and vulnerabilities or that update existing risk dimensions, priorities, and treatment.

Act

- Maintain and improve the information risk management process through ongoing monitoring and review.

According to this standard, all risk management activities should be structured as follows [7]:

- **Input**: identifying information necessary to perform the activity
- **Action**: Describes the activity
- **Implementation Guidance**: provides a guide on how to perform the activity. It is necessary to consider that the proposed guidance does not fit all cases
- **Output:** Identification of any information that derives from the activity of execution

The information security risk management process should contribute primarily to the following points [7]:

- Risk identification
- Risk assessment in terms of their consequences for the business and likelihood of its occurrence
- The likelihood and consequences of risks should be communicated and understood
- Establish a priority order for treatment of risks
- Establish a priority order of actions to reduce the occurrence of risks
- Involvement of stakeholders when decisions under risk management are made and keep them

informed of the status of the various risk management processes

- Effectiveness of treatment of risk monitoring
- Monitoring and review of the risk management process on a regular basis
- Systematically gather information to improve the adopted risk management solution
- Management and organization of staff should be informed of the risks and their actions to mitigate

As represented in Figure 4, it is possible that treating risk will not immediately lead to an acceptable level of residual risk, needing more iterations.

The risk treatment process can be divided in: [6]

- Treatment risk rating;
- Decide whether residual risk levels are acceptable;
- Generate a new treatment of risk the risk levels are not acceptable;
- Evaluate the effectiveness of treatment of risk.

When it comes to the risk acceptance phase, one must ensure that the risks are explicitly accepted by the managers of the organization. This is especially important in a situation where the implementation of controls is omitted or postponed (due to cost). [6]

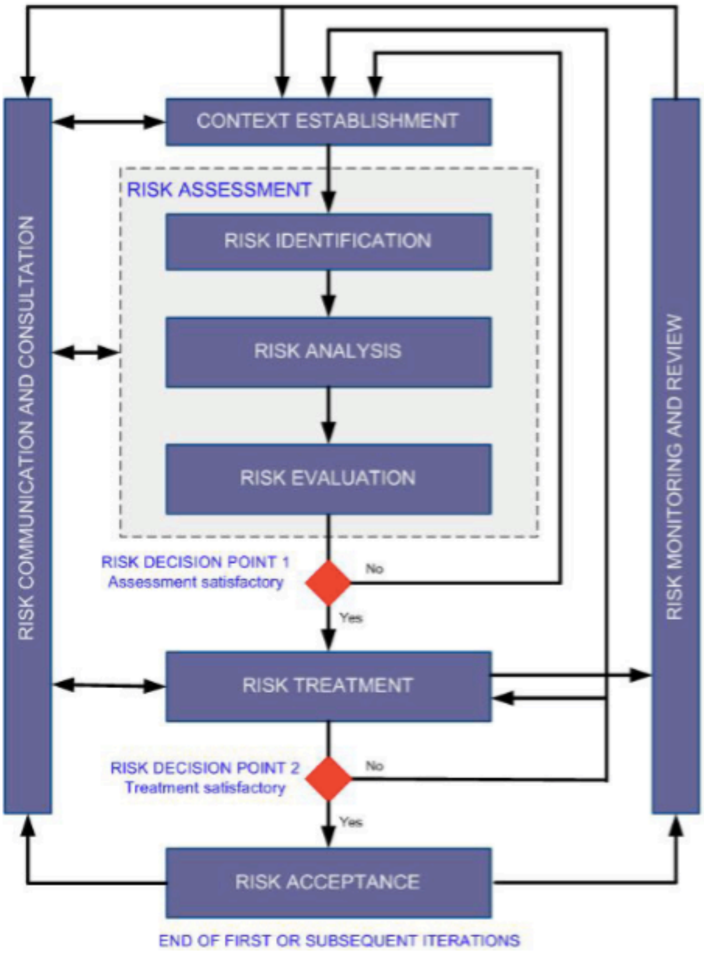


Figure 4 – Information security risk management process [7]

2.2.2. COBIT

COBIT is a comprehensive governance and enterprise IT management framework from ISACA, an international association specializing in IT governance. It includes risk assessment, and has become popular in the US for businesses subject to heavy regulation or auditing. It is likely to suit organizations where legal and regulatory compliance are of utmost importance. [15] Organizations that want to use COBIT should always ensure their chosen risk assessment method appropriately reflects their threats, vulnerabilities and impacts. [15]

ISACA defines information security as something that “ensures that within the enterprise, information is protected against disclosure to unauthorized users (confidentiality), improper modification (integrity) and non-access when required (availability).” [16]

COBIT 5 for information security is an extended view of COBIT 5, containing principles, drivers and benefits from the information security perspective, such as: [16]

- The need to describe information security in an enterprise context.
- An increasing need for enterprises to:
    - Keep risk at acceptable levels.
    - Maintain availability to systems and services.
    - Comply with relevant laws and regulation.
- The need to connect to and align with other major standards and frameworks
- The need to link together all major ISACA research, frameworks and guidance

Some of the benefits include [16]:

- Reduced complexity and increased cost-effectiveness due to improved and easier integration of information security standards
- Informed risk decisions and risk awareness
- Improved prevention, detection and recovery
- Reduced impact of security incidents
- Improved management of costs

2.2.3. OCTAVE

OCTAVE “is a risk-based strategic assessment and planning technique for information security. It is self- directed, meaning that people from within the organization assume responsibility for setting the organization’s security strategy”. [12]

The original OCTAVE method has 3 phases, including the organizational view, leading into the technological view, leading into risk Analysis; generally created for the “multi-layered hierarchy” company that maintains “their own computing infrastructure” [12].

The three phases of OCTAVE are:

- **Phase 1: Build Asset-Based Threat Profiles**
    - Process 1: Identify senior management knowledge
    - Process 2: Identify operational area knowledge
    - Process 3: Identify staff knowledge
    - Process 4: Create threat profiles
- **Phase 2: Identify Infrastructure Vulnerabilities**
    - Process 5: Identify key components
    - Process 6: Evaluate selected components
- **Phase 3: Develop Security Strategy and Plans**
    - Process 7: Conduct risk Analysis
    - Process 8: Develop protection strategy

OCTAVE Allegro is a more streamlined approach that “optimizes the process of assessing information security risks to that an organization can obtain sufficient results with a small investment in people, time, and other limited resources” [13].

The difference with Allegro focuses primarily on the use, storage, transport, and processing of information assets, and asset exposure to threats, vulnerabilities, and disruptions.

Allegro is like the original with eight processes, but has four phases; establishing drivers, profiling assets, identifying threats, identifying/mitigating the resulting risks [12].

Allegro has the following eight steps, divided in four main categories:

- **Establish Drivers**
    - Establish risk measurement criteria
- **Profile Assets**
    - Develop an information asset profile
    - Identify information asset containers
- **Identify Threats**
    - Identify areas of concern
    - Identify threat scenarios
- **Identify and Mitigate risks**
    - Identify risks
    - Analyse risks
    - Select mitigation approach

2.2.4. NIST

NIST is a unit of the United States Commerce Department, founded on 1901. [11]

NIST is one of the U. S’s oldest physical science laboratories, and was established by Congress to remove a major handicap to U.S. industrial competitiveness at the time—a second-rate measurement infrastructure that lagged behind the capabilities of the United Kingdom, Germany, and other economic rivals [11].

Today, NIST supplies users with Standard Reference Materials (SRMs). These documents are certified as having specific characteristics and content, used for measuring equipment, procedures, quality control benchmarks for industrial processes, and experimental control samples [11].

The **NIST 800 Series** is a set of documents that describe United States federal government computer security policies, procedures and guidelines.

They are a result of exhaustive research into methods for optimizing the security of information technology systems and networks in a proactive manner. The publications cover all NIST-recommended procedures and criteria for assessing and documenting threats and vulnerabilities and for implementing security measures to minimize the risk of adverse events, can be used as guidelines for enforcement of security rules and as legal references in case of litigation involving security issues. [11]

The purpose of the **NIST 800-39** document is to provide guidance on the risk management process, using a structured, yet flexible approach for managing risk that is intentionally broad-based, with the specific details of assessing, responding to, and monitoring risk on an ongoing basis.

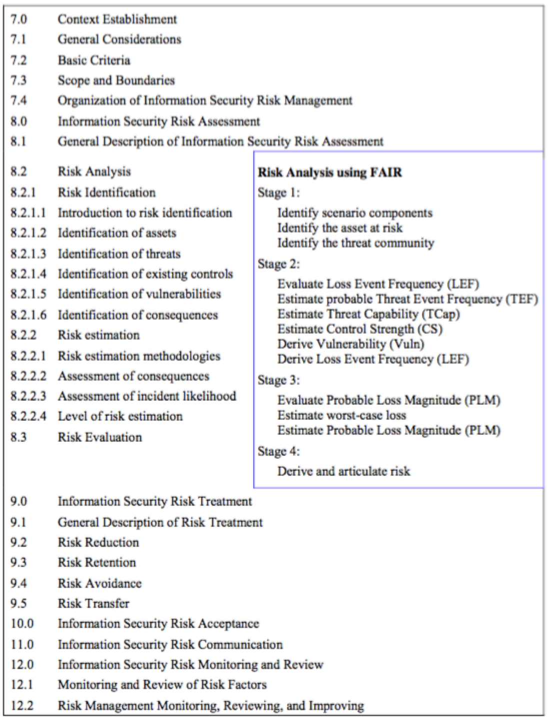
This document describes a process for managing information security risk including [6]:

- a general overview of the risk management process;
- how organizations establish the context for risk-based decisions;
- how organizations assess risk considering threats, vulnerabilities, likelihood, and consequences/impact;
- how organizations respond to risk once determined; and
- how organizations monitor risk over time with changing mission/business needs, operating environments, and supporting information systems.

2.2.5. FAIR

FAIR is a framework for understanding, analysing and measuring information risk [10]. The main idea behind FAIR is consistency, applying a taxonomy for threats, vulnerabilities and risks so that all individuals involved in the risk assessment “speak the same language”.

The main objective of FAIR is to apply risk assessment to any object or asset in an ISO/IEC 27005 structured process (as represented on Figure 5), defending or challenging risk determination using advanced analysis and understanding how time and money will affect the organization's security profile. [10]



7.0 Context Establishment
7.1 General Considerations
7.2 Basic Criteria
7.3 Scope and Boundaries
7.4 Organization of Information Security Risk Management
8.0 Information Security Risk Assessment
8.1 General Description of Information Security Risk Assessment
8.2 Risk Analysis
8.2.1 Risk Identification
8.2.1.1 Introduction to risk identification
8.2.1.2 Identification of assets
8.2.1.3 Identification of threats
8.2.1.4 Identification of existing controls
8.2.1.5 Identification of vulnerabilities
8.2.1.6 Identification of consequences
8.2.2 Risk estimation
8.2.2.1 Risk estimation methodologies
8.2.2.2 Assessment of consequences
8.2.2.3 Assessment of incident likelihood
8.2.2.4 Level of risk estimation
8.3 Risk Evaluation

Risk Analysis using FAIR

Stage 1:
Identify scenario components
Identify the asset at risk
Identify the threat community

Stage 2:
Evaluate Loss Event Frequency (LEF)
Estimate probable Threat Event Frequency (TEF)
Estimate Threat Capability (TCap)
Estimate Control Strength (CS)
Derive Vulnerability (Vuln)
Derive Loss Event Frequency (LEF)

Stage 3:
Evaluate Probable Loss Magnitude (PLM)
Estimate worst-case loss
Estimate Probable Loss Magnitude (PLM)

Stage 4:
Derive and articulate risk

9.0 Information Security Risk Treatment
9.1 General Description of Risk Treatment
9.2 Risk Reduction
9.3 Risk Retention
9.4 Risk Avoidance
9.5 Risk Transfer
10.0 Information Security Risk Acceptance
11.0 Information Security Risk Communication
12.0 Information Security Risk Monitoring and Review
12.1 Monitoring and Review of Risk Factors
12.2 Risk Management Monitoring, Reviewing, and Improving

Figure 5 – How FAIR works with ISO/IEC 27005 [1]

Having clarified the main differences between the selected ISRM references, it is time to define the ontology of concepts that will be present in our proposed domain model. According to our research of the ISRM domain, the main reference found was ISSRM [19].

2.3. ISSRM

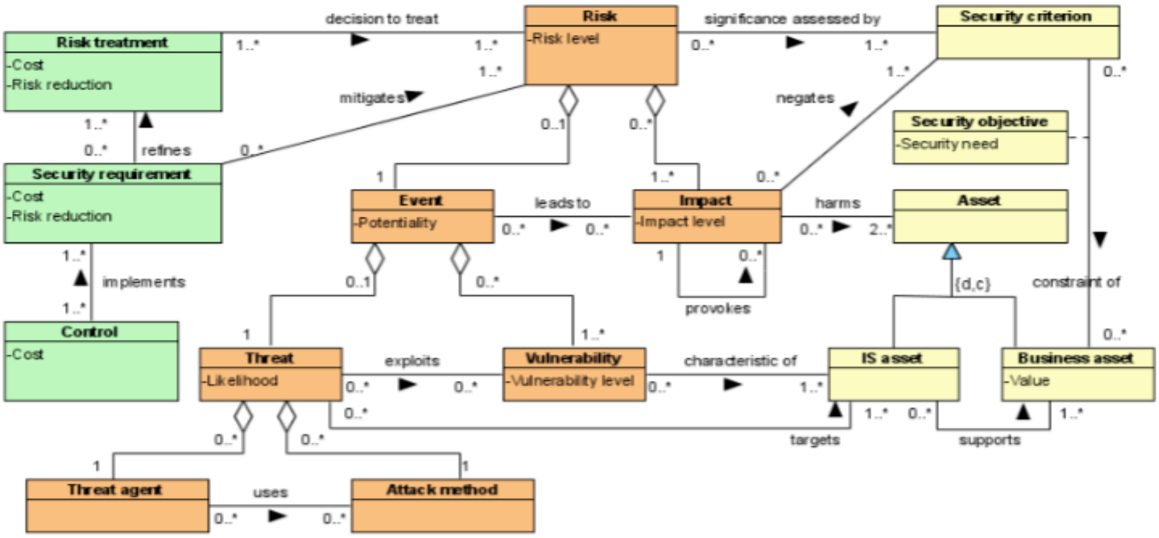


Figure 6 – ISSRM meta-model

Contrary to the previous 2.2.X sub-sections of this chapter, in which different information security frameworks are presented, ISSRM [19] presents what we consider to be a rigorous approach to build a domain model for ISRM, already containing an ontology of related concepts, as it can be seen on Figure 6.

