



Enterprise Risk Management

An Information Management Tool to Support Enterprise Risk
Management

Miguel Azevedo da Silveira

Thesis to obtain the Master of Science Degree in

Information Systems and Computer Engineering

Supervisors: Prof. José Luís Brinquete Borbinha
Dr. Ricardo João Correia Vieira

Examination Committee

Chairperson: Prof. Pedro Tiago Gonçalves Monteiro
Supervisor: Prof. José Luís Brinquete Borbinha
Member of the Committee: Prof. Sérgio Luís Proença Duarte Guerreiro

September 2021

Acknowledgments

I would like to show my eternal gratitude to Dr. Ricardo Vieira for his knowledge, constant monitoring and tireless patience, and to Prof. José Borbinha for their availability and guidance throughout this journey, without them this work would not be possible.

I would like to thank all DPR members for their friendship and for providing me with an excellent environment to grow as an academic, professional and as a person.

I want to thank my parents for their love, support, affection and for having encouraged me to persevere and never give up.

Last but not least, I want to thank all my friends but particularly Fábio and Francisco, for offering me their constant patience, emotional support and for the miles walked at night, and Inês, for her love and unconditional friendship.

To each and every one of you – Thank you.

Abstract

Risk Management is one of the pillars of most processes and activities in one organization. Given the relevance in this context nowadays, the need for effective Enterprise Risk Management processes becomes urgent. Gathering, analyzing, and evaluating data in the most appropriate, appealing, and intuitive way helps prevent and respond timely to critical and harmful incidents in companies. Given the importance and scope of this topic, the literature is vast regarding acceptable practices and regulations. However, due to the lack of centralization of practical implementations, the current market has a collection of heterogeneous solutions geared towards specific applications and according to specific references. Our work explores this information gap by identifying functional requirements for ERM solutions and validating them in a corporation's software. As an organization with multiple businesses, the Portuguese Mint and Official Printing Office (INCM) wanted to dematerialize its risk management process using the JIRA tool, which was already used for other purposes inside the company, given its flexibility and ability to adapt to different use cases. This challenge allowed us to test our requirements in a new platform, not meant for processes with this complexity, adapting the tool to a process and not the other way around, while reaching the stability, effectiveness, and efficiency needed to solve both problems successfully. In the future, this thesis dissertation may be improved and seen as an asset for suppliers looking to cover more sectors in the market and for customers looking for dynamic and flexible solutions tailored to their needs.

Keywords

Enterprise Risk Management; Functional Requirements; Jira Software; Process Dematerialization.

Resumo

A gestão de risco é um dos pilares de suporte de grande parte dos processos e atividades de uma organização. Dada a sua importância, torna-se urgente a necessidade de um processo eficaz de Gestão de Risco Corporativo. Recolhendo, analisando e avaliando dados da forma mais adequada, apelativa e intuitiva ajuda a prevenir e responder atempadamente a incidentes críticos e danosos nas empresas. A literatura é vasta em referências de boas práticas e normativos sobre o mesmo. No entanto, devido à falta de centralização quanto a implementações práticas, o mercado atual possui um conjunto de soluções heterogêneas direcionadas para setores específicos de aplicação seguindo referências específicas. O nosso trabalho explora esta falta de informação ao identificar um conjunto de requisitos funcionais para soluções de Gestão de Risco Corporativo, validando-os num software corporativo. A INCM enquanto organização com múltiplos negócios, optou por desmaterializar o seu processo de gestão de risco na ferramenta JIRA, já utilizada para outros fins dentro da empresa, dada a sua flexibilidade e capacidade de adaptação a diferentes casos de uso. Este desafio permitiu-nos testar os requisitos numa nova plataforma que não se destinava a processos com esta complexidade, conseguindo adaptar uma ferramenta a um processo e não o contrário, conseguindo atingir a estabilidade, eficácia e eficiência necessárias para resolver ambos os problemas com sucesso. Esta dissertação poderá no futuro ser melhorada e vista como uma mais-valia tanto para fornecedores, que procurem abranger mais setores no mercado, como para clientes, que procurem soluções dinâmicas e flexíveis à sua medida.

Palavras Chave

Gestão de Risco Corporativo; Requisitos Funcionais; Jira Software; Desmaterialização de Processos;

Contents

1	Introduction	1
1.1	Problem Description	2
1.2	Motivation and Objectives	3
1.3	Results	4
1.4	Document Structure	5
2	Related Work	7
2.1	Fundamental Concepts	8
2.2	ISO/IEC 31000	10
2.3	ISO/IEC 27005	13
2.4	Committee of Sponsoring Organizations of the Treadway Commission	16
2.5	Discussion	21
3	Problem Analysis	23
3.1	Enterprise Risk Management Process Structure at INCM	24
3.2	Requirement Analysis	29
3.2.1	User and Group Management Module	30
3.2.2	Permissions Module	32
3.2.3	Notifications Module	34
3.2.4	Data Management Module	35
3.2.5	Search and Reporting Module	38
3.2.6	Exporting Module	41
3.3	Conclusions	42
4	Solution Design and First Prototype	45
4.1	Analysis of the JIRA Technology	46
4.2	Limitations of the JIRA Technology	49
4.3	First Prototype	51

5	Final Solution	59
5.1	Automation System	60
5.2	Usage	61
5.2.1	Risk Assessment	62
5.2.1.A	Department's Perspective	62
5.2.1.B	CRO's Perspective	67
5.2.2	Risk Treatment	68
5.2.3	Review and Reporting	71
6	Evaluation	75
6.1	Method	76
6.2	Analysis of the Results	77
6.3	Discussion	80
7	Conclusions and Future Work	81
7.1	Conclusions	82
7.2	Future Work	83
A	Risk Management User Manual	89
B	Usability Test Guide	107

List of Figures

2.1	Risk Management Process - ISO31000	11
2.2	Information Security Risk Management Process - ISO27005	14
2.3	COSO ERM Framework Structure of 2004	16
2.4	COSO Strategy in Context (2017)	18
2.5	COSO ERM Framework Structure of 2017	19
3.1	BPMN Model of ERM workflow on INCM As Is	26
3.2	ERM Process on INCM	27
3.3	Negative Impact Matrix	28
3.4	Likelihood of Derived Loss Scale	29
3.5	Risk Level Matrix	29
4.1	JIRA Concept Diagram	46
4.2	BPMN Model of ERM workflow To Be Implemented	52
4.3	Risk Management Project Issue Types	54
4.4	Risk State Machine	55
4.5	First Control State Machine	56
4.6	Options on risk level field	56
4.7	It is possible to see the progress in a detailed view of an issue	57
5.1	Final Control State Machine	61
5.2	Creating a ticket	63
5.3	Defining the issue type	63
5.4	Risk Identified visualization	64
5.5	An analyzed risk with a moderate risk level	66
5.6	An analyzed risk with a moderate risk level	66
5.7	A risk in control monitorization waiting for treatment	67
5.8	A risk already controlled	68

5.9	Control to be implemented, with a risk associated	69
5.10	Example of a control in progress	69
5.11	Example of an email of an overdue control	70
5.12	Example of an implemented control	70
5.13	Implemented controls are marked in every link they have	71
5.14	Control status pie-chart	71
5.15	Time concerning tables	72
5.16	Cross table with risk level and status	73
5.17	Risk treatment table	74
6.1	Questionnaire 2nd part results	79
6.2	Efficiency Improvement Questionnaire	80

List of Tables

2.1	Risk Definitions	9
2.2	Risk Treatment Strategies	12
3.1	User and Group Management Module	32
3.2	Permissions Module	33
3.3	Notifications Module	35
3.4	Data Management Module	38
3.5	Search and Reporting Module	41
3.6	Exporting Module	42
5.1	Risk Identification Fields	64
5.2	Risk Analysis Fields	65
5.3	Risk Identification Fields	68
6.1	SUS average values for each question	78

Acronyms

CEO	Chief Executive Officer
INCM	Imprensa Nacional Casa da Moeda
CRO	Chief Risk Officer
SUS	System Usability Scale
ISMS	Information Security Management System
API	Application Program Interface
ERM	Enterprise Risk Management

1

Introduction

Contents

1.1 Problem Description	2
1.2 Motivation and Objectives	3
1.3 Results	4
1.4 Document Structure	5

Over the last decade, corporate risk management went from a small insurance and financial sector to a whole new high-level enterprise strategy wrapping different ranges of risks across all market areas. Nowadays, every organization faces a certain level of risk associated with its business, scope, processes, and projects creating uncertainty on completing its objectives. Risk Management is defined as the "coordinated activities to direct and control an organization concerning risk" [1] focusing on creating value for the organization, securing the identification of threats, and management systems. [2] [3] Enterprise Risk Management (ERM) takes this and uses the culture, capabilities, and practices to integrate it with strategy setting and performance, minimizing the uncertainty on decision making and reaching a multi-dimensional assessment and a holistic perspective of risks in an organization. [4] Nowadays, it is considered essential to have risk-based thinking to plan, modify, or implement processes in an organization, identify risks and opportunities, and establish an effective management and security system. [1] [5]

The focus on Risk Management has been increasing as new legal requirements emerge. New standards and new formulations have been raised in the scope of Enterprise Risk Management, both due to the constant mutation of risk associated with the organizations and the further development of the risk identification, analysis, and assessment processes, influenced by the changing context and needs of each organization. Consequently, new tools have been developed with different methods, implementations, and designs, but with the same purpose: to manage risks effectively.

This dissertation focuses on the dematerialization of risk management activities present in an organization - the Imprensa Nacional Casa da Moeda (INCM).

1.1 Problem Description

Despite the several guidelines, acceptable practices, and normative references for ERM processes, there are no standards on what requirements a risk management system should have. This information gap led to a growth of multiple solutions in the market, which, despite serving the same purpose, have very distinct and inflexible functionalities, forcing the companies to adapt their processes to the tool and not the other way around. Following this idea, INCM wanted to dematerialize its ERM process so that the solution used could, contrary to what happens, be adapted to the process and characteristics of the organization. INCM is a public capital society resulting from the National Printing Office's merge with the Portuguese Mint. The organization is responsible for producing goods and services essential to the Portuguese State, such as travel and identity documents, coin minting, and security seals.

INCM has its Risk and Compliance Department and a Chief Risk Officer (CRO) to deal with the Risk Management matters. Despite the centralized risk data flow topology in this department, they have found limitations when managing information from all around the organization regarding risks. They

have currently implemented a risk information system that it considers outdated, supported by Excel spreadsheets, with scattered and inefficient information. For this reason, INCM intends to dematerialize its risk management process and find a solution that answers in a reliable, appropriate, and integrated way in its business structure. Since one of the organization's objectives is to manage the information making use of the fewest possible tools, they found one already adopted called JIRA, which could be appropriate to do the job given its flexibility, despite not having records of being used for these types of processes.

1.2 Motivation and Objectives

INCM analyzed a set of tools that could solve their challenge, choosing JIRA Software, since acquiring other risk management systems could require adapting the process, which was not desired. Also, as mentioned, it was an existing tool in the organization, thus saving resources, reducing the learning curve of its configuration, and ensuring interoperability between different processes.

Our thesis explores the existing literature, guidelines, frameworks, and good practices about enterprise risk management and develops a list of functional requirements that could be used to support ERM solutions. By using those requirements and research on multiple approaches to risk management, we can configure a platform that, through iterative deployments and modifications, would **overcome the INCM challenge** but could also cover other contexts within the ERM topic using JIRA technology. Those requirements should also **solve the lack of standards on what requisites a risk management system should have** giving us the possibility to validate them in a physical and corporate environment.

Since JIRA is an issue-tracking system conceived especially for software development and project management, the results of this research can also validate the tool's flexibility and give an example of how these complex processes that interact with all parts of an organization can be dematerialized using it.

Our objective was to reach a sufficient level of abstraction to reproduce our results by other organizations with different business sectors, processes, and workflows.

Our development began in the first months by collecting ERM process requirements from the existing regulations, requirements from the one already implemented in the INCM, and the objectives of the proposed dematerialization. We simultaneously started configuring other projects in the JIRA tool, which led us to gain some groundwork and find workarounds for situations that we anticipated that could be problematic in the future. With our list of functional requirements created, we developed our first draft of the platform. By the time we began configuring the ERM project, we already knew that the platform lacked the automation mechanisms necessary to implement an efficient and functional process. For that reason, the organization acquired a plugin called Automation for JIRA to solve this issue, giving us our

most significant milestone to reach the objectives defined. We also created a user manual to help the platform's future users.

