Enterprise risk management

Risk communication and consultation

Guilherme Pinho de Sá Santos

Thesis to obtain the Master of Science Degree in

Information Systems and Computer Engineering

Supervisors: Prof. José Luís Brinquete Borbinha

Examination Committee

Chairperson: Prof. Francisco João Duarte Cordeiro Correia dos Santos
Supervisor: Prof. José Luís Brinquete Borbinha
Members of the Committee: Prof. André Ferreira Ferrão Couto e Vasconcelos

October 2018

To never give up...

Acknowledgments

I would like to start by showing my gratitude to my internship chief, Mr. Ricardo Vieira, for his guidance and support throughout this thesis. His deep knowledge and experience certainly contributed to develop my research and obtain a more consolidated work. Additionally, I would like to address my gratitude to Prof. José Borbinha, for also guiding me through this thesis and for his availability whenever needed. Not least important, I would like to thank to all the INCM members that worked closest to me. I'm also thankful to my closest friends. They were unconditionally present every time I needed and with them I shared some of the most important during my years at the University. Finally, my utmost gratitude words go to my family but particularly to my mother and stepfather, for their endless support and advice during these years, and to Cristiana, for her love and unconditional friendship.

Abstract

Enterprise risk management is becoming a business competitive advantage. Thus, organizations are trying to develop and implement enterprise risk management strategies. Enterprise risk management strategies are based in the implementation of a risk management process and, additionally, structures to support this process, which, together, form a framework. In order this framework to be effective, the risk management process has to include the risk communication and consultation activity and, to materialize it there is a need to create a communication model.

The proposed communication model considers the different needs of the identified groups of stakeholders and, therefore, consists in creating the different views for each one of them. Apart from creating these views, the risk information needs to be presented in an appealing and intuitive way in order to be effectively analyzed. Developing and implementing such communication model implies the understanding of the information architecture that emerges from a specific enterprise risk management framework and, additionally, understanding which information visualization techniques can explore this architecture in an intuitive way. Therefore, this dissertation describes the proposal of a generic communication model applied to a real case study.

The case study is the enterprise risk management framework from *Imprensa Nacional Casa da Moeda*, which is in early development. The proposed communication model was implemented from scratch and shaped to the risk management information architecture of the organization.

As a result of this work, the maturity of the case study framework increased and is now closer to the best practices guidelines, described in the international standards related with this theme. Even though the work brought an increase of maturity, the main goal of this dissertation was to create a risk communication and consultation strategy that could create awareness to stakeholders regarding the enterprise risk management situation and, ultimately, to lead the studied organization to create value through its enterprise risk management framework.

Keywords

Risk, risk management, enterprise risk management, risk communication and consultation, risk management report, information architecture, communication model

Resumo

A gestão de risco corporativo está a tornar-se uma vantangem competitiva de negócio. Assim sendo, as organizacões estão a tentar desenvolver e implementar estratégias de gestão de risco corporativo. As estratégias de gestão de risco corporativo baseiam-se na implementação de um processo de gestão de risco e de estruturas que o suportem. Em conjunto, este processo e as referidas estruturas formam uma *framework*. Para que esta *framework* seja eficaz, o processo de gestão de risco tem de incluir a actividade de comunicacao e consulta de risco e, de forma a materializa-la, existe a necessidade de criar um modelo de comunicação.

O modelo de comunicação proposto considera as diferentes necessidades dos grupos de partes interessadas identificados e, assim sendo, consiste na criação de diferentes vistas para cada um desses grupos. Para além de criar estas vistas, a informação de risco tem de ser apresentada de forma apelativa e intuitiva de modo a ser analisada eficazmente. O desenvolvimento e implementação de um mocelo de comunicação implica o conhecimento e exploração da arquitetura de informação que emerge de uma *framework* de gestão de risco corporativo em especifico. Adicionalmente, perceber quais as técnicas de visualização de informação que podem explorar estas arquitetura de forma intuitiva. Assim sendo, esta dissertação descreve a proposta de um modelo de comunicação genérico aplicado a um caso de estudo real.

O caso de estudo é a *framework* de gestão de risco corporativo da Imprensa Nacional Casa da Moeda, que se encontra num estado inicial de desenvolvimento. O modelo de comuniçãcao proposto foi implementado de raíz e moldado à arquitetura de informação da gestão de risco da organização.

Como resultado deste trabalho, a maturidade da *framework* do caso de estudo aumentou e está agora mais perto das boas praticas descritas nas normas internacionais relacionadas com este tema. Apesar do trabalho ter resultado num aumento de maturidade, o principal objetivo desta dissertação é criar uma estratégia de comunicação e consulta de risco que torna as partes interessadas conscientes do estado da gestão de risco corporativo e, em última análise, levar a organização do caso de estudo a criar valor através da sua *framework* de gestão de risco corporativo.

Palavras Chave

Risco, gestão de risco, gestão de risco corporativo, comunicação e consulta de risco, relatório de gestão de risco, arquitetura da informação, modelo de comunicação

Contents

1 Introduction **2**

1.1 Problem description . . . 3

1.2 Motivations and Objectives . . . 4

1.3 Development method . . . 5

1.4 Document Structure . . . 5

2 Related Work **7**

2.1 Risk management fundamentals . . . 8

2.1.1 Risk management as a process . . . 9

2.1.2 Examples of application domains . . . 14

2.1.3 Conclusions: risk management before and after ISO 31000 . . . 16

2.2 Enterprise risk management . . . 16

2.2.1 Committee of Sponsoring Organizations of the Treadway Commission . . . 17

2.2.2 ISO 31000:2018 as an ERM framework . . . 20

2.2.3 ISO 31000:2018 as a management system standard . . . 22

2.2.4 Alignment between COSO ERM framework 2017 and ISO 31000:2018 . . . 23

2.3 Communication in organizations . . . 25

2.3.1 Organizational communication as a process . . . 25

2.3.2 Organizational communication dimensions . . . 27

2.4 Risk communication and consultation . . . 28

2.5 Conclusion . . . 35

3 Problem analysis **36**

3.1 INCM ERM Framework . . . 38

3.2 Alignment between the INCM ERM framework and ISO 31000:2018 standard . . . 42

3.3 Requirement analysis . . . 44

3.3.1 Requirements for enterprise risks report . . . 44

3.3.2 Requirements for risk mitigation reports . . . 45

3.3.3 Requirements for specialized risks reports . . . 45

3.4 Information model . . . 45

3.5 Conclusion . . . 47

4 Proposed solution **49**
4.1 Communication model . . . 50
4.2 Representation of risk information . . . 51
4.2.1 Statistical information . . . 53
4.2.2 Performance indicator . . . 53
4.2.3 Treatment strategy . . . 55
4.2.4 State of controls . . . 55
4.2.5 Control effectiveness . . . 56
4.2.6 Impact distribution . . . 56
4.2.7 Category distribution . . . 57
4.2.8 Temporal evolution . . . 57
4.3 Risk management reports proposal . . . 58
4.4 Conclusion . . . 60

5 Results demonstration **62**
5.1 Dashboard instance . . . 63
5.2 Enterprise risks report . . . 66
5.3 Risk mitigation reports . . . 67
5.4 Specialized risks reports . . . 67
5.4.1 Information security risk management report . . . 67
5.4.2 Environment risk management report . . . 68
5.4.3 Corruption and related offenses risk management report . . . 69
5.5 Conclusion . . . 71

6 Evaluation **72**
6.1 Evaluation: iterative process . . . 73
6.2 Survey: results and discussion . . . 76

7 Conclusion and future work **81**
7.1 Conclusions . . . 82
7.2 Future work . . . 82

A Risk management: glossary **86**

B Risk assessment techniques **89**

C ISO 31000 and AnnexSL **90**

D Risk management reports survey **91**

List of Figures

1.1 DSRM process 5

2.1 Risk Management Process 9
2.2 Management system components 22
2.3 Organizational communication process: Transactional approach 26
2.4 Say do matrix 27
2.5 Risk matrix example 31
2.6 Example of a domain model to build a risk matrix 32
2.7 Bow-tie diagram example 32
2.8 Example of a domain model to build a bow-tie diagram 33
2.9 Fish-bone diagram example 34
2.10 Example of a compliance dashboard 34

3.1 ERM structure at INCM 38
3.2 Risk categorization at INCM 39
3.3 Negative impact scale 40
3.4 Likelihood scale 41
3.5 Level of risk scale and evaluation criteria 41
3.6 Detailed alignment: INCM ERM framework and ISO 31000:2018 standard 43
3.7 Domain model of the INCM ERM framework 46

4.1 RACI matrix 50
4.2 Dashboard 54
4.3 Evolution conclusions 59

5.1 Dashboard instance 64
5.2 Dashboard instance example 65

6.1 First iteration dashboard proposal 74
6.2 Second iteration dashboard proposal 75
6.3 Proposed improvement for temporal evolution 79
6.4 Proposed improvement for control effectiveness 80

B.1 Risk assessment techniques catalogue 89
C.1 ISO 31000 and AnnexSL alignment 90

List of Tables

2.1 Example of estimation of likelihood 11
2.2 Examples of estimation of negative impact 12
2.3 Example of estimation of a level of risk and consequent risk criteria 12
2.4 Examples of risk management standards 14
2.5 Information security standards 15
2.6 Project management standards 15
2.7 Relevant international norms 15
2.8 COSO ERM framework 2017&ISO 31000:2018 alignment 24

Acronyms

CEO	Chief Executive Officer
CFO	Chief Financial Officer
CISO	Chief Information Security Officer
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CRO	Chief Risk Officer
DSA	*Direção de Segurança e Apoio*
DPC	*Direção de Planeamento e Controlo*
DSRM	Design Science Research Methodology
ERM	Enterprise Risk Management
IA	Internal Audit
INCM	*Imprensa Nacional Casa da Moeda*
ISO	International Organization for Standardization

1

Introduction

Contents

1.1 Problem description 3

1.2 Motivations and Objectives 4

1.3 Development method 5

1.4 Document Structure 5

Nowadays, the more complex an organization is, the more complex the risks associated with its projects and everyday tasks are. This work is meant to approach the concepts **risk management** and **Enterprise Risk Management (ERM)**.

These subjects are critical to organizations because each project (even each single process) has one or more risks and its consequences can be harmful to business. Having this in mind, the majority of big organizations already have risks assessed but in a not standardized way. This happens because the implementation of the risk management process in these organizations is poor and incomplete, being supported by spreadsheets whether within departments, projects or even activities, making it difficult to integrate.

In order to standardize all aspects in the risk management scope, the International Organization for Standardization (ISO) launched the ISO 31000:2018 standard as the main standard regarding this theme, giving us the main principles and guidelines to properly manage risk. The risk management process proposed in this standard is one of the basis of knowledge for this work as it describes the main activities that are performed in risk management. After analyzing this overall picture about risk and risk management, the project will be centered in the concept of ERM.

ERM aims to create value for organizations through the use of risk information in strategic decision-making scenarios. The risk management process is crucial to create the risk information, however, there is a need to create a structure behind it to manage all the aspects emerging from an organization.

An appealing factor of implementing an ERM framework is its potential to increase the maturity level of the processes of an organization. If we conduct a full analysis of the risks we can find risks that affect the performance and reliability of one particular process and, by properly treating all identified risks we improve these factors, leading to an increase of the maturity level of the organization regarding its processes.

This dissertation is focused on the *Imprensa Nacional Casa da Moeda* (INCM) case study. This organization is implementing an ERM framework and offered an internship meant to explore the resulting issues of implementing such framework (issues described further in the report).

INCM is a society of public capitals that resulted from the merger of the "*Casa da Moeda*" and the national press in 1972. INCM is in charge of producing goods and services that are fundamental to the functioning of the Portuguese State, such as edition of official publications; mint; creation of citizen cards, driving licenses and others.

1.1 Problem description

According to [1], interest in ERM "(...) has grown rapidly during the past 15 years, with regulators, professional associations and even rating firms calling for its adoption."

There is a set of standards and certifications that organizations try to follow or accomplish and,

in their recent versions, they started to demand risk management. As a result, organizations rushed to accomplish this new requirement, [1], [2]. The problem with this situation has to do with the fact that while almost every standard mentions risk management, in many cases does not explain how organizations must do it. This resulted in organizations starting to do risk management in a way that is more suitable for them and certifications auditors. Performing risk management only to accomplish the certifications requirements, or just to prove that organizations are in conformity with the best practices, and not in a profitable way, leads to a fragmented risk management strategy. By doing this, organizations do not take advantage of the real purpose of performing ERM, which is creating value.

On the other hand, it is hard to create awareness about the benefits of implementing an ERM strategy among the members of an organization. To do this, organizations need to provide its members with the necessary knowledge on ERM. While this can be beneficial, it can also be a painful process, as providing employees with the appropriate knowledge is a complex process. This increase of complexity can be harmful to the performance of the ERM process.

In order for risk management to be effective and useful, the risk communication and consultation activity needs to be executed. This activity consists in collecting the output of the process and presenting it to the stakeholders, while having in mind that different stakeholders have different needs. Understanding these different needs and choosing which parts of the overall output should be communicated to the different stakeholders is a challenge. This challenge, since it is related with the information emerged from the risk management process and with its dependencies, is an information architecture problem.

After choosing the information, there is a need to present it in an appealing way for it to be used effectively in decision-making scenarios, which is an information visualization problem. The main challenge approached in this work is the risk communication and consultation involved in the risk management process, which, due to directly affecting the performance of this process, is deemed one of the biggest challenges in this area.

1.2 Motivations and Objectives

As stated before, implementing an ERM framework brings many challenges to organizations. In spite of the associated challenges, the benefits of implementing an ERM framework are far more appealing for organizations than the challenges associated with it.

The main motivation of this work is to understand how ERM can be implemented and how it can overcome the mentioned challenges, particularly, risk communication and consultation. This work specifically aims to demonstrate how an organization can perform risk communication, despite its size or context, in order to provide information to making strategic decisions.

To do so, it is necessary to explore a real organization. INCM offered an internship to assist the implementation of its new ERM framework and to actively collaborate in the risk communication and

consultation phase. The idea is to evaluate the proposed framework and then study how the resulting risk information can be presented to stakeholders and how it affects business.

1.3 Development method

This work was developed according to the Design Science Research Methodology (DSRM), which aims to produce knowledge for professionals of the discipline in question, to design solutions for their field problems, [3]. In this case, the discipline is ERM and, specifically, focusing on the risk communication and consultation problem. The DSRM is based on the process illustrated in figure 1.1.

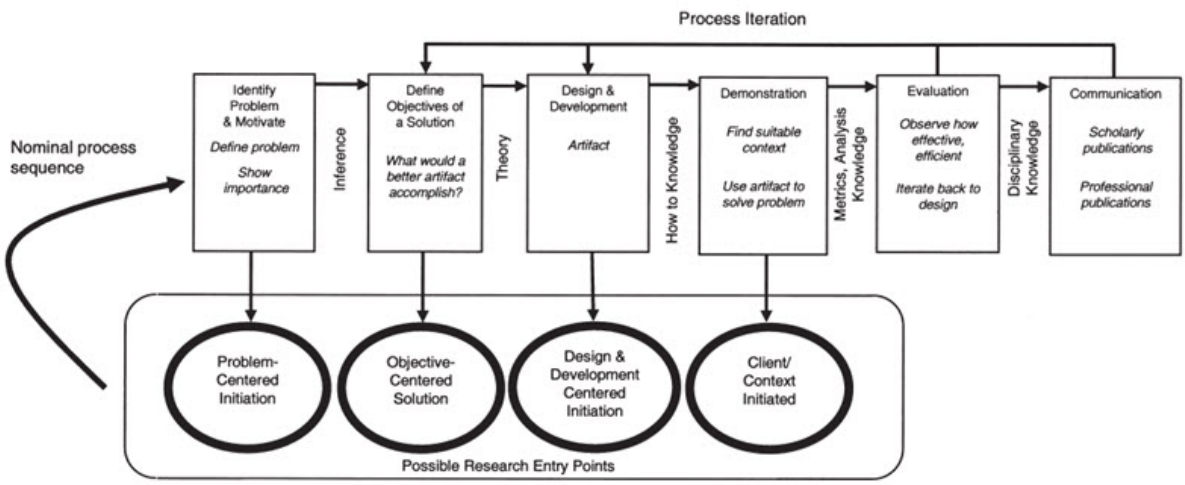

Figure 1.1: DSRM process

The DSRM process starts by **defining the specific research problem** and justifying the value of a solution, including a literature review to gain knowledge about the state of the problem. After the problem is defined, the second step is to **define the objectives** for the solution and then **create the solution** according to these objectives. In this methodology the solution is based in the creation of an artifact. After creating the artifact, its efficiency in solving the problem must be **demonstrated** by experimentation, simulation, a case study, proof, or another appropriate activity. **Evaluating the artifact** involves comparing the objectives of a solution to the actual observed results obtained from the use of the artifact in the demonstration. Lastly, the results must be **communicated** and the work concluded, [3]. In this dissertation, the research entry point was the pursuit of an objective-centered solution aiming to create an adequate artifact for the context of the risk communication and consultation at INCM.

1.4 Document Structure

The rest of this dissertation is organized in six chapters and four appendices. Chapter 2 presents related work to the detailed problem, which includes concepts of risk management and ERM, a section on organizational communication and a state of the art introducing the risk communication and consultation

problem.

Chapter 3 states the problem analysis, where it is described the context on which the problem is explored and where the requirements for the work are specified as well as the information model of the ERM framework in study. Then, chapter 4 presents the proposed solution for the problem in hands.

Chapter 5 explores the proposed solution in order to demonstrate how it tries to solve the problem.

Chapter 6 describes the results of the stakeholder experience and the conclusions made. The last chapter concludes the dissertation with an overall discussion of the work done and the future work proposed.

Finally, in the appendices it is presented a glossary with concepts related with subject of this dissertation, techniques recommended by one of the best practices standards in the subject, an alignment between two references described in the dissertation and, finally, the survey that was distributed to stakeholders in the evaluation phase.

2

Related Work

Contents

2.1 Risk management fundamentals 8

2.2 Enterprise risk management 16

2.3 Communication in organizations 25

2.4 Risk communication and consultation 28

2.5 Conclusion 35

2.1 Risk management fundamentals

According to [4], a risk ”begins with the possibility of an event occurring, i.e. a change on a set of circumstances. An event can create the effect of uncertainty on a business’ objectives and that effect is called risk”, more concisely a risk is the ”effect of uncertainty on objectives”, [4]. Note that, an effect can be negative, positive or both, meaning that risks can be considered as threats and also as opportunities to achieve objectives.

These citations lead us to consider the **causes and consequences** of risks. Causes correspond to the uncertainty associated with the environment of organizations, which can lead to certain events. Consequences correspond to the impact of those events, correlated with its causes, upon the objectives of the organization.

Risk management starts with the necessity of managing these consequences directly assigned with organizations objectives. Risk management can be defined as the ”coordinated activities to direct and control an organization with regard to risk”, [5]. This definition provides us with the vision that risk management is the effort put by organizations in controlling and anticipating those events and its impacts in order to minimize its effects upon business objectives.

The overall goal for risk management is to reduce these impacts, and to do so risks should be treated. Risk mitigation tries to increase the probability of achieving the objectives of the organization and, so, it tries to reduce the likelihood of events occurring or its impacts. That being said, there is a need to conduct a series of activities that enable the control of risks. These on going activities must include the identification of the events that can lead to risks, its likelihoods of occurring and its consequent impacts. Additionally, the ways in which risks can be mitigated must be considered.

Although these activities are the basis of risk management, executing only them does not ensure that risk management will accomplish its objective. There are other activities that should be executed in order to perform an efficient and effective risk management. All of these concerns are described in the ISO 31000:2018 standard.

The ISO 31000:2018 standard addresses risk management in a holistic way, however, there are several other standards that address risk management applied to specific domains. As will be explained further in the report, risk management has several application domains, each with different terminology and concerns.

Regarding the benefits of implementing a risk management strategy, ultimately, risk management increases the likelihood of achieving objectives and improves operational effectiveness and efficiency, leading to a decrease in losses of the organization as a whole.

For further analysis regarding the concepts within this theme, the appendix A shows the main risk management glossary that will be used in this report.

2.1.1 Risk management as a process

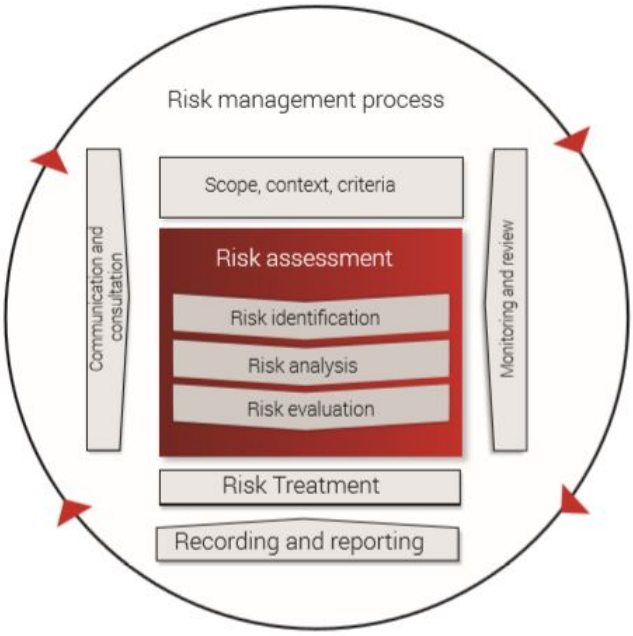

Figure 2.1: Risk Management Process

As stated before, the ISO 31000:2018 addresses risk management in a holistic way and, thus, it proposes a generic risk management process, illustrated in figure 2.1. The objective of this standard is to allow organizations to conduct an effective and efficient risk management. It explores the main aspects of risk management and even establishes several generic principles and guidelines. These guidelines include aspects about the scope of risk management, since it should be part of decision-making scenarios and be an integral part of all organization processes. The ISO 31000:2018 appoints the creation and protection of value for organizations as a goal of risk management.

These principles and guidelines are very generic because each organization has its context and should try to adjust their risk management approach to follow these principles. The adjustments and methodologies used to adjust the risk management approach can vary between organizations since the standard presents the possibility of establishing any scope and context for the risk management strategy.

Note that the ISO 31000:2018 standard is not just a risk management process. It is composed by three main components: Framework, principles and process. Since the main goal of this section is to present a perspective on the fundamentals of the risk management process, the other two components of the ISO 31000:2018 standard will be approached further in this dissertation.

Focusing on the process, according to [4], It "(..) should be an integral part of management, embedded in the culture and practices and tailored to the businesses processes of the organization." This process should be **iterative**, leading to an increased depth and detail of the assessment at each itera-

tion. The iterative approach provides a good balance between minimizing the time and effort spent in identifying controls, while ensuring that high risks are appropriately assessed.

Considering an overall perspective of the process, it can be noticed that the context is established first. Afterwards, a risk assessment is conducted and, should this provide sufficient information to effectively determine the actions required to modify the risks to an acceptable level, then the task is completed and will be followed the risk treatment. If the information is insufficient, another iteration of the risk assessment with revised context (e.g. risk evaluation criteria, risk acceptance criteria or impact criteria) will be conducted, possibly on limited parts of the total scope. The activities of this process, which is represented in figure 2.1, will be detailed below. The inputs, outputs, main concepts and methods for executing each activity will be explored.

Scope, context and criteria: in this activity, the context on which risk management will be performed, as well as the risk criteria, are defined. For example:

- Risk evaluation criteria (prioritize for risk treatment)
- Risk acceptance criteria (defines when a risk is accepted or not)

This activity is critical to the process, as it defines the scope and boundaries for the risk management implementation.

Risk assessment: Using the information obtained in the previous activity as its input, this activity consists on performing the required actions to assess the risks. These actions are divided in three sub-activities:

1. Risk identification
2. Risk analysis
3. Risk evaluation

Risk assessment can be seen as the insight on the risks of each organization, how they affect the objectives and, in the end, its goal is to create the information that will be used for the decision-making in next activity. A catalog of techniques to support this activity, where the techniques that can be applied to the three sub-activities are described, is presented in the ISO 3101 standard, [6] (appendix B).

The output of this activity consists on a list of assessed risks prioritized according to the risk evaluation criteria, previously defined.

Risk identification: the first sub-activity of risk assessment is the identification of risks. Risk identification consists on the creation of an initial list of risks that are identified based on events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives. This identification should be very detailed as the risks that do not appear in the output of this activity will not be addressed in the following steps of the process.

According to the ISO 31000 standard, [4], a risk should be identified through, at least, three concepts: event, consequence and cause (definitions can be found in appendix A) and, additionally, each risk should have a risk owner assigned to it.

As stated before, the techniques that can be applied to risk identification are described in [6] and include: brainstorming, Delphi technique, interviews, cause & effect (a.k.a. Fishbone/Ishikawa), check-lists, among others.