The ISSRM domain model features three main groups of concepts: (i) asset-related concepts, (ii) risk-related concepts, and (iii) risk treatment-related concepts.

Asset-related concepts describe what are the important assets to protect, and what are the criteria to guarantee asset security. The concepts are [19]:

- **Asset** – anything that has value to the organization and is necessary for achieving its objectives. Examples: technical plan; structure calculation process; architectural competence; operating system; Ethernet network; people encoding data; system administrator; air conditioning of server room.
- **Business asset** – information, process, skill inherent to the business of the organization that has value to the organization in terms of its business model and is necessary for achieving its objectives. Examples: technical plan; structure calculation process; architectural competence.
- **IS asset** – a component or part of the IS that has value to the organization and is necessary for achieving its objectives and supporting business assets. An IS asset can be a component of the IT system, like hardware, software or network, but also people or facilities playing a role in the IS and therefore in its security. Examples: operating system; Ethernet network; people encoding data; system administrator; air conditioning of server room.
- **Security criterion** (also called security property) – property or constraint on business assets that characterizes their security needs. Security criteria act as indicators to assess the significance of a risk. Examples: confidentiality; integrity; availability; non-repudiation; accountability.

The second group of concepts are risk-related concepts. They present how the risk itself and its components are defined [19]:

- **Risk**– the combination of a threat with one or more vulnerabilities leading to a negative impact harming one or more of the assets. Threat and vulnerabilities are part of the risk event and impact is the consequence of the risk. Examples: a hacker using social engineering on a member of the company, because of weak awareness of the staff, leading to unauthorized access to personal computers and loss of integrity of the structure calculation process; a thief entering a company building thanks to deficient physical access control, stealing documents containing sensitive information and thereby provoking loss of confidentiality of technical plans.
- **Impact** – the potential negative consequence of a risk that may harm assets of a system or an organization, when a threat (or an event) is accomplished. The impact can be described at the level of IS assets (data destruction, failure of a component, or at the level of business assets, where it negates security criteria, like, for example, loss of confidentiality of an information, loss of integrity of a process, etc. Examples: password discovery (IS level); loss of confidentiality of technical plans (business level).
- **Event** – the combination of a threat and one or more vulnerabilities. Examples: a hacker using social engineering on a member of the company, exploiting weak awareness of the staff; a

thief entering a company building thanks to deficient physical access control.

- **Vulnerability** – the characteristic of an IS asset or group of IS assets that can constitute a weakness or a flaw in terms of IS security. Examples: weak awareness of the staff; deficient physical access control; lack of fire detection.
- **Threat** – potential attack, carried out by an agent that targets one or more IS assets and that may lead to harm to assets. A threat is constituted of a threat agent and an attack method. Examples: a hacker using social engineering on a member of the company; a thief entering a company building and stealing media or documents.
- **Threat agent** – an agent that can potentially cause harm to assets of the IS. A threat agent triggers a threat and is thus the source of a risk. Examples: staff members with little technical skills and time but possibly a strong motivation to carry out an attack; hacker with considerable technical skills, well equipped and strongly motivated by the money he could make.
- **Attack method** – standard means by which a threat agent carries out a threat. Examples: system intrusion; theft of media or documents.

Risk treatment-related concepts describe what decisions, requirements and controls should be defined and implemented in order to mitigate possible risks. According to [19] these are “different levels of design decisions on the IS”:

- **Risk treatment** – the decision of how to treat the identified risks. A treatment satisfies a security need, expressed in generic and functional terms, and can lead to security requirements.
- **Security requirement** – a condition over the phenomena of the environment that we wish to make true by installing the IS, in order to mitigate risks.
- **Control** (also called countermeasure or safeguard) – a designed means to improve security, specified by a security requirement, and implemented to comply with it. Security controls can be processes, policies, devices, practices or other actions or components of the IS and its organization that act to reduce risks.

Although ISSRM appears to have a solid proposal for a ISRM domain model, having defined an ontology of concepts and the relationships between them, it is necessary to get into a more detailed analysis of all the core concepts inside the ISRM domain, in order to build a solid domain model proposal.

After taking into consideration the various ISRM references viewed, we can observe the problem, in which organizations and risk managers find it difficult to identify the ontology of risk concepts and relationships that should be used in the risk management process, since there is such a consolidated body of knowledge. As previously stated at the beginning of chapter 1, the risk register is the tool to support the recording of information relevant for the all phases of the risk management process, meaning that it should be developed according to the pre-defined risk management model.

On the next chapter, we will start by making a comparative analysis between the references analysed, and then retrieving the core concepts presented in them, in order to build our model proposal.

3. Problem Analysis

This chapter describes the steps taken towards defining the proposal for a ISRM model. Having identified the problem at the end of the previous chapter, the comparative analysis between the ISRM references reviewed on the previous chapter is made, as well as a core concept alignment, which will be the base for our ISRM model proposal.

3.1. Analysis of ISRM References

This section provides a comparative analysis of the references described before, which will be the basis for a new proposal of a well-defined ISRM domain model proposal. This comparative analysis is performed with the purpose to clarify the key aspects of that new proposal.

There are many factors to be analysed when choosing a risk management framework and assessment process, that an organization must consider, such as [14]:

- Cost
- Scope of Project
- Required resources are sustainable and proportionate
- Commercial aspects that could restrict its use

As stated in [24], many risk frameworks have been developed over the years, and each has its own advantages and disadvantages, and they all require organizational discipline to define assets, list threats, evaluate controls, and conclude with an estimate of the risk magnitude.

OCTAVE defines assets as including people, hardware, software, information and systems. [21]

The latest product in the OCTAVE series is Allegro, which takes a more focused approach than its predecessors. These series include using surveys and worksheets to gain information during focused discussions and problem-solving sessions. These can either be used directly or customized for a particular organization. [24]

The NIST framework can be applied to any asset, following a similar structure to OCTAVE. It doesn't provide the wealth of forms that OCTAVE does, but is relatively straightforward to follow. [24] Its brevity and focus on more concrete components (e.g., systems) makes it a good candidate for organizations new to risk assessment. Furthermore, because it is defined by NIST, it is approved for use by government agencies and organizations that work with them. [24]

Organizations should have a formal risk assessment methodology, and if not, they should start by reviewing the risk assessment requirements in ISO/IEC 27001 and 27002 and consider the 27005 or NIST approach, since the ISO standards provide a good justification for formal risk assessments and outline requirements, and NIST document provides a good introduction to a risk assessment framework. [24]

COBIT is a IT management and security framework that requires organizations to already have a risk management program. It has its own version of a risk management framework: RISK IT [15], which is a framework based on a set of principles for effective management of IT risk. Just like ISO/IEC 27005, it recommends a repeatable methodology and specifies when risk assessment should take place. The ISO 27000 series is designed to deal with security, while COBIT encompasses all of IT [24], meaning that risk assessment in COBIT, described in RISK IT, goes beyond security risks, including development, business continuity and other types of operational risk in IT, whereas ISO/IEC 27005 concentrates on security exclusively, making it more appropriate to use on the information security domain. [24]

ISO/IEC 27005 specifies in more detail the management of risk, providing guidelines for development of risk assessment context, risk communication, and treatment, including steps called context establishment, risk identification and estimation, in which threats, vulnerabilities and controls are considered, and a risk analysis step that discusses and documents threat likelihood and business impact. [24]

The FAIR methodology can be used in the context of ISO/IEC 27005 to compliment the risk analysis phase*,* by providing the detailed methodology for risk assessment and risk evaluation, being a strong compliment to the ISO/IEC 27005 process in support of the ISMS. Figure 5 illustrates how FAIR methodology fits inside the ISO/IEC 27005 process. [1] [22]

In conclusion, and according to the analysis made, being the most recent framework available after consolidating years of research on the field of ISRM, ISO/IEC 27005 seemed like the logic approach to consider for the basis of this document. However, although ISO/IEC 27005 provides the guidelines for ISRM, defining a set of concepts that can be relevant to ISRM, it does not fully prescribe a risk management model. This is where ISSRM comes in, having what we consider to be a solid proposal for a ISRM domain model, and having defined an ontology of concepts and the relationships between them. This is why, having defined the base framework (ISO/IEC 27005), it is also necessary to make a body of knowledge concept alignment, considering all main concepts and metrics for the development of a domain model. The concepts, present on all the references analysed, considered of most importance for building a domain model proposal, can be found on sections 3.2.1 to 3.2.8 of this chapter.

3.2. Analysis of the Core Domain Model Concepts

This section contains an analysis of the core concepts found in the ISRM body of knowledge, which will become the basis for building our domain model proposal.

3.2.1. Asset

The definition of information security, according to [2], is the "preservation of confidentiality, integrity and availability of information", with information being the primary asset to preserve. On Table 2, below, the definition of "asset" from each of the references analysed can be seen.

ISO	Anything that has value to the organization. [8]
COBIT 5	Something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation. [16]
FAIR	Any data, device, or other component of the environment that supports information-related activities, which can be illicitly accessed, used, disclosed, altered, destroyed, and/or stolen, resulting in loss. [1]
OCTAVE	Something of value to the enterprise. Assets are used by organizations to achieve goals, provide a return on investment, and generate revenue. The overall value of the organization can be represented collectively by the value of its assets. [12]
NIST 800 series	A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems. [6]
ISSRM	Anything that has value to the organization and is necessary for achieving its objectives. [19]

Table 2 – Asset definition according to the various references analysed

While FAIR focuses on its property to represent future loss, instead of referring that assets need protection against threats, or the value that they can bring to an organization, which is the case of the ISO, OCTAVE, COBIT and ISSRM definitions. Our proposal is to define asset as something of either tangible or intangible value that is worth protecting against threats and that has value to the organization.

3.2.2. Threat

Organizations need to protect their information assets to prevent any threat from harming them. On Table 3, the definition of "threat" from each of the references analysed can be seen.

ISO	Potential cause of an unwanted incident, which may result in harm to a system or organization. [2]
COBIT 5	Anything (e.g., object, substance, human) that is capable of acting against an asset in a manner that can result in harm. [16]
FAIR	Anything that is capable of acting in a manner resulting in harm to an asset and/or organization; for example, acts of God (weather, geological events, etc.), malicious actors, errors, failures. [1]
OCTAVE	Indication of a potential undesirable event. [12]
NIST 800 series	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. [6]
ISSRM	Potential attack, carried out by an agent that targets one or more IS assets and that may lead to harm to assets. [19]

Table 3 – Threat definition according to the various references analysed

The threat concept is mostly identical in ISO, COBIT, FAIR and ISSRM, being slightly vague on OCTAVE. A very complete definition can be found on NIST. However, the correlation between threat and asset vulnerability is not mentioned in any case. Our proposal is to define threat as any circumstance or event with the potential to adversely impact organizations operations, assets, individuals, other organizations or the Nation through exploiting their vulnerabilities.

3.2.3. Vulnerability

Threats can harm organization's assets by exploring the weaknesses of the systems in place. These weaknesses can be called vulnerabilities. The definition of "vulnerability" from each of the references analysed can be seen below, on Table 4.

ISO	Weakness of an asset or control that can be exploited by one or more threats. [2]
COBIT 5	A weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threats from threat events. [16]
FAIR	The probability that an asset will be unable to resist actions of a threat agent. [1]
OCTAVE	*Although present throughout the OCTAVE documentation, there is no explicit definition for the term vulnerability.*
NIST 800 series	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. [6]
ISSRM	The characteristic of an IS asset or group of IS assets that can constitute a weakness or a flaw in terms of IS security. [19]

Table 4 – Vulnerability definition according to the various references analysed

When it comes to the vulnerability concept, FAIR focuses on the asset's inability to withstand the effects of the actions of a threat agent, whilst ISSRM focuses on IS assets exclusively and ISO, NIST and COBIT focus on the weakness of any processes inside an organization. According to our analysis the most embracing and complete definition can be found on ISO [2]. Our proposal is to define vulnerability as a weakness of an asset or control that can be exploited by one or more threats in order to negatively affect an organization's assets.

3.2.4. Control

Having identified a vulnerability, controls need to be implemented in order to minimize any damage that can be caused by threats. On Table 5, below, the definition of "control" from each of the references analysed can be seen.