The learning curve reached its peak at the same time as the latest features were implemented on the platform. Until the delivery of this document, constant maintenance was carried out, correcting and improving the solution based on the evaluations made and the continuous monitoring of the CRO before reaching the final version.

1.3 Results

To evaluate our platform's efficiency and functionality, we performed usability tests with the users responsible for the risks in each department. We used the System Usability Scale [6] [7] as the primary evaluation method since it is commonly used to test these platforms and reach a concise result on how the user experience is satisfactory and acceptable. In this system, if the score achieved is greater than 80,3, which is the highest limit based on the given criteria, then the users are pleased with the development made and will recommend it to their peers. Although our scores ranged from 57,5 to 100, our average score was 83,9, meaning that the implementation was successful.

A deeper analysis from interviews and questionnaires pointed us to a relation between the lower scores achieved and the user's lack of technical knowledge and experience with the JIRA tool, meaning that the platform can still be improved for generic users. The organization's culture can also impact these lower values, as the "resistance to change" is a reality, as mentioned by some interviewees.

By checking our designed functional requirements list, we concluded that our platform misses several requirements of the Exporting Module, which proves the limitations indicated in Section 4.2 about the JIRA technology, where the lack of adequate export possibilities was one of the most criticized points in the known literature. This is a limitation of the JIRA tool itself and not of the configuration performed.

Our questionnaires showed that users consider our platform to be a substantial improvement to the organization's existing process overall. Even if the JIRA tool is not mature on INCM yet, people who are not experienced can still perform risk management activities without effort.

In the end, we have shown that it was possible to adapt the JIRA software to an ERM process using our list of functional requirements. It reached the desired abstraction level to be physically applied, not only on risk management tools but also on others with some flexibility and deliver an acceptable solution without adapting the process to a pre-designed platform. These conclusions allow us to recognize that other suppliers can reproduce our requirements in their platforms and possibly achieve similar results in different organizations with distinct characteristics.

1.4 Document Structure

This document contains seven chapters. The second chapter will show enterprise risk management's state of art and fundamentals, based on standards, guidelines, and acceptable practices for the topic, describing the alignment between the document's frameworks and processes.

The third one shows a detailed analysis of the problem, explaining how the INCM's risk management process is structured and our developed requirements for an acceptable ERM application.

The fourth chapter specifies the proposed solution, describing the tool used, its advantages, limitations, and its structure. It also explains our list of functional, communicational, and non-functional requirements based on the research made, which should provide insight on what should be met and what is left to be developed.

The fifth chapter explains the implementation steps of the application, with the milestones reached. In here we will also explain its usage and how to execute risk assessment, treatment, monitoring, reporting and communication phases of the risk management process.

The sixth chapter consolidates the user test results and shows the analysis made.

The seventh is the last chapter, concluding the dissertation, discussing the work produced, and the possible future work.

2

Related Work

Contents

2.1 Fundamental Concepts	8
2.2 ISO/IEC 31000	10
2.3 ISO/IEC 27005	13
2.4 Committee of Sponsoring Organizations of the Treadway Commission	16
2.5 Discussion	21

The global financial crisis, terrorism, and even more recent, the SARS-COV-2 coronavirus breakout brought risk to a higher profile. These, along with smaller threats, have affected society, enterprises, and commerce in general that feel the need to act quickly under these events. Most of these hazard risks are so improbable that it becomes hard for individuals to face them, evaluate them and decide the right response; in fact, the recent pandemic proved that most countries and enterprises could not act appropriately to a disruptive event of this dimension. Evaluating the risk and deciding the most appropriate response is the core of risk management and should produce benefits to prevent the issues introduced and help the decision-making process on a day-to-day basis.

Given the relevance and diversity of risk management, there is a wide variety of references, standards, and guidelines on this topic. This chapter shows some of the core references for Risk Management and Enterprise Risk Management that should be sufficient to understand the meaning behind general risk, and corporate risk, the value that its management brings to organizations, and address the differences between them. Let us first focus on fundamental concepts.

2.1 Fundamental Concepts

Organizations face a wide range of risks that can impact the outcome of their operations. Although risks are mostly considered malicious or harmful, it does not mean that they will always bring adverse consequences; some risks may indeed deny or delay the objectives that the company aims to achieve (hazard risks). However, others may enhance the probability of success (opportunity risks). This depends most of the time on the criteria defined by the individual/organization. For example, according to [8], many organizations consider compliance requirements as hazard risks whereby the failure to comply can only be damaging. However, achieving compliance can be seen as an additional benefit for other organizations that aim to reach a certain level of quality and reliability, covering more demanding clients and markets. There are numerous definitions of risk in many sources. Some of them are described below on Table 2.1.

Risk management is a decision-making process with action implementations to increase the likelihood of achieving the objectives pursued, ensuring that the organization can continue functioning. In the strictest sense, risk management is organizational work, involving a change of culture, demanding job assignments, leadership, monitoring, improvement, and control of the activities undertaken. It is essentially a procedure designed to respond effectively to emerging risks, accurately identifying threats, efficiently eliminating them, and noticing emerging opportunities. [8]

Source	Definition
ISO 31000	Effect of uncertainty on objectives. Note that an effect is a deviation from the expected, usually defined in terms of risk sources, events, their consequences and likelihood. It can be positive, negative or both, and can address, create or result in opportunities and threats [1]
COSO	The possibility that events will occur and affect the achievement of strategy and business objectives. Risk relates to the potential for events, often considered in terms of severity. In some instances, the risk may relate to the anticipation of an expected event that does not occur [4]
NIST 800-37	Risk is a measure of the extent to which an entity is threatened by a potential circumstance or event, and a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence [9]

Table 2.1: Risk Definitions

Enterprise Risk Management 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"* [4], taking into account every risk interdependency, *"which allows a better assessment of the company's risk situation and further improves the decision-making process regarding strategic and operational developments."* [10]

More than being a function or a department, ERM is a collection of values, capabilities, and practices that organizations integrate with decision-making processes and strategy setting [4]. It is an element by which a company in an industry gains access, controls, exploits, and monitors risks across the enterprise to increase its long and short-term value for its stakeholders, based on its risk appetite (high-level view of evaluating the level of risk management the entity is ready to accept as reasonable). [11] It can and should be conducted independently of the organization size, in a broad way throughout its business sectors, requiring more than making a collection of the present risks and being more than a simple checklist, carrying out a monitoring system, learning, and continuous improvement. [4]

Over the years, other researchers have shown different models related to finance, accounting, insurance, and project management organizations. [12] [13] [14] Others have chosen to use existing models and frameworks and describe methodologies to cover gaps that are not intuitive when physically implementing them in a company, like culture change or expectations vs. reality. [15] [16] However, one of the most used and trusted models is the COSO's ERM integrated framework [4] that provides a risk management infrastructure with well-described components, principles, and process stages, available for every organization's characteristics.

2.2 ISO/IEC 31000

ISO/IEC 31000 is an important international standard for Risk Management created by the International Organization for Standardization, that provides comprehensive guidelines and good practices to help organizations manage their risk-related processes and properly assess inherent risks. According to [1], risk is defined by the effect of uncertainty on objectives and starts with the possibility of an event occurring. This event is an occurrence or a change of a particular set of circumstances that may or may not be expected to happen, which causes the effect mentioned called risk. As said before, if this effect leads to a negative impact, then it is considered a threat. If it leads to a positive one, it's seen as an opportunity to reach a particular objective.

Risks are expressed in terms of these potential **events**, their **consequences**, **risk source/cause**, and their **likelihood**. Consequences correspond to an outcome of an event that can be expressed qualitatively and quantitatively concerning the impact on the objective affected. Likelihood measures the chance of the risk happening, whether qualitatively, quantitatively, objectively, or subjectively.

Following this idea, Risk Management should focus on the creation and protection of business value, improving its efficiency, encouraging innovation, and supporting the achievement of objectives. [1]

The Standard provides a few fundamental principles to improve the effectiveness and efficiency of risk management processes and framework:

- A **Integrated** - Risk Management should be an integral part of all organizational activities
- B **Structured and comprehensive** - Structured and comprehensive approach to risk management delivers consistent and comparable results
- C **Customized** - Framework and process are customized and proportionate to the organization's context.
- D **Inclusive** - To reach a level of improved awareness in the organization, the processes should be inclusive and stakeholders should be involved
- E **Dynamic** - Should anticipate, detect and acknowledge events and changes in an appropriate and timely manner
- F **Best Available Information** - It should take into consideration historical information, expectations and limitations to timely and clearly inform stakeholders
- G **Human and cultural factors** - Human and cultural factor should be taken into consideration on all levels of Risk Management
- H **Continual improvement** - Meant to continually improving through learning and experiences

Risk management is often referenced in a significant part of the management and continuous improvement processes, like information security(ISO/IEC 27001), security printing procedures(ISO/IEC14298), or quality management systems(ISO/IEC 9001), by offering fundamental activities for its operations' completeness, minimizing adverse effects and making the most of opportunities that arise.

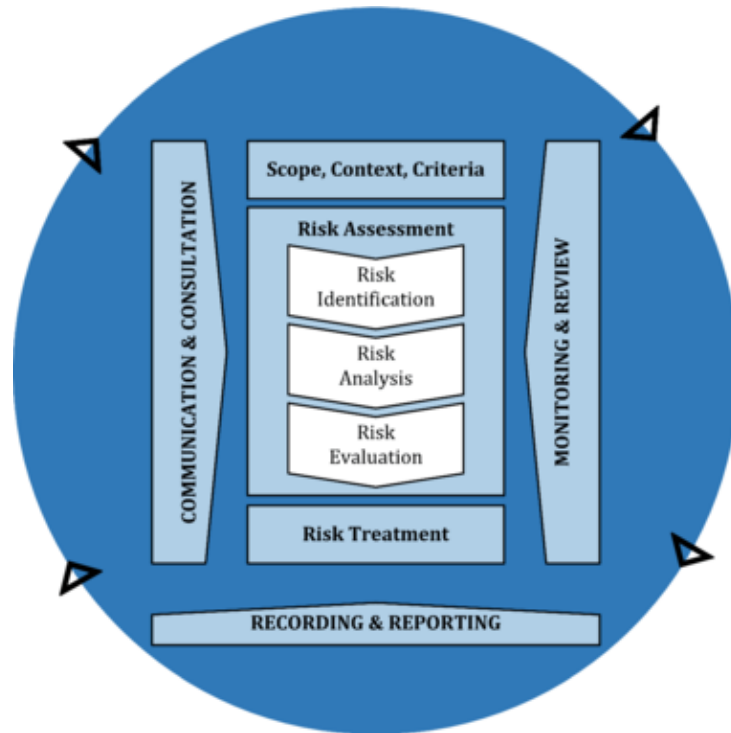


Figure 2.1: Risk Management Process - ISO31000

This process described in the Standard is shown from a holistic perspective in Figure 2.1, involving the systematic application of policies, procedures, and practices in communication and consultation activities, establishing the context, monitoring, reviewing, recording, and reporting risk. This iterative approach increases the assessment depth and detail in each iteration. It creates a balance between temporal efficiency and effort spent identifying controls while ensuring the appropriate assessment of the most relevant risks.

It is also relevant to remember that ISO 31000:2018 standard is not just a risk management process by nature. It intends to capture three main components: Principles, framework, and methodology. It can approach multiple risk management techniques, scopes, and strategies; thus, organizations can choose the best design that suits their circumstances to treat their risk-related practices.

The process starts when the **context, scope and criteria are established**. The company should have a framework describing its structure, mentioning the human resources needed, the responsible parties and the communication plan among them. It is also here where risk categorization should be defined along with the metrics about likelihood, impact and risk level.

Then the risk is **assessed**. This activity is structured in 3 stages: Risk Identification; Risk Analysis and finally Risk Evaluation.

Risk Identification determines the “why”, “how” and “when” a potential event may occur, as well as the person or department responsible for it. It includes the identification of risks that may affect one or more assets¹, returning a list with the type and source of the threat and the existing controls, with their state of implementation and use.

Risk Analysis is performed on the list of identified risks to understand its nature, characteristics, and risk level. Analysis techniques can be: Qualitative by using a scale of qualitative attributes to describe the magnitude of potential consequences and their likelihood, offering a better perception, but greater subjectivity on the scale; or Quantitative by using a numerical scale for both consequences and likelihood, depending on the precision of the values. Both can also be used, depending on the purpose, reliability, and availability of information and resources. How consequences and likelihood are defined and how they are combined to provide an impact may vary depending on the type of risk and the purpose for which the risk assessment output will be used.

