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

Gonçalo Bernardo Mateus
Instituto Superior Técnico - Taguspark
Telephone: +351961610308, PT
mate8725@gmail.com

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

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 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, the 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 our domain model proposal.
- **Chapter 4 – Application:** In this chapter, the proposed domain model is 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. 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 1, 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, presented in Figure 1, 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]

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

- **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?

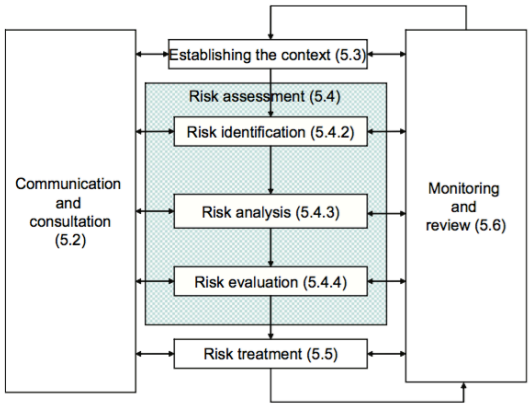


Figure 1 - Risk management process [3]

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 that can be seen on [7].

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 2, 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]

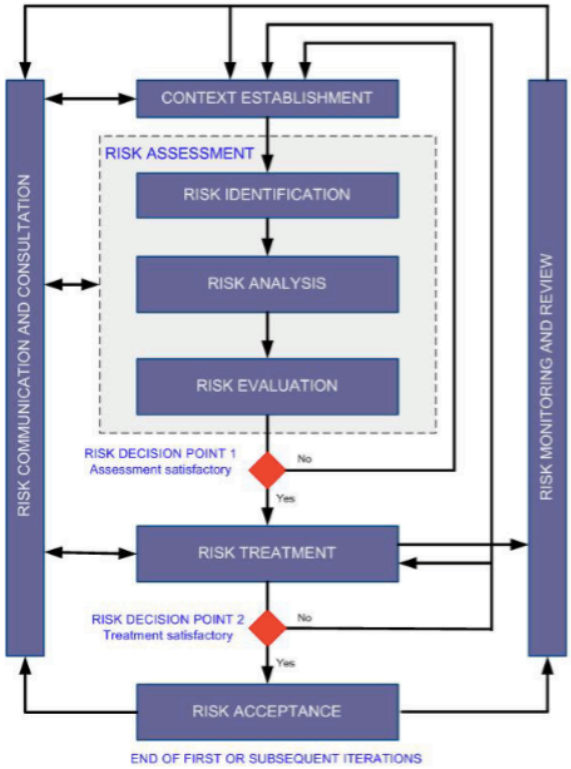


Figure 2 - Information security risk management process [7]

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

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]

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.

2.2.4 NIST

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

2.2.5 FAIR

FAIR is a framework for understanding, analyzing 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, defending or challenging risk determination using advanced analysis and understanding how time and money will affect the organization's security profile. [10]

Having clarified the main differences between the selected ISRM methods, 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].

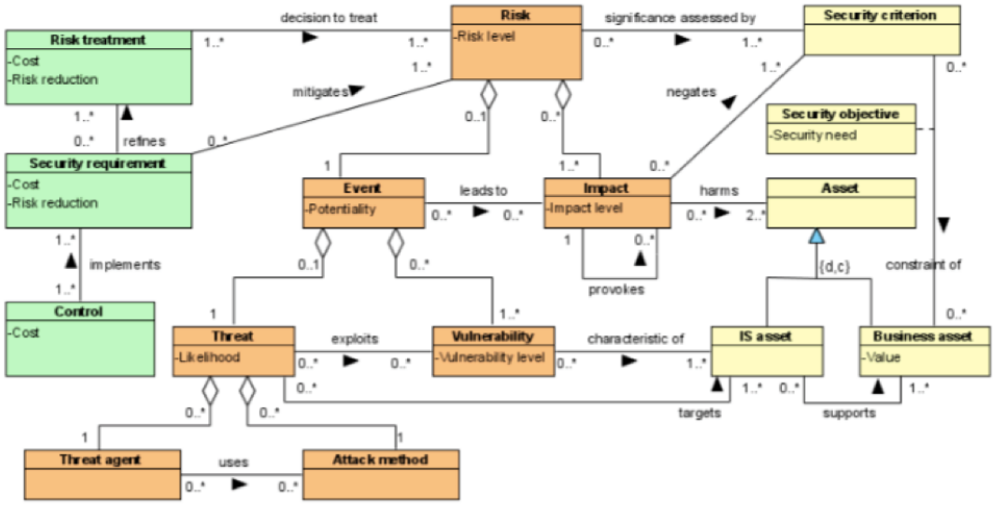


Figure 3 - ISSRM meta-model

2.3 ISSRM

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 3.