ISO	Measure that is modifying risk. [2]
COBIT 5	The means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of an administrative, technical, management, or legal nature. [16]
FAIR	Those things that will contribute to an ability to resist a threat community. [1]
OCTAVE	*Although present throughout the OCTAVE documentation, there is no explicit definition for the term control.*
NIST 800 series	*Although present throughout the NIST documentation, there is no explicit definition for the term control.*
ISSRM	A designed means to improve security, specified by a security requirement, and implemented to comply with it. [19]

Table 5 – Control definition according to the various references analysed

COBIT 5 refers controls as policies, guidelines and practices of various natures, whilst ISO and FAIR take a more general approach, not entering in any specific detail. ISSRM refers to controls as designated means to improve security. According to our analysis, both COBIT 5 and ISSRM present valuable points in their definitions, so what we propose is a combination of both, referring to control as a designed means to improve security and minimize damage, using procedures, guidelines or practices of various natures to resist threats.

3.2.5. Risk

If well applied, controls can reduce the possibility of assets being harmed by threats, reducing the level of risk. On Table 6, below, the definition of “risk” from each of the references analysed can be seen.

ISO	Effect of uncertainty on objectives. [5]
COBIT 5	The combination of the probability of an event and its consequence. [16]
FAIR	The probable frequency and probable magnitude of future loss. [1]
OCTAVE	Possibility of suffering harm or loss. Refers to a situation where a person could do something undesirable or a natural occurrence could cause an undesirable outcome, resulting in a negative impact or consequence. A risk is composed of an event, a consequence, and uncertainty. [12]
NIST 800 series	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. [6]
ISSRM	The combination of a threat with one or more vulnerabilities leading to a negative impact harming one or more of the assets. [19]

Table 6 – Risk definition according to the various references analysed

The concept of risk always involves the possibility of harm, loss or negative impact, as specified on OCTAVE and ISSRM. Although all the risk definitions are somehow similar, the one featured in NIST seems like the most technical one. However, we consider that the ones found in ISO and COBIT complement each other, resulting in a simple but accurate definition of risk. Our proposal is to define risk as the combination of the probability of an event and its consequence, with effect of uncertainty on objectives.

3.2.6. Event

According to our previous proposed definition, risk is the outcome of combining an event probability with its consequence. Now we will start by analysing the definition of “event” from each of the references analysed can be seen on Table 7, below.

ISO	Occurrence or change of a particular set of circumstances. [2]
COBIT 5	Something that happens at a specific place and/or time. [16]
FAIR	*Although present throughout the FAIR documentation, there is no explicit definition for the term event.*
OCTAVE	*Although present throughout the OCTAVE documentation, there is no explicit definition for the term event.*
NIST 800 series	Any observable occurrence in a network or system. [6]
ISSRM	The combination of a threat and one or more vulnerabilities. [19]

Table 7 – Event definition according to the various references analysed

Although NIST presents a more detailed concept (specifying network or system), ISO, COBIT and NIST have very similar definitions, however somehow vague given the ISRM context. The definition we propose is the one present on ISSRM due to being the most accurate and incorporating key concepts already added to our domain model proposal. Event can, therefore, be defined as the combination of a threat and one or more vulnerabilities.

3.2.7. Consequence

Every event has consequences that can have a positive or negative impact for assets inside an organization. On Table 8, below, the definition of "consequence" from each of the references analysed can be seen.

ISO	Outcome of an event affecting objects. [2]
COBIT 5	*Although present throughout the COBIT documentation, there is no explicit definition for the term consequence.*
FAIR	Loss of effectiveness, adverse operating conditions, loss of business, reputation, damage, etc. [1]
OCTAVE	*Although present throughout the OCTAVE documentation, there is no explicit definition for the term consequence.*
NIST 800 series	*Although present throughout the NIST documentation, there is no explicit definition for the term consequence.*
ISSRM	*Although present throughout the ISSRM documentation, there is no explicit definition for the term consequence.*

Table 8 – Consequence definition according to the various references analysed

From the ISO perspective, a consequence does not equal negative impact, simply meaning there will be an outcome from an event, that will affect the objects involved. FAIR defines consequence as an adverse impact, loss or damage. Our proposal is to define consequence as an outcome of an event, affecting objects in any (positive or negative) way.

3.2.8. Impact

Every consequence caused by any given event has an immediate impact on the organization. On Table 9, below, the definition of "impact" from the frameworks and domain model analysed can be seen.

ISO	Adverse change to the level of business objectives achieved. [7]
COBIT 5	Magnitude of loss resulting from a threat exploiting a vulnerability. [16]
FAIR	*Although present throughout the FAIR documentation, there is no explicit definition for the term impact.*
OCTAVE	The effect of a threat on an organization's mission and business objectives [12]
NIST 800 series	The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability. [20]
ISSRM	The potential negative consequence of a risk that may harm assets of a system or an organization, when a threat (or an event) is accomplished. [19]

Table 9 – Impact definition according to the various references analysed

Given that the context is information security risk management, it is assumed that impact has to have a negative meaning. The OCTAVE definition does not specify this, or the concept of vulnerability, and therefore we consider it did not present the necessary terms to be considered as the "impact" definition. The ISO, NIST and ISSRM definitions all consider impact to be a "harm" or "potential negative consequence", and COBIT speaks of "exploiting a vulnerability". Considering all the definitions, our proposal is to define impact as the potential negative influence of a threat in an organization, by exploring the vulnerabilities found in assets.

Having defined the set of concepts and the base framework, it is necessary to build our ISRM model proposal using a modelling component for providing better support in formalizing different information and knowledge created and exchanged.

On the next chapter of the document, our domain model is represented, using a UML class diagram.

4. Application

On this chapter of the document, the proposed solution is described, and applied to a real life case study of a known organization, following a proposed process to support the development of a reference risk register.

4.1. Domain Model Proposal

The domain model proposal, which can be seen in Figure 7, encompasses all the concepts aligned, as well as the relationships between them:

- **Asset:** something of either tangible or intangible value that is worth protecting against threats and that has value to the organization.
- **Threat:** any circumstance or event with the potential to adversely impact organizations operations, assets, individuals**,** other organizations or the Nation through exploiting the vulnerabilities of organizations systems. Threats also have a likelihood, which can be reduced by the implementation of controls.
- **Vulnerability:** weakness of an asset or control that can be exploited by one or more threats in order to negatively affect an organization's assets.
- **Control:** designed means to improve security and minimize damage, using procedures, guidelines or practices of various natures to resist threats. If well applied, controls can reduce the initial level of risk, leaving only a so called residual risk.
- **Risk:** can be defined as the combination of the probability of an event and its consequence, with effect of uncertainty on objectives. risk has a risk owner, which is the "person or entity with the accountability and authority to manage a risk" [2] and a level of risk, which can be obtained by combining the probability of an event and its consequence. [16]
- **Event:** the combination of a threat and one or more vulnerabilities. Events have likelihood, which can be reduced by the implementation of controls.
- **Consequence:** an outcome of an event, affecting objects in any (positive or negative) way. Consequences can negatively impact organizations, and that negative impact can be reduced thanks to the implementation of controls.
- **Impact:** the potential negative influence of a threat in an organization, by exploring the vulnerabilities found in assets. Negative impact can be reduced thanks to the implementation of controls.

Having arrived to our domain model proposal, we will use it to support the development of a reference risk register proposal in the ISRM domain. To develop this proposal, the proposed domain model will be applied to a real life case of an organization, which will be described on the next section of this document.

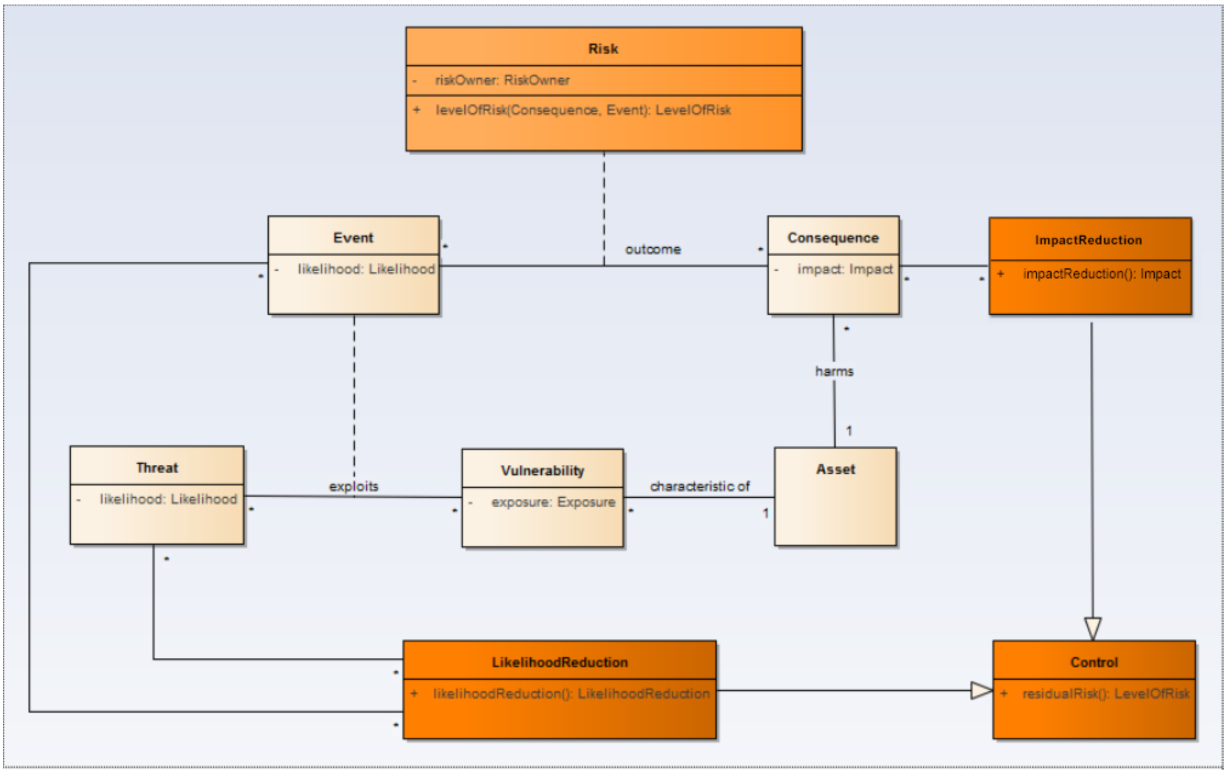


Figure 7 – Domain model proposal

4.2. Case Study

As previously stated, the Case Study is a Portuguese state owned company, operating worldwide.

The Case Study shared information with INESC-ID regarding a information security certification process in the context of a tachograph. A tachograph[2] is a device used to record information about driving time, speed and distance, for transportation vehicles.

The main objective of the analysis of the tachograph practical case was to improve the quality of information, regarding risk identification, based on good practices of risk management in the context of information security. The work done is organized into three major steps, following a proposed process that can be seen in Figure 8, and can be described on the next section of the document.

[2] Tachographs: Rules for Drivers and Operators, Website: https://www.gov.uk/tachographs/overview

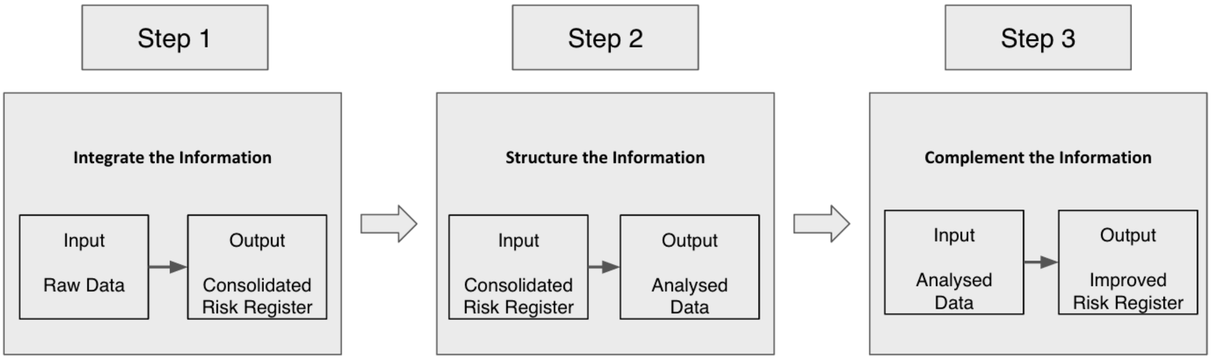

Step 1
Step 2
Step 3
Integrate the Information
Input
Raw Data
Output
Consolidated Risk Register
Structure the Information
Input
Consolidated Risk Register
Output
Analysed Data
Complement the Information
Input
Analysed Data
Output
Improved Risk Register

Figure 8 – Process of using a reference risk register inside an organization

Step 1

- **Integrate the information:** On this phase, the initial raw data that was sent by the Case Study for analysis was consolidated into one Risk Register containing all the risk information supplied.

Step 2

- **Structure the information:** On the second phase, having the information supplied by the Case Study organized into one risk register, it was time to analyse the data, determining whether the information is coherent and what could be improved according to ISO/IEC 27005 and the previously established domain model.

