Enterprise Risk Management - Risk communication and consultation

Extended Abstract

Guilherme Pinho de Sá Santos
Instituto Superior Técnico
guilherme.pinho@ist.utl.pt

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 stakeholders and, therefore, consists in creating the different views for each type of stakeholders. 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 along the process iterations 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

1 INTRODUCTION

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).

ERM aims to create value for organizations through the use of risk information in strategic decision-making scenarios. In order to use the risk information, it has to be communicated in an appealing and intuitive way. This communication is materialized by the risk communication and consultation of the risk management process.

The work was developed under the Design Science Research methodology (DSRM) and it was focused on the “Imprensa Nacional Casa da Moeda” (INCM) case study. This organization is implementing an ERM framework and offered an internship meant to develop a risk communication strategy.

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.

2 RELATED WORK

According to [3], 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’s objectives and that effect is called risk”, more concisely a risk is the “effect of uncertainty on objectives”, [3]. 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 objectives of organizations. Risk management can be defined as the “coordinated activities to direct and control an organization with regard to risk”, [2]. 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 description presented above presents risk management as a process. A risk management process was proposed by ISO 31000:2018, which is illustrated in figure 1. Since this standard takes a holistic approach on this matter, the presented risk management process is generic, [3].
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.

Additionally, there is risk communication and consultation, which is responsible to connect 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.

Since the theme of this dissertation is ERM, it is necessary 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. Executing the risk management process is not sufficient to create an ERM framework.

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. COSO proposes 4 risk categories, [1]: 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. Apart from risk categorization, the ERM framework proposed by COSO is based on a group of five components: governance and culture; strategy and objective setting; performance; review and revision, and information, communication and reporting.

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.

As seen, in both references there is the notion of communication and recording risk information. Risk communication and consultation “is often the key differentiator in management’s perception and understanding of ERM value creation” [10]. 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, [10] [4] [6]: Who? When? What? Why? How?

Even though risk communication and consultation is context dependent, some of these questions 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), [7] [10].

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”, [10]. 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.

Afer understanding who the stakeholders are and why this activity is needed, 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", [4]. 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"; [7]. 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", [4]. 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)" [7].

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", [6].

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 into the current state of this problem, "the main genre 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", [6]. 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 "key method of communicating risk across business units and between multiple layers of an entity";[4]. 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.

Regarding risk matrices, they are highly appealing and the color scheme enables rapid insight into the severity of the risks represented. For this type of technique, the ERM framework has to contemplate 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.

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 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.

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.

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 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. 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.

3 PROBLEM DESCRIPTION AND ANALYSIS

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 ("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", [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, 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. 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.

The way that INCM tries to solve this problem is through the production of risk management reports. The ERM framework of INCM defines that 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.[11]:

- **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).

### 3.1 Requirement analysis

As explained in the previous section, the ERM framework of INCM already defines 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.

#### 3.1.1 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.

#### 3.1.2 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 which controls should be implemented with priority.
- **R3**: 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.
- **R4**: 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.

#### 3.1.3 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.

### 3.2 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 is based on the fact that 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 2.
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 it last updated date.

Since the risk management process described in the ERM framework of INCM 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.

## 4 PROPOSED SOLUTION

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, they are ERM stakeholders. They are responsible for consolidating all the information that emerges in the different contexts and processes. Looking into the responsibilities of the identified stakeholders and into their roles inside an organization, it is possible to design a RACI matrix, which is illustrated in figure 3.

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 be informed about its risk information. For example, 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. Therefore, 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 2.

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 with exploration 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, 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 eight 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 data 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.

The decision of developing a dashboard is based on the analysis performed to figure 2. 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 data, performance indicator, treatment strategy, state of controls, control effectiveness,
impact distribution, (sub)category distribution and temporal evolution.

4.2.1 Statistical data: in this section, the date when the dashboard was created is represented, enabling the user to trace the versions of the risks represented in the dashboard itself. The 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. Additionally, the number of identified risks (which were analyzed to create the current dashboard) and mitigated risks are presented, as well as the global level of risk for the set of risks. 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 risks and mitigated ones make it possible to understand if the current dashboard corresponds to the analysis of all the organization risks or just to a specific 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 data. Since the data 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:

\[
\text{Risk management performance indicator} = \frac{\text{Total Level of Risk}}{\text{Maximum Level of Risk}}
\]

\[
\text{Total Level of Risk} = \sum \text{Level of Risk}
\]

\[
\text{Maximum Level of Risk} = N \times \text{Maximum Level of Risk}
\]

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 the result of the indicator.

The visualization technique used 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, corre-
ating 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 visualization technique used 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 pro-
viding 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 characte-
ristics have to be considered: time and type of data. Regarding the type
of data, 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 data 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]", [12]): 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 data 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 [9]. 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 of the percentages
to exceed 100%.

4.2.7 Category distribution: as described in the ERM framework,
the risks were categorized according 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 data 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 data to present, the risk category at-
tribute is nominal (self-explanatory given the name of the attribute
itself). Having this in mind and knowing that the intention of hav-
ing this section is to compare distribution across categories, the
chosen solution was to use a bar charts, which is aligned with the
reference [9].

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 differ-
ent attributes: number of risks and performance indicator result.
Remember that these two attributes are different in type: the num-
ber 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 repre-
\(^2\)When "users already know both what theyâĂŹre looking for and where it is, then
the search type is simply lookup"[9]
the performance indicator, before and after treatment, at the same points in time.

To represent the evolution of the performance indicator results 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, [12].

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.

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. The reasons for choosing this chart are the same as explained before.

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 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 risks 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. 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.

5 RESULTS DEMONSTRATION AND EVALUATION

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.

The proposal for the structures of the three types of risk management reports, which are the specification of the communication model in the INCM case study, are based in the thesis that different instances of the proposed dashboard materialize the needs of the different groups of stakeholders in an appealing and intuitive way. Materializing this thesis, during the time of the internship, an enterprise risks report, eighteen risk mitigation reports and three specialized risks reports were developed and communicated to their respective stakeholders.

The final evaluation of the developed work was conducted with a survey. 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 one question, where the percentage of “Disagree” answers is superior than the others. On the other hand, the percentage of answers correspondent to the choice “Strongly disagree” is 0%.
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 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.

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.”

6 CONCLUSION AND FUTURE WORK

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.

After the work done in this dissertation, the possible future steps can include:

- 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.
- 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.

REFERENCES