In **Risk Evaluation**, the previous results are compared with the established criteria to determine which risks need to be addressed, their priority, and what corrective actions should be taken.

If this assessment provides enough information to determine the necessary actions to modify the risk to an acceptable level, it will move on to the **Risk Treatment** phase. The risk treatment uses the data resulting from the assessment phase in strategy procedures and decision-making about eventual residual risks, cyclically evaluating the treatment process’s effectiveness.

In Table 2.2 we describe each of the risk treatment strategies.

Decision	Action
Risk Mitigation	The level of risk must be changed by introducing, removing, or changing controls to reduce the impact or likelihood, and the residual risk can be reassessed as being acceptable
Risk Avoidance	Avoid the activity or condition that gives rise to the risk
Risk Sharing	The risk is shared with other entity(ies) when its consequences impact more than one department.
Risk Acceptance	Accepting a risk means that the risk level is within the risk acceptance criteria, meaning no extra actions should be performed
Risk Pursue	When the risk is regarded as an opportunity to achieve objectives, actions should be performed to increase the exposure to the risk

Table 2.2: Risk Treatment Strategies

¹An asset is considered anything that is of value to the organization and needs to be secured.

After risk treatment and the remediation actions have been performed, the threat or vulnerability that remains is called residual risk. Suppose the level of residual risk is still not acceptable after a risk treatment. In that case, another iteration to the risk assessment may be necessary, once again reviewing the context and the inherent criteria, with the subsequent treatment of risk. Otherwise, the risk is accepted, **recorded and reported** across the organization.

All results **should get documented in detail and communicated** between the operational and top management during the entire RM process, constantly providing relevant information that could be valuable for decision-making and stakeholders' awareness.

2.3 ISO/IEC 27005

INCM is an organization whose core business consists of producing security goods and services. Among the many existing sectors, information security is one of the organization's main objectives, to which its management system is regularly monitored and audited following ISO27001. Due to the relevance of this standard, it makes sense to use the branch that introduces risk management to this system to show a more objective implementation than ISO31000. This relationship is transcribed in a new standard, the ISO/IEC 27005.

ISO/IEC 27005 is an international standard in information security that bridges the risk management perspective shown in ISO/IEC 31000 to the information security management systems present in ISO/IEC 27001. It provides a strict perspective on the process presented above, using it as a reference and shaping it to the domain of information security. Its purpose can be to support an Information Security Management System (ISMS), legal compliance and evidence of due diligence, prepare a business continuity plan or an incident response plan, and describe the information security requirements for a product or service. [17]

In general, the definition and concepts of risk management mentioned in the previous section of this chapter do not change. However, contrary to what ISO/IEC 31000 describes, risks are not seen as opportunities but threats to the confidentiality, integrity, and availability of information in information security. As shown in Figure 2.2, its process is identical to the ISO/IEC 31000, showing the iterative approach mentioned earlier based on risk decision points where the process can roll back to a particular activity if the criteria do not meet satisfactory needs.

Contrary to ISO 31000, which describes Risk Assessment in a high-level perspective, ISO 27005 pays particular attention to it in the scope of information security. Risk assessment is probably the most distinct phase between the two standards since identifying assets and the consequent assessment is explicitly directed towards confidentiality, integrity, and availability of information.

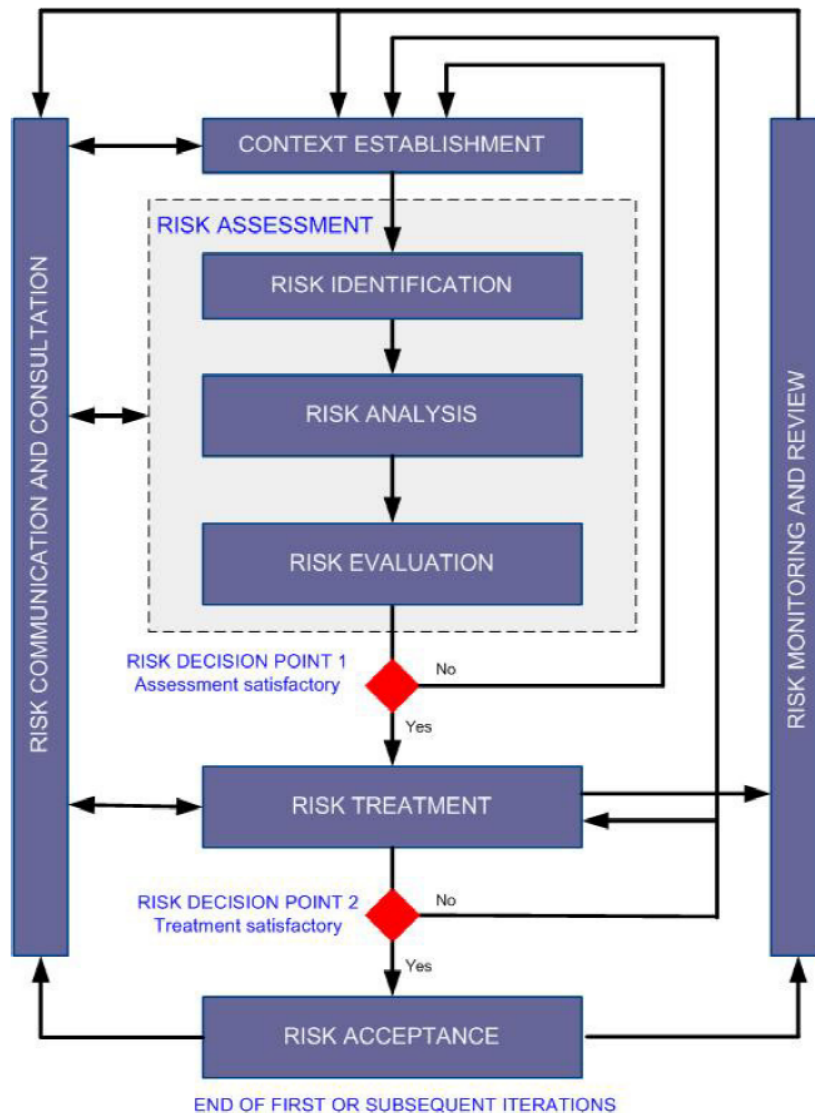


Figure 2.2: Information Security Risk Management Process - ISO27005

There is often an inability to implement all controls simultaneously, demonstrating the need to address only the most critical risks. For this reason, a high-level assessment is carried out first, to identify potentially high risks grouped by general risk domains addressing a global view of the organization and its information systems instead of starting with a systematic analysis of threats, vulnerabilities, assets, and consequences. This way, resources and money can be applied where they are most needed, and systems likely to be in the greatest need of protection will be addressed first. The next iteration can involve further in-depth consideration of potentially high risks revealed in the initial iteration, prioritizing them.

The first phase is Risk Identification, and it aggregates four parts:

- **Assets Identification** consists of identifying a list of assets (more than hardware and software) that have value to the organization, requiring protection. This identification should provide an asset owner that takes responsibility and accountability for it and a suitable level of detail, which can be rearranged in further iterations of risk assessment if needed.
- The second step involves the **Identification of Threats**. Here, the information obtained about threats from incident reviewing, asset owners, and other sources from within the organization will be used to identify threats, which assets they affect, the source that leads the event to happen, and the consequence of that specific event. Internal experience from incidents, threat catalogs, and past threat assessments should be considered in the current assessment. In the end, this step should offer a list of threats with the identification of threat type and source.
- Next, the standard mentions the **Identification of Existing Controls**. This step should use the documentation of controls and risk treatment implementation plans and use it to develop a list of existing controls and their efficiency while avoiding duplicates and evaluating if one is inefficient or justified to be removed, replaced, or reevaluated. In the end, it should provide a list of all existing and planned controls, their implementation, and usage status.
- The list of known threats, assets, business processes, and existing controls will be used to **Identify Vulnerabilities** and **Consequences** that losses of confidentiality, integrity, and availability may have on the assets, providing a list of incident scenarios with the consequences of those respective assets and business processes affected.

After the Risk Identification is performed, there is a need for a Risk Analysis to provide in-depth information about the risk, explicitly using the pre-determined criteria developed at the beginning of the process and the data gathered from the identification phase to define the risk likelihood and impact, both qualitatively or quantitatively. By combining the likelihood of an incident scenario and its consequences, the risk level is calculated for each risk, facilitating its prioritization.

In the Risk Evaluation Step, the list of risks with the value levels assigned will be compared against risk evaluation criteria and risk acceptance criteria. The nature of the decisions about risk evaluation and risk evaluation criteria used to make those decisions would have been decided when establishing the context. The Risk evaluation criteria should be consistent with the defined external and internal ISRM context and consider the organization's objectives, stakeholder views, and other sources. Risk evaluation uses the understanding of risk obtained by risk analysis to make decisions about whether an activity should be engaged and priorities for the risk treatment, providing a list of risks prioritized according to risk evaluation criteria concerning the incident scenarios that lead to those risks.

2.4 Committee of Sponsoring Organizations of the Treadway Commission

Committee of Sponsoring Organizations of the Treadway Commission (COSO) is an entity that aims to provide comprehensive frameworks that help companies on improving their organizational performance in terms of enterprise risk management, fraud deterrence, and strategy setting.

COSO published two versions of their ERM framework. The first one was an overview of how entities could protect and enhance their stakeholders' value by adopting the right strategy and objective definition to achieve maximum growth.

Since then, the framework has suffered some changes. The latest document provided a greater insight into how ERM should correlate directly with the organization's efficiency and clarify the connections between corporate strategy, risks, and performance. The document also strengthened the anticipation of risk, mentioning the bond between change and opportunities that arise, setting it as an essential variable that should be considered in decision-making.

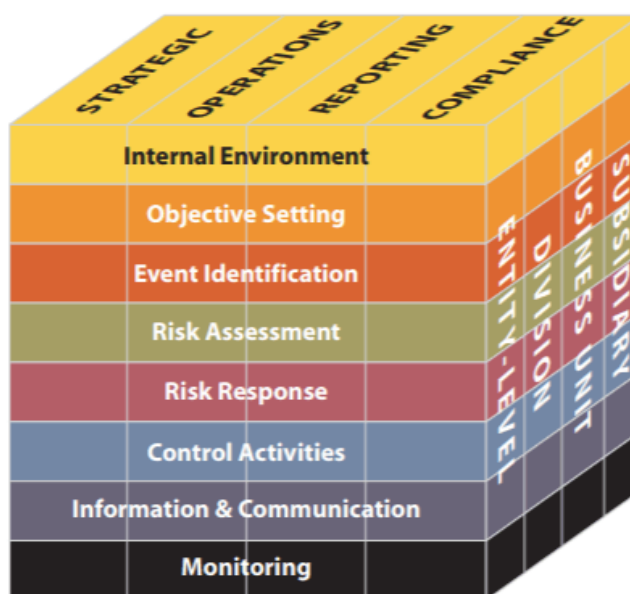


Figure 2.3: COSO ERM Framework Structure of 2004 [18]

The framework indicates that in order for management to maximize firm value, it must develop objectives and strategies that increase the firm's probability of meeting growth benchmarks and achieving satisfactory market returns within an acceptable level of risk efficient deployment of resources. [18] This document reveals a risk management infrastructure in terms of 3 main elements: objective categories, organization level, process components. Eight components are placed under each of the four objective

categories that should be developed across all organization levels. The cube mentioned in Figure 2.3 represents this structure with different layers of depth to ease its understanding.

According to this framework, ERM components are:

- **Internal environment** - establishes the basic ideology regarding risk management, including risk culture, the entity's competence, ethical values, responsibilities, and accountability.
- **Objective setting** - sets the risk strategy based on the entity's risk appetite, risk tolerance, and mission.
- **Event identification** - is the identification process of both risks and opportunities that affect an entity's objectives from the internal and external environment.
- **Risk assessment** - permits an entity to consider the impact and likelihood of events and analyze risk using quantitative and qualitative approaches, measuring the related objectives.
- **Risk response** - management should select a proper response that aligns with the entity's risk tolerance and risk appetite.
- **Control activities** - includes the policies and procedures that will help to ensure that risk responses are performed effectively at all levels of the organization;
- **Information and communication** - communicate pertinent information regarding ERM and other activities flowing down, across, and up the organization.
- **Monitoring** - monitoring of ERM process and activities through separate evaluations, ongoing monitoring activities, or both and modifications made as necessary.