Step 3

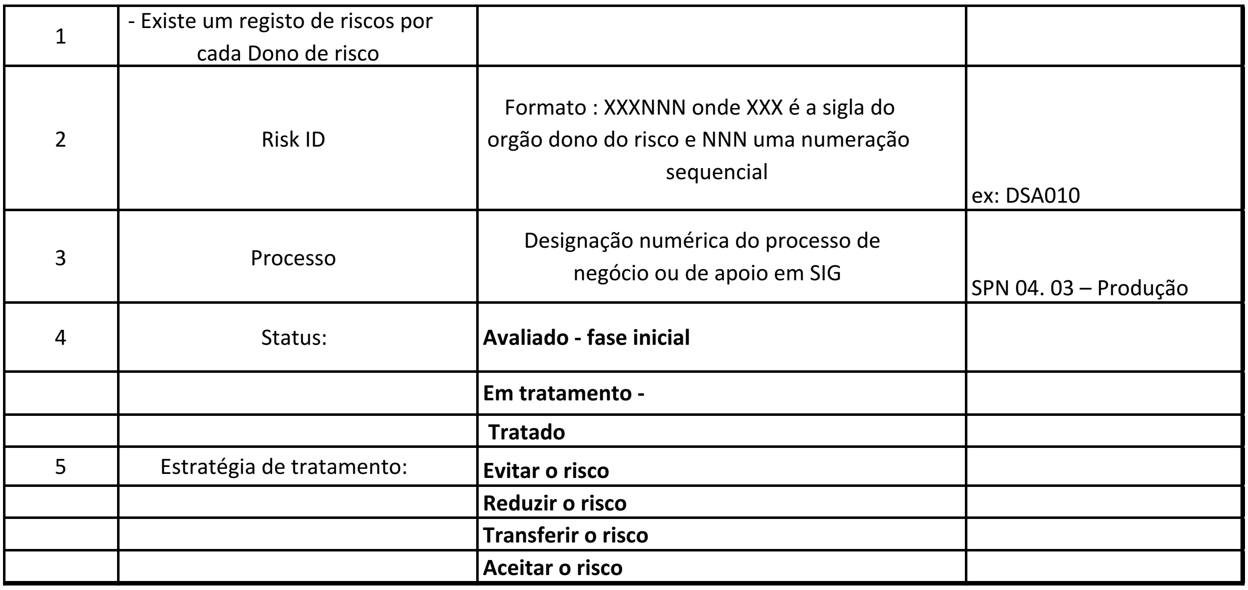
- **Complement the information:** On the third phase, based on the knowledge acquired from literature, improvements and complements to the information are presented resulting in our final reference risk register proposal.

4.3. Process Description

The Case Study started the process by sending a file containing 7 different risk registers, corresponding to 7 different departments inside the organization.

Since the Case Study is a Portuguese organization, all the risk registers information is in native Portuguese. Because of this, it is possible to find on Appendix A the major concepts translated to the English language for a better understanding of the information presented throughout this document.

The structure of the different registers is the same, and is specified on Figure 9.



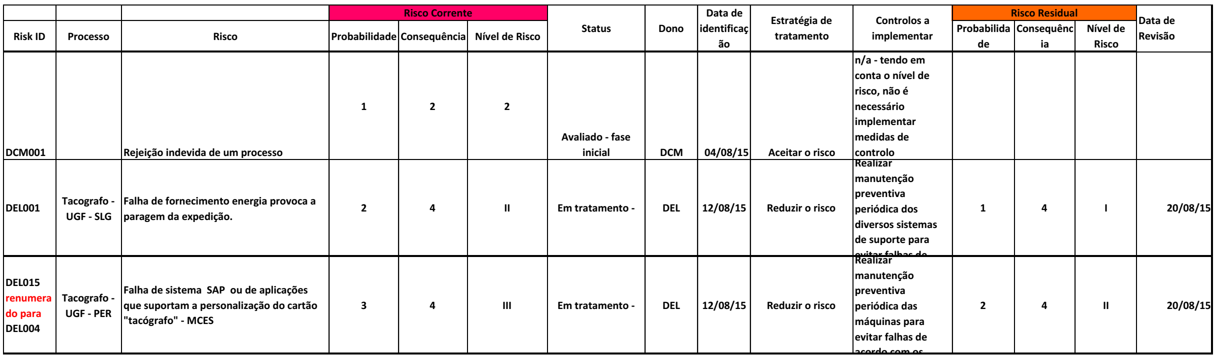
1	- Existe um registo de riscos por cada Dono de risco		
2	Risk ID	Formato : XXXNNN onde XXX é a sigla do orgão dono do risco e NNN uma numeração sequencial	ex: DSA010
3	Processo	Designação numérica do processo de negócio ou de apoio em SIG	SPN 04. 03 – Produção
4	Status:	**Avaliado - fase inicial**	
		Em tratamento -	
		Tratado	
5	Estratégia de tratamento:	**Evitar o risco**	
		Reduzir o risco	
		Transferir o risco	
		Aceitar o risco	

Figure 9 – Structure of the Case Study's risk registers

4.3.1. Integrate the information

Looking at the data for the first time, the first step to take was to consolidate all this information into a single risk register, instead of having the information spread across 7 different departments. Since the proposed work involved every department in the organization, it seemed like a good starting point. A sample of the consolidated risk register can be seen on Figure 10. The risk register can be divided into eleven different sections, related like so: The **risk ID** is the unique identifier to each risk. The **process** is described, according to the information from the Case Study, as the numerical designation of the business process in question. The **status** describes the phase of risk treatment. The states can be "Evaluated – Initial State", "In treatment" or "Treated". The **risk owner** is the "person or entity with the accountability and authority to manage a risk" [2]. The **identification date** specifies when the risk was detected inside the department, as the **revision date** specifies when the risk was last reviewed. Finally, the **risk treatment strategy** and implementation of **controls** describe the strategy and measures to be applied to modify the risk, trying to minimize the Probability of occurrence, and, therefore, turning **current risk** into **residual risk**.

This risk register was then presented on a meeting by INESC-ID to the Case Study as the first product of our work. A more detailed sample of the risk register can be seen on Appendix B.



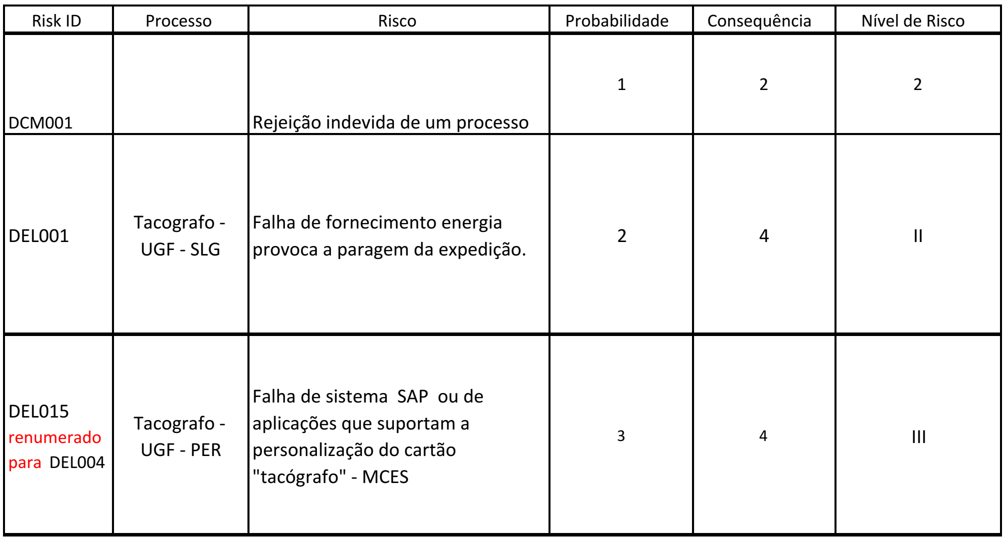
			Risco Corrente								Risco Residual			
Risk ID	Processo	Risco	Probabilidade	Consequência	Nível de Risco	Status	Dono	Data de identificação	Estratégia de tratamento	Controlos a implementar	Probabilidade	Consequência	Nível de Risco	Data de Revisão
DCM001		Rejeição indevida de um processo	1	2	2	Avaliado - fase inicial	DCM	04/08/15	Aceitar o risco	n/a - tendo em conta o nível de risco, não é necessário implementar medidas de controlo				
DEL001	Tacografo - UGF - SLG	Falha de fornecimento energia provoca a paragem da expedição.	2	4	II	Em tratamento -	DEL	12/08/15	Reduzir o risco	Realizar manutenção preventiva periódica dos diversos sistemas de suporte para evitar falhas de	1	4	I	20/08/15
DEL015 renumerado para DEL004	Tacografo - UGF - PER	Falha de sistema SAP ou de aplicações que suportam a personalização do cartão "tacógrafo" - MCES	3	4	III	Em tratamento -	DEL	12/08/15	Reduzir o risco	Realizar manutenção preventiva periódica das máquinas para evitar falhas de acordo com os	2	4	II	20/08/15

Figure 10 – Sample of the consolidated Case Study's risk register

After consolidating the complete information provided by the Case Study, it was time to make a deeper analysis on not only what could be improved, but also to try populate the risk register with more useful information, making it easier for a later analysis.

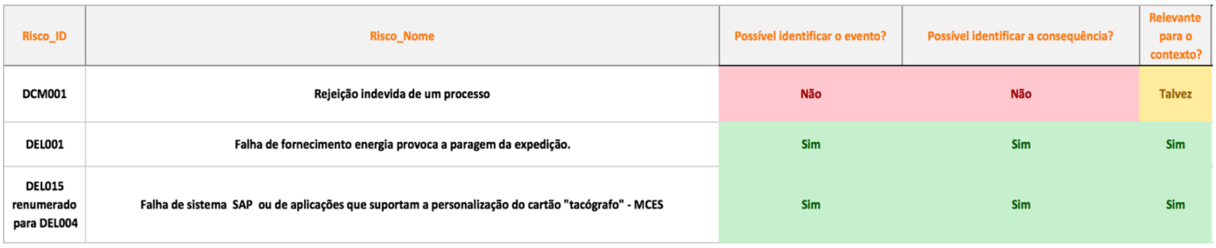
4.3.2. Structure the information

The visual representation of all the information on a single risk register allowed for a facilitated and more effective risk analysis. The first aspect that caught our attention was the domain model used as basis for building each of the department risk registers. In this domain model that the Case Study specified, only the concept of risk is identified. The identified risk is then estimated using three metrics: probability, consequences and risk level, and it can be seen in Figure 11.



Risk ID	Processo	Risco	Probabilidade	Consequência	Nível de Risco
DCM001		Rejeição indevida de um processo	1	2	2
DEL001	Tacografo - UGF - SLG	Falha de fornecimento energia provoca a paragem da expedição.	2	4	II
DEL015 renumerado para DEL004	Tacografo - UGF - PER	Falha de sistema SAP ou de aplicações que suportam a personalização do cartão "tacógrafo" - MCES	3	4	III

Figure 11 – Risk examples retrieved from the consolidated risk register



Risco_ID	Risco_Nome	Possível identificar o evento?	Possível identificar a consequência?	Relevante para o contexto?
DCM001	Rejeição indevida de um processo	Não	Não	Talvez
DEL001	Falha de fornecimento energia provoca a paragem da expedição.	Sim	Sim	Sim
DEL015 renumerado para DEL004	Falha de sistema SAP ou de aplicações que suportam a personalização do cartão "tacógrafo" - MCES	Sim	Sim	Sim

Figure 12 – Partial sample of the initial analysis made on the Case Study's risks

According to the data on Figure 11, it was assumed that both probability and consequence were being estimated using a scale of 1 to 5, based on the analysis of all the risks from the various departments, where the highest number observed was 5. The risk level is believed to have been estimated based on the multiplication of the probability and consequence. However, on two departments, the risk level is to be rated from I to IV, i.e. in roman numerals, as it can be seen on the risks from DEL presented on Figure 11.

Different scales for these types of metrics prevent the comparison between risks, unless there is a direct mapping between the two scales, which was not specified by any document sent by the Case Study. However, due to the analysis made on all risk registers, it was possible to arrive to the conclusion that direct mapping can be done. This matter will be analysed ahead on this chapter.

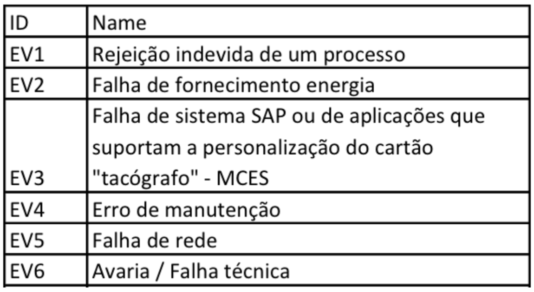
The analysis made also determined whether or not the information retrieved was useful for the problem context. The explanation why that was so, as well as actions recommended to take afterwards have been documented on a table, of which a complete sample can be observed on Appendix C. This table was later sent to the Case Study organization for evaluation purposes. An example of analysed risks can be seen above, on Figure 12.

This new analysis table is organized into 7 columns (from left to right):

- **Risk_ID:** unique identifier to each risk.
- **Risk_Name:** detailed description of each risk according to the Case Study.
- **Is it possible to identify the Event:** Answers can be "Yes" in case the event can be identified, or "No", in case there is not enough information to do so.
- **Is it possible to identify the Consequence:** Answers can be "Yes" in case the consequence can be identified, or "No", in case there is not enough information to do so.
- **Is it relevant to the context:** Answers can be "Yes" in case the risk threats information security, "No" in the case of not representing a threat to information security, or "Maybe" when is not very clear.
- **Interpretation/Explanation:** In case it is not possible to identify the event or consequence in the context of information security or in which way the risk can threat information security.

- **Recommended action:** Action recommended to take. Can either be “Maintain” or “Structure” the risk or “Review” in case it is not possible to identify the event, consequence or if it is not clear that the risk can threat information security.