Risk analysis: the risk analysis activity consists on updating the list obtained in the previous step of the assessment with core information. This information is consists on the impact of the consequences, the likelihood of the identified risks and how these two concepts combined define the level of the risk. All factors feasible of affecting the impact and the likelihood of an event occurring should be taken in consideration in this step.

Provided with the results of this activity, the risk owner is able to estimate the impact, likelihood and overall level of risk (as a relation between impact and likelihood). The estimates can consist in two main approaches:

(a) Qualitative risk analysis

(b) Quantitative risk analysis

Qualitative risk analysis uses a scale of qualifying attributes to describe the magnitude of potential consequences (e.g. Low, Medium and High) and the likelihood of occurrence of those consequences. Quantitative risk analysis uses a scale with numerical values (rather than the descriptive scales used in qualitative risk analysis) for both consequences and likelihood, based on a variety of sources.

The methodology chosen to perform risk analysis depends on the context and level of detail required for each risk. The way in which consequences and likelihood are expressed and the ways in which they are combined to provide an impact vary according to the type of risk and the purpose for which the risk assessment output will be used. Table 2.1 and Table 2.2 are examples of combining these two approaches to perform the analysis.

Risk evaluation: in this activity, an analysis of the output of the risk analysis activity is performed. This allows organizations to establish the risks that need treatment and, if so, which risks should be

Table 2.1: Example of estimation of likelihood

Score	Likelihood	Description
5	Very High	The event is expected to occur (once a month)
4	High	The event may occur under most circumstances (once per trimester)
3	Medium	The event is likely to occur (once per semester)
2	Low	The event is not likely, but may occur (once a year)
1	Very Low	It is estimated that the event occurs in exceptional circumstances (less than once a year)

Table 2.2: Examples of estimation of negative impact

Score	Impact	Description
5	Very High	Irreparable financial and reputation loss and consequent loss of credibility or integrity
4	High	It can cause a financial or reputation loss with a long recovery period
3	Medium	It may lead to a short-term financial or reputation loss, but without long-term consequences.
2	Low	Can be solved internally, but need to scale the problem at the department/functional unit level
1	Very Low	Can be resolved internally without escalating the problem

prioritized. The execution of the risk evaluation activity is based on the comparison between the level of risk and the risk evaluation criteria determined in the previous step.

After this activity, the process reaches its first decision point. The risk evaluation can either lead to the decision of not treating the risk in any way other than maintaining existing controls or to the decisions of defining a specific set of required controls that need to be implemented. The decision taken will be influenced by the risk appetite and the risk criteria that have been established. On other hand, if the aforementioned comparison ends up to be unsatisfactory, the process enters a new iteration. Table 2.3 shows an example of a possible estimation of a level of risk and the risk criteria as consequence of a risk appetite.

Table 2.3: Example of estimation of a level of risk and consequent risk criteria

Score	Level of risk	Description
20-25	Intolerable	Immediate action should be taken to reduce the risk before it manifests itself
15-19	Substantial	Efforts should be made to reduce risk as soon as possible
10-14	Moderate	Risk should be controlled. Efficacy of controls should be monitored
5-9	Tolerable	Risk can be accepted. Risk control shall be carried out on the basis of a cost / benefit analysis
1-4	Insignificant	Risk is not a problem for the organization. It should be monitored to ensure that it does not scale

Risk treatment: this activity consists in decision-making. Following the creation of the list containing the evaluated risks, it is necessary to decide which controls should be added to all the risks. Therefore, the risk owner must choose one of five risk treatment options (types of controls):

1. **Risk mitigation**: this option consists on adding controls to reduce the likelihood or the impact of

the risks until the residual risk[1] can be accepted.

2. **Risk acceptance:** should not be performed any action.

3. **Risk avoidance:** avoidance of the risk consists on avoiding the events that lead to risks.

4. **Risk sharing:** the risk is shared with another party which can deal with the risk more effectively.

5. **Risk pursue:** in cases in which the risk is considered an opportunity to achieve objectives, actions to increase the exposure to the risk should be performed.

Selecting the most appropriate risk treatment option involves balancing the costs and efforts of implementation against the benefits derived from it, with regard to legal, regulatory, and other requirements such as social responsibility and the protection of the natural environment. When decisions are made, it should also be noticed that a risk treatment can turn out to be unjustifiable on economic grounds, e.g. severe (high negative consequence) but rare (low likelihood) risks.

Parallel to these activities, there are two other activities that need to be executed: **Communication and Consultation** and **Monitoring and Review** of the process.

Monitoring and review: this is a current task along the execution of the risk management process, and its purpose is to monitor the effectiveness and efficiency of the process by analyzing the output of the process activities. Ultimately, its purpose is to continuously improve the process and ensure that all activities are being executed under the right scope.

Communication and consultation: this activity is important as it connects the main stakeholders and the process. This connection is fundamental to understand the basis on which decisions are made and the need of performing specific actions. Communication and consultation is current and should be executed continuously throughout the process since it is connected with all other activity. It begins when the context is established and only finishes when the risk is accepted. The execution of this activity can provide crucial input for all other activities. In short, the output of communication and consultation is the continual understanding of the risk management process and of its results.

To materialize the risk communication and consultation activity, organizations should develop communication and consultation plans that address the issues related with causes, consequences and controls of risks. This information is critical for decision-making scenarios, as the capacity of main stakeholders to understand the basis on which decisions are made, as well as the reasons behind the choice of a specific strategic path, depend on this activity. This dependency shows how this activity is important and, on the other hand, how challenging it can. If communication and consultation is not effective, the overall process also loses effectiveness i.e. the information resulting from the process is not useful for decision-making.

[1] Residual risk - ”Remaining risk after treatment of the same”, [5]

Regarding the techniques to perform this activity, the catalog in the ISO 31010 standard presents techniques that can be applied in risk communication and consultation, for example risk matrix, bow-tie diagrams, fish-bone diagrams and others (this is explored in the section 2.4 of this dissertation). This activity is the core theme approached in this dissertation, as will be further explained in the report. In this section, the main goal was only to describe the activity according to [4], where there is no focus on the challenges inherent to its execution.

Recording and Reporting: In 2018, when the new version of the ISO 31000 standard was released, ISO presented a new activity that complements communication and consultation. This activity, called "Recording & Reporting", is intended to guide communication and consultation and that such is recorded (guidance for this was not clear in the ISO 31000:2009 version, leaving to the readers interpretation on how it should be done).

2.1.2 Examples of application domains

The goal of this section is to provide a clear vision of the several application domains for risk management. To do this, the appearance of risk management in different domains will be described.

With ISO the 31000:2018 standard, organizations can apply the risk management process in all their business domains, i.e. as explained before, ISO 31000:2018 can be adapted to every industry, every organization, even to every department. Many industries follow their own risk management standards or have the need to follow specific standards which demand the execution of risk management. In fact, inside an organization is usual to use different risk management terminologies according to the business domain itself. Table 2.4 shows examples of risk management standards from three different domains. In these risk management standards for different domains, the terminologies for the same concepts diverge.

Regarding the information security domain, which is a critical concern to organization that deal with privacy issues, there are several standards regarding every aspect of the information security as a whole. Table 2.5 presents a sample of these standards and all of them mention risk management as a critical requirement for success of the given purpose. Essentially, in all aspects of information security there is

Table 2.4: Examples of risk management standards

Identification	Description
ISO 27005:2011 - Information technology – Security techniques - Information security Risk Management	Provides guidelines for information security risk management in an organization
ISO 1608:2006 - Systems and software engineering – Life cycle processes – Risk Management	Describes a process for the management of risk during systems or software acquisitions, supply, development, operations and maintenance
ISO 14971:2007 - Medical devices – Application of risk management to medical devices	Specifies a procedure by which a manufacturer can identify the hazards associated with medical devices and can manage it.

Table 2.5: Information security standards

Identification	Description
ISO 13335:2004 - IT Security Management	Contains guidance on the management of IT security
ISO 15408:1999 - Information Technology – Security techniques – Evaluation criteria for IT security	Defines criteria to be used as the basis for evaluation of security properties of IT products and systems
ISO 18028:2006 - Information Technology – Security Techniques – IT network security	Provides detailed guidance on the security aspects of the management, operation and use of information technology (IT) networks, and their interconnections.
ISO 14298:2013 - Graphic Technology – Management of security printing process	Specifies requirements for a security management system for security printers.

Table 2.6: Project management standards

Identification	Description
ISO 21500:2012 - Guidance on Project management	Provides high-level description of concepts and processes that are considered to form good practice in project management
PMBOK (Project management body of knowledge)	It is the entire collection of processes, best practices, terminologies, and guidelines that are accepted as standards within the project management industry.

a concern of risk management.

Furthermore, there is a correlation between project management and risk management. The objective of exploring project management is to understand that risk management application can be at project level. Table 2.6 presents two standards that have modules about this theme and both establish their one vision about the subject.

Another interesting scope to explore is certifications and international standards that, nowadays, are common in the organizations. As stated before, organizations try to accomplish certifications or follow international standards to gain competitive advantage, and in certain occasions, some clients specifically require that organizations accomplish these certifications in order to develop the intended products. Table 2.7 shows common international standards, that many organizations pursue, which have as requirement performing risk management.

Table 2.7: Relevant international norms

Identification	Description
ISO 9001:2015 - Quality Management Systems – Requirements	Specifies Requirements to implement Quality management systems
ISO 14001:2015 - Environmental management systems – Requirements and Guidelines	Specifies Requirements that enable to organizations achieve their objectives regarding their Environmental management systems

2.1.3 Conclusions: risk management before and after ISO 31000

It is possible to understand how risk management can be fragmented inside an organization. Having different terminologies for the same theme inside a single organization is not an efficient strategy and the need for standardize these issues is urgent.

In 2004, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) already began this work of standardizing risk concepts. With the COSO ERM framework 2004, COSO tried to fill "the need for an enterprise risk management framework, providing key principles and concepts, a common language, and clear direction and guidance (...)", [7]. As expected, the acceptance of this new framework was positive, leading the business world to start following its terminology. However, over the years, it became clear that this framework was too complex and complicated for organizations to implement, [2]. On the other hand, since ISO 31000:2009 or, more recently, ISO 31000:2018, is simpler, it is easier for organizations to follow it, [8].

The result is that, before ISO 31000:2009, each standard simply tried to define why it was important to perform risk management in its context and the ones who tried to explain how to do it, essentially, tried to gather topics from the others standards. After its creation, almost every standard started to reference ISO 31000:2009 as the main source of knowledge in this matter. Even when standards provide risk management processes with different terminologies, they all match with the process proposed in the ISO 31000:2009 standard. If we look into different industries, the risk management processes performed can be aligned with ISO 31000:2009. For example, if we compare the processes of the ISO 31000:2009 standard and the ISO 27005:2011 - Information technology – Security techniques - Information security Risk Management standard, we can correlate them and understand the similarities.

2.2 Enterprise risk management

Since the focus of this dissertation is ERM, here are described the main issues about this theme in order to understand how organizations can create a structure capable of executing, controlling and monitoring the events that appear from the chaotic environment in which an organization is built. Since ERM is a specification of risk management (as it applies the concepts and vision for risk management towards the organization domain), it is necessary to address the fundamentals about this theme and correlate them with risk management.

To describe ERM it is necessary to understand the scope of this them and what is not in it. To do this, here stands some considerations about what ERM is not about: it is not a department, it is more than just putting risks in spreadsheets and, more importantly, it is not dependent on the size of the company, [9]. Since ERM is a specification of risk management itself, the mentioned considerations also apply to risk management.

Now, the focus is to understand what ERM is about. Every organization has business strategies and

objectives that need to be executed or achieved to create value. That said, it is necessary to be aware of the continual changes that can lead to new objectives or new business strategies, which provides new challenges and opportunities. Besides the existent knowledge in change management and enterprise architecture, ERM frameworks can also be used to manage these circumstances. This vision gives the opportunity to view ERM as a tool to improve the performance of business strategies, as the identification of risks and its treatment can be useful to understand the next step for the business. ERM is as much about understanding the implications from the strategy and the possibility of strategy not aligning as it is about managing risks to set objectives. For COSO, ERM is ”the culture, capabilities, and practices, integrated with strategy setting and performance, that organizations rely on to manage risk in creating, preserving, and realizing value”, [9].

Since this type of management is built upon organizations, it is known that each organization has multiple dimensions and the risks associated with the business can vary from operational to financial. This notion of risk categorization brings a different view for risk management because the identification, analysis, monitoring and control of these risks enlarge the risk management scope from the one defined in the previous section. Risk management must include all the elements from an organization.

Another interesting issue to address is that a risk can be a challenge but also an opportunity, i.e. it can have a negative or positive impact. The risk response can be pursuing the risk as it can be an opportunity to increase the likelihood of achieving organization objectives, [4] [9].

As mentioned before, ERM operates in organizations as a whole, therefore, there are concepts with higher relevance like **risk appetite:** [9] ”amount of risk, on a broad level, that one organization is willing to accept in its pursuit of value.” This concept is important because it is the basis for managing risks, it is the criteria to make decisions about choosing strategies or evaluate performance targets. Managing risk within the risk appetite increases the ability of an organization to create, preserve and realize value.

Regarding the advantages of performing ERM, they are more focused than the ones described for the overall risk management approach, and increases the range of opportunities and the identification and management of entity-wide risks. Having in mind that the benefits will depend on the context of the organization, the assurance is that ERM helps every organization achieve its performance and profitability targets and prevent or reduce the loss of resources. Ultimately, it leads to increasing positive outcomes while reducing negative surprises.

2.2.1 Committee of Sponsoring Organizations of the Treadway Commission

The main bibliography about this theme is COSO, which released two versions of ERM frameworks, one in 2004 and one in 2017. The versions are different on terminology but the frameworks themselves coincide in the main aspects. In this chapter, the COSO ERM framework 2017, as well as relevant features present in COSO ERM framework 2004, will be presented.

As mentioned in the beginning of this chapter, an organization has multiple dimensions, which leads

to different types of risks, making it possible to categorize risks. COSO proposes 4 categories, [7]: Strategic, operational, compliance and reporting. With this categorization it is possible to identify risks throughout the organization, which is one of the main activities in ERM.

The next step is to define a framework that enables the execution of ERM, which is defined in [9]. The framework emphasizes that ERM should be integrated with the business activities in order to fulfill the mentioned benefits. As said before, ERM should not be seen as a function or department but, instead, it must be seen as an integrated part of the organization, being integrated in the culture of the organization. "Integrating enterprise risk management practices throughout an organization improves decision-making in governance, strategy, objective-setting, and day-to-day operations.", [9]. We can say that ERM is fully integrated when the risk information is actively used in strategy setting, decision-making scenarios and for the pursuit of performance targets of the organization.

The framework is based on a group of five components: governance and culture; strategy and objective setting; performance; review and revision, and information, communication and reporting. These components are supported by a set of principles.

- **Governance and culture principles** (Responsibility: board of directors) [9]:
    1. Exercises board risk oversight
    2. Establishes operating structures
    3. Defines desired culture
    4. Demonstrates commitment to core values
    5. Attracts, develops, and retains capable individuals
- **Strategy and objective setting principles** (Responsible: organization) [9]:
    1. Analyzes business context
    2. Defines risk appetite
    3. Evaluates alternative strategies
    4. Formulates business objectives
- **Performance** (Responsible: organization) [9]:
    1. Identifies risk
    2. Assesses severity of risk
    3. Prioritizes risks
    4. Implements risk responses
    5. Develops portfolio view

- **Review and revision** (Responsible: organization) [9]:
  1. Assesses substantial changes
  2. Reviews risk and performance
  3. Pursues improvement in ERM
- **Information, communication and reporting** (Responsible: organization) [9]:
  1. Leverages information and technology systems
  2. Communicates risk information
  3. Reports on risk, culture and performance

In order to implement these components and its principles, it is necessary to define an ERM structure. Regarding this matter, COSO ERM framework 2004 is more explicit than COSO ERM framework 2017, and from there, it is possible to infer that an ERM structure should be composed by, at least, 4 components: **Board of directors, Internal Audit (IA), Chief Risk Officer (CRO) and the risk owners**.

Additionally, the board of directors can create committees to help achieving specific objectives and, depending on the organization itself, this structure might have more components to support the ERM. These 4 components have specific responsibilities:

- **Board of directors responsibilities:**
  - As stated before, define the ERM strategy;
  - Approve the risk appetite aligned with the business strategies;
  - Provide and approve the necessary resources for ERM.
- **IA** - As established by COSO, internal auditors play a crucial role on the evaluation of the effectiveness of an ERM strategy. In order to fulfill these expectations, IA have the following responsibilities:
  - Evaluate the ERM process execution (namely, evaluate the identification, assessment and treatment activities);
  - Prioritize the tasks of the audit plan accordingly to the assessed risks.
- **CRO** - The board of directors should assign this role to a person with expertise and specialized knowledge on ERM. This role has the following responsibilities:
  - Define the ERM framework;
  - Aggregate and consolidate the risk information;
  - Categorize the risk information;

  - Communicate the risk information to its stakeholders;
  - Support the implementation of the proposed framework.

- **Risk owner** - Accordingly to COSO and ISO 31000:2018, risk owners are responsible for using the assigned priority to select and apply appropriate risk responses in the context of business objectives and performance targets. Risk owners are accountable for the effective management of identified risks.

2.2.2 ISO 31000:2018 as an ERM framework

In this subsection, it is described how the ISO 31000:2018 standard can be used as an ERM framework. Particularly, the principles and the framework, two components of the standard that were not explored in the section 2.1.1 Risk management process, will be described here. As appointed in the mentioned section, the ISO 31000:2018 is not just about the process and even this process is flexible enough to be applied to every context of every type of organization.

Additionally, as stated before, the main difference between risk management and ERM is the scope of the risk management itself and how that scope influences the risk management process i.e. In ERM, as explained in COSO ERM framework 2017, the scope is defined as performing risk management in a holistic way, involving the organization as a whole. Having a wider scope leads to a necessity of having a controlled environment. There is a need to assign and define responsibilities and specific roles to monitor and control this overall process.

These notions lead us to infer that ISO 31000:2018 can be seen as an ERM framework due to its flexibility. Indeed, it enables its readers to establish the scope of the process as being holistic and also by complementing this process with two other components that provide the guidelines to manage this holistic approach.

Since the risk management process has already been described, the principles and the framework components have to be explored. The **principles** are the criteria to the effectiveness of the risk management strategy. The main goal is the creation and protection of value and all the principles are intended to achieve that overall goal. These principles are: the risk management has to be continually improved; it should be integrated in all the organization activities; it should be structured and comprehensive; it should be customized to the needs of the organization; it should be inclusive and dynamic; it should be built with the best available information, and it should consider human and cultural factors , [4].

The **framework** is the component that, combined with the process (and establishing the scope of the risk management as being holistic), forms an ERM framework. This framework is composed of five components: integration, design, implementation, evaluation and improvement; and one driver: leadership and commitment.

Firstly, the driver: **Leadership and commitment**. For the risk management to be integrated in

all organizational activities and in order for it to be monitored and controlled in a effective way, the top management and the oversight bodies should demonstrate leadership and commitment. We can relate this with the roles and responsibilities assigned by COSO to the board of directors and other top management bodies. The responsibilities for the top management entities are: customizing and implementing all components of the framework; issuing a statement or policy that establishes a risk management approach; allocate resources; assign responsibilities; ensure that risks are adequately considered when setting the organization objectives; understand the risks facing the organization in pursuit of its objectives; ensure that systems to manage the risks are implemented and operating and, finally, **ensure communication**, [4].

The **integration** component, it is simple but determinant to the effectiveness of the risk management strategy. Integrating risk management into an organization should lead to risk management being part of the organizational purpose, governance, strategy, objectives and operations, [4]. To do that, there must be an understanding about the structures and context of the organization.

Having in mind that this theme is context dependent, the **design** of the risk management framework should, firstly, consist in understanding the organization and its external and internal context. Then, once again, the top management and the oversight bodies should articulate risk management commitment, assign organizational roles, responsibilities and accountabilities, and allocate resources. Finally, and directly connected with this dissertation, the design of the framework must incorporate the establishment of the communication and consultation channels, [4].

After the design, the framework should be **implemented** in a way to support the risk management process and to ensure that it is effective. The framework should be should be **evaluated** to ensure the continual improvement of the same. Its implementation should consist in developing an appropriate plan and in identifying the decision-making scenarios and its participants. Additionally, the framework should be implemented in a way that makes it possible to modify its characteristics when necessary [4]. Regarding the evaluation, the performance of the risk management framework should be evaluated periodically in order to understand if it is still suitable for its purpose, which is to help the organization to achieve its objectives.

The final component of the framework is the **improvement**, which is related with the result of the evaluation. The risk management framework should be constantly improved by adapting it to changes or by rebuilding it according to the periodical evaluations.

By analyzing this standard in its totality, it is possible to state that it can also be seen as an ERM framework since it establishes and provides guidelines on how an organization can manage risks in a holistic way, leaving it to the organization to choose if its risk management strategy is ERM or if it is just applied to a certain context.

2.2.3 ISO 31000:2018 as a management system standard

According to ISO, a management system is ”the framework of policies, processes and procedures employed by an organization to ensure that it can fulfill the tasks required to achieve its purpose and objectives”, [10]. When an ISO standard reaches a high maturity level, it can be considered a management system standard. Basically, it becomes the reference to follow in a given domain like, for example, the ISO 9000 standard, related with quality management, and the ISO 27000 standard, related with information security management.

In order to categorize these management systems standards, ISO created the document ”Annex SL”, which describes in detail the structure of management system standards and other features about what a management system standard should be. The mentioned structure is composed by two major component: scope and design and control and development, [11]. The figure 2.2 summarizes these two components.

Nowadays, none of the existent risk management standards reached the management system standard state, however, the ISO 31000:2018 standard is getting there. By comparing the structure of the Annex SL with the structure of the ISO 31000:2018 it is possible to see that it fulfills all the requirements to be a management system standard, [10]. To further analysis, the appendix C presents a table that details this comparison.

Assuming that the ISO 31000:2018 standard reaches the level of management system standard, the advantage would be the complete integration of risk management into the strategic level of an organization and also with other management systems that it implements. Seeing risk management as a management system would enable organizations to treat it as a crucial system to achieve their objectives”

The alignment between ISO 31000:2018 and Annex SL enables organizations that perform risk management following the guidelines of ISO 31000:2018, to state that they are performing risk management

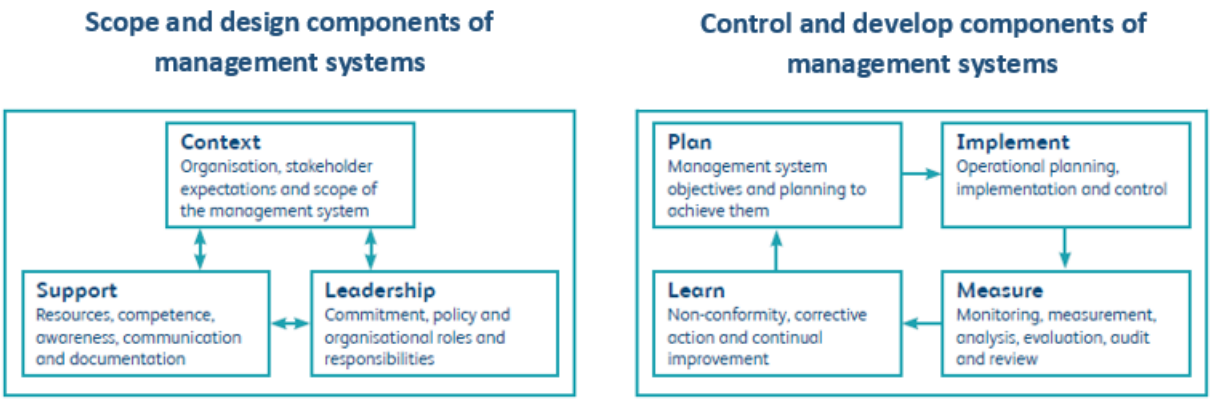

Figure 2.2: Management system components, [10]

in a way that is more profitable to them and that their risk management strategy is directly connected with the achievement of their strategic objectives. On the other hand, a management system can be auditable and, in the case of the ISO management system standards, it can be certified. Creating a certification for risk management leverages this theme into another level as, being certifiable, it can become a real competitive advantage in the business world.

This means that clients can demand, as a requirement, organizations to be certified in risk management. This happens in the cases of quality management (ISO 9000) or environment management (ISO 14000), and the organizations that do not have this certification start to lose business. Ultimately, this forces the risk management world to converge into the ISO 31000:2018 standard terminologies and guidelines.

Looking at ISO 31000:2018 standard as a management system standard is still a recent topic. The interest in approaching this vision in this dissertation is based on the fact that the ERM framework of the case study organization needs to be analyzed i.e. With this new vision about risk management, ERM frameworks can be analyzed and evaluated in a way that can be inferred if they are designed and implemented as the best practices demand, being considered the best practices the ones described in the ISO 31000:2018 standard as it can be seen as management system standard.