The framework suggested that a company's enterprise risk management structure should be divided into four objectives that should be followed by every component: **strategy** - when referring to high-level objectives that are in line with the mission of the organization; **operations** - referring to short-level objectives that are related to the efficient and effective resources use; **reporting** - pointing to the quality of a company's reporting system and data; and finally **compliance** - by acting according to internal and external regulations and laws.

Finally, the structure considered four organization levels where the components must be embedded: **Enterprise-level, Division, Business unit** and **Subsidiary**.

Along the years, some critics were made concerning the 2004 COSO framework: Demidenko & McNutt [19] state that should be considered a scale of ethical maturity based on the duty and responsibility of the practical implementation, to ensure better governance, contributing with theoretical principles to the debate on good governance and ethics of ERM.

Williamson [20] says that the COSO framework on business risk management is a valuable contribution to the ERM emerging practice but has severe limitations as it does not provide a viable standard for identifying the proposed processes' effectiveness. Its definition of risk diverts attention from opportunities and uncertainties outside its perspective of closed rational systems. By adopting an approach of order and control, the framework ignores the management of uncertainties shared with external parties and ERM's social implications. As a result, threats will be created if widely followed this structure, which seems likely, since the ERM is institutionalized within the regulations, the professional practice, and known management standards.

This criticism seems to have been considered since, as previously mentioned, in June of 2017, COSO published a new ERM framework titled Enterprise Risk Management-Integrating with Strategy and Performance. This document shows a more detailed and complex approach by integrating it with strategy-setting and business performance, offering a more profound insight into recognizing the role of governance and culture.

Since the document is so recent, there is not much information in the literature that carries out the new framework's implementation. Besides that, organizations do not usually publish their ERM implementations, making it tough to find successful use cases to present here. Let us begin with the main differences in the latest framework.

Risk is often focused on discovering its potential impact on an already pre-defined strategy. However, this framework considers two additional aspects of ERM that should modify the company's value: The possibility of the strategy not aligning with the organization's mission, vision, or core values; and consequences that a specific strategy can have on an organization when chosen. [4]



Figure 2.4: COSO Strategy in Context (2017) [4]

The possibility of having a strategy that does not align with the organization's values is a significant occurrence that should impact the strategy selection. A chosen strategy must support the organization's mission and vision. By having a misaligned strategy, the organization may not realize these elements, and it could compromise its core values, even if a strategy is implemented successfully.

By **considering the implications or consequences from the strategy chosen**, the management and the board of directors have the opportunity to decide which strategy works in accordance with their risk appetite and profile, deciding the trade-offs needed, aiming for an efficient way to set objectives and allocate resources. For this reason, COSO built a strategy (Figure 2.4) in the context of the mission, vision, and core values mentioned, that should guide an organization towards the right direction and higher performance.

The document defines ERM's new framework shown in Figure 2.5, quite different from the first published. The figure illustrates an ERM system fully integrated with strategy setting, decision-making scenarios, and performance on objectives pursuit, thus, enhancing value. The framework is defined as a set of principles organized into five interconnected components: governance and culture; strategy and objective-setting; performance; review and revision; information, communication, and reporting.



Figure 2.5: COSO ERM Framework Structure of 2017 [4]

- **Governance and Culture:** Governance and culture form a basis for all other enterprise risk management components. Governance sets the company's tone, reinforcing enterprise risk management's importance, and establishing oversight responsibilities. Culture is reflected in decision-making. This component has five main principles:
 - Exercises Board Risk Oversight
 - Establishes Operating Structures
 - Defines Desired Culture
 - Demonstrates Commitment to Core Values
 - Attracts, Develops, and Retains Capable Individuals
- **Strategy and Objective-Setting:** ERM, strategy, and objective-setting work together in the strategic planning process. Here is the stage where risk appetite is established and aligned with strategy and where business objectives use the defined strategy as a basis for assessment and treatment of the risk. This stage should follow four steps:

- Analyzes Business Context
 - Defines Risk Appetite
 - Evaluates Alternative Strategies
 - Formulates Business Objectives
- **Performance:** At this stage, the company assesses risks that may impact strategy and business objectives. Based on the metrics determined on risk acceptance, the organization selects risk responses and treatments and takes a portfolio view of the inventoried risks. Finally, the relevant data that results from this process is reported to the responsible parties. Summing up, it:
 - Identifies Risk
 - Assesses Severity of Risk
 - Prioritizes Risks
 - Implements Risk Responses
 - Develops Portfolio View
- **Review and Revision:** The company performs regular reviews on ERM components to estimate its performance, acting accordingly, and carrying out the changes needed to fulfill its requirements. It should:
 - Assess Substantial Change
 - Review Risk and Performance
 - Pursue Improvement in Enterprise Risk Management
- **Information, Communication, and Reporting:** This section acts in the same way as the previous framework's "Information and communication" component by:
 - Leveraging Information Systems
 - Communicating Risk Information
 - Reporting on Risk, Culture, and Performance

Finally, similar to the 2004 ERM structure, this document also describes the Roles and Responsibilities for Enterprise Risk Management, but with a model of accountability lines. This model provides guidance on the roles and responsibilities of the board of directors - responsible for providing risk oversight of enterprise risk management culture, capabilities, and practices; Chief Executive Officer (CEO) - accountable to the board of directors and also responsible for overall enterprise risk management culture, capabilities, and practices required to achieve the company's strategy and business objectives;

CRO - responsible for defining the company's ERM framework as well as for all the activities related to it, in terms of context definition, risk assessment, risk treatment, reporting and communication of risk information to responsible parties, and support and maintenance needed to its related activities; Risk Owners - responsible for using the priority assigned to apply an appropriate risk response in the context of business objectives and performance targets; and Internal Auditor - responsible for evaluating the ERM process execution and activities and to create priorities on the audit plan depending on the assessed risks. [4]

2.5 Discussion

This chapter analyzed three relevant guidelines and acceptable practices, both on risk management and enterprise risk management. Although different, these frameworks gave us insight into how risk management should be implemented in an organization. It is possible to understand that ISO/IEC 31000 offers a framework built generically, not limiting it to a specific ambit. Instead, it can be accommodated in multiple contexts and business scopes, offering a process that, when implemented, should be at the company's discretion to make the necessary adjustments on the elements that compose it according to its needs, risk appetite, and objectives. ISO/IEC 27005 shows risk management applied to the information security ambit, providing an example of how it can be implemented directly in a specific context, not changing the process of ISO/IEC 31000 itself but the type of risks and assets that should be emphasized. On the other hand, COSO tells us how ERM is all about the culture, capabilities, and practices, integrated with strategy setting and performance, creating, preserving, and realizing value, and suggests a framework capable of covering all risk scopes of an organization. Despite not offering a specific process to follow and implement, it shows the basic ERM structure that must exist to deploy one likely to succeed, focusing primarily on the values that make an organization resilient regarding risk and how the many stakeholders could benefit from it.

3

Problem Analysis

Contents

3.1 Enterprise Risk Management Process Structure at INCM	24
3.2 Requirement Analysis	29
3.3 Conclusions	42

Adopting ERM in an organization can increase its resilience to uncertainties, centralize information management, respond effectively and promptly to threats, and facilitate the pursuit of opportunities. It will also help develop the organizational culture by allowing the correct understanding of the stakeholders regarding the risk and adoption of controls as part of their daily practices. [3]

In the previous chapter, we described a set of practices, implementation measures, and guidelines for Risk Management processes and how they specialized in a corporate context. Those pointed us to a weighted, iterative, and well-structured system to derive maximum value from risk assessment and use it on an organization's strategic decisions. These practices serve as a basis for most other organizations' activities and processes, mainly for information security, quality management, and continuous improvement, which find an added value in integrating their business models with risk management. [1] [17] [5]

Despite the extensive literature on how these processes can be structured, only the conceptual model is shown and justified, leaving the responsibility of each organization to choose the most appropriate solution given its organizational context and needs, which can be challenging. INCM, by wanting to dematerialize its risk management process and implement a new management system, faced precisely this problem.

We had two challenges at hand, the first one more generic, that if solved, could be reproduced in future ERM solutions, and the other in the context of a particular organization. This chapter makes a detailed analysis of the existing process at INCM, its limitations, and a collection of requirements for ERM solutions evaluating the possibility of solving both problems.

3.1 Enterprise Risk Management Process Structure at INCM

INCM has an enterprise risk management framework with a description of the process, showing its structure, methods, and metrics. This framework is aligned with ISO/IEC 31000:2018, ISO/IEC 27005:2018, and COSO ERM 2017, mentioned earlier. As it is integrated with a large part of the company's organizational processes and contexts, the framework used many other normative references such as ISO 9001(for quality management systems), ISO 14001(for environmental management systems), ISO 27001(for information security management systems), ISO 14298(for security printing process management) and more recently GDPR(Protection of sensitive data) to achieve compliance with these different international standards.

Although the framework is well-structured, its implementation on the organization had several flaws. The risk-related data was managed on spreadsheets, lacking efficiency, reporting methods, and dispersed information among several departments. It was a challenge to reach every organic unit adequately, leading to the loss of value from the process that affects its entire management system. In this way, INCM faces the challenge of dematerializing it and finding a solution that responds adequately to

these flaws and shortcomings, integrates it into its business structure, and adapts to its specificity.

INCM's ERM mention the following objectives:

- **Promote the creation of risk management value** by ensuring that decision-making strategies consider relevant risk information and risk management principles align with INCM's mission and strategy.
- **Promote a risk management culture** where preventive measures are privileged to ensure the achievement of objectives.
- **Ensuring stakeholder awareness** by identifying roles and responsibilities in the Corporate Risk Management Structure and respective training and awareness.
- **Promote the sharing and reuse of risk information** in different INCM contexts through the definition of references transversal to the organization.
- **Ensure compliance of the risk management process** with internal and external requirements (normative, legal, etc.).

The framework also clearly establishes responsibilities within the process.

The **Board of Directors** is accountable for choosing the strategy and the resources necessary for enterprise risk management and approving the risk criteria. The second element is the **ERM Committee** composed of responsible parties of the Organic Units and the other existing committees. These offer support to the board of directors and should have some responsibility on all the business strategies related to the risk management framework and sector. [21] The **Chief Risk Officer** is the person with the most experience and specialized knowledge in risk management and is responsible for supporting and monitoring the process and the framework. **Internal Audit** represents another element responsible for evaluating the process and prioritizing the audit plan based on the identified risks. **Risk Owner**, **Process Owner**, and **E2E Process Owner** are respectively the responsible people for the risk, the process where the risk occurs, and the chain value that covers that specific process. The **Department's Promoters** are a specific group in INCM responsible for managing most communications between their department and others within the organization, including risk-related information. All these groups should be taken into consideration when creating a risk.

Let us start by describing the workflow of the previous process shown in 3.1. When an event occurs that leads to a risk, a person from the department identifies it by filling a form and sending it to the CRO via email. If the person is not the risk owner and did not perform the analysis, the CRO will forward the data to the department responsible for making the respective analysis. Then, the CRO would evaluate if the information provided is enough and validate the methodology presented.