Based on the research described on chapter 2, and on the ISRM domain model proposal on chapter 3 of this document, is was possible to determine that some key concepts such as event and consequence could be retrieved from some of the risks (since risk is the outcome between event and consequence according to the proposed domain model), while others were impossible to determine because of insufficient information. In the case of the first risk present on Figure 12, DCM001, it was not clear what the event and consequence were, so we marked “No” on the “Is it possible to identify the event” and “Is it possible to identify the consequence“ sections, and marked “Maybe” on the “Is it relevant to the context” section. On the second risk observed on Figure 12, DEL001, the risk name can be translated to “power supply failure causes shipment stop”. In this case, we identified the event as being “power supply failure” and consequence as “shipment stop”. Samples of the lists of events, extracted from the Case Study’s risk registers can be seen below on Figure 13. The complete lists of events, consequences and controls retrieved from the Case Study’s risk information can be seen from Appendix D to F.

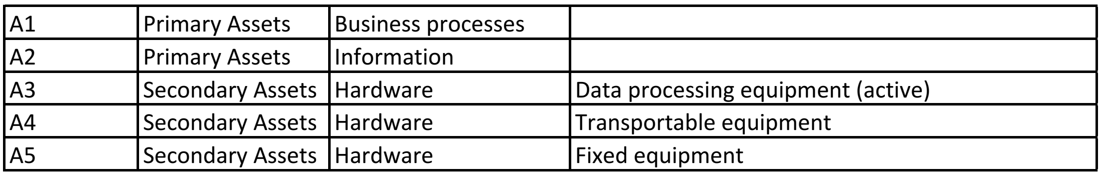


ID	Name
EV1	Rejeição indevida de um processo
EV2	Falha de fornecimento energia
EV3	Falha de sistema SAP ou de aplicações que suportam a personalização do cartão "tacógrafo" - MCES
EV4	Erro de manutenção
EV5	Falha de rede
EV6	Avaria / Falha técnica

Figure 13 – Sample of event list retrieved from the Case Study risk information

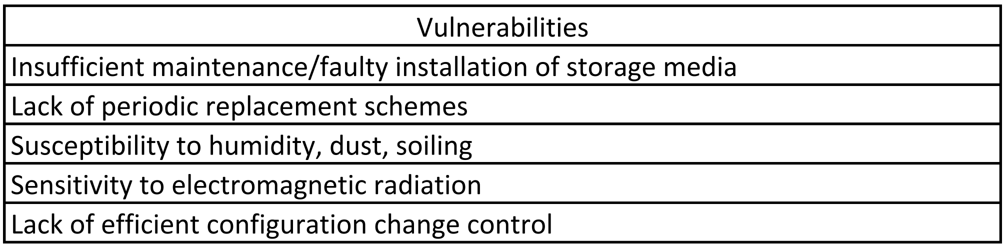
After this analysis, however, it was necessary to enter in even more detail. This was achieved by extracting the maximum information possible from the original risk register, based on the information extracted from ISO/IEC 27005, related to assets, vulnerabilities and threats. Samples of the information retrieved from ISO/IEC 27005 can be seen below, on Figure 14, Figure 15 and Figure 16.

The complete lists of assets, vulnerabilities and threats retrieved can be seen from Appendix G to Appendix I.



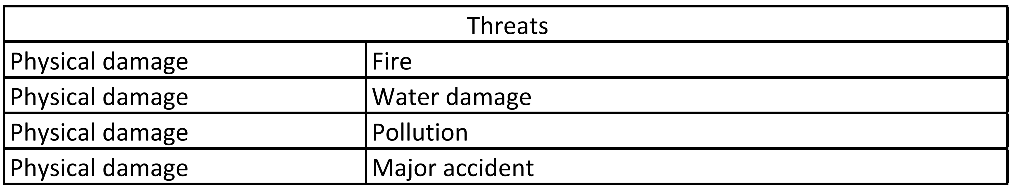
A1	Primary Assets	Business processes	
A2	Primary Assets	Information	
A3	Secondary Assets	Hardware	Data processing equipment (active)
A4	Secondary Assets	Hardware	Transportable equipment
A5	Secondary Assets	Hardware	Fixed equipment

Figure 14 – Sample of ISO/IEC 27005 list of retrieved assets



Vulnerabilities
Insufficient maintenance/faulty installation of storage media
Lack of periodic replacement schemes
Susceptibility to humidity, dust, soiling
Sensitivity to electromagnetic radiation
Lack of efficient configuration change control

Figure 15 – Sample of ISO/IEC 27005 list of retrieved vulnerabilities



Threats	
Physical damage	Fire
Physical damage	Water damage
Physical damage	Pollution
Physical damage	Major accident

Figure 16 – Sample of ISO/IEC 27005 list of retrieved threats

Based on the information retrieved form ISO/IEC 27005, our previous analysis was complemented with more information, which took a form of our final proposed risk register, described on the next section of this document.

4.3.3. Complement the information

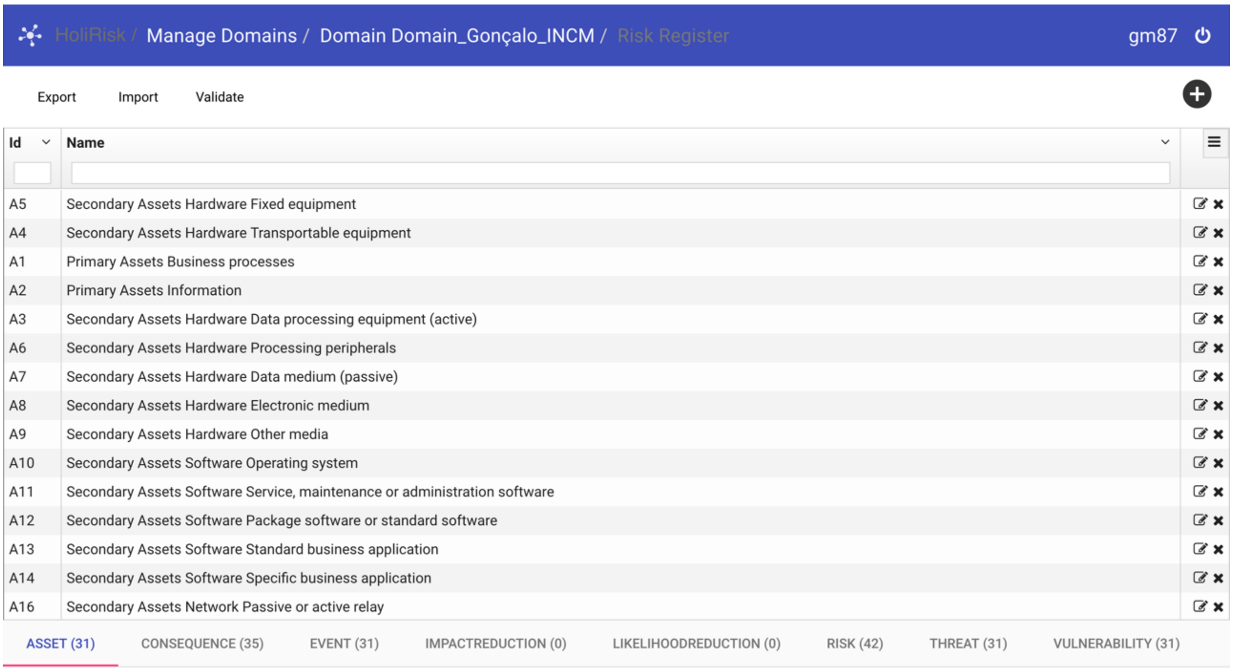
On this section, our final proposal for a reference risk register is presented. This final proposal took into account all the analysis described in this document. A sample of this risk register can be seen on Appendix J.

Our proposed risk register is organized as such (from left to right):

- **Current risk & Residual risk:** on previous risk registers observed in this chapter, the current & residual risk can be described has having three main components: probability, consequence and risk level. As already stated on this chapter, risk level is calculated differently in different departments, therefore, it was necessary to create a uniform grading scale, common to every department. The formula used to calculate risk level on every department is $(\frac{Probability*Consequence}{4})$, with the results rounded to the nearest one. The results are expressed on a quantitative (from 1 to 4) and qualitative scale (from I to IV).
- **Control_ID:** unique identifier to each control.
- **Event_ID:** unique identifier to each event.
- **Event_Name:** Event description, extracted from the risk name.
- **Consequence_ID:** unique identifier to each consequence.
- **Consequence_Name:** Consequence description extracted from the risk name.

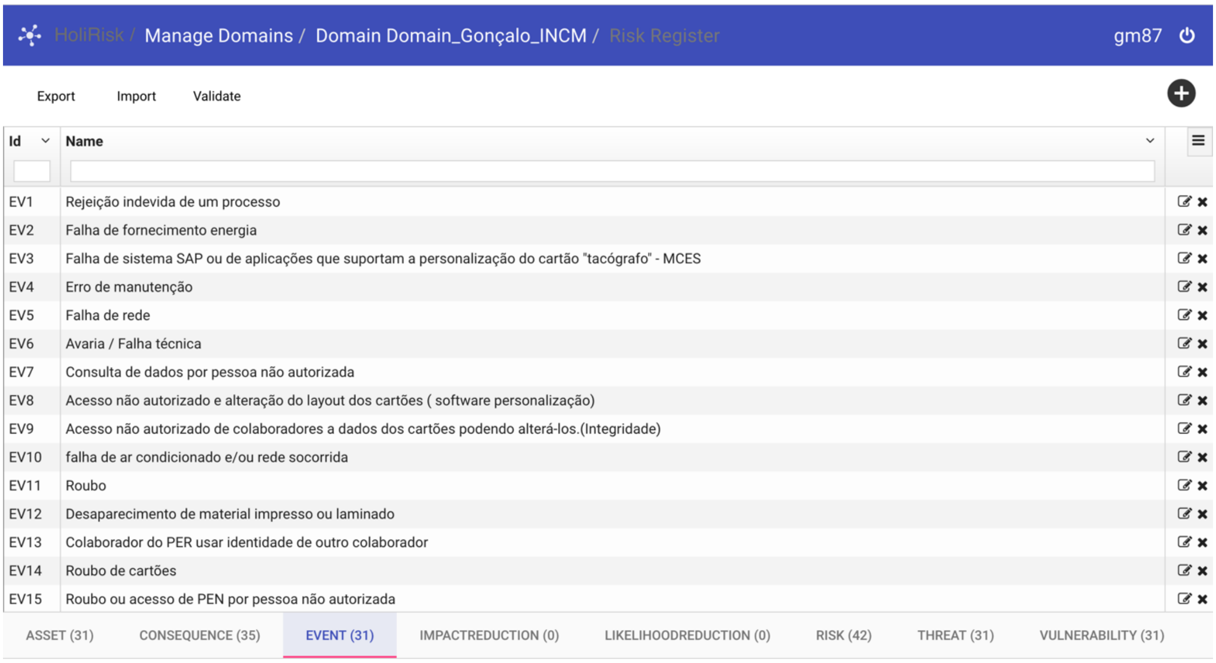
- **Is it possible to identify the Vulnerability:** It was not possible to identify any vulnerabilities within the information provided from the Case Study.
- **Is it possible to identify the Threat:** It was not possible to identify any threats within the information provided from the Case Study.
- **Is it possible to identify the Asset:** Although this information was not explicit within the data provided by the Case Study, according to the information extracted from ISO/IEC 27005 it was possible to identify some of the Assets associated to the risks. In case they weren't completely explicit the term "Uncertain" was used to describe the Assets and in case they could not be found at all the term "No" was used.
- **Asset_Type:** Asset description according to the information extracted from ISO/IEC 27005.
- **Interpretation/Explanation:** In case it is not possible to identify the event or consequence in the context of information security or in which way the risk can threat information security.
- **Recommended action:** Action recommended to take. Can either be "Maintain" or "Structure" the risk or "Review" in case it is not possible to identify the event, consequence or if it is not clear that the risk can threat information security.
- **Revison date:** last date in which the risk was reviewed.

Having completed the risk register information using the Holirisk tool (see below from Figure 17 to 20), and according to the proposed domain model and from the information extracted from ISO/IEC 27005, namely regarding assets, threats and vulnerabilities, it was time once again to send the work done to the Case Study organization, for further analysis and comments on the solution.