2.2.4 Alignment between COSO ERM framework 2017 and ISO 31000:2018

Since, COSO and ISO are the main references used in this dissertation, analyzing the alignment between both of them is of interest. Before doing this alignment, we have to see if both frameworks are compatible. The answer is yes, they are compatible because both share relevant properties [8]:

- **Process based:** COSO proposes a process consisting of ongoing tasks and activities. ISO 31000:2018 emphasizes the process approach throughout the standard.
- **Affected by people:** both frameworks are affected by people.
- **Guideline documents:** both allow for an organization to architect, design, deploy, and assure risk management systems based on its context.
- **Provide reasonable assurance, not absolute assurance:** COSO emphasizes reasonable assurance, which is implied in ISO 31000:2018.
- **Provide for internal auditing:** both COSO ERM framework 2017 and ISO 31000:2018 rely on internal auditing to provide the requisite monitoring of control effectiveness.
- **Focus on the achievement of business objectives in operations and compliance:** both focus on meeting business objectives. ISO 31000:2018 focuses on the achievement of objectives, which can be scoped to specific management system objectives.

- **Adaptable to different organizations:** both can be used in different types of organizations in different sectors.

After ensuring both frameworks are compatible, it will now be described how they can be aligned. This alignment is performed by comparing the ISO 31000:2018 standard features (process activities and framework components) with the components of the COSO ERM framework 2017.

Table 2.8: COSO ERM framework 2017&ISO 31000:2018 alignment

COSO ERM framework 2017 components	ISO 31000:2018 framework and process
Governance and culture	Framework: integration and design; Process: scope, context and criteria
Strategy and objective setting	Framework: integration and design; Process: scope, context and criteria
Performance	Process: risk assessment and risk treatment
Review and revision	Framework: evaluation and improvement; Process: monitoring and review
Information, communication and reporting	Framework: design; Process: communication and consultation

Starting with table 2.8, it is possible to see the matches between the two mentioned parts. According to ISO 31000:2018 the establishment of the context is the definition of the scope and boundaries for the application of risk management. This means it is necessary to define risk criteria as well as additional features about the organization itself, such as the internal environment, culture, values and strategy setting.

In turn, COSO EREM framework 2017 defines this activity in two components: Governance and culture and strategy, and objective setting. The principles for these two components are compatible with the output of the scope, context and criteria activity, proposed by ISO 31000:2018 standard. Besides the compatibility with the process activity, the COSO ERM framework 2017 governance and culture, and strategy and objective setting components are also compatible with the integration and design components of the ISO 31000:2018 framework. The referred components of the ISO 31000:2018 framework consist on the analysis of business context, definition of risk appetite, exercising board risk oversight, establishing of operating structures, definition of desired culture, and more.

Regarding the performance component, it is clear that the risk assessment activity, composed by risk identification, risk analysis and risk evaluation, and risk treatment are completely fulfilled by the principles of the COSO ERM framework 2017 performance component.

Finally, the components review and revision, and information, communication and reporting of the

COSO ERM framework 2017 match with the monitoring and review, and communication and consultation risk management process activities, described in the ISO 31000:2018 standard, together with the evaluation, improvement and design components of the ISO 31000:2018 framework. Even though they match,there is a significance difference between where both frameworks place these activities in their processes. For ISO 31000:2018 both activities are current i.e. take place across the entire process since they are connected with all the other activities. For COSO ERM framework 2017, these activities are executed only in the end of the process.

2.3 Communication in organizations

After getting familiarized with ERM concepts, it is relevant to explore the concept of communication. Since the problem centered in communicating risk across an organization, there are concepts and methodologies about this theme that are useful to approach. Therefore, the goal of this section is to provide a basis of knowledge to enable correlating risk communication with with the environmental characteristics of an organization.

Communication in organizations has been a topic of debate for the past years and, as a consequence, there are several definitions for it. For example, communication can be ”understood as a process of exchanging signs and symbols instigated and led by at least one of the conscious subjects” [12] or as a ”tool for exchanging of experience and values as well as transfer of meanings and knowledge”, [12].

A common ground for all definitions is that communication in organizations can be seen as a process. Thus, the definition that will be used in this dissertation states that organizational communication is ”the process by which individuals stimulate meaning in the minds of other individuals by means of verbal or non-verbal messages in the context of a formal organization”, [13]. This process will be explored in the next subsection.

2.3.1 Organizational communication as a process

An organization is a complex system and trying to represent the flows of the information by modeling a process is a difficult task. Therefore, over the years, this process has been changing and, nowadays, there are two different models for it. The first model has a linear approach and it approaches the process as a one-way process of sending messages to its destination. This approach is quite simplistic and does include important concepts that need to be taken into account. These concepts are the encoding and decoding of messages, noise, goal and context for communication as well as the notion of iterations. The organizational communication process needs to be seen as an iterative process, [14].

Almost all of these concerns are approached in the transactional model, illustrated in figure 2.3. Looking into the activities and the participants of the process, firstly, the **source/sender** encodes, or behaves, the message that it wants to communicate. After the verbal or non-verbal message is encoded

(being encoded in a way that has meaning to the receiver), it is passed through a **channel**. A channel is anything that allows the message to be carried from the sender to the **receiver**. Finally, the receiver decodes the message and, if necessary, gives feedback in the same way.

Parallel to these activities, in all the stages of the process there is the notion of **noise**. This noise can arise from many sources, however, the main source of noise in this process is mostly related with cultural differences, [14]. This noise is a variable of the communication process and has direct impact in its effectiveness.

The organizational communication process is an interpersonal process deeming it highly dynamic, which means that a single communication can have multiple iterations. The source becomes the receiver multiples times in order to accomplish the initial goal and the message itself is carried in different channels ("All persons are engaged in sending and receiving messages simultaneously. Each person is constantly sharing in the encoding and decoding process and each person is affecting the other", [14]).

Note that there is a necessity to define a **goal** for the communication. In organizational communication, there are three main goals: developing interpersonal relationships, gaining compliance, and gaining understanding, [13]. In most cases, they are not achieved independently as the process is executed by humans i.e. since this process highly dynamic, when the main goal for the communication is established, it easily changes during the time of the execution of the process, becoming a overlap of the three main goals simultaneously.

In this transactional model the **context** on which the process is executed is not contemplated, however, the context is an important variable to determine the message itself as people do not communicate exactly the same way within any two different contexts. In order for communication be effective, the context needs to be well defined since it defines the type of communication that is being executed (the

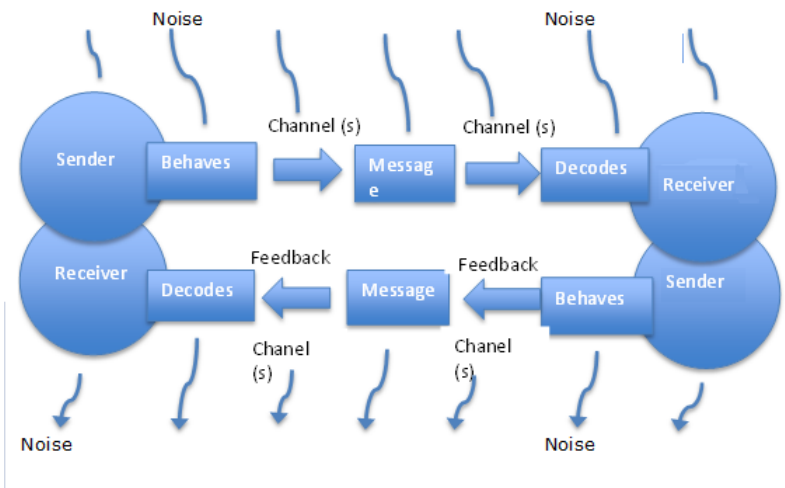

Figure 2.3: Organizational communication process: Transactional approach, [14]

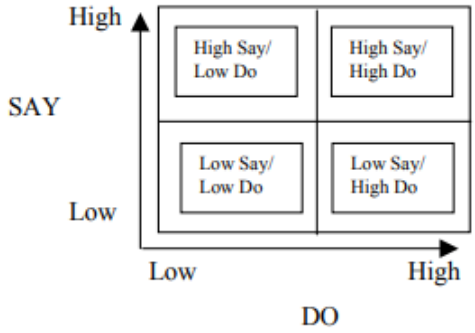

Figure 2.4: Say do matrix

different types of communication are discussed in the next subsection). To control this, there are types of communication that provide ways of focusing the process and avoiding having more interactions that the ones needed. These types of communication are materialized in dimensions.

2.3.2 Organizational communication dimensions

Inside the organizational environment there are several ways of communicating. It is possible to characterize communication in three dimensions: formal vs informal, direction, and internal vs external, [15].

Regarding the first dimension, historically, informal communication has been seen as an inefficient way of communicating. Nowadays, this vision is different as the top management started to realize that the message can be more understandable if it is more flexible and, therefore, the top management became more receptive to directly communicate with low hierarchical levels.

This being said, there is still a debate about the dimension informal vs formal and how it affects the efficiency of organizational communication and, indirectly, how this affects productivity. To explore this dimension, an evaluation matrix, denominated say do matrix, was developed and is illustrated in figure 2.4.

By looking at this matrix, every organization can evaluate the efficiency of the communication, regarding this dimension. When an organization is evaluated as being in the high say/low do quadrant, it means that the informal and formal communications are in conflict, affecting the productivity. When the informal and formal communications coexist in stability, the organization is producing sufficient communication and its receivers are actually decoding the message and performing the demanded actions (high say/high do quadrant), [15].

Advancing to the second dimension, communication direction. There are three possible directions: vertical, horizontal and diagonal, [15]. Vertical communication happens when the sender and the receiver have different hierarchical levels. It can be upwards or downwards, depending on the sender

having a lower hierarchical level than the receiver (upwards), or a higher one (downwards).

Downwards communications are directly connected with work distribution, and upwards communications are directly connected with status reporting. Normally, having an efficient upwards communication is harder than an efficient downwards communication since the upwards communication deals with common challenges, such as time and difficulty into passing the message. Normally, the high level members have less time to be the receiver than the source. Additionally, there is still the stigma that it is not possible to communicate with higher hierarchical level entities with openness, affecting the efficiency of the communication.

In horizontal communication, such hierarchical issues are not present. When organizational members with the same hierarchical level communicate, there are less challenges. The idea that the sender does not have any hierarchical association with the receiver avoids issues related to openness. Nowadays, with the agility of the processes in organizations, the communication is not only horizontal or vertical. Diagonal communication is becoming increasingly frequent, as the different organizational units require knowledge about each other.

Finally, communication can be internal or external. The amount of internal communications is far superior to external communications and this is affected by the way that different organizations interact with each other. The external communication tends to be only formal, which can affect its efficiency. On the other hand, communicating informally with external entities can create an uncontrolled flow of information.

Relating with the previous subsection, the three dimensions are directly associated with the efficiency of the organizational communication process. Depending on the source and the receiver, the direction and the destiny of the communication should be defined. Related with the context and the goals of communication, it should be decided whether the best way of executing the process is in an informal or formal way. Depending on this decision, the message should be encoded accordingly. Making an analysis of these concerns enables better efficiency in communication inside (and with external entities) the organization.

2.4 Risk communication and consultation

Risk communication and consultation "is often the key differentiator in management's perception and understanding of ERM value creation", [16]. This theme is highly discussed in the current days and there are several steps that need to be considered when creating risk communication plans.

The main consensus is that risk communication plans require the answer to several questions. Many think these questions should be answered orderly and others in parallel but most articles related with this theme refer that the following questions define the communication model, [16] [17] [18]: Who? When? What? Why? How?

Answering these questions enables the CRO, who is responsible for creating the risk communication plans, to understand how the communication plan will affect the perception of the different stakeholders on ERM. It is important to notice that every organization can answer these questions in different ways. Risk communication and consultation is a context dependent problem and, thus, every organization will create different communication plans.

Even though risk communication and consultation is context dependent, there are questions that can be answered in a generic way i.e. who are the entities that need to be informed and why is there a need to create these plans are two questions that can be applied to all organizations

With minor differences, it is consensual that the stakeholders of the ERM are mostly the members of the ERM structure described in the COSO ERM framework 2017. Namely, senior management bodies or the board of directors, the ERM committee, CRO, risk owners, internal audit and the participants in the risk management process. Besides these members, most articles refer other management bodies that are usually interested in ERM, namely, the Chief Financial Officer (CFO) and Chief Executive Officer (CEO), [19] [16].

Since risk communication and consultation is often the key differentiator in management's perception and understanding of ERM value creation, it is highly important to create risk communication plans. Additionally, "providing accurate, timely, and relevant communications is a critical component in building and sustaining a successful Enterprise Risk Management (ERM) program", [16]. The current answer to the question "Why?", in the business world is clear: it is a critical factor for the success of ERM frameworks as well as to create a risk culture inside organizations. Without these plans it is difficult to create the necessary awareness about the benefits of developing ERM strategies and, as stated in the best practices, this awareness is the main enabler to the success of ERM.

When communication occurs it is completely dependent on the context of the organization. Regarding the "what?" question, it is directly connected with the stakeholders, therefore, it can only be answered after identifying them.

After understanding who the stakeholders are, we have to understand their needs and their roles. Nowadays, most people try to answer this question with RACI matrices, which describe the different roles of the stakeholders. These roles are: responsible, accountable, informed and consulted. Evaluating stakeholders according to these roles enables us to understand their different needs and to develop the risk communication plans.

When a stakeholder is responsible for one activity, he is "the person assigned to deliver/execute a particular activity", [17].The responsible person is the one "who must ensure that the activities are completed successfully", [19]. Accountable means that the stakeholder "owns the required resources and have the authority to approve the execution and/or accept the outcome of an activity", [19]. He is "the ultimate decision-maker and owner of the activity and its associated outcomes", [17].

A stakeholder that needs to be consulted is ”the party/parties who expertise and/or opinions must be sought and clarified prior to undertaking the activity of making decisions”, [17]. Finally, the stakeholders that need to be informed are ”those who are kept up to date on the progress of an activity (one-way communication)” [19]. In other words they are ”the party/parties who are required to know that the particular activity or decision has been undertaken”, [17].

Regarding the remaining question, how to present the information is by far the most difficult question to answer. It is completely dependent on the context and on the information architecture. These dependencies make this question a topic of discussion but there is ”still very little research or documentation on how to visualize risks”, [18].

Before entering in the risk visualization topic, there are steps that are known and discussed in the literature that are useful when building an answer to this question. These steps are determining the communication type and method and establishing a common language, [18]. These steps are related with three organizational communication activities of the process, illustrated in figure 2.4, namely the definition of the channel, the encoding and the decoding of the message. Defining the type and method of communication consists in choosing the channel and, nowadays, common channels are risk forums and committees, face-to-face meetings, internal reporting channels and others, [17]. Apart from the channel, establishing a common language is critical for communication to be effective. The way the message is encoded is a key factor for the success of the communication process since the receiver needs to know how to decode the message in order to make decisions with it. This common language is established in two fronts, first the ERM framework should clarify all the terms and concepts that are in the ERM universe of the organization. Apart from this, the way the information is presented affects the decoding of the message. For example, if a non-consensual chart that is not very usual in the business world is used, it is likely that the receiver will not be able to decode the message that this chart is trying to pass.

When exploring the concern of having visualization techniques to represent risk information, it has to be taken into account that this is also an information architecture problem. There are visualization techniques that can only be used if the information architecture emerged from the ERM framework contemplates specific concepts.

Looking at the current state of this problem, ”the main genres of visualization that can be used for risk-related purposes are quantitative or numeric charts, qualitative or conceptual diagrams, geographic or conceptual maps, and visual metaphors”, [18]. In detail, the visualization techniques that are commonly used nowadays are risk matrix, bow-tie diagrams and fish-bone diagrams. These techniques are present in ISO 31010 catalog, meaning that they can be used in risk assessment activities and also in risk communication and consultation.

With these information visualizations it is possible to enrich the risk reporting. Risk reporting is a

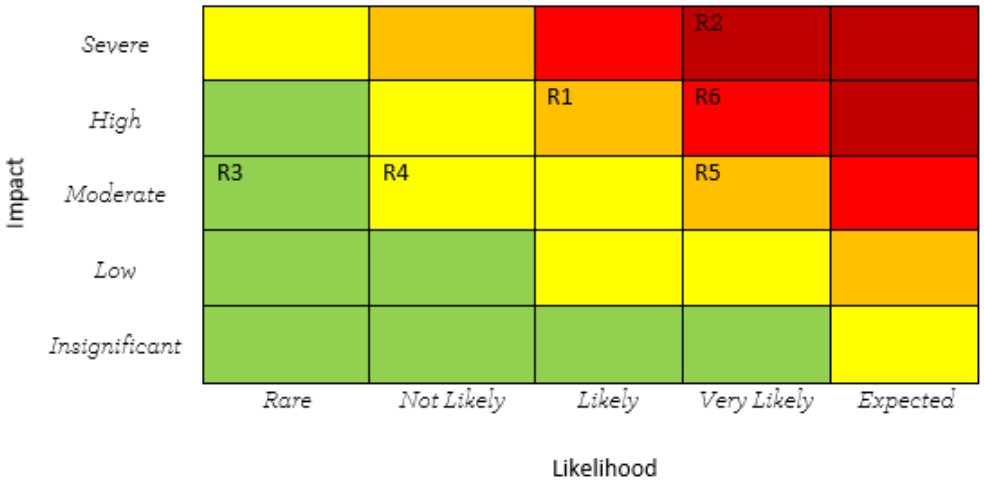

Figure 2.5: Risk matrix example

”key method of communicating risk across business units and between multiple layers of an entity”, [17]. Creating risk reports using visualization techniques to present the risk information that are suitable to every stakeholder is the answer to all the questions. This is the output of the development of a risk communication plan.

Focusing on each of the mentioned visualization techniques, an analysis regarding the advantages and disadvantages and the information architecture each require will now be presented that each require.

Regarding **risk matrices**, they are highly appealing and the color scheme enables rapid insight into the severity of the risks represented, example illustrated in figure 2.5. For this type of technique, the ERM framework has to contemplate the concepts that allow to build at least the domain model presented in figure 2.6. This domain model is an example of an information architecture that has the minimum number of concepts and relationships that enable the creation of a risk matrix. Basically, to create this type of visualization it is necessary that the ERM framework includes three concepts that have meaning when combined. Most commonly, these concepts are the likelihood, the impact and the level of risk.

The main disadvantage of risk matrices is the scalability of data. Due to its graphic construction, if the number of risks represented in the matrix is high, the matrix is illegible. Aggregation techniques can fight this disadvantage by reducing the number of represented risks.

Another technique is bow-tie diagrams. This technique requires that the ERM framework defines the risk identification as established in ISO 31000:2018 i.e. a risk must be identified by three elements: event, cause and consequence. An example of a bow-tie diagram is illustrated in figure 2.7.

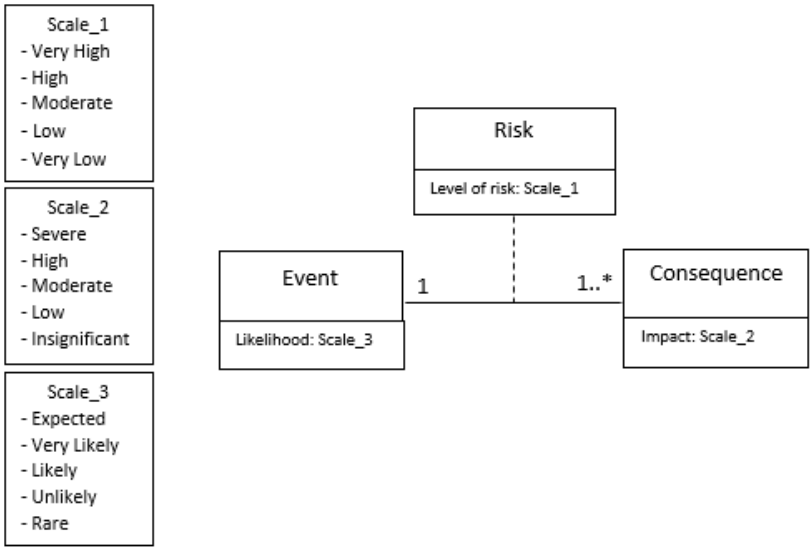

Figure 2.6: Example of a domain model to build a risk matrix

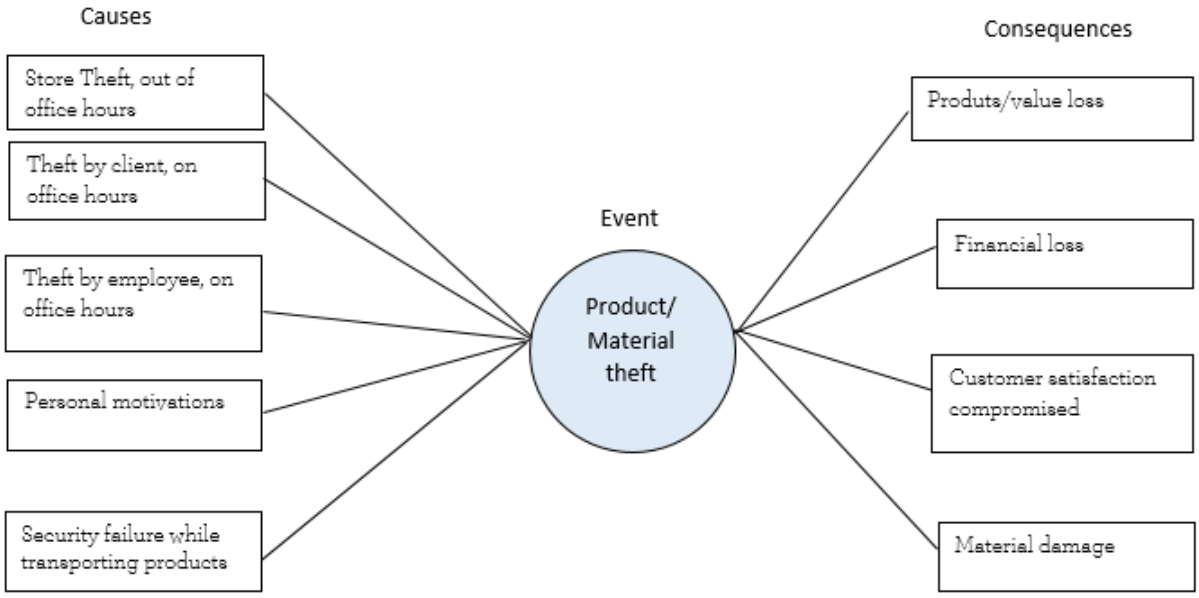

Figure 2.7: Bow-tie diagram example

The bow-tie diagram allows to aggregate risks through events. An event can have several causes, with different likelihoods, and several consequences with different impacts. This variety gives rise to a number of risks that share the same event and may be aggregated to then be presented in the form of bow-tie.

The advantages of using bow-tie diagrams are its appeal and, more importantly, the fact that they are good to deal with a high number of risks. On the other hand, this type of diagram can only be used

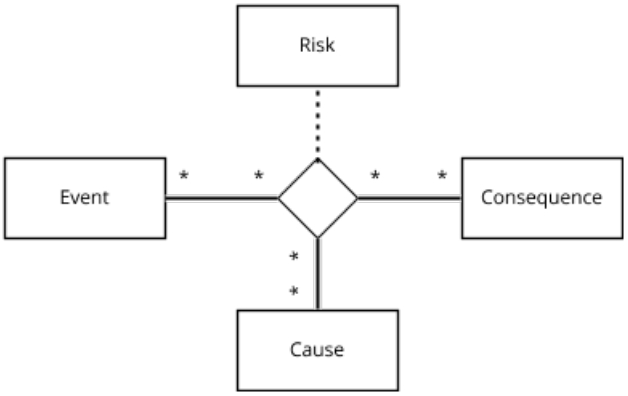

Figure 2.8: Example of a domain model to build a bow-tie diagram

to represent the three elements and not the level of risk or the likelihood of the events. Additionally, this technique requires a semantic analysis of data, which adds complexity. Bow-tie diagrams require, at least, the information architecture represented by the domain model in figure 2.8.

Lastly, the fish-bone diagrams. These diagrams are used to aggregate risks through consequences and, specially, to represent the dependence relations between the causes that give rise to the events that lead to these consequences, illustrated in figure 2.9.

As in bow-tie diagrams, in fish-bone diagrams there is the need to conduct a semantic analysis on the risks in order to find dependencies between the different causes. Since this analysis is semantic, it is complex and often requires that it is dealt with by an experienced person.

Using this technique within a risk management report enables the better understanding about the events that lead to the consequence in study in a way that is possible to determine which the priority causes that need specific controls are. Ultimately, this diagram can be used to increase the performance of risk treatment. The minimum information architecture required to create this diagrams is the same as the architecture for bow-tie diagrams, as illustrated in figure 2.8.

The main disadvantage of these three techniques is the human dependency. It is very difficult to automatize them, which leads to higher complexity when the reports are created.