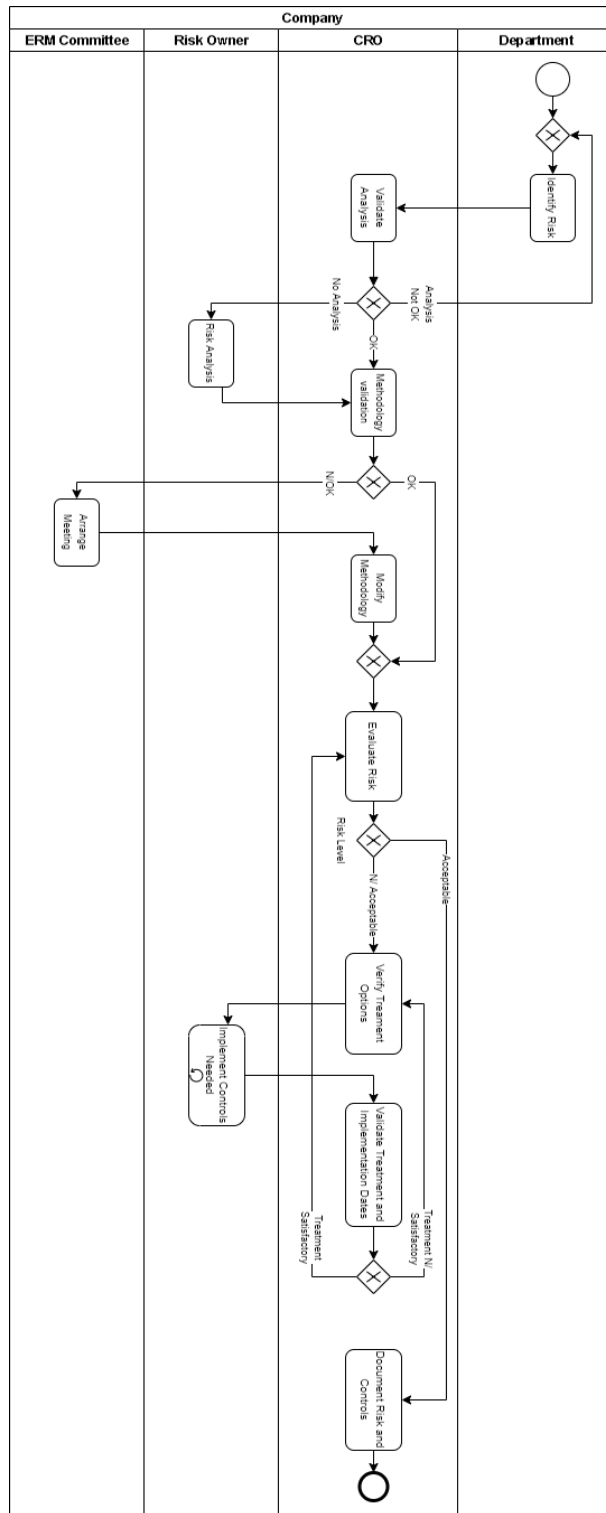


Figure 3.1: BPMN Model of ERM workflow on INCM As Is

Next, he proceeds to evaluate the risk. If the risk level is not acceptable, the risk passes through a treatment phase where the necessary controls are implemented to lower its likelihood, impact, or both.

After the CRO validates the controls implemented, he reevaluates the risk until it reaches the acceptance criteria to be documented along with its controls.

In the end, the data from the entire risk assessment process is present in a spreadsheet that could be consulted by the responsible parties if needed. Meetings were also periodically held with the areas to ensure that controls were implemented and the risk data was up to date.

The dematerialization approach must ensure that the relevant information, like risk creation, risk level update, or controls implemented, gets to its specific owners and responsible elements in the organization. Since the INCM's organic structure is recurrently changing, it is relevant to allow the possibility to easily configure these elements in the application, thus avoiding time waste and constraints.

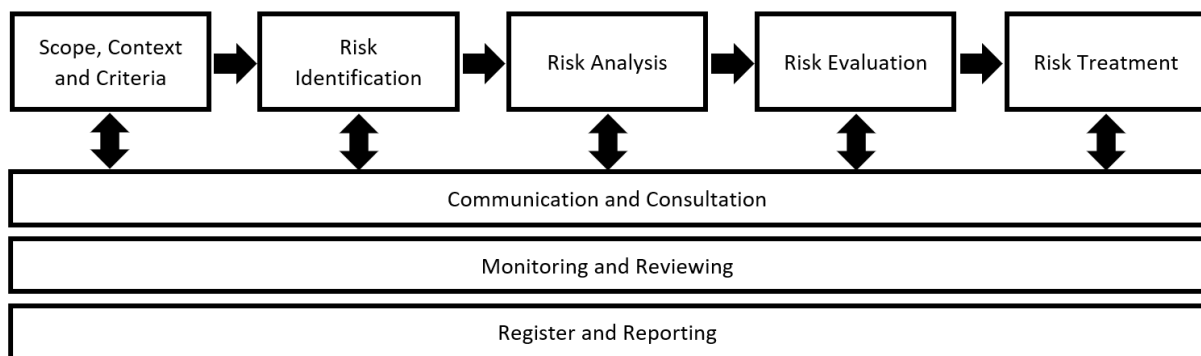


Figure 3.2: ERM Process on INCM [21]

As we can see, the ERM process at INCM aligns itself with activities and procedures mentioned in the process of ISO/IEC 31000 shown in Figure 3.2

The description of each of these phases is present in Chapter 2. It is relevant to describe the particularities in the Risk Assessment stage, where the organization's context and criteria should be applied, and define where the different elements should be shown. On Risk Identification, the elements that define the risk should be identified, specifically the **event, consequence, cause, existent controls**, and the **risk owner**. Anyone in the company can perform this identification, but it is mostly made by project managers, risk owners, process owners, and E2E process owners, as described at the beginning of the section.

On Risk Analysis, we can measure the risks previously identified using metrics such as **likelihood, impact**, and **risk level**. Each of these elements has a designated scale in the document that should delimitate all levels of severity. The metrics must have comparable scales to allow the comparison of risk information. However, recognizing different management contexts, it is expected that the metrics have different dimensions depending on the context. For that reason, each risk should be identified by the different types of impact: strategic, operational, financial, reputation, information security, regulatory, security and infrastructures, and environmental. These impacts are characterized by their negative im-

impact and the qualitative description, as shown in Figure 3.3. In the end, a maximum impact is estimated based on the previous ones, representing a quantifiable value of the real impact of a given event. The risk owners should perform this analysis as they are the only ones to know the likelihood, impact, and severity of a risk.

	Negative Impact Matrix				
	1	2	3	4	5
	Insignificant	Low	Moderate	High	Severe
Strategic	<ul style="list-style-type: none"> • Delay or deflection in the plan of actions • Without any impact in the established goals 	<ul style="list-style-type: none"> • Prevents from achieving one or more established intercalary goals • Without any impact in indicators achievement 	<ul style="list-style-type: none"> • Prevents from achieving one or more established goals • Without any impact in objective achievement 	<ul style="list-style-type: none"> • Prevents from achieving one or more established objectives 	<ul style="list-style-type: none"> • Prevents from achieving one or more organization's strategic objectives
Operational	<ul style="list-style-type: none"> • Insignificant impact in the business processes • Impact can be mitigated with routine operations 	<ul style="list-style-type: none"> • Low impact in business processes • Can originate recoverable delays • Impact can be mitigated at operational level 	<ul style="list-style-type: none"> • Moderate impact in the business processes • Business performance affected, preventing form achieving established strategic goals 	<ul style="list-style-type: none"> • High impact in the business processes • Business performance affected with high negative consequences (service delays, financial losses, customer insatisfaction, regulatory faults, etc.) 	<ul style="list-style-type: none"> • Severe impact in the business processes • Unavailability of services and/or people critical for the business
Financial	<ul style="list-style-type: none"> • Insignificant financial impact • <1% impact in the project/budget cost 	<ul style="list-style-type: none"> • Low financial impact • 2-5% impact in the project/budget cost 	<ul style="list-style-type: none"> • Moderate financial impact • 5-10% impact in the project/budget cost 	<ul style="list-style-type: none"> • High financial impact • >10% impact in the project/budget 	<ul style="list-style-type: none"> • Severe financial impact • >30% impact in the project/budget cost
Reputational	<ul style="list-style-type: none"> • Incident with limited negative publicity. Quickly forgotten. • Without damage in the reputation/brand 	<ul style="list-style-type: none"> • Incident with negative publicity at local/regional level • Low limited damage (short-term) in the reputation/brand 	<ul style="list-style-type: none"> • Incident with negative publicity at local/regional level • Pressure to INCM mitigate the impact • Moderate damage in the reputation/brand 	<ul style="list-style-type: none"> • Incident with negative publicity at nacional level • Intense pressure to INCM mitigate the impact • High damage in the reputation/brand 	<ul style="list-style-type: none"> • Incident with negative publicity at internacional level • Impact mitigation require strategic changes • Severe damage in the reputation/brand
Information Security	<ul style="list-style-type: none"> • Public information compromised in its integrity or availability 	<ul style="list-style-type: none"> • Information sensible for internal interests compromised in its confidentiality, integrity or availability. 	<ul style="list-style-type: none"> • Information sensible for organization's operation compromised in its confidentiality, integrity or availability. 	<ul style="list-style-type: none"> • Information sensible for organization's interests compromised in its confidentiality, integrity or availability. 	<ul style="list-style-type: none"> • Critical information for the organization operation compromised in its confidentiality, integrity or availability.
Regulatory	<ul style="list-style-type: none"> • Danger of incurring in legal or contractual fault 	<ul style="list-style-type: none"> • Isolated act in legal fault • Contractual fault detected by one of the parts 	<ul style="list-style-type: none"> • Activity or routine in legal fault • Contractual fault with contractual break or penalties threat 	<ul style="list-style-type: none"> • Legal fault resulting from authorities investigation • Contractual fault with penalties 	<ul style="list-style-type: none"> • Legal fault leading to severe penalties • Contractual fault with contract break
Security and Infrastructures	<ul style="list-style-type: none"> • Insignificant damage • Insignificant material losses 	<ul style="list-style-type: none"> • Damages that require first aid • Low material losses recoverable in short-term (< 24hours) 	<ul style="list-style-type: none"> • Damages or injuries that require doctor intervention (deep cuts, fractures, burns, etc.) • Moderate material losses with long-term recovery (>24 hours) 	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • Severe injuries (limbs loss, hearing, vision, etc.) or death • Irrecoverable severe material losses. Require equipment replacement.
Environmental	<ul style="list-style-type: none"> • Insignificant environmental impact 	<ul style="list-style-type: none"> • Reparable low environmental impact 	<ul style="list-style-type: none"> • Moderate environmental impact requiring mitigation actions 	<ul style="list-style-type: none"> • High environmental impact with parcial irrecoverable damages 	<ul style="list-style-type: none"> • Severe environmental impact with irreversible damages

Figure 3.3: Negative Impact Matrix [21]

The likelihood is directly related to the "prevention control effectiveness" since a well-implemented control can reduce a risk reappearance chance. For that reason, a matrix was created to help calculate the likelihood of derived loss, as seen in Figure 3.4.

		Likelihood of Derived Loss				
		Event Likelihood				
		Rare	Not Likely	Likely	Very Likely	Expected
Effectiveness of Prevention Control	Very Low	Very Low	Low	Moderate	High	Very High
	Low	Very Low	Very Low	Low	Moderate	High
	Moderate	Very Low	Very Low	Very Low	Low	Moderate
	High	Very Low	Very Low	Very Low	Very Low	Low
	Very High	Very Low	Very Low	Very Low	Very Low	Very Low

Figure 3.4: Likelihood of Derived Loss Scale [21]

Finally, with the estimated likelihood and maximum impact values, we can calculate the risk level, which is also represented in a specific matrix.

		Risk Level				
		Likelihood of Derived Loss				
		Rare	Not Likely	Likely	Very Likely	Expected
Maximum Impact	Very High	Very Low	Low	Moderate	High	Very High
	High	Very Low	Very Low	Low	Moderate	High
	Moderate	Very Low	Very Low	Very Low	Low	Moderate
	Low	Very Low	Very Low	Very Low	Very Low	Low
	Very Low	Very Low	Very Low	Very Low	Very Low	Very Low

Figure 3.5: Risk Level Matrix [21]

3.2 Requirement Analysis

More than a paper-to-digital migration of documents inherent to the activity of an organization, dematerialization involves the reformulation of a process as a whole. This reformulation implies that the internal

services associated with these activities are also checked, changed accordingly and if needed. So it is necessary to ensure that there is no loss of information, that it remains secure and available constantly.

However, the benefits of dematerialization must be clear. If the methodology for carrying out a given activity requires the same amount of effort for all the actors, either the dematerialization has not been done well, or there is no need for one. It may happen because there is a tendency to follow the same methodology to which the participants are already accustomed. In general, going fully digital would increase productivity by using automatic processes. Furthermore, because there are already authentication methods that allow it, digital documents are already auditable and legally recognized (taking into account compliance methods concerning the integrity of the documents, preventing them from being tainted).

Before developing a solution, we intended to analyze the problem and search for a holistic set of requirements for ERM processes that could be used to produce new tools in this domain. It opened a door for us to design something new and unique that can be used not only for this project but for other solutions that need to respond to the limits imposed by ERM guidelines [1] [4] while integrating it in any business sector regardless of its maturity. This can be seen as an added value for suppliers, who seek to cover more sectors in the market and for customers looking for dynamic and flexible solutions tailored to their needs.

We planned to configure JIRA to support an ERM process in light of the needs, specificities, limits, and rules of INCM using these functional requirements and following the guidelines, standards models, and structures present in the literature. Our intention was an easy-to-use solution with an appealing interface that facilitated communication and access to information derived from the process's activities to obtain the maximum value from the identified risks and related controls.