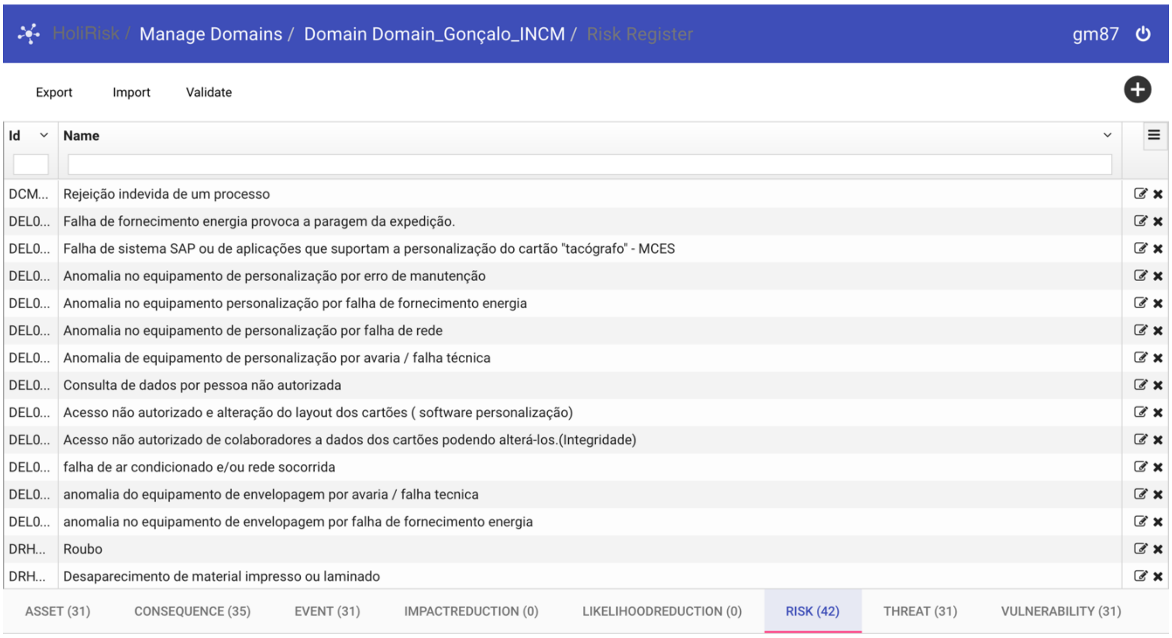
Id	Name
A5	Secondary Assets Hardware Fixed equipment
A4	Secondary Assets Hardware Transportable equipment
A1	Primary Assets Business processes
A2	Primary Assets Information
A3	Secondary Assets Hardware Data processing equipment (active)
A6	Secondary Assets Hardware Processing peripherals
A7	Secondary Assets Hardware Data medium (passive)
A8	Secondary Assets Hardware Electronic medium
A9	Secondary Assets Hardware Other media
A10	Secondary Assets Software Operating system
A11	Secondary Assets Software Service, maintenance or administration software
A12	Secondary Assets Software Package software or standard software
A13	Secondary Assets Software Standard business application
A14	Secondary Assets Software Specific business application
A16	Secondary Assets Network Passive or active relay

Figure 17 – Screenshot of the Holirisk tool showing part of Case Study's asset list



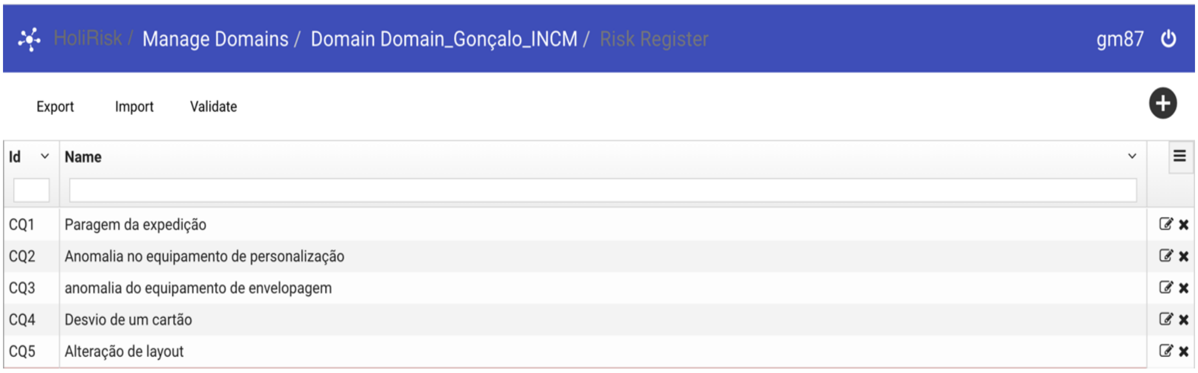
Id	Name
EV1	Rejeição indevida de um processo
EV2	Falha de fornecimento energia
EV3	Falha de sistema SAP ou de aplicações que suportam a personalização do cartão "tacógrafo" - MCES
EV4	Erro de manutenção
EV5	Falha de rede
EV6	Avaria / Falha técnica
EV7	Consulta de dados por pessoa não autorizada
EV8	Acesso não autorizado e alteração do layout dos cartões (software personalização)
EV9	Acesso não autorizado de colaboradores a dados dos cartões podendo alterá-los.(Integridade)
EV10	falha de ar condicionado e/ou rede socorrida
EV11	Roubo
EV12	Desaparecimento de material impresso ou laminado
EV13	Colaborador do PER usar identidade de outro colaborador
EV14	Roubo de cartões
EV15	Roubo ou acesso de PEN por pessoa não autorizada

Figure 18 – Screenshot of the Holirisk tool showing the Case Study’s event list



Id	Name
DCM...	Rejeição indevida de um processo
DELO...	Falha de fornecimento energia provoca a paragem da expedição.
DELO...	Falha de sistema SAP ou de aplicações que suportam a personalização do cartão "tacógrafo" - MCES
DELO...	Anomalia no equipamento de personalização por erro de manutenção
DELO...	Anomalia no equipamento personalização por falha de fornecimento energia
DELO...	Anomalia no equipamento de personalização por falha de rede
DELO...	Anomalia de equipamento de personalização por avaria / falha técnica
DELO...	Consulta de dados por pessoa não autorizada
DELO...	Acesso não autorizado e alteração do layout dos cartões (software personalização)
DELO...	Acesso não autorizado de colaboradores a dados dos cartões podendo alterá-los.(Integridade)
DELO...	falha de ar condicionado e/ou rede socorrida
DELO...	anomalia do equipamento de envelopagem por avaria / falha tecnica
DELO...	anomalia no equipamento de envelopagem por falha de fornecimento energia
DRH...	Roubo
DRH...	Desaparecimento de material impresso ou laminado

Figure 19 – Screenshot of the Holirisk tool showing the Case Study’s risk list


HoliRisk / Manage Domains / Domain Domain_Gonçalo_INCM / Risk Register
gm87
Export
Import
Validate

Id	Name
CQ1	Paragem da expedição
CQ2	Anomalia no equipamento de personalização
CQ3	anomalia do equipamento de envelopagem
CQ4	Desvio de um cartão
CQ5	Alteração de layout

Figure 20 – Screenshot of the Holirisk tool showing the Case Study's consequence list

After a few weeks, the Case Study sent a last version of the risk register, with improvements based on the analysis and comments discussed in this document. A sample of the last risk register sent by the Case Study organization can be seen on Appendix K.

This last register has information consolidated from every department, as suggested by the work done. Threats and vulnerabilities are now specified, showing that our comments and analysis of previous versions were taken into consideration. Asset classification was also made based on ISO/IEC 27005 and our proposed uniform grading scale for risk levels is being used.

Having arrived to the final risk register proposal, it is now time to gather the final conclusions from the work made, and have a discussion about the future work that can be done on this subject.

5. Conclusions and Future Work

In this section of the document, the final conclusions, lessons learned and future work thoughts are discussed.

5.1. Conclusions

During the course of this work, we've analysed in depth the information security risk management domain, specializing in how our proposed process can improve organizations to achieve better understandings of their corporate risks related to ISRM.

We began by gathering research on the information security domain, analysing the frameworks and domain model references to determine the base framework for the work proposed. Then, it was time to build a proposed reference ISRM domain model based on the analysis made. Having completed the proposed model, it was time to present a proposed process to improve the quality of information on organizations, that culminated on a proposal for a reference risk register which was applied to an organization, having proved to add value to their initial solution.

The goal of this research is that more organizations, like the observed Case Study, use our proposed process and conclusions to build their reference risk registers, to record information in a ISRM process more efficiently. After applying our proposed methodology to improve the Case Study's risk register solution using the Holirisk tool, we finally arrived to the latest version of it, that was used inside the Case Study organization. Holirisk will be able to produce detailed risk reports in the future, based on the analysed information, however this feature is still under development.

Although the product of our analysis produced results that were taken into consideration by the Case Study to improve their risk register's quality of information, further steps could have been taken to improve our solution. One of those steps could be apply our process to more organizations, allowing us to observe the effect of our proposal in other contexts, perhaps leading to an improved proposal.

5.2. Lessons

Throughout the course of this project, the ISRM domain was analysed in order to build our risk register proposal. To arrive to our proposed solution, our research consisted in analyzing existing references, and compare them to retrieve the core concepts that were the basis for building our domain model proposal, which later translated in our reference risk register proposal.

It has now become clear that to build a reference risk register proposal, being in the ISRM domain, or other risk management domain, an organized and structured method must be applied in order to arrive to a proposed solution. To build this type of structured solution, here are the steps that describe what we have learned:

- Start by analysing the most important references about the domain in question, making a comparative analysis between them to:
    - Define the risk framework system whose purpose will be to ensure the fulfilment of the goal of risk management;
    - Identify the ontology of risk concepts and relationships that should be used in the risk management process to build our proposed domain model.
- Arrive to the domain model proposal, apply it to a real life case of an organization, by following a process to integrate, structure and complement the information about their risk activities.
- Arrive to a solid reference risk register proposal as the final result of the proposed process.

These steps can surely be improved following further research on the subject of risk management, hence our future work recommendation on the next section of this document.

5.3. Future Work

The most important aspect of a ISRM reference model and process is ensuring that the organization will use it, using a systematic method and applying it regularly. As said in [24], "consistent and repeatable risk assessments provide the mechanism to not only understand risk, but also to demonstrate to auditors and regulators that the organization understands risk."

We believe our proposed method to arrive to a reference risk register is reusable, as it is common to find organizations addressing risk management starting like in the Case Study (by raising the information in spreadhseets, and then struggling with the complexity), allowing organizations to improve their risk assessment strategies.

Our proposed domain model is aligned with the ISO27005, but usually the risk management process can be supported by simpler models (less "powerfull", but much "cheaper" to manage). This raises an interesting question on how to manage an environment where an organization decided to use more than one model.

References

[1] FAIR – ISO/IEC 27005 Cookbook. Published by the Open Group, October 2010.

[2] ISO 27000, Information Technology - Security techniques - information security management systems - Overview and Vocabulary, 2014.

[3] ISO/FDIS 31000, risk management — Principles and guidelines, 2009.

[4] ISO/FDIS 31010, risk Assessment — risk Assessment techniques, 2009.

[5] ISO Guide 73, risk management – Vocabulary, 2009.

[6] NIST 800-39 - Managing information security risk - Organization, Mission and Information System View, 2011.

[7] ISO/IEC 27005, Information technology — Security techniques — information security risk management, 2011.

[8] ISO/IEC 27001, Information technology — Security techniques — information security management systems — Requirements, 2013.

[9] ISO/IEC 27002, Information technology — Security techniques — Code of practice for information security controls, 2013.

[10] Violino, Bob. "IT risk Assessment Frameworks." CSO. Www.CSOOnline.com, 03 May 2010. Web. 29 June 2013.

[11] National Institute of Standards and Technology (NIST) web site. *www.nist.gov*.

[12] Panda, Parthajit, CISA, CISM, CISSP, PMP. "The OCTAVE® Approach to information security risk Assessment." ISACA Journal 4 (2009).

[13] Caralli, Richard; Stevens, James; Young, Lisa; Wilson, William. Introducing OCTAVE Allegro: Improving the information security risk Assessment Process. CMU/SEI- 2007-TR-012. Carnegie Mellon University, Software Engineering Institute, May 2007.

[14] UK government's National Technical Authority for Information Assurance (CESG) web site. *https://www.gov.uk/government/organisations/cesg/[Online].*

[15] ISACA, COBIT 5 for information security, 2012.

[16] ISACA, COBIT 5 – A Business Framework for the Governance and management of Enterprise IT, 2012.

[17] Ken Peers, Tuure Tuunanen, Marcus A Rothenberger, and Samir Chatterjee. A design science research methodology for information systems research. Journal of management information systems, 24(3), 2007.

[18] Järvinen, P. Action research is similar to design science. Quality & Quantity, 41, 1 (2007).

[19] Nicolas Mayer, Éric Dubois, Raimundas Matulevicius and Patrick Heymans. Towards a Measurement Framework for Security risk management.

[20] NIST 800-60 - Volume 1 – Guide for Maping Types of Information and Information Systems to Security Categories, 2008.

[21] Christopher Alberts, Audrey Dorofee. Managing information security risks – The OCTAVE Approach, 2002.

[22] Dan Ionita, Current Established risk assessment methodologies and Tools, 2013.