Apart from these three techniques, common diagrams can be used instead, such as bar charts, pie charts, line charts and others, illustrated in figure 2.10. The greatest advantage of these diagrams is that there is no need to educate people on how to read them and that these techniques enable the automation of risk management dashboards as all the tools that deal with information visualization have these kind of diagrams available. Another relevant factor is that these common techniques do not have a strong dependency with the domain model.

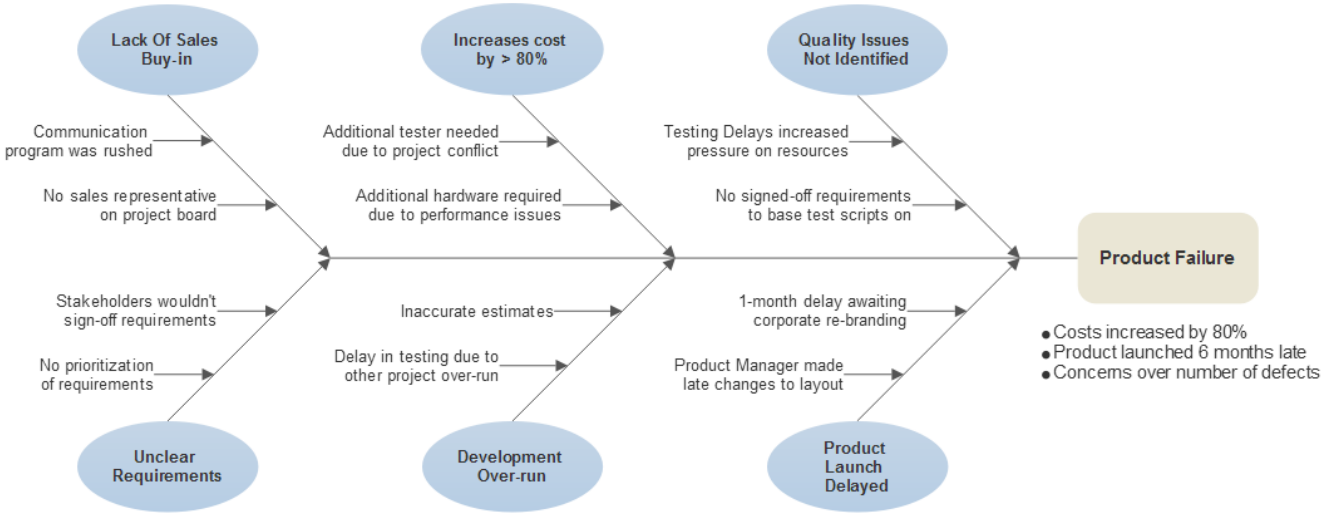

Figure 2.9: Fish-bone diagram example

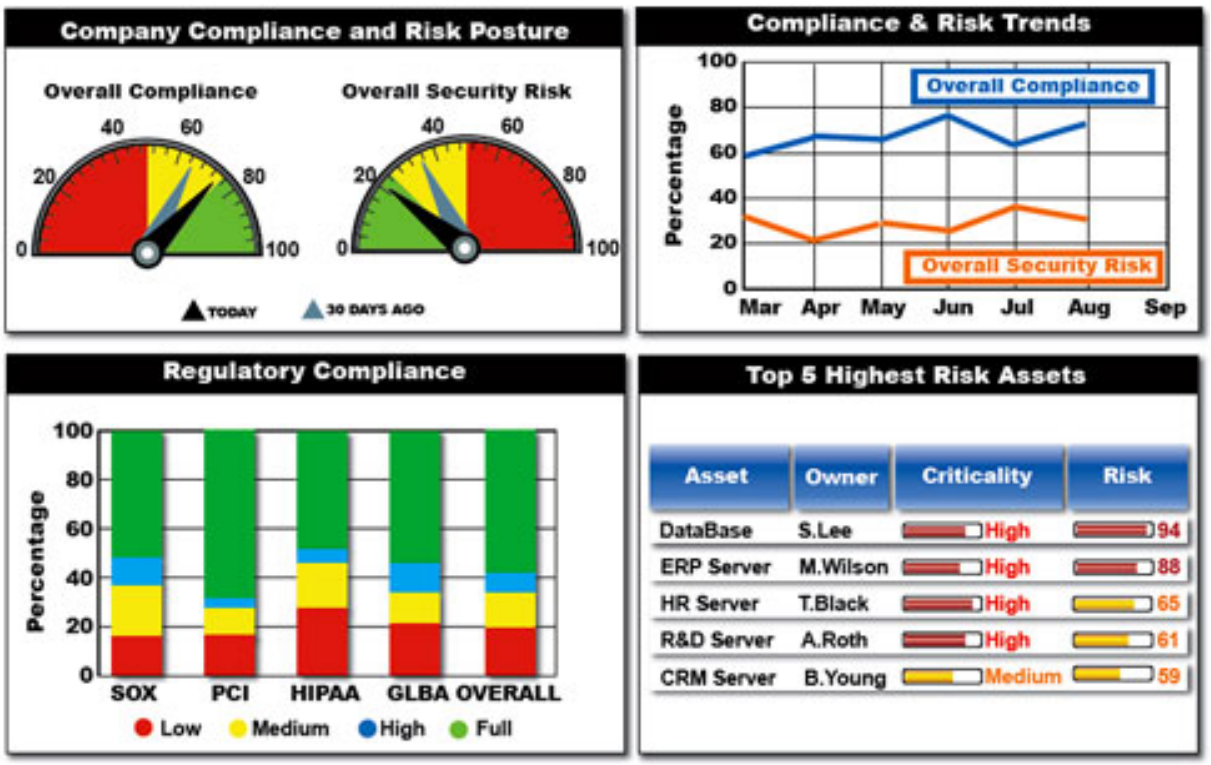

Figure 2.10: Example of a compliance dashboard

2.5 Conclusion

With this chapter, it is possible to analyze the risk communication and communication problem. Despite being just one activity of the risk management process, risk communication and consultation is the channel to relate all the risk management stakeholders. To define and create this channel we need to understand all the characteristics of the ERM framework. These notions about risk communication and consultation make it a context dependent activity, as all organizations should customize the channel according to its needs and characteristics.

Extrapolating to the organizational communication point of view, only after analyzing the ERM framework is it possible to understand how the process is executed, namely, who the participants are and which type of communication is imposed by the framework, if there is any imposition. Despite this obligation of analyzing the ERM framework, and looking to the two main references, there are stakeholders (participants in the communication process) that should be present in all ERM strategies, which are the members of the ERM structure: ERM committee, CRO, board of directors, IA and risk owners. It is possible to draw the conclusion that the needs of these main stakeholders are the main factors that define the communication model.

Having this in mind and moving from section 2 to section 3, another conclusion to draw is that it is impossible to create risk management reports without understanding the information architecture of the ERM framework. This conclusion leads to a mandatory set of steps when approaching the problem.

First, the ERM framework of the organization in study should be described and analyzed in order to retrieve the resulting information architecture and, only then, is it possible, to analyze the existing visualization techniques and their information architecture requirements to see if both information architectures match. With this comparison it is possible to understand which techniques can be used in order to fulfill the different needs of the several stakeholders.

These conclusions lead to a deeper knowledge about the risk communication and consultation problem as, now, it is possible to understand that this problem can be split into two. One part is to understand the communication model, where the needs of the different stakeholders are considered in way that they define different views. The other part is understanding the information architecture dependencies and how they affect the fulfillment of the mentioned needs.

3

Problem analysis

Contents

3.1 INCM ERM Framework 38

3.2 Alignment between the INCM ERM framework and ISO 31000:2018 standard 42

3.3 Requirement analysis 44

3.4 Information model 45

3.5 Conclusion 47

As mentioned in the problem description section, establishing a holistic ERM strategy entails many challenges. A big challenge is using the information provided by the ERM process at a strategic level. In order to make that possible, the context on which the process is executed should be clearly defined and, consequently, the risk assessment should provide useful information for strategic decision-making scenarios. This challenge is focused on the risk communication and consultation activity as, ”given the complexity of the global business world today, distilling risk information down to that which is most pertinent for disclosure to the organization’s board of directors can be difficult”, [20].

Since this activity is one of the main challenges in ERM, it is the focus of the developed work in this dissertation. As seen in section 2.1.1 Risk management as a process of this dissertation, this is a current activity with the main goal of providing risk information to all stakeholders. Risk communication and consultation is described as a ”continuous and iterative process in the organization in order to provide, share and obtain information, and establish dialogue with risk management stakeholders.”, [5]. With these definitions it is possible to infer that this challenge is set on five questions: when? why? who? what? and how?

The first question is strongly dependent on the business model of the organization. When the information is presented to the stakeholders, it can vary from every quarter to once a year and, on other hand, it also depends on the destination as different stakeholders have different needs. Regarding the second question, as stated in section 2.4 Risk communication and consultation, risk communication and consultation is a critical factor for the success of ERM frameworks. It is the only way stakeholders understand the outputs of the risk management process, as well as how to create action plans based on ERM.

Moving on to question four (what?), according to the literature this question is seen independently from the others. As stated in section 2.4 Risk communication and consultation, first we need to identify the stakeholders (who?) and only then can we understand their needs (what?). From this point on, as both questions are based in stakeholders, they will be treated as one. Therefore, the main focus of this dissertation is on ”what?” and ”how?” i.e. in the creation of reports, which satisfy the needs of different stakeholders, enabling the use of risk information on a strategic level.

Risk management reports gather the risk information resulting from the risk management process and the way that information is presented is the key factor for risk management effectiveness in decision-making scenarios. Being a key factor, the need to understand the different requirements for different stakeholders (what?), as well as the need to use right information visualization techniques (how?) is critical.

Each one of these questions can be explored differently. As explained, the information that needs to be presented results directly from the needs of the stakeholders. The way this should be explored is by trying to create a communication model that represents these needs. The way information should be

presented constitutes an information architecture problem since every ERM framework has a different information architecture and such architecture defines two things: what is the possible information that can be communicated and which visualization techniques can be applied to it.

To conclude, in order to understand how the risk communication and consultation problem can be placed in the INCM case study, the next step is to describe the INCM ERM framework.

3.1 INCM ERM Framework

The CRO of this organization created a framework that aims to follow the best practices established in the two references appointed in this dissertation, ISO 31000:2018 and COSO ERM framework 2017. This framework is composed of five components: Mission and strategy, risk management culture, ERM structure, risk categorization and ERM process.

As appointed by COSO, ERM implies the creation of an ERM structure. At INCM this structure is composed of the elements shown in figure 3.1. As it can be seen, it also describes the interaction between the structure elements.

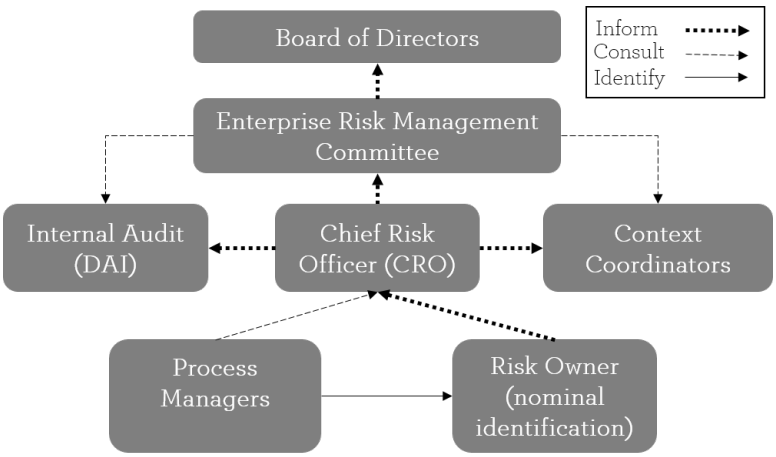

Figure 3.1: ERM structure at INCM, [21]

This structure is aligned with the one proposed by COSO as it contains the 4 main elements described in that reference: board of directors, CRO, risk owner and internal audit. Therefore, the responsibilities assigned to these elements can be seen in section 2.2.1 Committee of Sponsoring Organizations of the Treadway Commission.

Regarding the other elements, the responsibilities of the **ERM committee** are supporting the board of directors in risk management; approving and monitoring the ERM framework; debating and analyzing the risks of the organization and ensuring the quality of the risk management process and, ensuring the communication of the risk information to its stakeholders, [21].

INCM is a large organization with various independent products and contexts. In order to manage these contexts, the organization nominates context coordinators. Their responsibilities in ERM are mon-

itoring and promoting the identification of the risk information related to its contexts.

Additionally, a manager is assigned to each process of the organization, who participates in the ERM process by identifying, analyzing and evaluating the enterprise risks related to its process. The manager also ensures that the operations comply with the ERM strategy, as well as that the alterations performed in its process are communicated and reflected in the risk assessment.

Apart from the structure, it is important to understand the risk categorization. Since the INCM is a multidimensional organization, its risks have many sources and characteristics. Therefore, risk categorization has to be very detailed, as can be seen in figure 3.2.

Strategic					
Governance			Business Model		
Environmental Responsability	Social Responsability	Corruption and Related offenses	Inovation and Development	Partner and Customer satisfaction	Competition and Market
Reputation and Image	Political and Economic	Regulatory	Investment and Projects	Financial	New products and Internalization
			Business Continuity		

Operational					
Process				Human Resources	
Loss and/or Obsolescence	Efficiency and effectiveness	Supply chain	Information technology	Competences development	Authority boundary
Material and personal damage	Information security	Product/Service quality	Resource dependency		

Figure 3.2: Risk categorization at INCM, [21]

Lastly, the ERM process of INCM is similar to the process described in section 2.1.1 Risk management as a process. First, the context is established, leading to the risk assessment and further treatment. Simultaneously, the risk communication and consultation take place, as well as the monitoring and review of process.

In this ERM framework, the risk identification is established in a way that each risk should be composed of its causes, event and consequences, and should also have risk owner. Note that the risk management process present in this framework is oriented by business process, leading to the identification of the business process(es) associated with each risk.

	Negative Impact Matrix				
	1	2	3	4	5
	Insignificant	Low	Moderate	High	Severe
Strategic	• Delay or deflection in the plan of actions • Without any impact in the estblished goals	• Prevents from achieving one or more established intercalary goals • Without any impact in indicators achievement	• Prevents from achieving one or more established goals • Without any impact in objective achievement	•Prevents from achieving one or more established objectives	• Prevents from achieving one or more organization's strategic objectives
Operational	• Insignificant impact in the business processes • Impact can be mitigated with routine operations	•Low impact in business processes • Can originate recoverable delays • Impact can be mitigated at operatioal level	• Moderate impact in the business processes • Business performance affected, preventig form achieving established strategic goals	• High impact in the business processes • Business performance affected with high negative consequences (service delays, finantial losses, customer insastifaction, regulatory faults, etc.)	• Severe impact in the business processes •Unavailability of services and/or people critical for the business
Financial	• Insignificant financial impact • <1% impact in the project/budget cost	• Low finantial impact • 2-5% impact in the project/budget cost	• Moderate finantial impact • 5-10% impact in the project/budget cost	• High finantial impact • >10% impact in the project/budget	• Severe finantial impact • >30% impact in the project/budget cost
Reputational	•Incident with limited negative publicity. Quickly forgotten. • Without damage in the reputation/brand	•Incident with negative publicity at local/regional level • Low limited damage (short-term) in the reputation/brand	• Incident with negative publicity at local/regional level • Pressure to INCM mitigate the impact • Moderate damage in the reputation/brand	• Incident with negative publicity at nacional level • Intense pressure to INCM mitigate the impact • High damage in the reputation/brand	• Incident with negative publicity at internacional level • Impact mitigation require strategic changes • Severe damage in the reputation/brand
Information Security	• Public information compromised in its integrity or availability	• Information sensible for internal interests compromised in its confidientiality, integrity or availability.	• Information sensible for organization's operation compromised in its confidientiality, integrity or availability.	• Information sensible for organization's interests compromised in its confidientiality, integrity or availability.	• Critical information for the organization operation compromised in its confidientiality, integrity or availability.
Regulatory	• Danger of incuring in legal or contractual fault	• Isolated act in legal fault • Contractual fault detected by one of the parts	• Activity or routine in leagl fault •Contractual fault with contractual break or penalities threat	• Legal fault resulting from authorities investigation • Contractual fault with penalties	• Legal fault leading to severe penalties • Contractual fault with contract break
Security and Infrastructures	• Insignificant damage • Insignificant material losses	• Damages that require first aid • Low material losses recoverable in short-term (< 24hours)	• Damages or injuries that require doctor intervention (deep cuts, fractures, burns, etc.) • Moderate material losses with long-term recovery (>24 hours)	• Serious injuries implying long absence. Discharge superior to 30 days •High material losses with long-term partial recovery (>24 hours).Requires material renovation or replacement	• Severe injuries (limbs loss, hearing, vision, etc.) or death • Irrecoverable severe material losses. Require equipment replacement.
Environmental	• Insignificant environmental impact	• Reparable low environmental impact	• Moderate environmental impact requiring mitigation actions	• High environmental impact with parcial irrecoverable damages	• Severe environmental impact with irreversible damages

Figure 3.3: Negative impact scale, [21]

Regarding the risk analysis, the impact, likelihood and resulting level of risk are considered for each risk. To allow the comparison of risk information, it is necessary that the metrics have comparable scales. However, recognizing the existence of different risk management contexts, it is expected that the metrics will have different dimensions depending on the context. Therefore, for each risk the following impacts should be identified: strategic, operational, financial, reputation, information security, regulatory, security and infrastructures, and environmental. In the framework, for each impact there is a different description for the possible scores, shown in figure 3.3. This way, it is possible to objectively compare the different

types of impacts. To calculate the level of risk of one risk, the maximum score of all impacts associated with this risk is multiplied by its likelihood. The scales for likelihood, level of risk and consequent evaluation criteria are illustrated in figures 3.4 and 3.5, respectively.

The risk treatment options are the same as the ones presented in the ISO 31000:2018. Apart from the treatment options, each risk has the attribute ”treatment state”, which has three possible values: implemented, in progress and planned. Basically, a risk is associated with a list of controls and each control can already be implemented or not. If all the controls associated with one risk are implemented, the ”treatment state” of this risk is ”implemented”. If some controls are implemented and others are not, the ”treatment state” is ”in progress” and, finally, if none of the controls are implemented, the ”treatment state”is ”planned”.

Continuing the process, the monitor and review activity is also aligned with the references. At INCM, the ERM framework defines that the risk communication and consultation activity is ensured through the production of risk management reports. These reports should include the necessary risk information and be structured and presented in accordance with the concerns and needs of its destiny. To materialize this, the framework considers the creation of three types of risk management reports, [21]:

Likelihood scale			Score
5	Expected	It is expected that the event occurs	80-90%
4	Very Likely	The event may occur in the majority of the circumstances	60-79%
3	Likely	The event is likely to occur	40-59%
2	Unlikely	The event is not likely to occur, but may occur	20-39%
1	Rare	The event only occur in exceptional circumstances	1-19%

Figure 3.4: Likelihood scale, [21]

Level of risk (Likelihood X Impact)		Min. Score	Max. Score
Very High	Immediate action should be taken to reduce the risk	20	25
High	Efforts should be made to reduce risk as soon as possible.	15	19
Moderate	Risk should be controlled. Efficacy of controls should be monitored	10	14
Low	Risk can be accepted. Risk control shall be carried out on the basis of a cost / benefit analysis.	5	9
Very Low	Risk is not a problem for the organization. It should be monitored to ensure that it does not scale	1	4

Figure 3.5: Level of risk scale and evaluation criteria, [21]

- **Enterprise risks report**, which must inform the ERM Committee of the risks of the organization, highlighting, for the consideration of the board of directors, the risks with high risk level and that consequently require awareness and immediate intervention. Due to the broad scope of ERM, risk information should be presented using techniques that allow a rapid comparison of identified risks.

- **Risk mitigation reports**, which should inform risk owners of the monitoring and implementation of risk controls implemented or to be implemented.

- **Specialized risks reports**, which should inform the stakeholders of the risks of specialized contexts. Specialized risks reports typically consist of lists of risks grouped or ordered by identified risk elements (for example, risks ranked by their level of risk, likelihood or impact, risks grouped by cause, event or consequence, among others).

Reaching this point, the ERM structure, risk categorization and ERM process have already been described, leaving the mission and strategy, as well as the risk management culture components to be addressed. These two components regard the alignment between the ERM strategy and the objectives and mission of the organization. They promote the creation of value by the ERM strategy as well as a management culture and awareness. Additionally, they ensure that the risk management process is in conformity with the internal and external requirements.

3.2 Alignment between the INCM ERM framework and ISO 31000:2018 standard

The goal of this section is to understand how the risk communication and consultation problem can be placed in the INCM case study. To achieve that, a possible step is to make an alignment between this framework and the ISO 31000:2018 standard. This possibility is based on the fact that, as explained in section 2.2.3 ISO 31000:2018 as a management system standard, this standard can be seen as having a high maturity level.

While at first the INCM framework may seem very mature, it is not. In spite of trying to follow the best practices, this framework is very young and some of its components are not completely aligned with the best practices yet. As will be further explained in this section, one of those components is the risk communication and consultation activity.

Beginning the alignment with the two risk management processes, it is noticeable that they are almost identical. The only difference between them is that, the ERM process conducted at INCM does not split the risk reporting and recording and risk communication and consultation into two activities. In spite of this difference, at INCM, the communication and consultation activity materializes all the guidelines of the two activities present in the ISO 31000:2018 standard.

The other components of the ISO 31000:2018 framework are described in section 2.2.2 ISO 31000:2018 as an ERM framework; and the remaining components of the INCM framework are described in section 3.1 INCM ERM Framework. With these descriptions it was possible to build the alignment, which is illustrated in figure 3.6.

It is possible to conclude that there are gaps between the two frameworks and that one of those gaps is related with risk communication and consultation. This gap can be seen as a motivation to perform the work described in this dissertation. Ultimately, trying to eliminate this particular gap between both frameworks could lead to a maturity increase of the INCM ERM framework.

ISO 31000:2018 Framework components		INCM ERM Framework		
		NA	PA	A
1.	Leadership and Commitment			
1.1	Customizing and implementing all components of the framework			x
1.2	Issuing a statement or policy that establishes a risk management approach			x
1.3	Resources are allocated			x
1.4	Responsibility assignment			x
1.5	Ensure that risks are adequately considered when setting the objectives of the organization	x		
1.6	Understand the risks facing the organization in pursuit of its objectives			x
1.7	Ensure that systems to manage the risks are implemented and operating	x		
1.8	Ensure communication		x	
2.	Integration			
2.1	Knowing the context and structures of the organization			x
2.2	Everyone in the organization has responsibility in risk management		x	
2.3	Roles and accountability			x
3.	Design			
3.1	Understanding the organization and its context			x
3.2	Articulating risk management commitment			X
3.3	Assigning organizational roles			X
3.4	Establishing communication and consultation		X	
3.5	Allocating resources			X
4.	Implementation			
4.1	Developing a plan that includes time, resources and decision-making processes			x
4.2	Give awareness to the stakeholders about the procedures			x
4.3	Adapt the plan when necessary			x
5.	Evaluation			
5.1	Periodically evaluate the framework and infer if it still is suitable	X		
6.	Improvement			
6.1	Adapting			x
6.2	Continually improving			X

NA – Not Aligned **PA**- Partially Aligned **A**- Aligned

Figure 3.6: Detailed alignment: INCM ERM framework and ISO 31000:2018 standard

Exploring the alignment and focusing on the points related with risk communication and consultation, the point 1.8 ”Ensure communication” is related with the commitment of the top management and oversight bodies. It is their responsibility to ensure that risk information is communicated to the stakeholders, what, currently, does not occur at INCM. The risk communication plan had already been created but its implementation and materialization is performed by the CRO. The top management does not ensures it. The level of alignment was set to ”partially aligned” because the plan exists and there is a body that ensures its execution, even though this body does not belong to top management.

Looking at the point 3.4 ”Establishing communication and consultation”, the level of alignment was set to ”partially aligned” because, as explained before, at INCM, there already are notions about how to perform risk communication and consultation. However, even though the channels are defined, they have not been completely explored yet. The framework does not completely answers the most important questions of this problem: ”what?” and ”how?”. It tries to answer the first question (what?) by introducing the existence of three different risk management reports, however, it does it in an incomplete way. Basically, the only thing missing in the INCM ERM framework regarding this question is the exploitation and implementation of these channels. The intended result of this dissertation is to complete these channels and fully answer the second question (how?), which is not answered at all in this case study.

3.3 Requirement analysis

As explained in the previous section, the ERM framework of INCM already had defined a communication and consultation strategy, however, it was not implemented yet and, therefore, it was considered as incomplete. Based on the analysis of the ERM framework, a possible step to complete the alignment between this strategy and the best practices guidelines consists on a requirement analysis.

Since at INCM the risk communication and consultation strategy is based on the production of three different types of risk management reports, the following subsections detail the requirements for each one of them.