Even though the approaches for ERM software solutions are of different types, this document attempts to make them uniform so that their data is well represented, manageable, and its access is controlled. To achieve this uniformization, we bundled the functional requirements into six modules that, put together, should describe the full functionality of an ERM process.

3.2.1 User and Group Management Module

To achieve successful management of a corporate platform, good management of users and groups is crucial. All business systems share this exact need. Consequently, many system tools are available that manage it and integrate it with the organization's user database. This dissertation does not mandate the protocols that ERM solutions should use for user authentication and user and group management. The user and group module should provide a set of requirements that act as a wrapper, allowing either an external corporate directory system or a custom directory service to access it and manage it.

Name	Summary	Description
R1.1	The platform must only be accessed by active authenticated users with at least the following attributes: - Unique ID - User's Name - Email - Groups Associated	Authentication is the process of establishing the user's identity so that the platform can provide an appropriate level of access to perform actions and associate them with users and entities created or changed. This authentication can be performed by giving personal credentials such as login and password and can be associated, for example, with systems like Active Directory using LDAP.
R1.2	The platform must offer an option for creating new user entities with the properties listed under requirement R1.1 .	The first users to be created must be users with higher privileges, commonly called admins. These can be assigned by the supplier that is deploying the platform. Next, these admins should create the subsequent new users and attribute their roles. Admins should be able to give privileged access to other users
R1.3	The platform must offer an option for updating user's data like email or name.	This document does not define how this mechanism should be implemented. However, there must be a separate section for a user to view and edit these fields outside of the actual ERM process area.
R1.4	The platform must offer an option for disabling inactive users.	This document does not define how this mechanism should be implemented. When a user does not enter the platform for an extended period defined by the organization, he should be considered inactive. When this happens, its license can be revoked if needed. Only admins should have access to this feature.
R1.5	The platform must offer an option for revoking access to users that left the organization or the active directory.	This document does not define how this mechanism should be implemented. It may be performed externally by deleting users from the active directory and synchronizing to it later. Only admins should have access to this feature.
R1.6	The platform must be able to store groups or areas with at least the following attributes associated: - Unique ID - Group Name - Members List	This mechanism is needed to designate users to a specific group or area to aggregate more people to be assigned to a risk, opportunity, or control as the responsible party or access them.
R1.7	The platform must offer an option for creating groups or areas with the properties listed under requirement R1.6 .	This document does not define how this mechanism should be implemented. However, only admins should have access to this feature.
R1.8	The platform must offer an option for updating any attributes to reflect changes to the group's details.	This document does not define how this mechanism should be implemented. However, only admins should have access to this feature.
R1.9	The platform must offer an option for adding and removing users from a group or an area.	This document does not define how this mechanism should be implemented. It must allow to add or remove one or multiple users at the same time. Only admins should have access to this feature.

Name	Summary	Description
R1.10	The platform must offer an option for deleting a group or area.	This document does not define how this mechanism should be implemented. If the group or area has users in it, the platform must deny the deletion as it can affect its management. Only admins should have access to this feature.
R1.11	The platform must offer an option for list the members of a group or area.	This document does not define how this mechanism should be implemented. Any authenticated user should be able to see the list of users of a particular group or area.
R1.12	The platform must offer an option for consulting data of specific users and groups.	This document does not define how this mechanism should be implemented. Any authenticated user should be able to consult the user's and group's data.

Table 3.1: User and Group Management Module

3.2.2 Permissions Module

The permission module is essential for the correct progression in the ERM process. Authenticated users must have the necessary access to perform their functions and watch the risk data they are responsible for. This module should allow the different phases of risk assessment and treatment to be managed by the correct responsible entities, assigning different responsibilities to groups and users. This dissertation does not explain how the module should be implemented as long as the requirements are met and features achieved.

Name	Summary	Description
R2.1	The platform must provide a permissions system to define user authorization.	This system should be in a separate section along with all the administrative properties of the platform. Each permission should be separated, e.g., creation permission and edition permissions should have separated authorizations, so groups or areas that can create an element could be restricted from editing. Only privileged users should edit the users' permissions; however, any authenticated user should be able to see its permissions.
R2.2	The platform must allow at least one authorized user with high privileges to define the system R2.1 permissions.	This document does not define how this functionality should be implemented. Note that it should have at least one privileged user responsible for assigning the system's permissions in R2.1 to users, groups, or areas.
R2.3	The platform must allow creating roles in the system R2.1 , such as CTO, ERM committee, or CRO, and associate it with users under R1.1 .	This document does not define how this functionality should be implemented. These roles can be associated with the permission system of R2.1 and the notification system of R3.1 instead of giving a specific user's name. If needed, a role can be assigned to another user, facilitating permissions and notifications management if the organization's structure changes. The roles' names should be entirely configurable at any point only by privileged users.

Name	Summary	Description
R2.4	The platform must offer an option for defining who can see an already created risk, opportunity, or control under the system R2.1 .	This document does not define how this functionality should be implemented. This permission should restrict groups or areas from seeing risks, opportunities, and controls that are not their responsibility. However, it is up to the organization who should have access to what. In the middle of the workflow, a user can identify a particular group or area to allow them to have access to that particular element.
R2.5	The platform must offer an option for defining who can identify a risk, opportunity, or control under the system R2.1 .	This document does not define how this functionality should be implemented. In general, this permission can be open to any authenticated user in the organization since every user should be able to identify those three elements.
R2.6	The platform must offer an option for defining who can edit a risk, opportunity, or control under the system R2.1 .	This document does not define how this functionality should be implemented. This permission is relevant to define where and when the groups responsible for it must have the possibility to edit the element's fields. However, the platform must establish that a user should not edit inputs that another group has given without authorization.
R2.7	The platform must offer an option for defining who can delete a risk, opportunity, or control under the system R2.1 .	This document does not define how this functionality should be implemented. Note that this permission should have different behaviors for each type of these three elements.
R2.8	The platform must offer an option for defining who can analyze a risk or an opportunity under the system R2.1 .	This document does not define how this functionality should be implemented. This permission is needed since only one or multiple groups or areas responsible for a particular risk should analyze it, depending on the organization's criteria about ERM. If the assigned group for risk analysis is not the one that identified the risk, then that group should first see it as mentioned in R2.4 and secondly be allowed to analyze it.
R2.9	The platform must offer an option for defining who can evaluate a risk or an opportunity under the system R2.1 .	This document does not define how this functionality should be implemented. In general, the CRO should be the one to evaluate the risk, but a group or area can also be assigned, depending on the organization's structure.
R2.10	The platform must offer an option for defining who is responsible for risk treatment under the system R2.1 .	This document does not define how this functionality should be implemented. In the evaluation phase, a user should assign a group or area to risk treatment, and the users from that group should have the permissions to implement the controls needed and have all the information necessary from the respective risks.
R2.11	The platform must offer an option for defining who can give inputs to an already created risk, opportunity, or control under the system R2.1 .	This document does not define how this functionality should be implemented. This permission is needed to know where and when different groups or areas can give their inputs in the workflow.

Table 3.2: Permissions Module

3.2.3 Notifications Module

Notifications facilitate the communication between departments and all responsible parties in an ERM process. This module points to a solution that can create alerts based on specific events. Events like identification of risks, data updates, or any input given by users on risks or controls should generate an alert to the competent authorities inside the organization so they can react on time.

Name	Summary	Description
R3.1	The platform must provide a notification system to notify a group of users through email or others when an event occurs.	These events can be defined by default or created if needed. This system should be in a separate section along with all the administrative properties of the platform, managed by a privileged user. Each notification should be separated and give different information based on its event, e.g., events about creation and updates should be separated and send different notifications. Note that responsible parties can change along a workflow, so does the notifications.
R3.2	The platform must allow at least one authorized user with high privileges to define the system R3.1 notifications.	This document does not define how this functionality should be implemented. Note that it should have at least one privileged user responsible for assigning the system's notifications in R3.1 to users, groups, or areas.
R3.3	The platform must offer an option for defining a list of groups and users to notify given a particular event under the system R3.1 .	The platform should allow only privileged users to chose who are the responsible parties to notify based on the events in R3.1 .
R3.4	The platform must offer an option of notifying the responsible parties when a risk, opportunity, or control is created under the system R3.1 .	The platform must generate an event every time one of these three elements is created and, the responsible parties chosen for that particular event in R3.1 should be notified.
R3.5	The platform must offer an option of notifying the responsible parties when a risk, opportunity, or control is deleted under the system R3.1 .	The platform must generate an event every time one element is deleted and, the responsible parties chosen for that particular event in R3.1 should be notified.
R3.6	The platform must offer an option of notifying the responsible parties when the data of a risk, opportunity, or control is updated under the system R3.1 .	The platform must generate an event every time one element is updated and, the responsible parties chosen for that particular event in R3.1 should be notified. However, a method should be established to notify only those responsible and permitted to see the respective risk, opportunity, or control. Users without that permission cannot be notified.

Name	Summary	Description
R3.7	The platform must offer an option of notifying the responsible parties when a risk, opportunity, or control changes its status under the system R3.1 .	The platform must generate an event every time one element transitions through the workflow and, the responsible parties chosen for that particular event in R3.1 should be notified.
R3.8	The platform must offer an option of notifying users, groups, or areas indicated by other authorized users throughout the workflow.	The system in R3.1 is defined previously to any element creation, which means that it can be challenging to establish an event to a particular change of status or field. For example, if a user decides that another group should be responsible for a particular risk, that group should start getting notified. The platform should adapt notifications based on group identification fields that an authorized user can change while the ERM process progresses.
R3.9	The platform must offer an option of notifying the responsible parties when a user gives input on a risk, opportunity, or control under the system R3.1 .	The platform must generate an event every time one element is commented and, the responsible parties chosen for that particular event in R3.1 should be notified.
R3.10	The platform must offer an option of bundling notifications to send instead of several repeated notifications.	Depending on the way system R3.1 is built, notifications need to be managed to send multiple notifications bundled into one, e.g., sending one email with every update within a period instead of multiple emails, to avoid generating what is commonly called "spam".

Table 3.3: Notifications Module

3.2.4 Data Management Module

After the support modules are defined and structured, we should be able to introduce functionality related to risk activities.

The Data Management Module is where the functionality should rely upon. It defines the characteristics of each risk element and what information they should have to be valid. It also describes how the risk assessment and treatment should be carried, how the different risk elements interconnect, and what actions the authenticated users should perform. This module is the core of a risk management system, and should be followed strictly so that the functionality of the platform is adequate to each business sector.

Name	Summary	Description
R4.1	<p>The platform must allow an authorized user to create new elements with at least the following system attributes:</p> <ul style="list-style-type: none"> - Unique ID - Descriptive Name - Detailed Description - Creation Timestamp - Last Update Timestamp - Creator ID/Name - Responsible Person or Group - Event History 	<p>These are the minimum properties to identify an ERM element correctly. Unique IDs and timestamps must be automatically generated and should not be editable or removable. It is up to the supplier if the unique ID should be a randomly generated key or an incremental value and if it changes based on the chosen element.</p>
R4.2	<p>The platform must support the creation of at least the following elements:</p> <ul style="list-style-type: none"> - Risks - Controls 	<p>Although it can be more elements, depending on the organization criteria, controls and risks should always be elements present in a risk management system.</p>
R4.3	<p>The platform must offer an option for associating the elements of R4.2 with the properties listed in R4.1 in a many-to-many relationship.</p>	<p>This document does not define how this mechanism should be implemented. Risks should be able to be associated with multiple controls and vice-versa. Any authorized user should be able to choose when and where to associate an element to another. However, this link can also be deleted by users with permission to do so.</p>
R4.4	<p>The platform must offer an option for creating new fields to be filled in.</p>	<p>The platform must allow the organization to choose what fields should be included to be filled in by the users. These fields should vary in types and the content that must be inserted. It should be possible to define whether the field is numeric, a list, multiple or singular selections, limited or open text field. It should also be possible to create fields to pick single or multiple users, groups, or areas present on the database. Only privileged users should be able to create these fields to be later added to the needed stages throughout the workflow.</p>
R4.5	<p>The platform must offer an option for adding new fields to transitions.</p>	<p>This document does not define how this mechanism should be implemented. The fields created in R4.4 need to be assigned to a form in a specific event or transition within a workflow. It should be able to order them in the form presented to the user. Only privileged users should be able to assign fields to a transition.</p>
R4.6	<p>The platform must offer an option for defining different statuses and transitions in workflows and associate them with the platform elements.</p>	<p>Each status and transition should have properties that can be cloned. Transitions must have a source status and an ending status as well as conditions to be performed (e.g., a risk can only transition if the responsible party has been identified, or only the CRO can perform the evaluation transition). A transition can also have a form with fields attached. Only privileged users should be able to manage these statuses and transitions.</p>