[23] Marian Firoiu, General considerations on risk management and Information System Security Assessment According to ISO/IEC 27005:2011 and ISO/IEC 31000 Standards, December 2015

[24] Richard Mackey, Choosing the right Information Security Risk Assessment Framework, Information Security Magazine, March 2011

Appendixes

Appendix A – Translation of Portuguese terms to English

Portuguese terms	English terms
Ação recomendada	Recommended action
Ativo	Asset
Ameaça	Threat
Consequência	Consequence
Contexto	Context
Controlos a implementar	Controls to be implemented
Data de identificação	Identification date
Data de revisão	Revision date
Dono	Owner
Estratégia de tratamento	Treatment strategy
Evento	Event
Interpretação	Interpretation
Nível de risco	Risk level
Nome	Name
Probabilidade	Probability
Processo	Process
Registo de riscos	Risk register
Risco	Risk
Risco corrente	Current risk
Risco residual	Residual risk
Tipo	Type

Appendix B – Sample of Case Study's consolidated risk register

Appendix B1 – Risk ID, Process, Risk Name, Current Risk (Probability, Consequence and Risk Level), Status, Risk Owner, Identification Date and Treatment Strategy

			Risco Corrente			Status	Dono	Data de identificação	Estratégia de tratamento
Risk ID	Processo	Risco	Probabilidade	Consequência	Nível de Risco				
DCM001		Rejeição indevida de um processo	1	2	2	Avaliado - fase inicial	DCM	04/08/15	Aceitar o risco
DEL001	Tacografo - UGF - SLG	Falha de fornecimento energia provoca a paragem da expedição.	2	4	II	Em tratamento -	DEL	12/08/15	Reduzir o risco
DEL015 renumerado para DEL004	Tacografo - UGF - PER	Falha de sistema SAP ou de aplicações que suportam a personalização do cartão "tacógrafo" - MCES	3	4	III	Em tratamento -	DEL	12/08/15	Reduzir o risco
DEL005	Tacografo - UGF - PER	Anomalia no equipamento de personalização por erro manutenção	2	3	II	Em tratamento -	DEL	12/08/15	Aceitar o risco

Appendix B2 – Controls to Implement, Residual Risk (Probability, Consequence and Risk Level), Revision Date

Controlos a implementar	Risco Residual			Data de Revisão
	Probabilidade	Consequência	Nível de Risco	
n/a - tendo em conta o nível de risco, não é necessário implementar medidas de controlo				
Realizar manutenção preventiva periódica dos diversos sistemas de suporte para evitar falhas de acordo com os planos de manutenção definidos A11.2.2	1	4	I	20/08/15
Realizar manutenção preventiva periódica das máquinas para evitar falhas de acordo com os planos de manutenção definidos - limpeza de disco, desfragmentação	2	4	II	20/08/15
Realizar manutenção preventiva periódica das máquinas para evitar falhas de acordo com os planos de manutenção definidos A11.2.4	2	3	II	20/08/15

Appendix C – Sample of first risk register after analysis of the Case Study's risks

Appendix C1 – Risk ID and Risk Name

Risco_ID	Risco_Nome
DCM001	Rejeição indevida de um processo
DEL001	Falha de fornecimento energia provoca a paragem da expedição.
DEL015 renum para DEL004	Falha de sistema SAP ou de aplicações que suportam a personalização do cartão "tacógrafo" - MCES
DEL006	Anomalia no equipamento de personalização por erro de manutenção
DEL007	Anomalia no equipamento personalização por falha de fornecimento energia

Appendix C2 – Possible to Identify: Event, Consequence, Context; Interpretation and Recommended Action

Possível identificar o evento?	Possível identificar a consequência?	Relevante para o contexto?	Interpretação/Justificação	Acção Recomendada
Não	Não	Talvez	Não é possivel identificar de que forma o segurança da informação	Rever
Sim	Sim	Sim		Manter/Estruturar
Sim	Sim	Sim		Manter/Estruturar
Sim	Sim	Sim		Manter/Estruturar
Sim	Sim	Sim		Manter/Estruturar

Appendix D – Events extracted from Case Study's consolidated risk register

ID	Name
EV1	Rejeição indevida de um processo
EV2	Falha de fornecimento energia
EV3	Falha de sistema SAP ou de aplicações que suportam a personalização do cartão "tacógrafo" - MCES
EV4	Erro de manutenção
EV5	Falha de rede
EV6	Avaria / Falha técnica
EV7	Consulta de dados por pessoa não autorizada
EV8	Acesso não autorizado e alteração do layout dos cartões (software personalização)
EV9	Acesso não autorizado de colaboradores a dados dos cartões podendo alterá-los.(Integridade)
EV10	falha de ar condicionado e/ou rede socorrida
EV11	Roubo
EV12	Desaparecimento de material impresso ou laminado
EV13	Colaborador do PER usar identidade de outro colaborador
EV14	Roubo de cartões
EV15	Roubo ou acesso de PEN por pessoa não autorizada
EV16	Incêndio
EV17	Acesso não-autorizado PEN
EV18	Falha técnica (sistema SAP)
EV19	Sobrecarga de tráfego SAP
EV20	Ataque destrutivo Comunicações e Software
EV21	Visualização de ficheiros de pré impressão, do cartão "Tacógrafo", por pessoa não autorizada
EV22	Falha de sistema SAP ou de aplicações que suportam a personalização do cartão "tacógrafo"
EV23	Acesso não autorizado de colaboradores a dados dos cartões
EV24	Acesso indevido
EV25	Homologação cartões
EV26	Alteração do modo de entrega
EV27	Erro na produção de chapas ,no contexto de protecção da informação da própria chapa
EV28	Erro na troca de chapa de impressão ou tinta, no contexto do tratamento de produto não conforme e a protecção da informação que lá exista
EV29	Não cumprimento dos procedimentos definidos para a personalização do cartão "Tacógrafo"
EV30	Erro de operador
EV31	Deterioração da PEN

Appendix E – Controls extracted from Case Study’s consolidated risk register

ID	Name		
CT1	n/a - tendo em conta o nível de risco, não é necessário implementar medidas de controlo	CT17	- Impementação de sistemas, automáticos e/ou manuais, de deteção e/ou extinsão de incêndio (DSA) A11.1.3 - Formação e realização de simulácros (DSA) A11.1.3
CT2	Realizar manutenção preventiva periódica dos diversos sistemas de suporte para evitar falhas de acordo com os planos de manutenção definidos	CT18	(A.17.2.1) -A solução SAP está em alta disponibilidade. -Em vias de renovação tecnológica e no âmbito do
CT3	Realizar manutenção preventiva periódica das máquinas para evitar falhas de acordo com os planos de manutenção definidos - limpeza de disco, desfragmentação, checkdisk, instalação de actualizações do fabricante - A.11.2.4;	CT19	(A.17.1.1) -Existem backups.
CT4	Realização de Backups periódicos de softwares e imagens de discos para salvaguarda da informação sensível e garantia de reposição de sistemas em funcionamento em caso de falha de hardware A12.3	CT20	(A.13.1.2) -Existem sistemas de prevenção de ataques (IPS, antivirus, antispam, FW). Identificação a validação que os componentes criticos estão salvaguardados.
CT5	Implementação de restrições de acesso apenas às aplicações e funcionalidade necessárias à produção (desactivação de acesso a outras aplicações e funcionalidades do sistema operativo) - A9.4	CT21	(A.18.2.2) -Necessário rever procedimentos para comportamentos humanos de segurança.
CT6	Activação de Gestão de Acessos de utilizadores de todos os computadores das máquinas: sistema operativo e aplicações - A9.2;	CT22	(A.9.1) -acesso a informação e aos recursos;
CT7	definição de previlégios para alteração de layouts para chefia da secção - A9.2.3	CT23	(A.13.1.3) Esta área é segregada logicamente
CT8	Antes da relação contratual: ASPA 01.02.01 - (A.7.1.1) -Solicitados vários documentos (CV, Registo Criminal e Declaração de Inexistência de Problemas com Instituições Oficiais) e Declção de Confidencialidade.	CT24	A.8.2.3 Acesso a pen's
CT9	No acolhimento e integração: - (A.7.1.2)Fornecida informação sobre a segurança de informação. ASPA 01.02.02	CT25	A.8.3.1 Acesso a pen's
CT10	Durante a relação laboral: -(A.7.2.1) - Manual de Recursos Humanos -Plano de Formação ASPA	CT26	Todo o fluxo é rastreável em sistema. (A.12.4.3)
CT11	(A.7.2.2) -Realizadas ações de sensibilização para a temática da segurança da informação. - Solicitado anualmente registo criminal.	CT27	Implementação da compoenente de Event do SIEM corporativo. (A.12.4.1)
CT12	- (A.7.2.3) -Participação à DJU sempre que algum comportamento possa consubstanciar infração disciplinar. ASPA 01.01.02	CT28	Revisão do processo de controlo de acessos em SAP - GRC. . (A.9.2.3 , A.9.4.1)
CT13	Cessação da relação contratual: (A.7.3)	CT29	Definição do procedimento interno. (A.12.1.1)
CT14	(A.8.1.4) - Documento para as áreas envolvidas (DSA, DSI) para que cada uma delas atue em conformidade, nomeadamente na retirada de acessos e devolução de ativos - RGQ 137 (Cessação	CT30	(A.12-1.4) - Implementação da solução da Gemalto para personalização de cartões de teste. A nova solução interna irá contemplar esta funcionalidade, mas estará apenas pronta em Dezembro de 2015.
CT15	- Implementação de sistemas de segurança (DSA) A11.1.1;	CT31	Criação de lista de nomes autorizados. Criação de pasta na rede para colocação das copias digitalizadas das guias assinadas
CT16	- Controlo de saída de ativos (DSA) A11.1.2		

Appendix F – Consequences extracted from Case Study's consolidated risk register

ID	Name
CQ1	Paragem da expedição
CQ2	Anomalia no equipamento de personalização
CQ3	anomalia do equipamento de envelopagem
CQ4	Desvio de um cartão
CQ5	Alteração de layout

Appendix G – Asset list from ISO/IEC 27005

	Assets		
A1	Primary Assets	Business processes	
A2	Primary Assets	Information	
A3	Secondary Assets	Hardware	Data processing equipment (active)
A4	Secondary Assets	Hardware	Transportable equipment
A5	Secondary Assets	Hardware	Fixed equipment
A6	Secondary Assets	Hardware	Processing peripherals
A7	Secondary Assets	Hardware	Data medium (passive)
A8	Secondary Assets	Hardware	Electronic medium
A9	Secondary Assets	Hardware	Other media
A10	Secondary Assets	Software	Operating system
A11	Secondary Assets	Software	Service, maintenance or administration software
A12	Secondary Assets	Software	Package software or standard software
A13	Secondary Assets	Software	Standard business application
A14	Secondary Assets	Software	Specific business application
A15	Secondary Assets	Network	Medium and supports
A16	Secondary Assets	Network	Passive or active relay
A17	Secondary Assets	Network	Communication interface
A18	Secondary Assets	Personnel	Decision maker
A19	Secondary Assets	Personnel	Users
A20	Secondary Assets	Personnel	Operation/Maintenance staff
A21	Secondary Assets	Personnel	Developers
A22	Secondary Assets	Site	Location - External environment
A23	Secondary Assets	Site	Location - Premises
A24	Secondary Assets	Site	Location - Zone
A25	Secondary Assets	Site	Location - Essential services
A26	Secondary Assets	Site	Location - Communication
A27	Secondary Assets	Site	Location - Utilities
A28	Secondary Assets	Organization	Authorities
A29	Secondary Assets	Organization	Structure of the organization
A30	Secondary Assets	Organization	Project or system organization
A31	Secondary Assets	Organization	Subcontractors / Suppliers / Manufacturers

Appendix H – Threat list from ISO/IEC 27005

Threats	
Physical damage	Fire
Physical damage	Water damage
Physical damage	Pollution
Physical damage	Major accident
Physical damage	Destruction of equipment or media
Physical damage	Dust, corrosion, freezing
Natural Events	Climatic phenomenon
Natural Events	Seismic phenomenon
Natural Events	Volcanic phenomenon
Natural Events	Meteorological phenomenon
Natural Events	Flood
Loss of essential services	Failure of air-conditioning or water supply system
Loss of essential services	Loss of power supply
Loss of essential services	Failure of telecommunication equipment
Disturbance due to radiation	Electromagnetic radiation
Disturbance due to radiation	Thermal radiation
Disturbance due to radiation	Electromagnetic pulses
Compromise of information	Interception of compromising interference signals
Compromise of information	Remote spying
Compromise of information	Eavesdropping
Compromise of information	Theft of media or documents
Compromise of information	Theft of equipment
Compromise of information	Retrieval of recycled or discarded media
Compromise of information	Disclosure
Compromise of information	Data from untrustworthy sources
Compromise of information	Tampering with hardware
Compromise of information	Tampering with software
Compromise of information	Position detection
Technical failures	Equipment failure
Technical failures	Equipment malfunction
Technical failures	Saturation of the information system
Technical failures	Software malfunction
Technical failures	Breach of information system maintainability
Unauthorised actions	Unauthorised use of equipment
Unauthorised actions	Fraudulent copying of software
Unauthorised actions	Use of counterfeit or copied software
Unauthorised actions	Corruption of data
Unauthorised actions	Illegal processing of data
Compromise of functions	Error in use
Compromise of functions	Abuse of rights
Compromise of functions	Forging of rights
Compromise of functions	Denial of actions
Compromise of functions	Breach of personnel availability