3.3.1 Requirements for enterprise risks report

This risk management report has the ERM committee and the board of directors as stakeholders, and both are interested in the outputs regarding to the organization as a whole.

- **R1:** The user should be immediately able to understand and analyze the state of art regarding the risk situation of the organization.
- **R2:** The user should be able to see, without effort, the priority risks that need to be treated.
- **R3:** The user should be able to infer the risk treatment effectiveness i.e. if the established controls are reducing the level of risks effectively.

- **R4:** The user should be able to infer the decisions to be made in order to create value for the organization.

3.3.2 Requirements for risk mitigation reports

These risk management reports are addressed to the risk owners. In this case study, the risk owners are the several organizational units of the organization.

- **R1:** The risk owner should be immediately able to understand and analyze all risks of its responsibility, highlighting the ones with higher level of risk.
- **R2:** The risk owner should be able to see the risks without implemented controls.
- **R3:** The risk owner should be able to see which controls should be implemented with priority.
- **R4:** The risk owner should be able to understand which are the risks he shares with others, even if he does not have the role of risk owner.
- **R5:** Through the risk management report, the risk owner should be able to monitor and control his risks and to make action plans according to the presented risk information.

3.3.3 Requirements for specialized risks reports

These risk management reports are addressed to the specialized context coordinators. The requirements for these reports are hard to describe as they depend on the context itself. Nevertheless, the following requirements can be associated with all specialized risks reports.

- **R1:** The stakeholder should be able to understand and analyze all risks related to the specialized context.
- **R2:** The presented information should be enough for the stakeholder to make decisions in the specialized context.
- **R3:** If the risk management report is communicated to external entities, and if those entities demand more requirements, the risk management report should also fulfill them.
- **R4:** The stakeholder should be able to compare the attributes of his risks with the overall risk situation in the organization.

3.4 Information model

Apart from the requirement analysis, it also became clear that one part of the problem has to do with information architecture. Since the second question of the risk communication and consultation problem

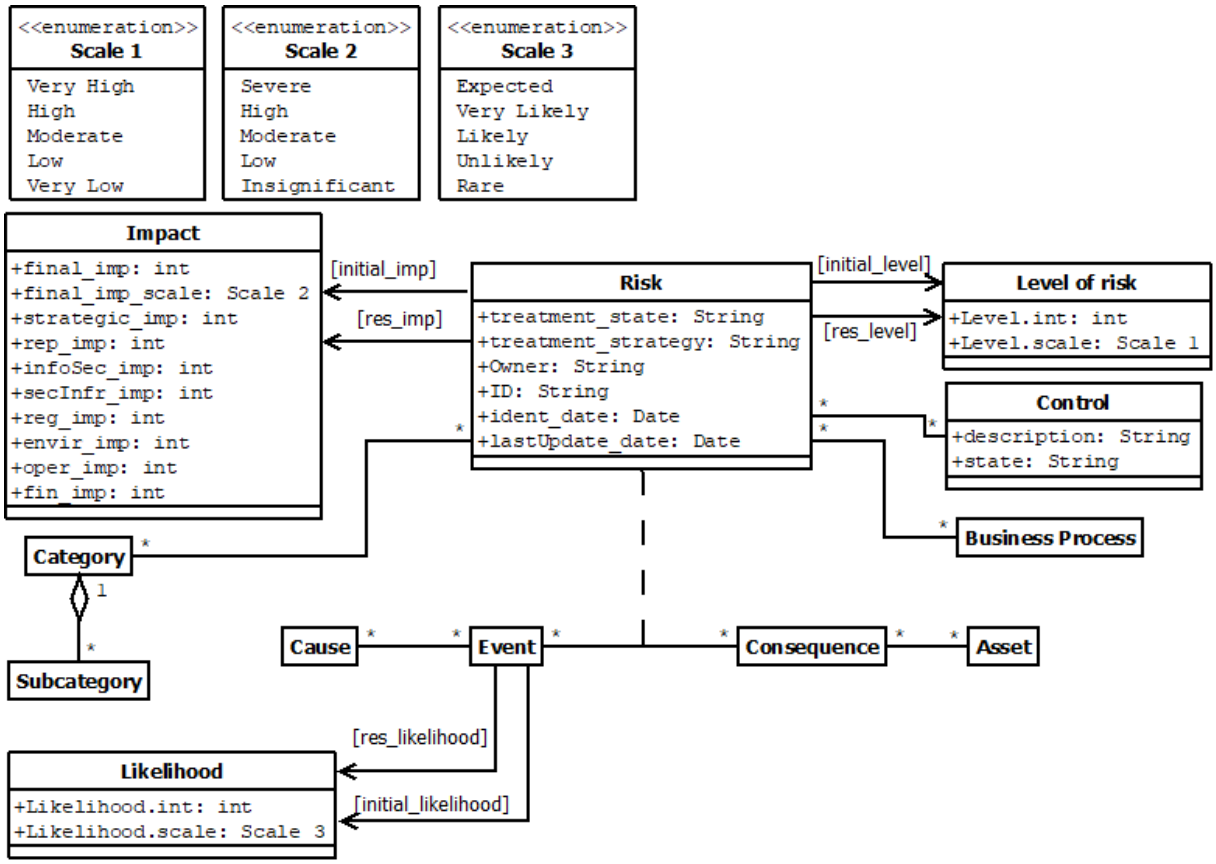

Figure 3.7: Domain model of the INCM ERM framework

is based on the fact that every ERM framework has a different information architecture, the next step is to analyze all the gathered information and produce the domain model from the ERM framework in study. The result of that work is illustrated in figure 3.7.

Describing the domain model, the ”Risk” association class is its core concept. Since a risk emerges from the connection between the consequences of the events that lead to uncertainty in the achievement of the objectives of the organization, the ”Risk” class must be modeled as an object that emerge from the association between ”Event”, ”Consequence”.

The ”Risk” class contains attributes and associations that are related with the execution of the risk management process as described in the ISO 31000:2018 standard. The attributes that emerge from this correlation are: level of risk, residual level of risk, risk owner, likelihood, treatment strategy. Additionally, ”Control”, ”Category”, ”Cause”, ”Event” and ”Consequence” are all concepts that also emerge from executing the risk management process as described in the ISO 31000:2018 standard.

Regarding the other attributes, they are consequence of customizing features of the ERM framework described in the best practices guidelines i.e. even though the best practices contemplate the concept of impact, their approach is not similar to the case study. At INCM the impact results from finding the

maximum impact in eight different contexts and not in a simple quantitative or qualitative scale. The result is that, the type of this attribute (and residual impact) must be a complex type. Another difference is the appearance of the ”treatment_state” attribute, which can have three values: planned, in progress and implemented. This attribute is directly connected with the association with the class ”Control” and, specially, with the attribute ”state” since, as explained in the framework, this attribute defines the value for the ”treatment_state” attribute. Additionally, since it is important to keep track of the different iterations of the risk management process, each risk have assigned its identification date and its last updated date.

Since the risk management process of the organization in study is oriented by business process, the domain model contemplates this association with the appearance of the ”Business process” class. Apart from the business process, the described process also contemplates the ”Asset” concept. Here the association cannot be modeled as a direct connection between ”Asset” and ”Risk” since the assets are directly connect with the consequences of the events that lead to risks, therefore, the association is materialized between the ”Consequence” and ”Asset” classes.

The association between ”Risk” and ”Category” is related with the risk categorization component of the INCM ERM framework. Since, at INCM, the risk categorization is based on a tree-approach, it is necessary to contemplate the aggregation association between categories and sub-categories.

3.5 Conclusion

The problem was divided in two questions, namely, ”what?” and ”how?”. One conclusion to draw is that, to answer to the second question in an efficient way, firstly, the first question needs to be answered. It is necessary to establish a communication model to then materialize it using information visualization techniques. In order to solve these two questions, this chapter described the main aspects of the ERM framework in study.

Throughout the chapter became clear that the risk communication and consultation problem has two fronts, each one with different focus. The first front is related with establishing different views and, since the ERM framework in study already approaches the topic of differentiating the communication of risks according to its receivers, the challenge is to understand if it is possible to create a generic communication model that defines views that can be applied to every ERM framework. Since this dissertation intends to solve the risk communication and consultation problem at INCM, this generic communication model has to be aligned with the communication strategy of the organization in study.

On the other hand, the second front of the problem has to due with the representation of the risk information. Since this is an information architecture problem, here the challenge is to propose a representation of the risk information using the domain model in the figure 3.7. This second front of the problem cannot be explored in a generic approach since it is not possible to break the dependencies between the possible solutions with the information architecture of the ERM framework.

Changing the scope, it is also interesting to analyze this problem in the context of organizational communication. Looking at the organizational communication process (section 2.3.1) and defining risk communication, at INCM as the context, it can be concluded that the problem sets on three instances of the communication process, one for each type of risk management report.

Each instance differs in all aspects, except in the source role, which is always performed by the CRO. Regarding the channel, it can be established that each type of risk management report is a different communication channel since each report carries different information to different receivers.

Regarding the different dimensions of the communication, for each instance of the process the communication is classified differently. The one thing that is similar across the three instances is that the communication is formal because it is materialized in the production of official written documents. When the receivers are the ERM committee and the board of directors, the direction of the communication is upwards. When the receivers are the risk owners, it is lateral. Finally, when the receivers are the context directors it is diagonal. Excluding the specialized risks reports, where the communication can be internal and external, all other communications are internal.

Just by analyzing the INCM ERM framework it is possible to determine all these features about the organizational communication process. Therefore, the only variable that needs to be solved is the message itself. Making a parallelism, the different instances of the organizational communication process establish the answer to the question ”what?”, and the encoding of the message establishes the answer to the second question, ”how?”.

4

Proposed solution

Contents

4.1 Communication model 50

4.2 Representation of risk information 51

4.3 Risk management reports proposal 58

4.4 Conclusion 60

In this chapter the proposed solution for this problem is described. The proposal is divided in two parts, each one answering different questions, namely ”what?” and ”how?”.

4.1 Communication model

Beginning with ”what?”, this question is focused on the needs of stakeholder and how these needs define the communication model. As stated before, the ERM stakeholders should, at least, consist on the members of the ERM structure defined in the COSO ERM framework 2004. Apart from these members, could be interesting to consider other entities, such as the CEO, the CFO, context coordinators and process managers as ERM stakeholders.

The CEO and CFO are common roles in organizations and should be taken into account. Context coordinators and process managers are present in the majority of the big organizations and, since they are responsible for managing the organization business structures as well as consolidating all the information that emerges in the different contexts and processes, they are ERM stakeholders. Looking into the responsibilities of all identified stakeholders and into their roles inside an organization, it is possible to design a RACI matrix, illustrated in figure 4.1.

This RACI matrix presents three clusters. In the first cluster, the risk information that contains priority risks, strategic risk and all the relevant outputs from the ERM process, should be analyzed by the ERM committee and, ultimately, sent to the high-level hierarchical members (top management). The cluster in orange represents the risk information that is addressed to certain contexts, like corruption, information security, environment and others. According to the context, the respective stakeholder should

	Board of directors	CEO	CFO	ERM committee	CRO	IA	Risk owners	Context coordinator	Process Managers
1.Context establishment	I	I		I	R	I			
2.Risk identification				I	A	I	I		R
3.Risk analysis				I	A	I	R		
4.Risk evaluation				I	A	I	R		
5.Risk treatment				I	A	I	R		
6.Monitoring and review	I	I		I	A	I			
7.Communication and consultation	-			-	-	-	-	-	-
7.1 Communicate the big picture of the current risk situation	I	I	I	C	R/A	I			
7.2 Communicate high priority risks	I	I	I	C	R/A	I			
7.3 Communicate strategic risks	I	I	I	C	R/A	I			
7.4 Communicate context dependent risks (information security, corruption, environmental, CRM, etc.)				I	R/A	I		I	
7.5 Communicate control plans				I	R/A	I	I		I
7.6 Communicate non-implemented controls				I	R/A	I	I		I
7.7 Communicate risk treatment effectiveness				I	R/A	I	I		I

R - Responsible A - Accountable
C - Consulted I - Informed

Figure 4.1: RACI matrix

be informed about its risk information e.g. the information security risks should be addressed to the information security coordinator. Lastly, the green cluster represents the risk information related to risk treatment. Since risk owners are responsible for monitoring and implementation of the action plans their risks, they should be informed.

In this RACI matrix, external stakeholders are not addressed, however, in certain case studies is required to contemplate their needs. In most cases, these stakeholders can be placed in the orange cluster of the RACI matrix since their needs are related with audits of certain contexts of the organization as, for example, corruption.

Looking at the risk communication and consultation problem under a generic approach, there is a noticeable need to create three channels for the risk communication and consultation activity. There are three different views[1] that fulfill the needs of the ERM stakeholders which, together, constitute a communication model. This generic approach makes this communication model valid for all organizations that perform ERM following the best practices described in this dissertation. Therefore, this generic communication model can be seen as the proposal to solve the first part of the risk communication and consultation problem.

As said in the previous chapter, after the definition of a generic communication model, its application to the case study is required. Looking at the description of the risk communication and consultation activity in the INCM ERM framework, it mentions three types of risk management reports. Comparing the proposed communication model with the description of these three types of risk management reports, it is possible to understand that, in this practical case study, the different reports materialize the three different views that were established in the RACI matrix. Even though INCM does not have the CEO and CFO roles, their absence does not affect the clusters. Ultimately, the top management is the board of directors.

Since the proposed communication model can be applied to the INCM case study, the next step is to advance to the second question (how?).

4.2 Representation of risk information

Communicating risk can be materialized by using one or more visualization techniques, as well in dashboard form, where two or more techniques are correlated. These independent visualization techniques or dashboards are commonly used to produce risk management reports that gather all the risk information that needs to be communicated.

Since the objective is to understand the information itself and how it should be represented, the answer to this question must be based on the evaluation of the different existing techniques in order to understand its dependencies to the information, making it an information architecture problem. There-

[1] In enterprise architecture a view is "a representation of a system from the perspective of a related set of concerns", [22]. In this case the three clusters are the different perspectives of the system, based on the different needs of the stakeholders.

fore, in order to solve this problem, an analysis of the domain model from the ERM framework in study is required, which is illustrated in figure 3.7.

Having in mind that every organization tends to create its own ERM approach and customize it according to its needs, this question cannot be explored in a generic way as it is completely dependent on the information architecture emerging from the ERM framework. Unlike the proposal for the first part of the problem, the proposal for the second part consists on an application for this particular case study.

Continuing to explore of the second part of the problem, the importance of analyzing the domain model is to understand what information can be used in the three types of risk management reports. The domain model is useful for selecting visualization techniques that can be used to produce the mentioned reports, i.e. comparing the information architecture that visualization techniques require with the INCM ERM domain model allows one to understand which techniques can be used or not.

After analyzing the domain model, the first hypothesis to be considered to solve this part of the risk communication and consultation problem was to use the visualization techniques described in the section 2.4 Risk communication and consultation, namely, the risk matrices, bow tie diagrams and fish bone diagrams. Even though these techniques are the most common, they were not suitable for this case study.

Regarding the risk matrices, and comparing the figures 2.6 and 3.7, it may seem that they are suitable for this ERM framework, however, although the information architecture of the INCM ERM framework includes the three concepts required by this technique, using a risk matrix would omit the different impacts.

A risk matrix has the capacity to encode three concepts and, looking at the case study, there are more than three concepts. In normal conditions, the level of risk results from multiplying a likelihood by an impact and, in reality, this is what happens in the studied framework. However, it is important to reiterate that there are 8 different impacts and only the maximum impact, together with the likelihood, is used to calculate the level of risk. Therefore, risk matrices would only be able to represent the maximum impact. Risk matrices do not allow this variety of the concepts and their correlation.

Regarding bow-tie and fish-bone diagrams, they are not suitable to this case study due to the fact that they are built using semantic analysis. Even though they are suitable for this domain model, they require spending time analyzing the information itself which is a very complex process. Ultimately, taking into account both the benefits and costs of using these techniques, it was decided that the costs of doing so were superior.

Another considered hypothesis was to use the remaining techniques mentioned in the section 2.4 Risk communication and consultation, namely, the common charts and diagrams like bar charts, line charts and others. These diagrams are highly flexible and do not present any issue regarding the domain model and complexity. This was the chosen approach to solve this part of the problem since the

proposal consists on the creation of a dashboard with 8 sections, illustrated in figure 4.2.

The decision of developing a dashboard is based on the analysis performed to figure 3.7. The idea was to present the main aspects of that model and, most importantly, to show how they are related with each other, which would be impossible using independent visualization techniques. The solution was the creation of a dashboard with 8 different sections, which are materialized with 8 visualization techniques that depend on each other. The mentioned sections are: statistical information, performance indicator, treatment strategy, state of controls, control effectiveness, impact distribution, (sub)category distribution and temporal evolution.

4.2.1 Statistical information

In this section, the number of identified and mitigated risks (which were analyzed to create the current dashboard) are presented, as well as the global level of risk for the set of risks in study. Additionally to the statistical information, the date when the dashboard was created is represented, enabling traceability of the versions of the represented risks. Risks can be updated and, to create a history of these versions, the date of the last update is used to record these changes. Then, the date of the creation of the dashboard allows the user to understand if the dashboard was created using the last version of its risks or not.

The importance of this information is simple: the date gives us the possibility of tracing the iterations of the risk management process and enables comparisons between those iterations. The number of identified and mitigated risks make it possible to understand if the current dashboard corresponds to the analysis of all the organization risks or just to a specific a set. The global level of risk presents the result of the performance indicator (next section of the dashboard) in a qualitative scale, enabling the rapid insight about the overall severity of the risks analyzed in the dashboard.

A small table is used to represent the statistical information. Since the information to be presented is simple, there is no need to use anything more complex than a table. The information is not supposed to be deeply analyzed, as it only represents general information about the risks, working as an introduction.

4.2.2 Performance indicator

This section is meant to present a risk management performance indicator regarding the level of risk before and after treatment. The idea behind presenting an indicator is to somehow demonstrate how risk treatment is affecting the overall level of risk of a group of risks. This indicator is calculated according to the following formulas:

$$\textit{Risk management performance indicator} = \textit{Total Level of Risk} / \textit{Maximum Level of Risk}$$

$$\textit{Total Level of Risk} = \sum \text{Level of Risk}$$

$$\textit{Maximum Level of Risk} = \textit{Nº of Risks} \times \textit{Maximum Level of Risk}$$

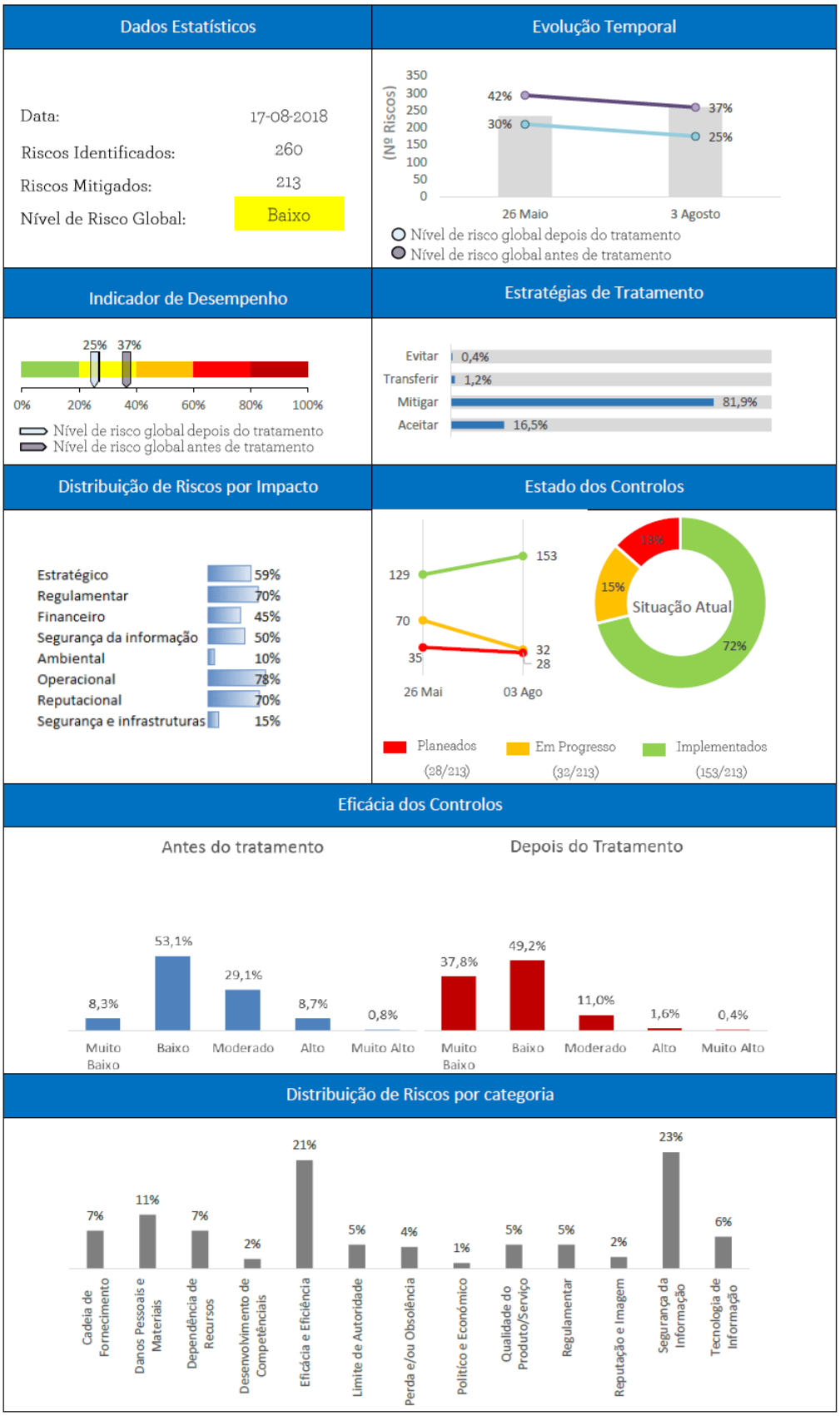

Figure 4.2: Dashboard

This indicator is weak when presented alone as it can distort the severity of the analyzed risks. However, when used in the dashboard with the other information visualizations, it is useful to understand how risk treatment is being affected by other factors. These factors will be explained in the other sections of the dashboard.

A horizontal gauge chart is used to represent the performance indicator. This visualization is simple but enables the representation of two points in time simultaneously: the result of the indicator before and after risk treatment. Additionally, this visualization enables the use of color to encode the severity of the result of indicator.

4.2.3 Treatment strategy

In this section the information about the different treatment strategies defined in the ERM framework is represented. A risk is associated with a treatment strategy, therefore, a distribution percentage for each type of strategy is shown in this section. As stated in the previous item, this is one of the factors that influences the performance indicator. Accepting a risk means that its residual level of risk is equal to its level of risk, leading to an approximation between the result of the indicator before and after the treatment. This means that we can look at the performance indicator section and, simultaneously, to the treatment strategy section and correlate them to analyze its results.

The used visualization technique was a horizontal fill gauges chart. This chart aims to represent the percentages of the four types of treatment strategy using fill gauges. It can be seen as variance of bar charts, except that it represents the percentage as a part of a whole, giving relevance to how close, or far, the current value is from 100%.

4.2.4 State of controls

Directly connected with the previous section, in this section, the percentage distribution of the three states of controls of the risks whose treatment strategy is mitigation is presented: implemented, in progress and planned. This is the most important section of the dashboard as it describes the unfinished treatments. All risks that do not have implemented controls (planned and in progress) have not been fully treated yet and, correlating this section with the performance indicator, it is possible to infer whether these untreated risks are severe or not. As in the previous section of the dashboard, the untreated risks have residual level of risk equal to the level of risk, leading to an approximation between the result of the indicator before and after the treatment. Here, the correlation can be deeper because, if the result of the indicator after treatment is high, the stakeholder can immediately understand if the untreated risks are severe or not.

The used visualization technique was a donut chart. Each portion of the donut chart represents the percentage of risks associated with the three states of controls. The advantage of using this visualization technique is that it enables the usage of color to encode other factors. In this case, it color was used to

highlight the urgency of implementing the non-implemented controls.

4.2.5 Control effectiveness

This section was created to help providing better insight on the severity of the risks before and after treatment. Here, the percentage of risks for each level of risks before and after treatment can be visualized. With this information, it is possible to see the effectiveness of the controls and decide if the need to implementing the controls that have not been implemented yet is urgent or not. This section together with the performance indicator, the strategy treatment and the state of controls, enables the stakeholder to make decisions. Correlating all these sections, it is possible to infer which the necessary next steps to follow are.