Name	Summary	Description
R4.7	The platform must offer an option for showing the progress of a particular issue.	This document does not define how this mechanism should be implemented. However, the workflow status of an element must be visible for any authorized user when he accesses it.
R4.8	The platform must offer an option for risk analysis that allows users to indicate the following properties: - Likelihood (qualitative/quantitative) - Impact (qualitative/quantitative)	Unlike the other transitions under R4.5 in which this document does not specify their use, the risk analysis phase should be an obligatory transition indicating the type of impact of an event and its likelihood.
R4.9	The platform must allow the organization to define the levels and values of every property used to calculate the risk level.	The qualitative/quantitative values of impact, likelihood and risk level should be configurable to reflect the organization's criteria for risk analysis.
R4.10	The platform must offer an option for risk evaluation that calculates the risk level automatically based on the properties of R4.8 .	The risk level should be calculated using the properties of R4.8 and following the organization's risk matrix in which a particular value of likelihood and impact should correspond to a level in the matrix. That risk level should be available to any authorized user.
R4.11	The platform must offer an option to automatically move an issue through a workflow based on certain criteria.	The platform should provide a way to transition an issue through the workflow when a trigger event happens, i.e. a due date is reached, a field value changes or no response from a user or group for a period of time.
R4.12	The platform must offer an option to close risks that have already been treated.	This document does not define how this functionality should be implemented. Entities that have already been treated should be set represented as closed or other ending state, permanently or temporary, depending on the organization's metrics.
R4.13	The platform must allow authorized users to assign issues to other users, giving them the needed access.	Authorized users should be able to designate another user to answer for a particular issue
R4.14	The platform must allow authorized users to correct their inputs on each issue.	Authorized users should have the possibility to edit fields that they filled. However, in the evaluation and treatment phases, editing properties should not be possible to avoid incongruities. Instead, the information should be communicated to the CRO or the team responsible. If the risk is already closed, it should be opened to edit its properties.
R4.15	The platform must allow authorized users to input information on their issues at any given point of the workflow without editing them.	Following the requirement R4.14 , authorized users should be able to input information in the form of comments or other mechanisms, at any given point in the workflow, without changing the element's data.

Name	Summary	Description
R4.16	The platform must offer an option of showing historical element values such as risk level, likelihood, and impact.	An authorized user must be allowed to see the previous values of risk level, likelihood, and the impact that a risk had in order to see its evolution over time.

Table 3.4: Data Management Module

3.2.5 Search and Reporting Module

Searching and reporting methods are essential for reliable data management, monitoring and faster access to relevant information. This module should lead an ERM solution to reach a viable method to return the information a user needs without compromising the confidentiality of the returned data, allowing for complex searches to be made in a friendly way. Reporting and monitoring should be facilitated so the responsible parties have a holistic way to see data without checking each risk element one by one.

Name	Summary	Description
R5.1	The platform must allow users to find, using a search query, any issues that they have been granted authorization to browse or inspect.	Users should be able to search for specific items that they have access to under the permission system in R2.1 . This should be reached by using any searching query that could retrieve the issues needed from the database.
R5.2	The platform must allow users to restrict searching results, under R5.1 , to issues of the types described in R4.2 .	The search result shall return a list of issues filtered by one or more issue types.
R5.3	The platform must allow a user to specify a search query, under R5.1 , comprising a single full-text search carried out across all textual attribute elements.	The search result shall return a list in which the elements have part of the text inserted as any of its textual attribute elements.
R5.4	The platform must allow a user to specify a search query, under R5.1 , that consists of one or a combination of search criteria, where each search criterion compares a particular system or contextual attribute against a value provided by the user.	The user should be able to use these search criteria separately. However, each criterion should influence the result of the values, combined with all the other ones used.

Name	Summary	Description
R5.5	The platform must allow a user to specify a search criterion, under R5.4 , that returns a match for any value of the specified attribute.	No description needed
R5.6	The platform must allow a user to specify a search criterion, under R5.4 , that returns a match for textual attributes based on full-text searching.	The text inserted must retrieve issues that fully or partially have that text section in any of its attributes.
R5.7	The platform must allow a user to specify a search criterion, under R5.4 , that uses the following value operators to compare numeric attributes and dates: - Equals - Not equals - Greater than - Less than	Alternatively, the platform can provide functions, symbolic elements, or operators to provide a similar way to compare values inserted.
R5.8	The platform must allow a user to specify a search criterion, under R5.4 , that returns a match for any issues created/updated/closed within a certain period of time using the operators of R5.7 .	No description needed.
R5.9	The platform must allow a user to specify a search criterion, under R5.4 , for Boolean attributes that check whether the element's value is true or false.	No description needed.
R5.10	The platform must allow a user to specify a search criterion, under R5.4 , for field attributes that checks whether the element's value is empty or not.	The search result shall return a list of the elements in which a specific value is empty or not. Alternatively, the value "null" can be used for the same purpose depending on the database characteristics.

Name	Summary	Description
R5.11	The platform must allow users to combine different search criteria, under R5.4 , using the Boolean operators AND, OR, and NOT in any combination, and change the order of precedence by which search criteria are evaluated using parentheses or an equivalent method.	No description needed.
R5.12	The platform must allow a user to specify a search criterion, under R5.4 , that returns only open or closed issues.	No description needed.
R5.13	The platform must allow a user to specify a search criterion, under R5.4 , for issues in a particular status in a workflow.	No description needed.
R5.14	The platform must provide the ability to order every column alphanumerically, sorting in an ascending or descending way.	No description needed.
R5.15	For large sets of search results, the platform must implement a method of pagination, or alternative, such that only a subset of the total search results is provided back to the user, and additional subsets are provided when required.	No description needed.
R5.16	The platform must provide the total number of issues that match the search query as part of the search results: this total must not include issues excluded from the search results under R5.17 .	No description needed.

Name	Summary	Description
R5.17	The platform must never allow a user by searching, browsing, or any other method to access issues or their attributes that the user does not have the authorization to inspect. All such issues should be excluded from search results.	This requirement is relevant to avoid any information security issues related to confidentiality non-conformities. User authorizations to see a particular entity should be under R2.1 .
R5.18	The platform must allow authorized users to save, modify, delete and share search queries.	No description needed
R5.19	The platform must provide the ability to search the history of one or multiple issues and the changes made with the respective timestamps.	The history of a particular entity must be searchable and should be possible for the user to see what fields changed and its timestamps. The historical changes of an issue could be helpful for further reports on risk evolution over time.
R5.20	The platform must allow authorized users to show any issues in the form of charts or any other type of graphic report.	As these are not a part of functional requirements, they are not mentioned how they should be implemented or how they should behave. However, the searching system must have the possibility to generate these charts given any filter, query and field. Charts should be available to ease the access to large data and provide an holistic view about risks, opportunities and controls.
R5.21	The platform must allow authorized users to create dashboards with charts chosen by them to illustrate a specific set of data.	These dashboards should be allowed to be saved, shared or configured by the users authorized to do so. Any dashboard created must only provide data related to issues that user has also access to inspect.

Table 3.5: Search and Reporting Module

3.2.6 Exporting Module

In addition to the platform where an ERM process is implemented, we should not forget that the data stored can be integrated with other systems depending on the culture and the organization's specificities regarding risk management. Therefore, it requires a methodology for exporting the existing data created within the platform that integrates these same data with other tools or for simple information sharing. This module introduces requirements that point to a solid export approach that allows data to be transmitted from one point to another, ensuring data integrity and confidentiality.

Name	Summary	Description
R6.1	The platform must allow an authorized user to export issues, search results, filters, and reports to XML, CSV, PDF, or an equivalent data file.	This document does not define how this mechanism should be implemented. However, the information exported must be available in an arranged way, thus giving the columns, fields, and entities provided in the same order and exhibition as the platform shows.
R6.2	The platform must allow an authorized user to export only the data that he has access to.	Once again, this requirement is relevant to avoid any information security issues related to confidentiality non-conformities.
R6.3	The platform must only allow exporting issues chosen by the user.	No description needed
R6.4	When a user exports issues under R6.1 , the platform must also export the software metadata such as timestamps, columns, and entity order.	This is relevant so the exporting system can be reliable and consistent. The information that the users see on the platform, should be the same information that the users export.
R6.5	The platform must allow an authorized user to export any data in the form of a chart.	As mentioned in R5.20 , charts should be available to ease the access to large data and provide an holistic view about risks, opportunities and controls. Therefore, it makes sense that they can also be exported.
R6.6	The platform must allow an authorized user to export any dashboard that he has access to.	Dashboards are the most significant aspect of reporting of communication. Dashboards can give multiple views on risk data, and that information should be retrievable and shared on other platforms between other departments.
R6.7	The platform must allow an authorized user to export the history of one or multiple entities under R5.19	This document does not define how this mechanism should be implemented. However, information and updated values could be retrieved as a list of events that a particular issue went through.
R6.8	The platform must allow an authorized user to export data from one or multiple entities from a particular point in time.	This document does not define how this mechanism should be implemented. The platform should be able to access a particular point in time and show status, values or field updates, made until that date.

Table 3.6: Exporting Module

3.3 Conclusions

In this chapter, We explained in detail the INCM's framework and its limitations. We could find its structure aligning with the previous guidelines and good practices for enterprise risk management mentioned in the related work by applying the same principles when establishing the context with a well-defined structure, responsibility matrix, and creating the metrics needed to assess and treat risk correctly. It is particularly relevant to note that their approach considers the organization's multiple contexts and

scopes using guidelines shown in other standards related to specific management systems like information security, quality, or environmental.

However, the implementation of its risk management system is far from being efficient. It is dispersed among several departments, is not regularly updated, and is mostly based on spreadsheets where the CRO receives the data from the departments and populates it, thus not providing the wanted value that this domain should give. It becomes clear that there is a need for a process dematerialization, where its structure should be reviewed and be implemented digitally. Acknowledging that JIRA is an issue tracking system implemented on INCM that had previous experience in digitalizing other systems, it makes sense to test its practicability on the risk management domain bringing up its pros and limitations. By this, we can consider that the solution that we will implement will be, at the same time, the first part of our problem as well. The previous thesis about the Risk and Consultation on this same process was also relevant to define a conceptual model on which we could base our solution.

From here, and from the complete system analysis, we could elaborate the second part of our solution, related to defining functional requirements that ERM tools should embrace to achieve acceptable efficiency and practicability levels. These requirements will guide our solution configuration and should support other developers or providers of similar software in the future to give what companies are searching for.

4

Solution Design and First Prototype

Contents

4.1 Analysis of the JIRA Technology	46
4.2 Limitations of the JIRA Technology	49
4.3 First Prototype	51

Rigorous work has been carried out to dematerialize processes into JIRA, taking shape in the configuration and monitoring of various projects at INCM, both internal and transversal, to the organization's various departments. This acquired experience was fundamental for discovering other useful functionalities for the Risk Management project and finding limitations to the solution, which made us formulate workarounds to reach the organization's objectives.

4.1 Analysis of the JIRA Technology

JIRA is part of a range of Atlassian products to help teams organize their work. Originally, JIRA was built to track bugs and tasks, but in a few years, it has evolved into a more developed tool for all types of cases, from requirements, test case management, project tracking to software development.