Appendix I – Vulnerabilities list from ISO/IEC 27005

Vulnerabilities	Unprotected public network connections
Insufficient maintenance/faulty installation of storage media	Absence of personnel
Lack of periodic replacement schemes	Inadequate recruitment procedures
Susceptibility to humidity, dust, soiling	Insufficient security training
Sensitivity to electromagnetic radiation	Incorrect use of software and hardware
Lack of efficient configuration change control	Lack of security awareness
Susceptibility to voltage variations	Lack of monitoring mechanisms
Susceptibility to temperature variations	Unsupervised work by outside or cleaning staff
Unprotected storage	Lack of policies for the correct use of telecommunications media and messaging
Lack of care at disposal	Inadequate or careless use of physical access control to buildings and rooms
Uncontrolled copying	Location in an area susceptible to flood
No or insufficient software testing	Unstable power grid
Well-known flaws in the software	Lack of physical protection of the building, doors and windows
No 'logout' when leaving the workstation	Lack of formal procedure for user registration and de-registration
Disposal or reuse of storage media without proper erasure	Lack of formal process for access right review (supervision)
Lack of audit trail	Lack or insufficient provisions (concerning security) in contracts with customers and/or third parties
Wrong allocation of access rights	Lack of procedure of monitoring of information processing facilities
Widely-distributed software	Lack of regular audits (supervision)
Applying application programs to the wrong data in terms of time	Lack of procedures of risk identification and assessment
Complicated user interface	Lack of fault reports recorded in administrator and operator logs
Lack of documentation	Inadequate service maintenance response
Incorrect parameter set up	Lack or insufficient Service Level Agreement
Incorrect dates	Lack of change control procedure
Lack of identification and authentication mechanisms like user authentication	Lack of formal procedure for ISMS documentation control
Unprotected password tables	Lack of formal procedure for ISMS record supervision
Poor password management	Lack of formal process for authorization of public available information
Unnecessary services enabled	Lack of proper allocation of information security responsibilities
Immature or new software	Lack of continuity plans
Unclear or incomplete specifications for developers	Lack of e-mail usage policy
Lack of effective change control	Lack of procedures for introducing software into operational systems
Uncontrolled downloading and use of software	Lack of records in administrator and operator logs
Lack of back-up copies	Lack of procedures for classified information handling
Lack of physical protection of the building, doors and windows	Lack of information security responsibilities in job descriptions
Failure to produce management reports	Lack or insufficient provisions (concerning information security) in contracts with employees
Lack of proof of sending or receiving a message	Lack of defined disciplinary process in case of information security incident
Unprotected communication lines	Lack of formal policy on mobile computer usage
Unprotected sensitive traffic	Lack of control of off-premise assets
Poor joint cabling	Lack or insufficient 'clear desk and clear screen' policy
Single point of failure	Lack of information processing facilities authorization
Lack of identification and authentication of sender and receiver	Lack of established monitoring mechanisms for security breaches
Insecure network architecture	Lack of regular management reviews
Transfer of passwords in clear	Lack of procedures for reporting security weaknesses
Inadequate network management (resilience of routing)	Lack of procedures of provisions compliance with intellectual rights

Appendix J – Sample of last proposed risk register

Appendix J1 – Risk ID, Process, Risk Name and Current Risk (Probability, Consequence and Risk Level)

Risco_ID	Processo	Risco_Nome	Risco Corrente		
			Probabilidade	Consequência	Nível de Risco
DCM001		Rejeição indevida de um processo	1	2	I
DEL001	Tacografo - UG SLG	Falha de fornecimento energia provoca a paragem da expedição.	2	4	II
DEL015 renumerado pa DEL004	Tacografo - UG PER	Falha de sistema SAP ou de aplicações que suportam a personaliza "tacógrafo" - MCES	3	4	III
DEL006	Tacografo - UG PER	Anomalia no equipamento de personalização por erro de manutenção	2	3	II

Appendix J2 – Status, Risk Owner, Identification Date, Treatment Strategy, Control ID and Control Name

Status	Dono	Data de identificação	Estratégia de tratamento	Controlo_ID	Controlo_Name
Avaliado - fase inicial	DCM	04/08/15	Aceitar o risco	CT1	n/a - tendo em conta o nível de não é necessário implementar r de controlo
Em tratamento -	DEL	12/08/15	Reduzir o risco	CT2	Realizar manutenção preven periódica dos diversos sistema suporte para evitar falhas de a com os planos de manutenção c A11.2.2
Em tratamento -	DEL	12/08/15	Reduzir o risco	CT3; CT4	Realizar manutenção preven periódica das máquinas para e falhas de acordo com os planc manutenção definidos - limpe disco, desfragmentação, checl instalação de actualizações c fabricante - A.11.2.4; Realização de Backups periódi softwares e imagens de discos salvaguarda da informação sen garantia de reposição de sisten funcionamento em caso de fal
Em tratamento -	DEL	12/08/15	Aceitar o risco	CT3	Realizar manutenção preven periódica das máquinas para e falhas de acordo com os planc manutenção definidos A11.2

Appendix J3 – Event ID, Event Name, Consequence ID, Consequence Name, Consequence Type and Asset Type

Evento_ID	Evento_Nome	Consequência_ID	Consequência_Nome	Consequência_Tipo	Asset_Tipo
EV1	Rejeição indevida de um processo				
EV2	Falha de fornecimento energia	CQ1	Paragem da expedição	Perda de Disponibilidade	
EV3	Falha de sistema SAP ou de aplicaçõ suportam a personalização do car "tacógrafo" - MCES		Impossibilidade de personalização d tacógrafo	Perda de Disponibilidade	
EV4	Erro de manutenção	CQ2	Anomalia no equipamento de personalização	Perda de Disponibilidade	Secondary Asset - Hardware

Appendix J4 – Interpretation, Residual Risk (Probability, Consequence and Risk Level), Recommended Action and Revision Date

Interpretação/Justificação	Risco Residual			Acção Recomendada	Data de Revisão
	Probabilidade	Consequência	Nível de Risco		
Não é possivel identificar de que forr ameaça a segurança da informaç	x	x	x	Rever	
	1	4	I	Manter/Estruturar	20/08/15
	2	4	II	Manter/Estruturar	20/08/15
	2	3	II	Manter/Estruturar	20/08/15

Appendix K – Sample of final version of risk register sent by the Case Study

Appendix K1 – Asset ID, Category, Asset Name, Risk Evaluator, Risk Owner, Threats

Asset ID	Categorias	Activo	Avaliador Risco	Dono Risco	Ameaças Aut Con o m atri acc
			DCM	DCM	Rejeição indevida de um processo
			SLG	DEL	Falha de fornecimento energia provoca a paragem da expedição (Local: SLG - Expedição)
			UGF	DEL	Falha de sistema SAP ou de aplicações que suportam a personalização do cartão "tacógrafo" - MCES (Local: UGF - Personalização)
			UGF	DEL	Anomalia no equipamento de personalização por erro de manutenção (Local: UGF - Personalização)
			UGF	DEL	Anomalia no equipamento de personalização por falha de fornecimento energia (Local: UGF - Personalização)

Appendix K2 – Vulnerabilities, Risk Description, Initial Risk (Impact, Probability and Risk Level)

		Risco Inicial					
		Impacto					
Vulnerabilidades	Descrição Risco INCM	C	I	D	C+I+D	Probabilidad do Risco	Nível de risco antes do controlo ativo
Por solicitação prévia do IMT os elementos da DCM/CGR podem rejeitar um pedido enviado à INCM através de uma transação especifica em SAP . Embora não do ambito da DCM/CGR, a produção (UGF/PER) também pode rejeitar um pedido/cartão por motivo de má qualidade das imagens (fotografia e assinatura do titular). Os pedidos que sejam rejeitados e que já tenham cartões produzidos são enviados diretamente para o IMT para sustentar a sua faturação.	Rejeição indevida de um processo				2	1	2 - I
	Falha de fornecimento energia provoca a paragem da expedição.				4	2	8 - II
	Falha de sistema SAP ou de aplicações que suportam a personalização do cartão "tacógrafo" - MCES				4	3	12 - III
	Anomalia no equipamento de personalização por erro de manutenção				3	2	6 - II
	Anomalia no equipamento personalização por falha de fornecimento energia				3	3	9 - II

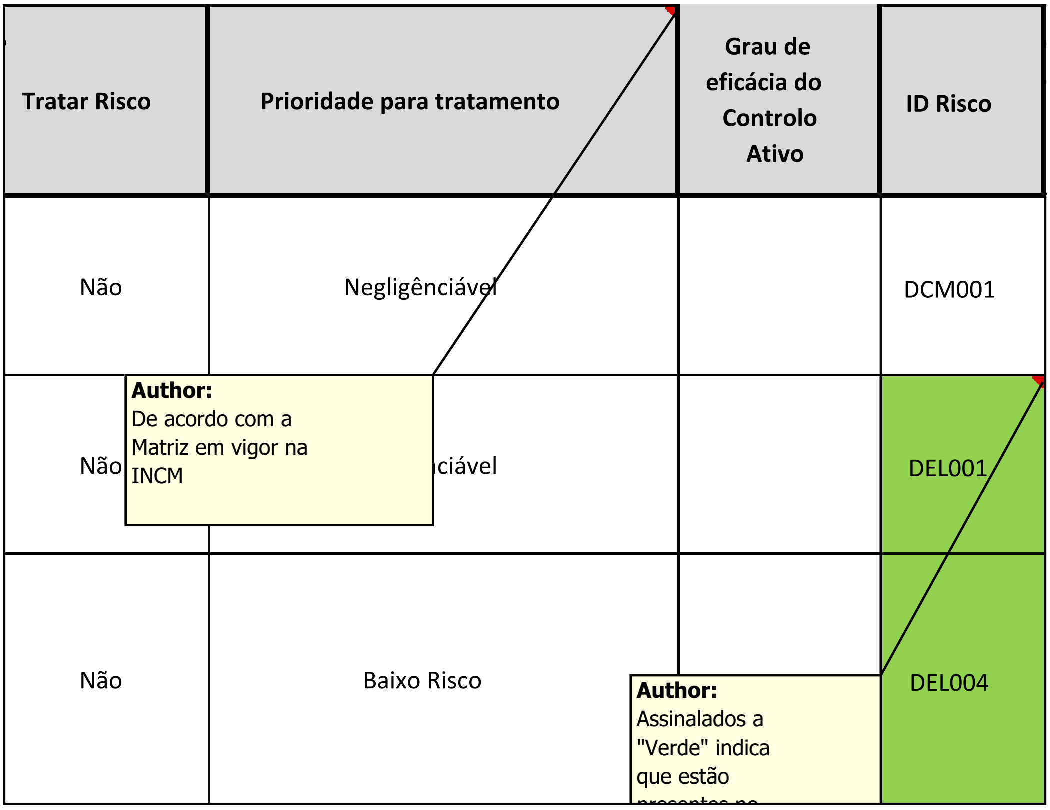
thor:
nsidera-se o
or dos 3
butos de
rdo com a

Author:
Considera-se o maior
dos 3 atributos de
acordo com a matriz

Appendix K3 – Active Controls, Current Risk (Impact, Probability and Risk Level after applying active control)

Controlos Activos	Risco Atual					
	Impacto				Probabilidade do Risco	Nível de risco depois do controlo ativo
	C	I	D	C+I+D		
Author: Considera-se o risco atribuído pelo Avaliador do Risco					Author: Considera-se o risco atribuído pelo Dono	2 - I Author: De acordo com a Matriz em vigor na INCM
Realizar manutenção preventiva periódica das máquinas para evitar falhas de acordo com os planos de manutenção definidos - limpeza de disco, desfragmentação, checkdisk, instalação de actualizações do fabricante - A.11.2.4; Realização de Backups				4	1	4 - I
Realizar manutenção preventiva periódica das máquinas para evitar falhas de acordo com os planos de manutenção definidos - limpeza de disco, desfragmentação, checkdisk, instalação de actualizações do fabricante - A.11.2.4; Realização de Backups periódicos de softwares e imagens de discos para salvaguarda da informação sensível e garantia de reposição de sistemas em funcionamento em caso de falha de hardware A12.3				4	2	8 - II
Realizar manutenção preventiva periódica das máquinas para evitar falhas de acordo com os planos de manutenção definidos A11.2.4				3	2	6 - II
Realizar manutenção preventiva periódica dos diversos sistemas de suporte para evitar falhas de acordo com os planos de manutenção definidos A11.2.2				3	1	3 - I

Appendix K4 – Treat Risk, Priority Treatment, Degree of efficiency of active control, Risk ID

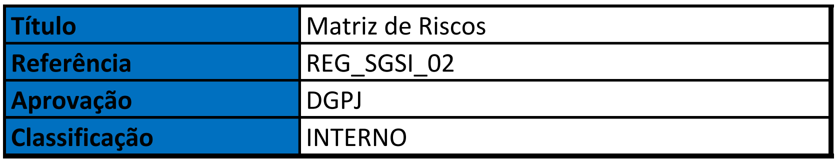


Tratar Risco	Prioridade para tratamento	Grau de eficácia do Controlo Ativo	ID Risco
Não	Negligênciável		DCM001
Não	ciável		DEL001
Não	Baixo Risco		DEL004

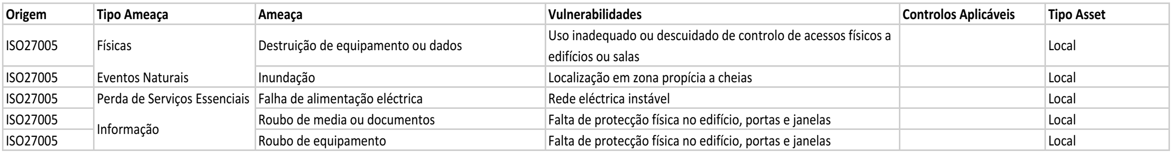
Author:
De acordo com a Matriz em vigor na INCM

Author:
Assinalados a "Verde" indica que estão presentes no

Appendix K5 – Final Case Study risk register auxiliary info



Título	Matriz de Riscos
Referência	REG_SGSI_02
Aprovação	DGPJ
Classificação	INTERNO



Origem	Tipo Ameaça	Ameaça	Vulnerabilidades	Controlos Aplicáveis	Tipo Asset
ISO27005	Físicas	Destruição de equipamento ou dados	Uso inadequado ou descuidado de controlo de acessos físicos a edifícios ou salas		Local
ISO27005	Eventos Naturais	Inundação	Localização em zona propícia a cheias		Local
ISO27005	Perda de Serviços Essenciais	Falha de alimentação eléctrica	Rede eléctrica instável		Local
ISO27005	Informação	Roubo de media ou documentos	Falta de protecção física no edifício, portas e janelas		Local
ISO27005		Roubo de equipamento	Falta de protecção física no edifício, portas e janelas		Local