For this section, the chosen visualization technique was the bar chart. Looking at the information to be presented, two characteristics have to be considered: time and type of information. Regarding the type of information, the level of risk attribute is nominal since it is divided in 5 categories: very high, high, moderate, low and very low. Regarding time, the information to be presented is divided in two points in time (two instants: ”instants are a model for single points in time [sometimes also referred to as time point, e.g., May 10, 2014]”, [23]): before and after treatment, being the treatment the event that changes the state of the data. Having this in mind, and knowing that the intention of having this section is to compare distribution across categories, the chosen solution is to use two separate bar charts, one for each point in time.

4.2.6 Impact distribution

As explained in the framework, a risk can have multiple impacts, in this case 8 different types of impacts. In this section, the percentage distribution of risks per each impact is presented. This is the only section where the sum of the percentages is not 100% and, therefore, the reason to have this section is related with information quality and consistency i.e. with this distribution we can see if the risk analysis is coherent. E.g. if we are analyzing risks of a business process related with production, it is expected that a high percentage of these risks will have operational impact. With this section we can see whether this really happens and, by applying this notion to every context it is possible to infer if the risk management process was well executed (essentially, the risk analysis activity as it is the stage where the impacts are evaluated).

For this section, the chosen visualization technique was the bar chart. The impact attribute is nominal as it is divided in 8 categories, one for each type of impact. Having this in mind and knowing that the intention of having this section is to lookup [2] the distribution across impacts, the chosen solution is to use a bar chart, which is aligned with the reference [24]. Note that the first intention of this section is not to compare the distribution across the 8 impacts, as one risk can have several impacts leading the sum

[2] When ”users already know both what they’re looking for and where it is, then the search type is simply lookup”, [24]

of the percentages to exceed 100%.

4.2.7 Category distribution

As described in the ERM framework, the risks were categorized according to the categories presented in figure 3.2. In this figure it is possible to see the first level risk categories but, apart from this level, second level categories were also created, leading to a tree categorization. This means that a risk is not only associated with a category but also with a subcategory. The interest in this sub categorization is to have a more concise risk distribution, as well as to avoid having semantically different risks associated with the same category. This section is meant to present the percentage distribution for all the categories, having in mind that there were categories that were not associated with any risk. Due to the fact that the categorization was conducted by semantic analysis, the advantage of presenting this information is to enable the stakeholder to have a more detailed idea about the risks. Another opportunity here is the possibility of understanding the information consistency. As in the previous section, the categories enable the stakeholder to understand if the set of risks was well analyzed or not.

For this section, the chosen visualization technique was the bar chart. Looking at the type of information to present, the risk category attribute is nominal (self-explanatory given the name of the attribute itself). Having this in mind and knowing that the intention of having this section is to compare distribution across categories, the chosen solution was to use a bar charts, which is aligned with the reference [24].

4.2.8 Temporal evolution

This section is meant to represent the evolution of the result of the performance indicator between two points in time: result before and after the treatment. Looking at the performance indicator formulas, it is clear that this result depends on the number of risks and, if the evolution of the number of risks is not considered, the evolution of the performance indicator means nothing. For example, if the performance indicator result after the treatment increases between two points in time, the stakeholder can infer that something went wrong; however, without knowing the evolution of the number of risks, the stakeholder cannot draw that conclusion. If there were added risks with higher level of risk than the existent ones, even if the added risks are all mitigated and with implemented controls, the percentage increases, which does not means that something went wrong.

The solution was to use a combination chart, which consists on a combination between a bar chart with a slope-graph chart. Combining these two graphs enables the encoding of two different attributes: number of risks and performance indicator result. Remember that these two attributes are different in type: the number of risks is a number and the performance indicator result is a percentage. That is why these two types of charts are required together (two different scales are required). The bar chart represents the number of risks in two points in time: previous state and present. The slope-graph chart represents the performance indicator, before and after treatment, at the same points in time.

To represent the evolution of the results of the performance indicator a slope-graph was chosen. This type of chart is useful for this purpose as the slope visually encodes the rate of change between the two points. It enables the viewer to understand rapidly what the evolution was since it is inborn for the human eye to preattentively differentiate slopes, [23].

Looking at this particular section, it has to be said that, just by itself, it does not provide all the relevant information regarding the temporal evolution since, as explained before, the performance indicator is weak when used alone. This section is useful when the **number of risks do not increase** from one time to another, as it can bring important information for the stakeholders. Figure 4.3 (next page) shows a table with the possible conclusions to be drawn according to the different scenarios. This table can be split into two parts: the first part represents the scenarios described so far, when the number of risks do not increase; the second part represents the scenario when the number of risks do increase by introducing a new attribute and consequent conclusions.

If the number of risks increases over time, this combination chart, alone, does not present enough information about the evolution. If, for example, the number of risks increases, both the performance indicator before and after treatment increase, making the conclusions unclear due to the lack of enough variables it is impossible to understand if the new risks are severe or if an update on the existing ones was conducted, deeming it impossible to understand why the performance indicators changed.

To fully understand the evolution of the risk situation, the stakeholder also needs to see the evolution of the state of controls. Analyzing the performance indicator and the state of controls simultaneously enables the stakeholder to understand if his risk situation improved since the previous state. Consult figure 4.3 to explore the scenarios that are possible after the addition of this attribute.

To represent the evolution of the state of controls, a **slope-graph chart** was used as the visualization technique, which is also present in the section state of controls of the dashboard, as it can be seen in figure 4.2. The reasons for choosing this chart are the same as explained before.

Now, analyzing the dashboard as a whole, it is possible to understand that it deeply explores the risk assessment and risk treatment activities of the risk management process. The reason why these activities were explored is because the output of those activities represents the core information about the current state of the organization. It can lead to making decisions regarding the next steps to follow.

In order to help making decisions, the dashboard is accompanied by a **filtered table with the non-implemented controls**. This table is sorted by severity of the risks that the mentioned controls intend to mitigate. This type of sort is useful for the stakeholder to consolidate the information that he perceives from the dashboard and to lead him to take action by prioritizing the controls to be implemented.

4.3 Risk management reports proposal

Now, gathering the proposals for the two parts of the problem and using them together, the idea is to replicate the proposed dashboard for the three risk management reports. The dashboard was

Nº of Risks	Implemented (or in progress) controls	Performance indicator results		Conclusion
		Before treatment	After treatment	
→	Not needed	→	→	Nothing changed.
			↑	The residual likelihoods or the residual impacts of the risks changed in a way that increased the global level of risks after treatment.
			↓	It means that there are more implemented controls, leading to a decrease on the global level of risk after treatment.
		↓	↑	An update on the existing risks was conducted and the likelihood or the impacts of the risks changed in a way that decreased the global level of risks before treatment. The residual likelihoods or the residual impacts of the risks changed in a way that increased the global level of risks after treatment.
		↑	↑	An update on the existing risks was conducted and the likelihoods or the impacts of the risks changed in a way that increased the global level of risks before treatment. Due to this update, controls are no longer as effective as before, increasing the result after treatment.
		↑ ↓	→	An update on the existing risks was conducted and the likelihoods or the impacts of the risks changed in a way that increased (or decreased) the global level of risks before treatment. The controls are still effective and the changes do not modify the result after treatment.
		↑ ↓	↓	An update on the existing risks was conducted and the likelihoods or the impacts of the risks changed in a way that increased (or decreased) the global level of risks before treatment. In spite of this, there were controls that were implemented since the last date that reduce the global level of risk after treatment.
↑	→	↑	↑	The new risks have a significantly higher level of risk than the existing ones. The new risks were not treated, leading to an increase of the global level of risk after treatment.
		↓	↑	The new risks have a slightly higher level of risk than the existing ones. Even though they have higher levels of risk, the new risks were not treated, leading to an increase of the global level of risk after treatment.
			↓	The new risks have lower levels of risk than the existing ones and, even though they are not treated, they decrease the global level of risk after treatment.
	↑	↑	↑	The new risks have a significantly higher level of risk than the existing ones. There are more implemented controls, however, having new severe risks leads to an increase of the global level of risk after treatment.
			↓	The new risks have a significantly higher level of risk than the existing ones. There are more implemented controls, and these controls significantly reduce the level of risk. Having a lower result after treatment means that the implemented controls were effective.
		↓	↑	The new risks have a slightly higher level of risk than the existing ones. The added controls are not effective enough to avoid the increase of the performance indicator after treatment.
			↓	The new risks have lower levels of risk than the existing ones. There are more implemented controls, and these controls significantly reduce the level of risk. It means that the implemented controls were effective.
	↓	↑ ↓	↓	The new risks have a significantly higher level of risk than the existing ones (or lower, according to the case). The only possible situation when the controls change to affect the performance indicator is related with the treatment strategy. If there are risks that were mitigated, and they were updated to being transferred, the residual level of risk becomes 0, leading to a decrease of the result of the indicator after treatment.

Figure 4.3: Evolution conclusions*

*The figure only shows the possible combinations of the variables. For mathematical reasons the other possibilities are impossible, or almost impossible, of occurring.

thought in a way that it gathers all the information architecture required to fulfill the needs of the different stakeholders. Having established the information architecture that fulfills all the requirements, the way to differentiate the stakeholder needs is presenting different instances of the information architecture itself i.e. change the set of risks to be represented in the dashboard leading to the creation of different instances of this information architecture. Therefore, in order to fulfill the requirements, the final step is to propose a structure for each type of risk management report.

Regarding the enterprise risks report the proposed structure consists in four sections: the first one with an instance of the dashboard presenting the information regarding all the risk of the organization together with a filtered table containing all the non-implemented controls of the organization. In the second section, an instance of the dashboard for each one of the risk categories described in the risk categorization component of the INCM ERM framework, illustrated in figure 3.2. Since the stakeholders of this risk management report have a high hierarchical level, the third section is similar to the previous one, however, here, instances of the dashboard were created for each business process and each support process instead of creating dashboards for each category. Finally, in the same line of thought as the previous sections, instances of the dashboards for each risk owner were created (keep in mind that risk owners are the INCM organic units).

For the risk mitigation reports, the proposed structure is: A first section with the instance of the dashboard that represents all the risks of the organization, a second section with instances of the dashboard correspondent to the processes that the risk owner in study is assigned with the role of manager. Additionally, a final section with the instance of the dashboard representing the risk of the risk owner in study. Within this last section of the report is also presented filtered table containing the non-implemented controls assigned to the risk owner in study.

Finally, for the specialized risks reports the proposed structure consists in two sections. In the first section, an instance of the dashboard representing all the risks of the organization is presented. The second section contains an instance of the dashboard presenting risks related with the context in study as well as a filtered table containing the non-implemented controls related with the risk of the context in study. The next chapter of this dissertation demonstrates how these proposed structures try to fulfill the requirements.

4.4 Conclusion

By splitting the problem in two parts, it was possible to develop a solution structured in two parts. The first part of the solution consisted on the creation of a generic communication model that can be applied to every organization. Afterwards, it was concluded that the risk communication and consultation strategy described in the ERM framework of the INCM is aligned with the mentioned communication model. Having established a communication model retrieving knowledge from the previous chapter,

the focus became the second part of the problem. Here, the proposal consisted on the creation of a dashboard.

After analyzing the proposed dashboard, it became clear that the concepts of the domain model that must be communicated to the stakeholders should be the ones related to risk assessment and treatment. As already said, these two activities of the risk management process provide as output the relevant information to create action plans. Regarding the risk assessment output, it enables the stakeholder to understand the current state of the organization regarding risk. Regarding the risk treatment output, it enables the stakeholders to understand what is the impact of the controls in the levels of risks and, consequently, if that impact is positive or negative.

Finally, joining the communication model with the dashboard, in the last section of the chapter it is proposed the structure for each type of risk management report. This proposal intends to fulfill the requirements described in section 3.3 by using the dashboard in a way that it can materialize the different views proposed in the communication model.

5

Results demonstration

Contents

5.1 Dashboard instance 63

5.2 Enterprise risks report 66

5.3 Risk mitigation reports 67

5.4 Specialized risks reports 67

5.5 Conclusion 71

This chapter is meant to demonstrate how the proposed solution solves the problem. To do this, it will be explained how the proposal fulfills the requirements.

As stated before, the problem was split into two questions, each one with a different proposal. For the first part of the problem, a generic communication model was proposed, which turned out to be compatible with the INCM ERM framework. For the second part of the problem, a dashboard was proposed, which was developed through the analysis of the INCM ERM information architecture.

In the section 4.3 Risk management reports proposal it is described how the risk management reports, which are the specification of the communication model in the INCM case study, were built, and how different instances of the dashboard were used to materialize the needs of the different groups of stakeholders in an appealing and intuitive way. Here the idea is to explore that proposal and described how it can fulfill the mentioned requirements.

5.1 Dashboard instance

Since the different instances of the dashboard are the core information that is used to build the risk management reports, this section intends to show how one of those instances can be explored. In order to explore an instance of the dashboard, figure 5.1 illustrates a real example of it. This example refers to an instance of the dashboard related with risks associated with the human resources department [1].

As risk owner, the director of the human resources is mostly concerned with the risks associated with its department. By introducing minor comments presenting conclusions to be drawn in each section of the dashboard, figure 5.2 demonstrates how it is possible to fulfill the needs of this risk owner.

Figure 5.2 tries to show how different instances of the dashboard represent different views of the domain model i.e. the key differentiator between those views are the risks that are represented on the instance of the dashboard and not the visualization techniques or the content of each section of the dashboard. Since the instances of the dashboard enable analysis of different instances of the domain model, they can represent different needs of different stakeholders.

A way of analyzing the information quality regarding the risks in study is to look at the impact distribution and category distribution sections. As shown in the example, these two sections provide tools to understand if the instance of the dashboard represent the expected risks or not. Analyzing the category distribution section in detail, apart from the highlighted categories, the percentage of risks associated with the information security category is also elevated, which can be strange at first sight. However, since the human resources department deals with sensible information regarding the employees of the organization, this number enables the stakeholder to infer that the risk analysis was well executed. This type of conclusions enrich the use of different instances of the same dashboard to materialize different views.

[1] Even though the example refers to a real risk owner of the organization in study, the values are distorted due to confidentiality issues.

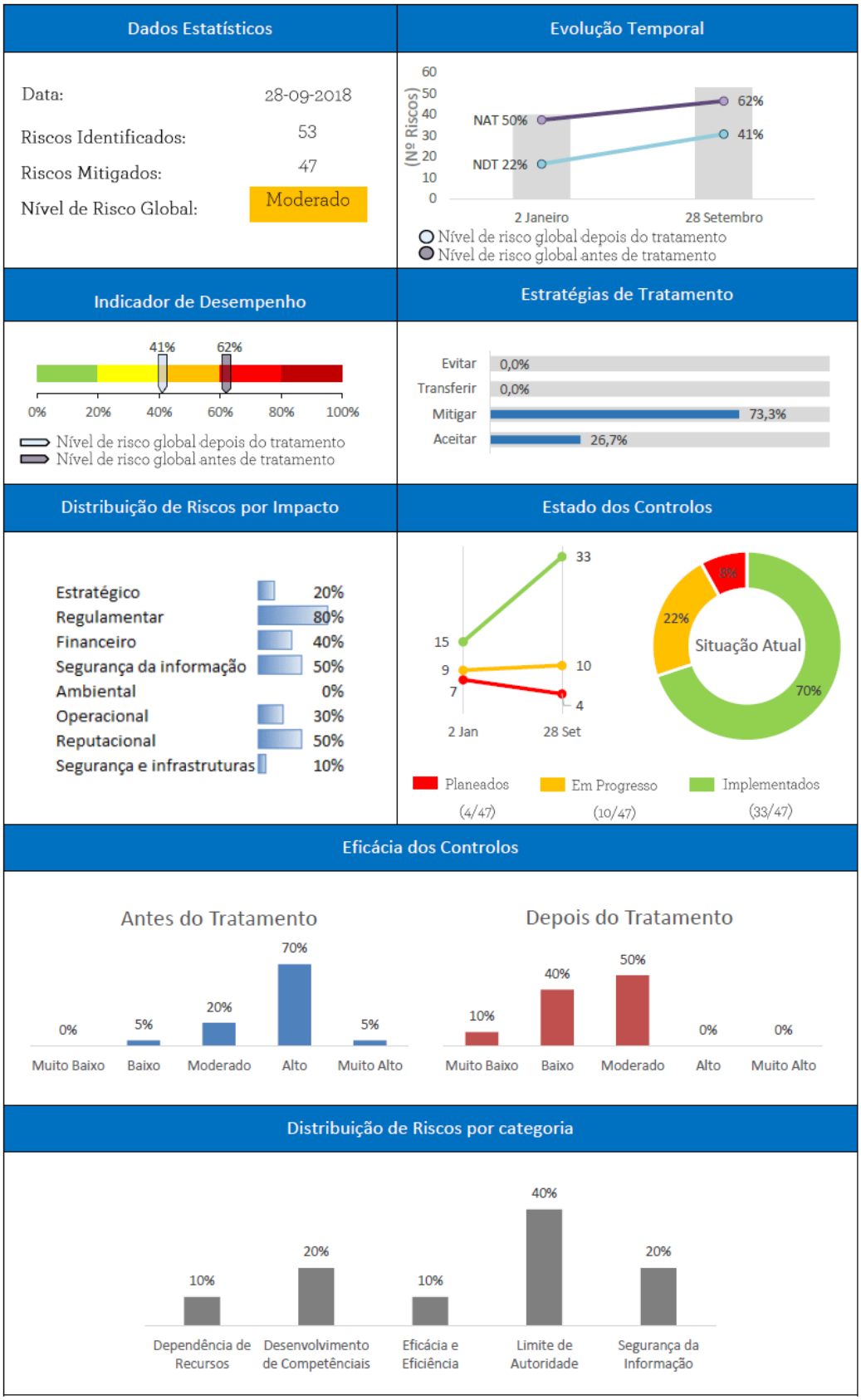

Figure 5.1: Dashboard instance example (Portuguese)

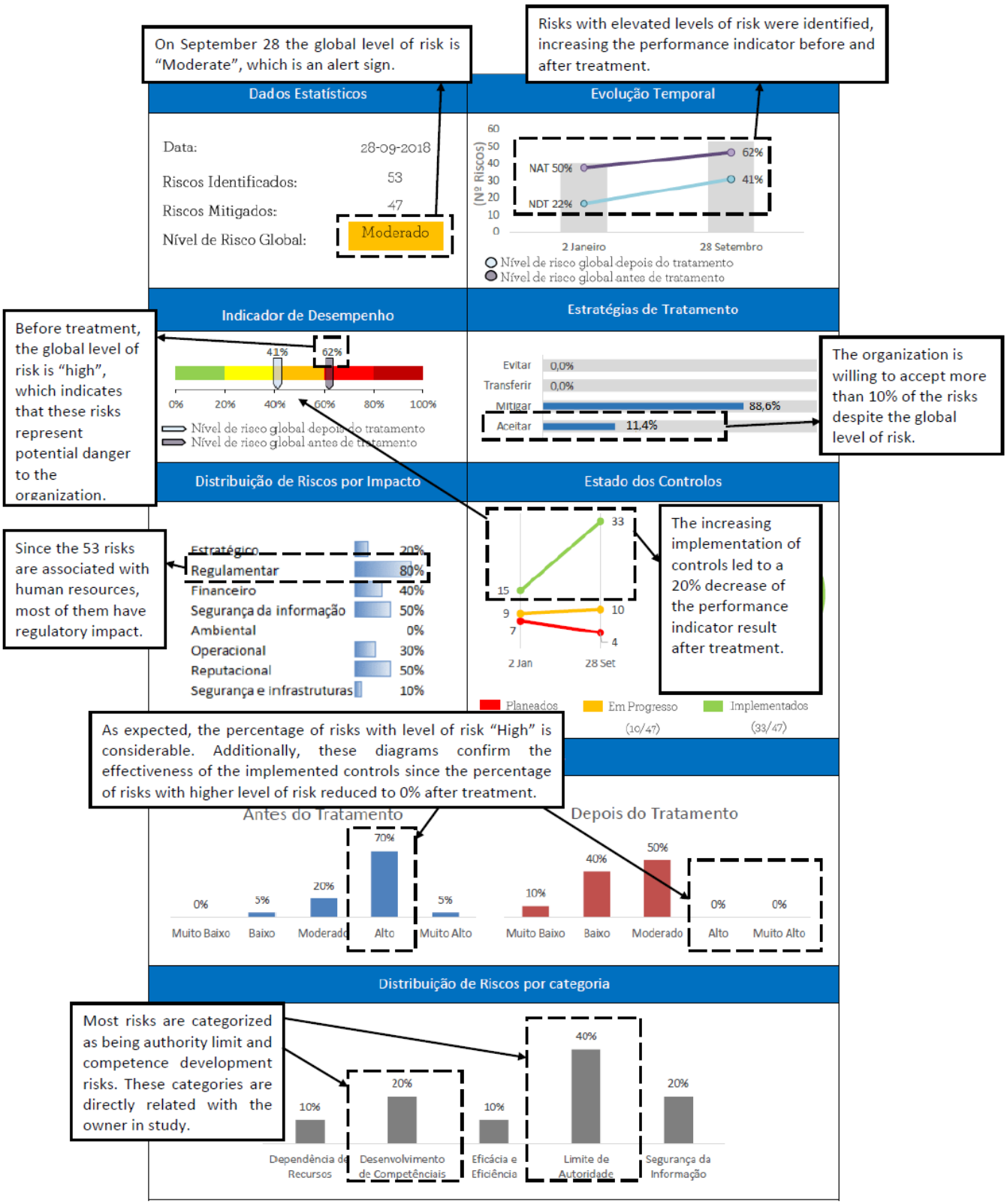

Figure 5.2: Dashboard instance example

5.2 Enterprise risks report

Looking into the requirements for this type of risk management report, the main concern is related with prioritizing the plans of action for the future i.e. it is expected that the stakeholders, which are the ERM committee and the board of directors become able to perceive the state of art of the risk situation of the organization and to plan the future steps to create value.

As stated before, this risk management report is structured in four sections: in the first section, the dashboard that contemplates all risks of the organization is presented (now on refereed to as enterprise risks dashboard). This dashboard enables the understanding of the current state of the organization regarding risk, which fulfills the requirement **R1**. As said before, this dashboard is presented together with a filtered table with all the controls that are not implemented, which fulfills the requirement **R2**.

The second section in the risk management report is related with the risk categories. This categorization was done in a tree based approach and so, a dashboard was developed for each one of the first level categories i.e. each one of these dashboards contains the set of risks correspondent to the category in study. In these dashboards, the category distribution section represents the percentage distribution of the second level categories, instead of representing the distribution of the first level categories.

By creating the dashboards for each category, the ERM committee and the board of directors gain awareness about the different types of risks that the organization has, which is related with the requirement **R1**. Since the categories are directly related with business and directly connected with the specialized contexts (corruption, reputation and image, social responsibility, information security, etc.), it is possible to understand if there any specific critical areas that need urgent analysis.

Since the stakeholders of this risk management report have a high hierarchical level, the third section is similar to the previous one, however, here, instances of the dashboard were created for each business process and each support process instead of creating dashboards for each category. The reason why this section is included is related with the fact that these kind of stakeholders are very concerned about the efficiency and effectiveness of the organization processes, which is related with the requirement **R4**. Basically, the analysis of the risks based on the processes enables the possibility for the stakeholders to understand where they are losing money and how can they solve it. The fact that these particular stakeholders have a deep knowledge about the organization business layer was also taken into account, making it easier for them to understand the information presented in these dashboards.

Finally, in the same line of thought as the previous sections, dashboards for each risk owner were created (keep in mind that risk owners are the INCM organic units), which is also related with the requirement **R4**. With this section, the stakeholders have the notion about risk accountability i.e. the risk owners are the accountable for implementing and monitoring the controls associated with their risks. Then, with this section, the ERM committee and the board of directors understand who are the risk owners that need to make action plans to improve their risk situation.

Regarding the requirement **R3**, keep in mind that the dashboard represents all the information about risk treatment. By containing the sections performance indicator, treatment strategy, state of controls and control effectiveness, the instances of the dashboard, present in this risk management report, all together fulfill the requirement. They enable the stakeholders to infer about the risk treatment effectiveness across the organization risks.

5.3 Risk mitigation reports

The risk mitigation reports have the risk owners as stakeholders. These reports have the main goal to inform the risk owners about the implementation and monitoring of the controls.

For each risk owner (organic unit), a risk mitigation report containing three sections was distributed. Firstly, the enterprise risks dashboard is presented for the risk owner to gain awareness about the overall risk situation of the organization. With this dashboard, the risk owner is able to understand if his risks have characteristics that diverge from the rest of the risk situation organization.

Secondly, as mentioned before, all the INCM's processes have a manager. This manager is the director of an organic unit, leading to an overlap of roles i.e. an organic unit director is, simultaneously, a risk owner and a process manager. Consequently, there are risks where he is considered the owner while also having indirect responsibility in the risks associated to the processes where he is the manager. Having this in mind, the process architecture of the organization was analyzed in order to understand who the process managers are, with the goal of presenting the dashboards correspondent to each process that the risk owner, in study, is responsible for. These dashboard instances fulfill the requirement **R4**.