The ISSRM domain model features three main groups of concepts: (i) asset-related concepts, (ii) risk-related concepts, and (iii) risk treatment-related concepts. These three main groups of concepts are carefully described on [19].

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, which is that 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 ISRM 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, a comparative analysis between the the 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.

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.

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 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 (seen on Figure 4).

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.

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

The main reason why organizations need to protect their information assets is precisely to prevent any threat from harming them.

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 the vulnerabilities of organizations systems.

3.2.3 Vulnerability

Threats can harm organization assets by exploring the weaknesses of the systems in place. These weaknesses can be called vulnerabilities.

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.

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.

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 result of combining an event probability with is consequence.

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.

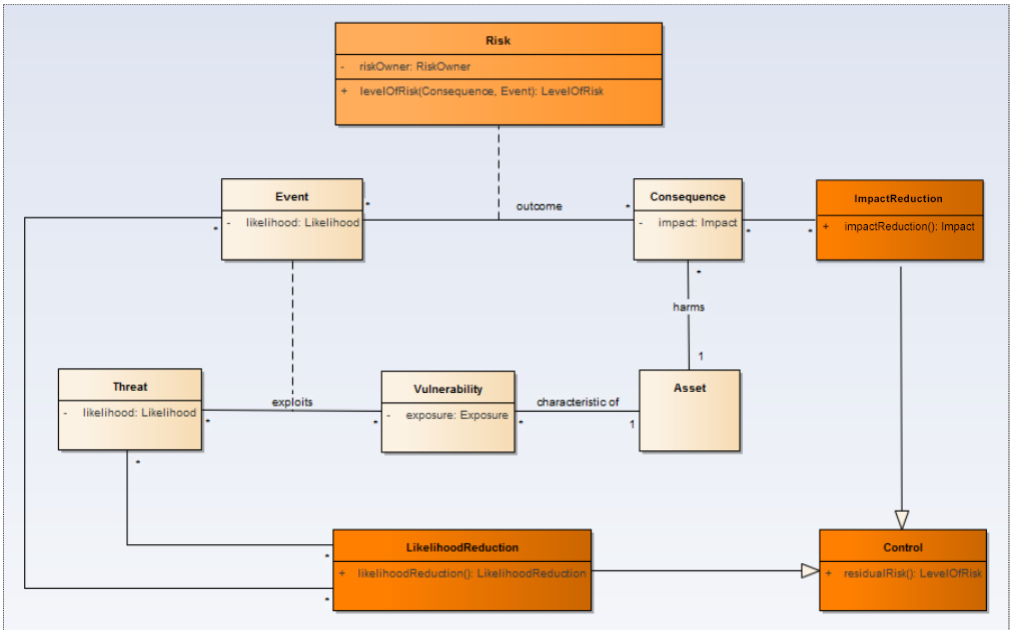
From the ISO perspective, a consequence does not equal negative impact, simply meaning there will be an outcome from an event, that will affect the objects involved. FAIR defines consequence as an adverse impact, loss or damage. Our proposal is to define consequence as an outcome of an event, affecting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

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

Figure 4 – Domain model proposal



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 section of the document, our domain model is represented using a UML class diagram.

3.3 Domain Model Proposal

The domain model proposal, which can be seen in Figure 4, 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 chapter of this document.

4. Application

On this chapter of the document, the proposed solution presented on the previous chapter is 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 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 (**integrate the information, structure the information and complement the information**), that can be described on the next section of the document.

4.2 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.

4.2.1 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. 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.

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

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

with more useful information, making it easier for a later analysis.

4.2.2 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.

According to the data, 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.

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, sent to the Case Study organization for evaluation purposes.

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.

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.

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.

4.2.3 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.

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.
- **Revision date:** last date in which the risk was reviewed.

Having completed the risk register information using the Holirisk tool, according to the proposed domain model, from the information extracted from ISO/IEC 27005, 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.

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.

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.

6. 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]*. **(only referenced on the thesis document)**

[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. **(only referenced on the thesis document)**

[18] Järvinen, P. Action research is similar to design science. Quality & Quantity, 41, 1 (2007). **(only referenced on the thesis document)**

[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. **(only referenced on the thesis document)**

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

[22] Dan Ionita, Current Established risk assessment methodologies and Tools, 2013*]*. **(only referenced on the thesis document)**

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

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