Lastly, the dashboard correspondent to the risk assigned to the respective owner is presented, fulfilling the requirement **R1**. The filtered table with the non-implemented controls assigned to this owner is also presented, fulfilling the requirements **R2** and **R3**.

With these three sections the stakeholder is able to understand all the information about its risks, as well as if the process(es) that he manages have risks that are assigned to other organic units. The dashboards, together with the filtered table, fulfill the requirement **R5**.

5.4 Specialized risks reports

Specialized risks reports are created according to the needs of the context coordinators. The specialized risks reports that were created were the information security risk management report, the environment risk management report and the corruption and related offenses risks management plan.

5.4.1 Information security risk management report

Regarding the information security specialized context, its coordinator is the Chief Information Security Officer (CISO). Looking at the risk categorization, it can be seen that there is a category correspon-

dent to information security, leading to the possibility of filtering the risks by this criterion. On the other hand, this category is not wide enough to gather all the risks that impact the information security and, if this risk management report only contained the information about the risks that were categorized as information security risks, it would be incomplete. There are risks associated with other categories that have impact on the information security, meaning that the report should also mention them.

Therefore, as established in the framework, one of the defined impacts was information security and, then, the impact was used as the selection criteria for this particular specialized risks report. All the risks that impact on information security were used to create the dashboard instance presented in the report, even if that impact is not the highest (as defined in the INCM ERM framework, to calculate the level of risk, the highest impact of the eight possible impacts is chosen). This dashboard instance fulfills the requirement **R1** of this type of risk management report.

There is a difference between the dashboard used in this specialized risks report and the one illustrated in the figure 4.2. As the set of risks is selected by impact, there is no reason to present the impact distribution section. To replace this section, a process distribution consisting in a distribution of information security risk across the processes was presented instead. The visualization technique did not change because the information is of the same type as the one presented in the impact distribution section of the dashboard.

Apart from the dashboard with this set of risks, the enterprise risks dashboard is also presented. As explained before, this dashboard enables an awareness about the overall risk situation of the organization, as well as enables the CISO to understand the placement of its risks in the organization, fulfilling the requirement **R4**.

The report also contains the table of the not implemented controls that are associated with the information security risks. With this table the context coordinator is able to monitor the risk owners that are responsible for the implementation of such information security controls, fulfilling the requirement **R2**.

Keep in mind that the requirement **R3** of this type of risk management reports is related with external stakeholders demanding additional requirements. Since this particular context has no external stakeholders there are no more requirements, and so the requirement **R3** does not have to be fulfilled.

5.4.2 Environment risk management report

The coordinator of this specialized context is the director of the *Direção de Segurança e Apoio* (DSA) organic unit. Looking at the risk categorization, it can be seen that there is a category related with environment, which is the environmental responsibility category. However, as in the information security context, this category do not gather all the risks that the stakeholder needs to see.

Once again, the selection criteria was the impact. For this report, the environment dashboard contains all the risks that were identified as having environmental impact, fulfilling the requirement **R1**.

The impact distribution section of the dashboard was also replaced by the process distribution, in the same condition as that of the information security context. Additionally, the enterprise risks dashboard is also presented, fulfilling the requirement **R4**.

As in the information security risk management report, here, the table of the non-implemented controls associated to the environmental risks is also presented, fulfilling the requirement **R2**. Additionally, there are no external stakeholders, resulting in no additional requirements. Therefore, the requirement **R3** does not have to be fulfilled.

5.4.3 Corruption and related offenses risk management report

This specialized context is different from the above. Here, there are internal and external stakeholders, meaning that the requirements for creating the report are more than the ones described in section 3.3.3 Requirements for specialized risks reports. The requirements demanded by the external stakeholder had to be taken into account as well.

For this report, the internal stakeholder is the IA department, which contains the coordinator of this context. Additionally, it has as external stakeholders a variety of government entities, such as the Portuguese court of auditors, which demands all governmental organizations to create this report. Even though the court of auditors demands it, it does not specify any requirement for the presentation of the risk information. The court of auditors only give three genera, listed below, [25]:

- The report should contain the identified risks of corruption and related offenses.
- The report should contain the adopted measures to prevent the identified risks.
- The report should contain the identification of the involved participants in the development of the report.

Even though these requirements are only guidelines, they were taken into account and fulfilled. The risk information is presented in an appealing way and, apart from that, the risk register containing the risks of corruption and related offenses is presented in table format as an appendix of this report. The adopted measures are the controls associated with each risk (which are also contained in the risk register as they are part of the information architecture of the ERM framework). In the beginning of the document there is a section that introduces the involved participants, which, combined with the risk register, fulfills the guidelines and, by inheritance, the requirement **R3** of this type of risk management report.

Before the work developed in this dissertation, the corruption and related offenses reports developed in the previous years only took in consideration these external guidelines, leading these reports to contain endless lists of risks that are not useful to making decisions. Therefore, the new report present the risk information in an appealing way and enables the analysis of the information.

Since the report is delivered to an external entity, it contains information regarding organizational structures and regulations that are not the scope of the work and, thus, only the techniques used to visualize the risk information are described here. The full report can be seen in the INCM public website (link in footnote [2]).

The risk information used in this plan results from filtering the global risk information. This filter consists in selecting the risks that were categorized as ”Corruption and Related Offenses” (see figure 3.2 Risk categorization at INCM), fulfilling the requirement **R1**.

Note that this is the only risk management report where the developed dashboard is not used. This happened due to time restrictions, which led this report to be the first to be created. The information visualization techniques used here are similar to the the ones used in the dashboard, however, when this report was developed the dashboard was yet in an initial stage of development.

Beginning the description of the report, the first visualization technique used was a pie chart. To use this visualization, the corruption and related offenses risks were sub categorized according to 7 categories: abuse of rights; information disclosure; human error; information unavailability; information integrity compromised; recovery of products or raw materials for destruction, and loss of assets.

The decision of using this pie chart was to present an initial overview of the information, making the stakeholders aware of the distribution of the risks in the categories. This is useful because the categories were created according to the Portuguese laws that are related to the crimes of corruption. Each category refers to one or more of these crimes i.e. A risk that is categorized as abuse of rights means that it is associated with the possibility of incurring in crimes of influence traffic, abuse of power or economic participation in business.

Another factor to consider was the notion that pie charts are only readable with twelve or less pies. In this case, we only have 7 categories and, thus, the readability of the chart was not affected, [24]. Additionally, the main concern of present this information is not to compare the percentages themselves, but only to present an overview and demonstrate that the risks were evenly categorized.

The information about the risk treatment was presented next in the report. The methodology used was the same as in the treatment strategy and state of controls sections of dashboard from the first iteration.

Additionally, the same information as in the control effectiveness section of the proposed dashboard is presented. The difference is in the calculation of the level of risk. The level of risk was calculated using only the regulatory impact i.e. in the framework it is established that the level of risk results from multiplying the likelihood of an event occurring with the maximum impact of the consequences of that event. In this case, since the context is centered in corruption, only the regulatory impact was considered, and not the maximum (see the domain model in figure 3.7). Another reason to this is the

[2] https://www.incm.pt/portal/arquivo/incm/plano_2018.pdf

fact that this specialized risks report is delivered to an external entity, and so, for the external stakeholder there is no interest in analyzing the other impacts contemplated in the ERM framework.

Finally, the performance indicator, which is also in the dashboard, is presented. Here, the overall risk management performance, which results from summing the levels of risks from all the corruption and related offenses risks is presented, followed by the performance indicator by category. The total level of risk is calculated for all the categories, by summing the level of risks of the risks for each category, fulfilling the requirement **R2**.

This context is very different from the others and, looking at the requirement **R4** of this type of risk management report, the external entities should not be able to compare the context risks with the overall risk situation of the organization. The overall risk situation of the organization is confidential and in that way, the requirement **R2** cannot be fulfilled for this particular specialized risks report.

5.5 Conclusion

Relating this chapter with the work methodology (DSRM), the result demonstration is intended to demonstrate the efficiency of the proposed solutions in solving the problem in study. Therefore, in this chapter, the risk management reports were describe in a way that enables the better understating about the choice of using different instances of the developed dashboard to fulfill all the requirements. Using the same dashboard structure to fill the different reports, changing only the risks to be analyzed, was proven to be an efficient way of fulfilling the requirements.

Establishing the need of having three different risk management reports and then establishing how a set of visualization techniques can fulfill the needs of the different groups of stakeholders were explored separately but with the ultimate goal of joining both in order to solve the problem as a whole. The proposal for answering the question ”what?” established the skeleton of the solution and the dashboard (how?) established the filling of the skeleton.

To conclude this chapter, it is clear that there is a report that is different from the others, namely, the corruption and related offenses report. This is the only risk management report that has external stakeholders, leading to more requirements. Apart from that, the appearance of external stakeholders leads to privacy concerns. Performing risk management in an organization enables the gathering of information that can contain internal issues, which should not be transmitted to external entities. Another concern about having external stakeholders is time restrictions.

To sum up, the introduction of external stakeholders increases the complexity of this problem. From the organizational communication point of view to the risk communication and consultation problem, having external stakeholders can change the way that organizations solve this problem.

6

Evaluation

Contents

6.1 Evaluation: iterative process 73
6.2 Survey: results and discussion 76

This work was developed according to the DSRM, which is based in an iterative process. For this work the development process reached to three iterations.

In the first two iterations, the produced artifacts were dashboards. In the third iteration, the artifacts were risk management reports, containing the instances of the produced dashboard. This means that the evaluation performed to the artifacts was different according to the iteration itself. Then, in this chapter, there are described all the three different evaluations and the consequent discussion.

6.1 Evaluation: iterative process

Starting with the first iteration, the developed dashboard is the one illustrated in figure 6.1 (*Portuguese*), in the next page. This dashboard has the same sections as the final dashboard, except the temporal evolution section. Another difference is the visualization techniques used in the treatment strategies and state of controls sections. In this first proposal, these two sections are represented with two sets of liquid fill gauges. A liquid fill gauge is a simple visualization that represents percentages, simulating the level of water corresponding to that percentage and, additionally, it enables the use of color to represent other features. In this case, the circles were used to represent, firstly, the percentage of risks that were controlled according to each type of controls established in the framework and then, for the risks that were mitigated, the percentage of controls that were already implemented, the percentage of controls with implementation in progress and, lastly, the percentage of the controls that are only planned to be implemented. For the states of controls, color was added in order to highlight the urgency of implementing the non-implemented controls. To create these charts, it was used the d3 technology[1].

In this first iteration, the evaluation group was composed by one member of the board of directors and the *Direção de Planeamento e Controlo* (DPC) organic unit, which contains the CRO. The evaluation method used was an informal non-structured interview with open questions. It was an informal process because in this first iteration the intention of evaluating the dashboard was more related with the process of its creation and minor aspects about the ”looks” of the dashboard itself.

Another reason for having an informal evaluation is related with the evaluation group. For this iteration, the evaluation group was very small and did not contain the main stakeholders.

The main conclusions drawn after this evaluation were: the 7 dashboard sections are adequate to represent the main concepts of the domain model and the visualization techniques represent the information in an appealing way. On the other hand, creating the liquid fill gauges with the d3 technology, for the treatment strategies and state of controls sections of the dashboard is not efficient for this scenario. The reason why it is not efficient is that this technology does not integrate with excel, which is where all the information was stored and where the dashboard was created. This leads to an unnecessary increase of time and complexity when creating the charts.

[1] https://github.com/d3/d3/wiki/Gallery

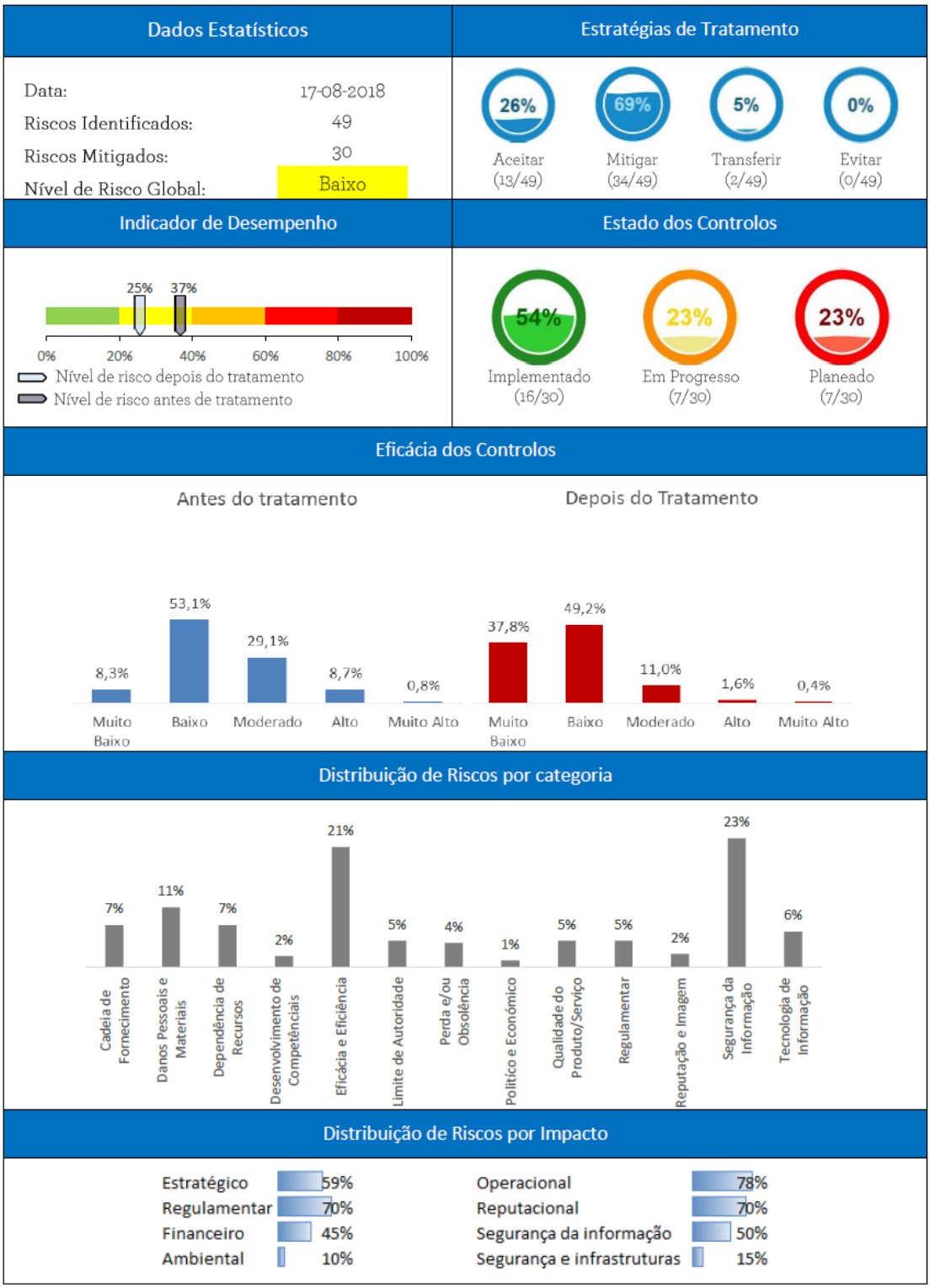

Figure 6.1: First iteration dashboard proposal

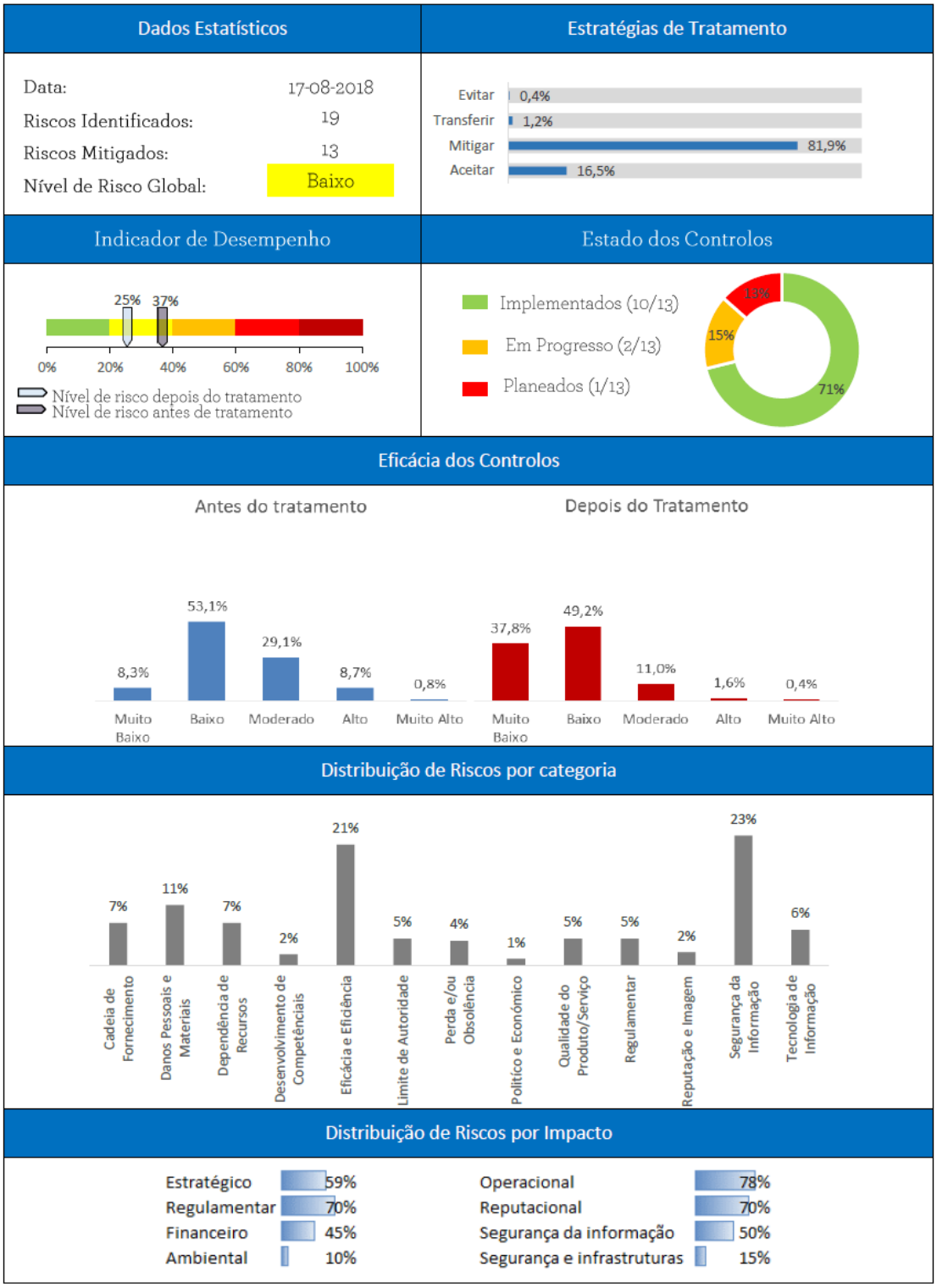

Figure 6.2: Second iteration dashboard proposal

Having in mind the conclusions taken from the first evaluation, in the second iteration the changes made to the dashboard consisted in the replacement of the visualization techniques used for the treatment strategy and state of controls sections. Instead of using the liquid fill gauges for both of them, the solution was to have two different visualization techniques: a horizontal gauge chart and a donut chart, respectively. The final result is illustrated in figure 6.2 (*Portuguese*), in the previous page.

The dashboard evaluation in this iteration was more profound as it was done by the ERM committee. The evaluation methodology was an informal non-structured interview with open questions as it consisted in a meeting between the ERM committee members.

At this point, the risk management process proposed in the INCM ERM framework had already started its second iteration i.e. new risks were already identified and more controls had been implemented. This being said, the focus of the evaluation was related with evolution. The ERM committee demanded a new requirement that stating that the dashboard should demonstrate the evolution of the risk situation, between two iterations of the ERM process.

To fulfill this new requirement, two changes were made to the dashboard. Firstly, it was analyzed which features could represent evolution in the risk situation. The conclusion was that the evolution should be measured according to the performance indicator and the state of controls. These changes are reflected in the dashboard presented in the chapter 4, namely in figure 4.2.

Having reached this point, the risk management reports were designed and developed as explained in the previous chapter. Afterwards, they were distributed to the respective stakeholders.

The evaluation for the risk management reports consisted in a survey (Appendix D). This survey was distributed to 30 members of the organization, namely to the organization monitors and to the directors of the organic units. There were received 18 answers, distributed across 15 organic units.

This survey is divided in four sections: introduction, evaluation of risk mitigation report, specialized evaluation of the dashboard and open discussion. The first section describes the purpose of the survey. The second section is intended to evaluate the risk management report as a whole. Note that the receivers of this survey were organic unit directors and their role in risk management is being risk owners. Therefore, taking into consideration that the different risk management reports have the same sections and are built in the same way, the survey only mentions the risk mitigation reports. Each director answers to this survey by looking at their risk mitigation report.

The intention of using a survey was to compare the final solution against the requirements, established in chapter 3. In the next subsection the results are described and discussed.

6.2 Survey: results and discussion

Since the survey is divided in three parts, the resulting analysis of the answers will be performed in three parts as well. Firstly, the results related with the evaluation of the risk management reports will be

discussed, then the discussion will be centered in the results related with the proposed dashboard and, finally, the open questions answers will be explored.

The overall conclusion regarding the first part of the survey is that the proposed risk management reports fulfill the requirements. Looking at each question individually, the percentage of answers ”Agree” and ”Strongly agree” is always superior to 78%, except in the question: ”it is possible to identify if the implemented controls are effective in the risk treatment”, where the percentage of ”Disagree” answers is superior than the others. Since there is a question where the results were not as satisfactory as expected, a deeper analysis regarding the mentioned results is necessary. On the other hand, the percentage of answers correspondent to the choice ”Strongly disagree” is 0%.

Analyzing the results of the mentioned question, it is possible to understand that the percentage of satisfactory answers are superior to the unsatisfactory ones. The percentage of disagrees is small (11%), however, since the question is related with the risk treatment effectiveness, this is a percentage that cannot be overlooked. Another interesting point is the percentage of ”Not applicable” answers, which is 22%. There are two possible conclusions to draw with these results: the first is related with the lack of awareness of the stakeholders regarding this theme since, as stated before, at INCM, ERM is still a recent topic and the importance of it is not very clear to all members of the organization. Since this question relates different concepts from different parts of the risk management report and of the ERM framework, its correlation could not be as clear as expected to the stakeholders; The other conclusion is that, in fact, the risk management report was not able to carry the intended message. To explore this conclusion, it is necessary to carry one to the second part of the survey since the question is related with the analysis of the dashboards present in the report i.e. in order to understand if the implemented controls are effective in the risk treatment, the stakeholder must analyze all the risk management report, comparing the present dashboards and filtered tables with each other. Therefore, it is necessary to analyze if the dashboard itself is able to help the stakeholder to infer about this question.

Considering the requirement related with the prioritization of the non-implemented controls, 78% of the respondents considered that the risk management report enables them to prioritize the controls that should be implemented. Since the risk analysis and the risk treatment activities were the main focus in the proposed solution, this question has higher relevance.

Since controls are the strategies to treat the risks and, thus, are responsible to decrease the levels of risk and since the decision making scenarios are based in the information about the controls, it is critical to stakeholders to have the possibility of prioritizing the actions to perform. Having this importance, the results of the survey demonstrates that the proposed solution is efficient in fulfilling this requirement.

Regarding the other questions, the percentage of answers ”Agree” and ”Strongly agree” is superior to 83% in all of them. These questions are related with the requirements that regard with the necessity of the stakeholder to understand its risk situation as well as the risk situation of the organization and

with the necessity of the stakeholder to understand the different roles that he might have in the ERM. As explained before, a risk owner can also be a process manager and, thus, in the risks mitigation reports there are sections correspondent to risks related with processes and to risks related with their owner.

Advancing to the second part of the survey, the questions are different from the previous ones. Here, the dashboard was treated as an interface and, therefore, the questions were thought to evaluate it accordingly (With the purpose of all stakeholders having the same starting point to answer the questions, figure 4.2 was added to this section of the survey as the example to analyze in order to answer the respective questions).

Except the first question, where it is asked how many identified risks there are present in the example dashboard, the other questions have true and false format. The idea was to have a question per section of the dashboard in order to analyze if its intended purpose was achieved.

Summing up, the conclusions to draw with these results are: The visualization technique used to represent the temporal evolution is not suitable; the stakeholders do not understand the impact distribution section; the stakeholders have difficulties to analyze the control effectiveness section, and, finally, that the other sections and its correspondent visualization techniques are suitable for the intended purpose.

Regarding the first conclusion, it is related with two questions, namely, ”the effectiveness of controls is higher on August 3 than on May 26” and ”the number of identified risks increased since May 26”. The correct answers to these questions should be false and true, respectively, since the control effectiveness is equal on both dates and the number of risk increased. However, 67% of the respondents answered true to the first question and 72% answered false to the second one. Looking at the chosen visualization technique for the respective section of the dashboard, which was a combination chart between a slope-graph diagram and a bar chart, it is clear that it is not a common use chart and, thus, its readability proven to be difficult to the respondents.

Even though this combination chart proven to be hard to analyze, looking at the answers to the question ”the number of implemented controls increased since May 26”, 89% of the respondents answered it correctly. Since the visualization technique used to represent the evolution of the state of controls is a slope-graph, it means that this diagram was highly efficient to represent evolution. In order to solve the problem discovered previously, a possible solution is to split the temporal evolution section into two: evolution of number of risks and evolution of the performance indicator, using the same visualization techniques (bar chart and slope-graph, respectively), as illustrated in figure 6.3 (Portuguese).

Regarding the impact distribution section of the dashboard, the conclusion is that the respondents do not understand it. The question that enabled this conclusion is: ”there are more information security risk than regulatory ones”, which is true, however, 61% of the respondents answered false. After analyzing the results of the survey it became clear that the majority of the stakeholders looked to the wrong section of the dashboard to answer this question. In place of looking at the category distribution, they looked at

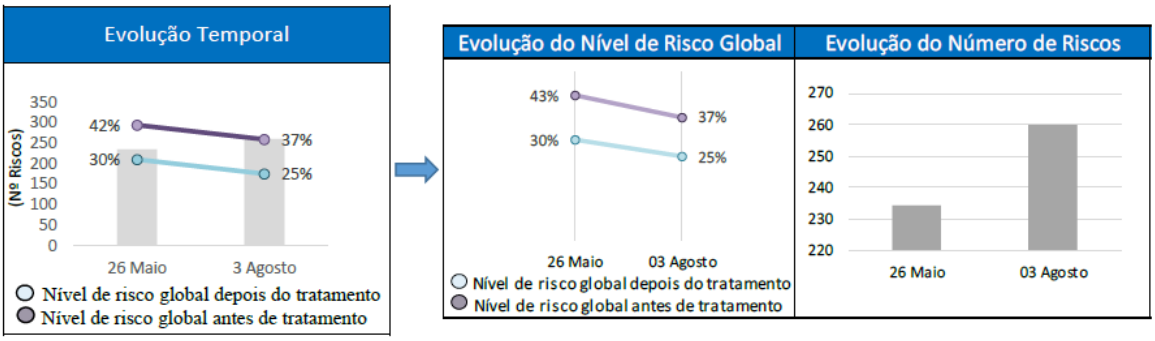

Figure 6.3: Proposed improvement for temporal evolution

the impact distribution section of the dashboard. This was not an expected outcome, however, it helped to discover that the stakeholders do not fully understand that a risk can have more than one impact and, thus, the distribution of risk per impact does not sum up to 100%. This lack of understanding can derive from the lack of knowledge of the ERM framework, which once again is related with the insufficient awareness regarding this theme.

Another conclusion taken is related with the control effectiveness section of the dashboard. The conclusion is that the respondents have difficulties in read the two bar charts that represent the percentage of risks for each level of risk before and after treatment. Looking at the answers to both questions that regard with this section of the dashboard, the results are very different from one to another since 89% of the respondents answered correctly to the first question (the implemented controls allowed to reduce the number of risks with level of risk ”very high”), however, only 39% answered correctly to the second question (there are more risks with level of risk ”high” before treatment than after treatment). This divergence leads us to conclude that the visualization technique is not efficient to represent its intended purpose.

A possible solution, given the high acceptance of using slope-graphs to represent evolution between two periods in time, is to replace the two bar charts with a slope-graph as shown in figure 6.4 (Portuguese).

Regarding the other questions, the percentage of correct answers exceeded 88% leading us to conclude that the respective sections of the dashboard are effective and efficient to represent its intended purpose.

Finally, analyzing the open questions, most of the respondents stated that, for this stage of maturity of the framework, the risk management reports and the dashboard give a ”global and effective vision”, however, there were appointed improvement opportunities regarding the risk management reports. One respondent appointed that the risk management reports ”could be smaller and simpler” and another respondent appointed that the risk management reports could present a new information: ”Success rate of the controls i.e. How many times the controls allowed to anticipate events that lead to risks.”.

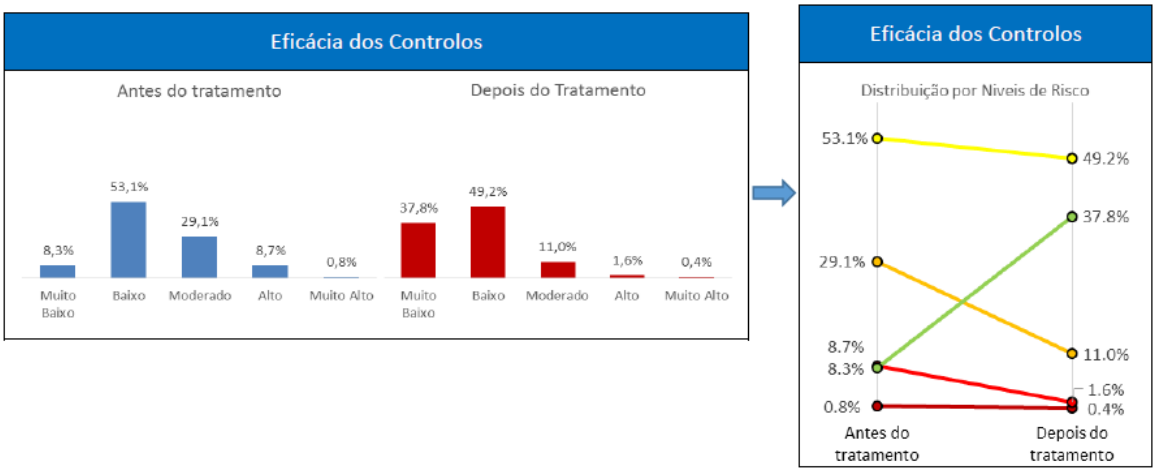

Figure 6.4: Proposed improvement for control effectiveness

Regarding the first improvement opportunity, it is interesting, however difficult to explore. Since the materialization of the communication model, at INCM, is through the creation of written documents, it is very difficult to pass all the information needed for stakeholders be able to make decisions with a reduce number of pages. Additionally, since this information should be presented in an appealing way, the purposed dashboard was thought in a minimalistic way as it only contains the minimum information that need to be represented. To reduce the number of reports, the materialization of the communication model must change is format, for example, to centralize the ERM strategy in a tool that enable CRO to create a permission management system. With this permission management system, the CRO is able to materialize the three different views by restraining what the different groups of stakeholder can see and analyze.

Regarding the other improvement opportunity, it is interesting, even though it is very difficult to keep record such information. Keeping record of the success rate of the controls can be very useful for increasing the maturity level of the INCM ERM framework since, relating with the section 3.2 Alignment between the INCM ERM framework and ISO 31000:2018 standard, there is a gap between both frameworks regarding the evaluation of the framework. This success rate can be used as an indicator to evaluate the ERM framework of INCM and, thus, is a great improvement opportunity.

To conclude, the proposed solution has the potential to, effectively, solve the risk communication and consultation problem at INCM. As seen throughout this section, the dashboard can be improved, however, in an overall appreciation of work, the evaluation, showed that the risk management reports are able to provide for its respective stakeholders the tools to create action plans in making-decision scenarios.

7

Conclusion and future work

Contents

7.1 Conclusions 82
7.2 Future work 82

This chapter concludes this dissertation and presents some future steps.

7.1 Conclusions

Nowadays, several organizations are trying to implement ERM frameworks into their businesses to gain competitive advantage in the market. Even though they are implementing ERM frameworks, many are stuck with endless spreadsheets with risks that no one really can take value from. Since it is a huge challenge, this dissertation only addressed one of the main features, the risk communication and consultation.

Having a risk communication and consultation strategy enables organizations to increase the maturity of its ERM strategy. Creating communication plans and channels to materialize those plans enable all the stakeholders to understand the risk situation of the organization and, from there, develop action plans.

In this dissertation the risk communication and consultation theme was explored in a real case study, namely at INCM. This work contributed to develop and implement the established risk communication and consultation strategy at INCM. To do this, risk management reports containing dashboards that were distributed across the existent stakeholders were created through an iterative process.

After the work, it is possible to draw three main conclusions:

1. Due to the information architecture dependencies, **it is impossible to generalize the dashboards to all organizations**, specifically, it is impossible to generalize the answer for the question ”how?”;

2. In spite of this, **for the organizations that follow the best practices, described in this dissertation, it is possible to generalize the proposed communication model**, which consists on defining the ERM stakeholders and their different needs, and on defining the resulting views. Summing up, it is possible to generalize the answer for the other fundamental question ”what?”;

3. **The final dashboard, and resulting risk management reports, are not the final solution for this problem of the organization. There is no final product in this matter**. Due to the characteristics of ERM, which is based on continuous improvement and change, the risk communication and consultation can be affected in accordance with the ongoing improvements.

7.2 Future work

After the work done in this dissertation, the possible future steps can be divided in two fronts. One is focusing on the case study organization and how it can improve its ERM framework; and the other front is consider the risk management theme as a whole.

Looking at the alignment performed in the section 3.2 of this dissertation, the following points should be addressed by INCM in order to increase the maturity of its ERM framework:

- The biggest gap between INCM ERM framework and the ISO 31000:2018 standard is related with **Leadership and commitment**. The top management entities are not yet using risk management as an enabler for creating value. In order to achieve this, the top management entities of INCM must start addressing risks when the objectives are being established. The establishment of objectives at INCM is performed by each organic unit director and then approved (and/or changed) by the board of directors and, at this stage, these objectives are not correlated with the existent risks.

- Still related with leadership and commitment, at INCM, the entity that ensures that the systems to manage risks are implemented and operating is the CRO. Once again, the next step is for top management entities to be more involved in the organization ERM strategy.

- Regarding the framework evaluation, INCM must **create evaluation indicators to evaluate the ERM framework**. These indicators can also be useful to be added to the risk management reports to be communicated.

Apart from the considerations emerged from the alignment, there is another challenge to be approached in the future, namely:

- The action plans that are associated with the implementation of new controls were not explored in this dissertation. For each control, the organization treats its implementation as a project, and, one possible step is to **integrate project management in the ERM framework** and include it in the communication as well.

Related with the risk management theme:

- It is urgent to develop a **tool that manages all the aspects of risk management**. This is, a tool that enables the management of the risk register and that can materialize the risk communication and consultation strategy. For this purpose, there is a tool that is being developed called Holirisk, but is not mature enough to be used yet.

Bibliography

[1] M. Arena *et al.*, "The organizational dynamics of enterprise risk management," *Accounting, Organizations and Society*, October 2010.

[2] D. Gjerdrum *et al.*, "New international standard on the practice of risk management – a comparison of iso 31000:2009 and the coso erm framework," *Society of Actuaries*, vol. Risk Management, Issue 21.

[3] K. Peffers *et al.*, "A Design Science Research Methodology for Information Systems Rsearch," *Journal of Management Information Systems*, vol. 24 Issue 3, pp. 45–78.

[4] "ISO 31000:2018 - risk management – principles and guidelines," International Organization for Standardization, Geneva, Switzerland, Standard, 2018.

[5] "ISO 73:2009 - risk management – vocabulary," International Organization for Standardization, Geneva, Switzerland, Standard, 2009.

[6] "ISO/IEC 31010:2009, "risk management – risk assessment techniques," International Organization for Standardization, Geneva, Switzerland, Standard, 2009.

[7] "ERM - integrated framework," Committee of Sponsoring Organizations of the Treadway Commission, Tech. Rep., 2004.

[8] A. Dias, "A more effective audit after coso erm 2017 or after iso 31000:2009?" *CEOS.PP – Centre for Organisational and Social Studies of P.*, 2017.

[9] "ERM - integrating with strategy and performance," Committee of Sponsoring Organizations of the Treadway Commission, Tech. Rep., 2017.

[10] IRM, "Review of the 2018 version of the iso 31000 risk management guidelines and commentary on the use of this standard by risk professionals," *A Risk Practitioners Guide to ISO 31000 – 2018*, 2018.

[11] BSI, “Introducing annex sl whitepaper - the new high level structure for all management system standards of the future,” *ISO Revisions*, August 2015.

[12] Kenan SPAHO University of Sarajevo, “Organizational communication process,” *Pages from Ekonomski Vjesnik*, 2012.

[13] L. M. James McCroskey and V. Richmond, “The nature of communication in organizations,” in *Organizational Communication for Survival: Making Work, Work.*

[14] P. Konttinen, “Developing Organizational Communication Improving Internal and Organizational Communication,” Master’s thesis, JAMK University of Applied Sciences, February 2018.

[15] K. A. Baker, “Organizational communication,” *Retrieved June*, vol. 7, 2002.

[16] PWC, “Erm program communication – not an optional activity,” *How to achieve excellent Enterprise Risk Management series*, May 2017.

[17] Australian Government - Department of finance, “Communicating risk,” *COMCOVER connect*, 2016.

[18] M. Eppler *et al.*, “A systematic framework for risk visualization in risk management and communication,” *Risk Management*, 2009.

[19] ISACA, *The Risk IT Framework*. ISACA, 2009, ISBN-10: 978-1-60420-111-6.

[20] B. Branson, “Reporting key risk information to the board of directors,” North Carolina State University, USA, Tech. Rep., 2015.

[21] R. Vieira, “*Plano de Gestão de Riscos Corporativos na INCM* (portuguese),” INCM, Tech. Rep., 2017.

[22] M. Lankhorst *et al.*, *Enterprise Architecture at Work: Modelling, Communication and Analysis (Enterprise Engineering Series)*, 3rd ed. Springer, 2012, ISBN-10: 3642296505.

[23] M. O. Ward *et al.*, *Interactive Data Visualization: Foundations, Techniques, and Applications*, 2nd ed. AK Peters.

[24] T. Munzner, *Visualization Design and Analysis: Abstractions, Principles, and Methods*. AK Peters, draft version: http://www.cs.ubc.ca/ tmm/courses/533-11/book/.

[25] C. de Prevenção de Corrupção, “*Recomendação do CPC sobre Planos de gestão de riscos de corrupção e infrações conexas* (Portuguese),” 1 Jul 2009.

Appendix A

Risk management: glossary

This Appendix is the main glossary for this project. Every concept is risk management domain-specific and will be presented in the following form:

Concept *(Type)*: description

There are 5 types of concepts:

1. *Activity:* behavior, which can be deployed as a single task or as a process coordinating multiple tasks.
2. *Object:* an information object created, used, or altered in an activity.
3. *Risk factor:* an element of risk, that is, a concept relevant for representation in a risk register.
4. *Stakeholder:* an interested party, including an actor in a sub-process or subprocess.
5. *Measure:* value that can be assigned to an attribute of a risk element (can be quantitative or qualitative)

Having all the types defined, here stands the concepts in alphabetic order (all of the descriptions can be found in [5] and others in [4]):

- **Risk analysis** *(Activity)*: process to understand the nature of risk and determine the risk Level.
- **Risk assessment** *(Activity)*: process of comparing the results of the risk analysis with the risk criteria in order to determine if the risk and / or its magnitude is acceptable or tolerable.
- **Cause** *(Risk factor)*: element that, by itself or combined with others, has the potential of creating a risk.
- **Communication and consultation** *(Activity)*: continuous and iterative process in the organization in order to provide, share and obtain information, and establish dialogue with risk management stakeholders.
- **Consequence** *(Risk factor)*: result that affects the objectives.
- **Control** *(Risk factor)*: action that modifies the risk
- **Risk Criteria** *(Risk factor)*: term of reference over which risk significance is assessed.
- **Risk description** *(Object)*: structured description of a risk, typically including three elements: events, causes and consequences.

- **Risk owner** *(Stakeholder)*: person or entity with responsibility and authority to manage the risk.
- **Context establishment** *(Activity)*: defining the external and internal parameters to be taken into account when managing risk, and establishing the scope and risk criteria for the risk management policy.
- **Risk management structure** *(Risk factor)*: a set of components that allow you to design, implement, monitor, review and continuously improve risk management in your organization.
- **Event** *(Risk factor)*: occurrence or change of a particular set of circumstances.
- **Risk management** *(Activity)*: coordinated activities with the purpose of managing and controlling an organization with respect to risk.
- **Risk identification** *(Activity)*: process of discovery, recognition and description of risks.
- **Monitoring** *(Activity)*: continuous review, supervision, critical observation or state determination in order to identify changes in required or expected performance levels.
- **Risk level** *(Measure)*: magnitude of risk or combination of risks expressed in terms of the combination of Consequences and their respective likelihoods.
- **Objective** *(Risk factor)*: result to be achieved.
- **Risk perception** *(Measure)*: risk perspective according to a stakeholder.
- **Risk management plan** *(Object)*: plan associated to the risk Management structure, specifying the approach, components and management resources to be used in risk management.
- **Risk management policy** *(Risk factor)*: statement of intent and direction of the organization with respect to risk management.
- **Likelihood** *(Measure)*: hypothesis of something happening. *Note:* The term used in the international literature for this concept is ”likelihood”, which can also be translated by estimate, which generally conveys better the concept that probability does not need to be understood as a mathematical probability.
- **Risk management process** *(Activity)*: systematic application of management policies, procedures and practices in the activities of communication, consultation, establishment of the Context, and identification, analysis, evaluation, treatment, monitoring and risk review.
- **Risk register** *(Object)*: registration of information on identified risks.
- **Risk management report** *(Object)*: form of communication with the intention to inform a stakeholder internally or externally by providing the current state of Risks and their management.

- **Review** *(Activity)*: activity performed to determine the adequacy, suitability and effectiveness of the element in meeting the established Objectives.
- **Risk** *(Risk factor)*: effect of uncertainty on Objectives.
- **Residual risk** *(Measure)*: remaining risk after treatment of the same.
- **Risk treatment** *(Activity)*: Process to modify risk.

Appendix B

Risk assessment techniques

Tools and techniques	Risk assessment process				
	Risk Identification	Risk analysis			Risk evaluation
		Consequence	Probability	Level of risk	
Brainstorming	SA[1)]	NA[2)]	NA	NA	NA
Structured or semi-structured interviews	SA	NA	NA	NA	NA
Delphi	SA	NA	NA	NA	NA
Check-lists	SA	NA	NA	NA	NA
Primary hazard analysis	SA	NA	NA	NA	NA
Hazard and operability studies (HAZOP)	SA	SA	A[3)]	A	A
Hazard Analysis and Critical Control Points (HACCP)	SA	SA	NA	NA	SA
Environmental risk assessment	SA	SA	SA	SA	SA
Structure « What if? » (SWIFT)	SA	SA	SA	SA	SA
Scenario analysis	SA	SA	A	A	A
Business impact analysis	A	SA	A	A	A
Root cause analysis	NA	SA	SA	SA	SA
Failure mode effect analysis	SA	SA	SA	SA	SA
Fault tree analysis	A	NA	SA	A	A
Event tree analysis	A	SA	A	A	NA
Cause and consequence analysis	A	SA	SA	A	A
Cause-and-effect analysis	SA	SA	NA	NA	NA
Layer protection analysis (LOPA)	A	SA	A	A	NA
Decision tree	NA	SA	SA	A	A
Human reliability analysis	SA	SA	SA	SA	A
Bow tie analysis	NA	A	SA	SA	A
Reliability centred maintenance	SA	SA	SA	SA	SA
Sneak circuit analysis	A	NA	NA	NA	NA
Markov analysis	A	SA	NA	NA	NA
Monte Carlo simulation	NA	NA	NA	NA	SA
Bayesian statistics and Bayes Nets	NA	SA	NA	NA	SA
FN curves	A	SA	SA	A	SA
Risk indices	A	SA	SA	A	SA
Consequence/probability matrix	SA	SA	SA	SA	A
Cost/benefit analysis	A	SA	A	A	A
Multi-criteria decision analysis (MCDA)	A	SA	A	SA	A

1) Strongly applicable.

2) Not applicable.

3) Applicable.

Figure B.1: Risk assessment techniques catalogue, [6]

Appendix C

ISO 31000 and AnnexSL

Clause	Annex SL heading	ISO 31000 (2018)
1.	**Scope**	
2.	**Normative references**	
3.	**Terms and definitions**	
4.	**Context of the organisation**	
4.1	Understanding the organisation and its context	Component 2 of the Framework: 'Integration' includes determining oversight roles and responsibilities and ensuring RM is part of all aspects of the organisation Component 2 of the Process: 'Scope, context and criteria' includes purpose and scope of RM, defining risk criteria and risk decision-making
4.2	Understanding the needs and expectations of interested parties	
4.3	Determining the scope of the management system	
4.4	The management system	
5.	**Leadership**	
5.1	Leadership and commitment	Component 1 of the Framework: 'Leadership and commitment' includes aligning RM, policy statement, resources and risk appetite Component 3 of the Framework: 'Design' includes internal and external context, roles and responsibilities, and communications and consultation
5.2	Policy	
5.3	Organisational roles, responsibilities and authorities	
6.	**Planning**	
6.1	Actions to address risks and opportunities	Component 1 of the Framework: 'Leadership and commitment' includes aligning RM, policy statement, resources and risk appetite Component 3 of the Framework: 'Design' includes internal and external context, roles and responsibilities, and communications and consultation
6.2	Management system objectives and planning to achieve them	
7.	**Support**	
7.1	Resources	Component 1 of the Process: 'Communication and consultation' includes involvement, risk information and ownership of risk Component 6 of the Process: 'Recording and reporting' includes information for decision-making and risk information for stakeholders
7.2	Competence	
7.3	Awareness	
7.4	Communication	
7.5	Documented information	
8.	**Operation**	
8.1	Operational planning and control	Component 4 of the Framework: 'Implementation' includes implementation deadlines, decision-making and implementation responsibilities Component 3 of the Process: 'Risk assessment' includes description of the identification, analysis and evaluation stages of risk assessment Component 4 of the Process: 'Risk treatment' includes the selection, design and implementation of risk treatment options
9.	**Performance evaluation**	
9.1	Monitoring, measurement, analysis and evaluation	Component 5 of the Framework: 'Evaluation' includes measuring framework performance and continued suitability of the framework Component 5 of the Process: 'Monitoring and review' includes monitoring RM outcomes, and inclusion of risk within performance reports
9.2	Internal audit	
9.3	Management review	
10.	**Improvement**	
10.1	Non-conformity and corrective action	Component 6 of the Framework: 'Improvement' includes value of RM, adapting the framework and integration of RM activities
10.2	Continual improvement	

Figure C.1: ISO 31000 and AnnexSL alignment, [10]

Appendix D

Risk management reports survey

Introduction

I ask for your cooperation to fill out this survey in order to make possible the evaluation of the risk management reports, distributed by the CRO.

This survey is for academic purposes, under the chair of dissertation for achieving the master's degree in computer engineering and computer science, at *Instituto Superior Técnico*, taking just 15 minutes of your time.

Thanks again for the availability and your attention!

Evaluation of risk mitigation report

In this section of the questionnaire, the focus is on the content of the "risk mitigation report" (attached to the email).

1. Select the option that you consider most appropriate for each item.

	strongly disagree	disagree	not applicable	agree	strongly agree
1. I know how to calculate the global level of risk of the organization.	☐	☐	☐	☐	☐
2. I can distinguish the risks of my process from the risks I own.	☐	☐	☐	☐	☐
3. I know the current state of the risks under my responsibility.	☐	☐	☐	☐	☐
4. It is possible to prioritize the controls to be implemented.	☐	☐	☐	☐	☐
5. It is possible to identify if the implemented controls are effective in the risk treatment.	☐	☐	☐	☐	☐

Specialized evaluation of the dashboard

In this section the scope of the questions focuses only on the dashboard illustrated in the figure 4.2 Dashboard[1].

This figure has no relation to the risk mitigation report explored in the previous section of the survey.

[1] This image was appended to the survey in order to the respondents be able to answer to the questions without looking to the risk mitigation reports. In this way, all the respondents answer to the questions about the same image with the same data, which facilitates the analysis of the results

1. Based on the figure 4.2, complete the following sentence: The number of identified risks is equal to _____

2. Based on the figure 4.2, select the option that you consider most appropriate for each item.

	True	False
1. The implemented controls allowed to reduce the number of risk with level of risk "Very High".	☐	☐
2. The global level of risk before treatment is "Moderate".	☐	☐
3. There are more risks with level of risk "high" before treatment than after treatment.	☐	☐
4. All the risk are mitigated.	☐	☐
5. 70% of identified risks have regulatory impact.	☐	☐
6. The number of identified risks has increased since May 26.	☐	☐
7. The number of implemented controls has increased since May 26.	☐	☐
8. The percentage of accepted risk is 20%	☐	☐
9. There are more information security risks than regulatory risks	☐	☐
10. The effectiveness of controls is higher on August 3 than on May 26.	☐	☐

Open discussion

1. Is there anything to improve on the content of the risk management report that you received? If so, what?

2. Is there anything to improve on the content of the dashboard? If so, what?