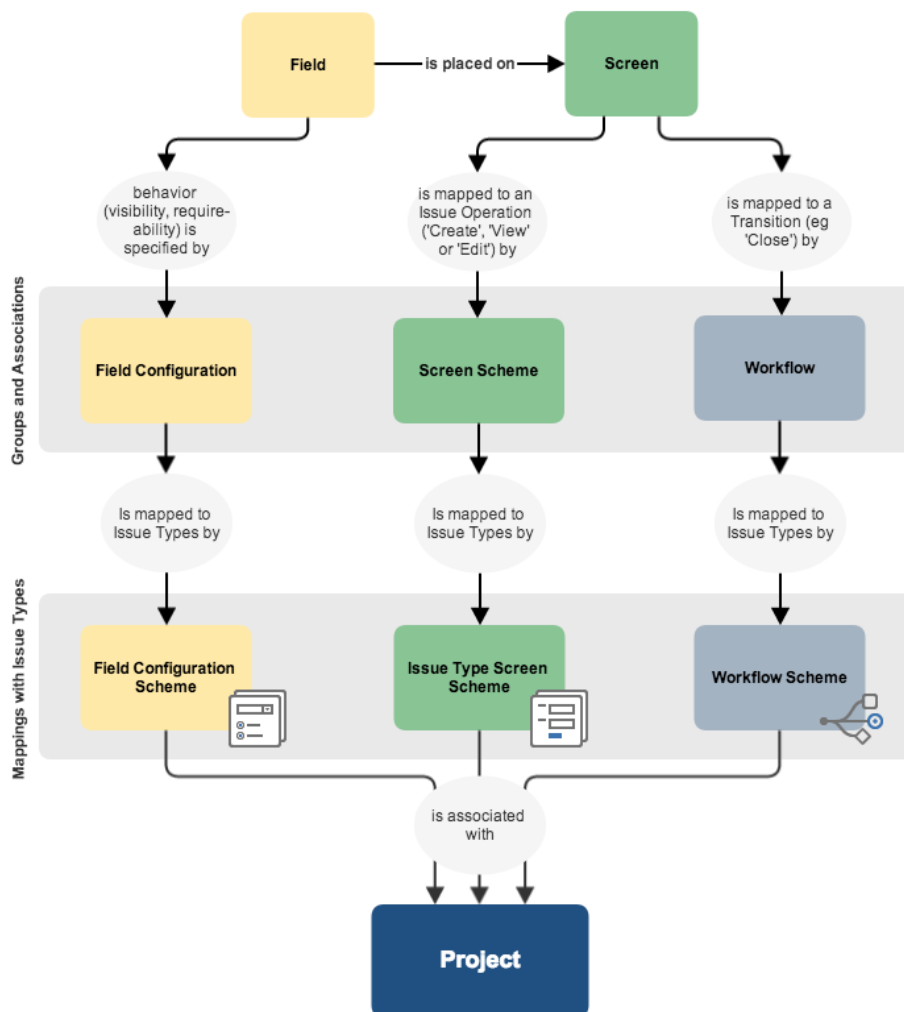


Figure 4.1: JIRA Concept Diagram ¹

Many companies acquire JIRA intending to digitize their business to integrate technology in all processes (or at least the organization's possible ones), which improves performance and updates old structures, changes procedural operations, and responds on-time more efficiently to its customers and their needs, in order, in general, to update itself on the current market. ² For a better understanding of INCM JIRA's context, we'll solely talk about JIRA Software applied on-prem from now on.

The first step should be understanding the conceptual structure of JIRA that is illustrated in general in Figure Figure 4.1

Issues are the building blocks of any JIRA project. An issue could represent a story, a bug, a task, or another issue type in a project. JIRA application issues are made up of **fields**. It's possible to choose any number of fields to appear in different **screens** when creating, editing, or transitioning issues. It also allows creating custom fields for teams working on issues within any of the existing JIRA projects. Custom fields allow users to add information specific to a team's needs.

Below are some of the most relevant basic features of the tool, considering this document's topic and the proposed solution for the problem mentioned in the previous chapter.

- **Dashboards:** The tool has Dashboards to report all information and status for a given project. This is where information that may be relevant should be reported and made explicit in maps, graphs, or tables, for easy analysis and data collection. These panels have a drag-and-drop system, are intuitive, dynamic, configurable in terms of fields, tasks, projects, filters, design, and object layout. Access to a panel can also be given or restricted and may, if necessary, make it available only to interested parties.
- **Workflows:** The existence of workflow customization within projects is perhaps the most useful aspect of this technology, giving the possibility of identifying and customizing the various issue status and configure the transitions in between with different characteristics, access permissions, and forms (called "screens" in JIRA) to progress in the workflow. In these transitions, it enables the use of simple post-functions, like updating some issue fields or trigger events (to send notifications to the responsible parties), and conditions (to make sure that the issue's status only changes if a particular parameter is "true"). This facilitates the visualization of information and the task's situation, obtaining an estimate of a project's condition when combined with graphics on the Dashboard.
- **Permissions:** Access permissions are available at the project and issue level. Here, it's possible to define who creates, edits, comments, or deletes items, who can see them, and who is allowed to manage the project. Imagine if there's a JIRA project configured for a department. However, there are some issues that only managers should have access. JIRA allows the project to be open

²Atlassian. (2019) What is JIRA used for?, <https://www.atlassian.com/software/JIRA/guides/use-cases/what-is-JIRA-used-for>
²Atlassian. (2020), Administering Jira application support, "Project screens, schemes and fields", <https://confluence.atlassian.com/adminjiraserver/project-screens-schemes-and-fields-938847220.html>

to the entire department but restrict its visualization to specific groups, areas, or people.

- **Dynamic Notifications:** Notifications are a crucial point in communicating changes within a given project. JIRA makes it possible to automatically inform interested parties by email if any items are created, modified, or deleted so that they can act accordingly and on time. In the email, a link to the project is provided, with the changes' specifications.
- **Fields and Configurable Screens:** Each field is fixed on one or more screens associated with one or more transitions. These fields are customizable data entries that the user can fill in or edit throughout the item's workflow. This customization is done only by the project administrators.
- **Filters and Search:** This type of search allows easy visualization of relevant data or items, allowing to filter information regarding field values, workflow states, relevant dates (creation, completion, updating), or even intervening users. With those filters, one can edit in bulk, depending on the issues selected. Filters offer even more value when combined with the graphs and tables on the Dashboard.
- **Flexibility of project types:** JIRA lets you choose from different project types depending on the goal of a team. For a software development approach, you have:
 - Scrum Software Development, where you can use it for agile development with a board, sprints, and stories;
 - Kanban Software Development, to optimize the development flow with a board;
 - Basic Software Development to track development tasks and bugs.

For a business approach:

- Project Management, to plan, track, and report all the work within a project;
 - Task Management to quickly organize and assign simple tasks for a team;
 - Process Management, to track all the work activity as it transitions through a streamlined process.
- **Reusability:** JIRA makes it possible to pick a default workflow and a default list of issue types or reuse ones used for another project. From that point forward, one can adopt many approaches depending on the intent by creating new fields, screens, and other configurations. However, you're allowed to choose from an already configured project, avoiding repetition of fields for the same purpose, redundancy, and, consequently, facilitating employees' work by offering them coherence between projects.

JIRA's extensive configuration capabilities, together with the variety of features coming from plugins from third-party companies, make it an easy-to-use tool, substantial flexibility, and adaptability to organizational processes. Which makes companies and teams, more than use it for software development (purpose for which it was designed), to use it for their enterprise processes and cases. [22]

In the case of Covance, JIRA was used in risk management processes, in addition to other applications. [22] This case uses the JIRA technology for risk management in clinical trials to collect the information and inputs necessary to correct the risk inherent in the function, using its features for creating workflows, filters, permissions, and exporting. This information is subsequently gathered from its REST Application Program Interface (API), which offers virtual access to all the information provided in the tool, facilitating integration with other applications and using the data for other purposes like data analysis, reporting, and monitoring.

It was also reported to purchase third-party plugins to customize the process to their needs, as it was impossible to obtain all the necessary functionalities with JIRA's base version.

4.2 Limitations of the JIRA Technology

While the technology showed signs of intense improvement to any process and project dematerialized into it, it also showed some limitations to the initial proposal. As mentioned multiple times before, JIRA offers excellent flexibility and configuration capacity, making it useful for software development and project and process management. Some companies tried to use it on a large scale [23], and others for different purposes than the original design of the tool [24].

In [23], when tested on a large scale, it has shown to leverage teams' capabilities and proven its configuration potential by tracking key metrics about the companies' development effort, making it an excellent tool to store and gather data from their different teams. Its search engine and change history also allowed quick access to what and when changes occurred. However, the organization found some limitations, specifically in **Field Level Permissions** and in the **Workload Tracking**.

JIRA doesn't provide an option to control editing capabilities within a JIRA issue. "If a field is available on an entry screen, then it can be edited by any user with permission to edit that JIRA issue" [23] where specific users or groups of users should only edit some of the custom fields in a JIRA issue. Field level permissions should also concern the INCM problem since risk assessment, for example, is performed by different groups of people, being relevant to establish when and who can edit the issues. The high workload of the organization, as well as the significant level of coordination between the teams, showed that while JIRA provides outstanding support for the current issue status, other tools are more useful to "plot historical trends and identify completion rate problems" [23] since there's no built-in timeline to track project progress. The company in question used 3rd party software to mine data from JIRA databases

and reported it elsewhere. The need for external applications was also mentioned in [22]. In this case, it was not due to an extensive workload but with the **Low Reporting Capabilities** that JIRA has shown, using the tool almost as a database to gather data from its REST API and reuse it somewhere with more dynamic reports.

As spoken to XpandIT, the representative partner of Atlassian in Portugal, risk management was a complex process that, although possible to implement, would probably be difficult to deploy for the tool was not meant for it. Over the months, we tried to understand if JIRA was viable for the process mentioned, performing intense testing, trying to learn all the capabilities, what limitations the organization should have to accept as a reality and finally, what workarounds did we have to configure. This testing resulted in a sharp learning curve that led to a deep understanding of the technology. Consequently, limitations were pointed out, which could offer some resistance to the INCM use case:

Lack of Automation - JIRA doesn't offer a simple way to automate projects. It lets you decide if you want to update a system field on a status transition, like the assignee, summary, or description but restricts it for custom fields. The idea of having this possibility in the risk management project was mainly to find a way to calculate the risk level based on the likelihood and impact filled on the risk assessment automatically. It would also be useful to find a way to change an issue's status based on particular fields, for example, switch to a "Overdue" status when the due date is reached. This offers restraints to achieving **R8** of the functional requirements for risk management described in the previous chapter.

Discrepancies in Language Packages - One of JIRA's main objectives was to use it across the organization. Being INCM, a Portuguese organization that produces Portuguese security documents and products, it makes total sense that JIRA covers the Portuguese language in its framework so that everyone can use it. The language pack exists, but it seems that the package only contains Brazilian Portuguese. It wouldn't be an issue, except that most terms used in the English version, like "issues" or "custom fields", appear to have not been well translated, showing different names to refer to the same term across the entire platform. The lack of coherence led to some confusion and made the tool harder to read and to work with. For that reason, it was chosen to use the default English language package but keep custom fields and internal dialog in Portuguese because it was found to be more accessible to users.

Data migration between servers - At INCM, the platform was separated into two environments: test and production. In the test server, one would be able to verify their project configurations before deploying it into the production one. Although this division was useful to avoid risks and maintain the tool's availability, JIRA has no straight forward way to automatically migrate the data and configurations from one server to another, which meant that the data must be duplicated by hand. There was no workaround for this issue. Therefore an add-on would be necessary for the

correct treatment of projects and management of information.

Report Exporting - The tool provides extensive report capabilities based on filters by specifying projects, fields, dates, and more. However, JIRA doesn't seem to be prepared for any dashboard, graphs, or any analysis export by default. It exports data and nothing else, and if there's a need for more, it probably requires the purchase of another add-on or external software to do it, as stated in the previous workarounds. This follows up to the final and probably most relevant limitation. It is a major issue for reporting an communication, and, although is not yet mentioned to be a critical limitation, since JIRA has Dashboards that already can provide relevant data analysis.

Add-Ons as Solution - After some extensive research, after the various doubts that arose in the configuration for INCM, and as we can deduce from the previous statements, JIRA, by default, is not yet prepared to deal with multiple issues. It seems reasonable that a project, process, and software management tool couldn't solve every organization's problem. Atlassian has a voting system that helps them pick exactly which feature organization's teams want more, and it becomes easier for them to define what to deploy. When asked for workarounds in the Atlassian Forum, the most common answer leads to add-ons purchase, which solves precisely the issue in question, but implies an extra price.

These limitations were soon mentioned to those responsible for JIRA and the administrative council, who wanted to evaluate if the tool would be useful for the future. Some of these were not impactful since there were "out of the box" alternatives that required more work, more time, or merely a feature that would be accepted as not being able to implement. However, after some time, the organization considered acquiring add-ons that could impact the Risk Management project and other future projects.

4.3 First Prototype

The existent licensing allows the distribution between a test server and a production server limited to a certain number of licenses. This division will allow the tests that need to be done in an "out of production" environment, which can be an added value if it becomes necessary to test backups, updates, plugins, or even project configurations. This environment will be mainly helpful to learn the tool capabilities for training purposes and will also be where the risk management process, like many others, began to be dematerialized.

We started by reformulating the previous process and simplify the BPMN model presented in Chapter 3 in Figure 3.1.

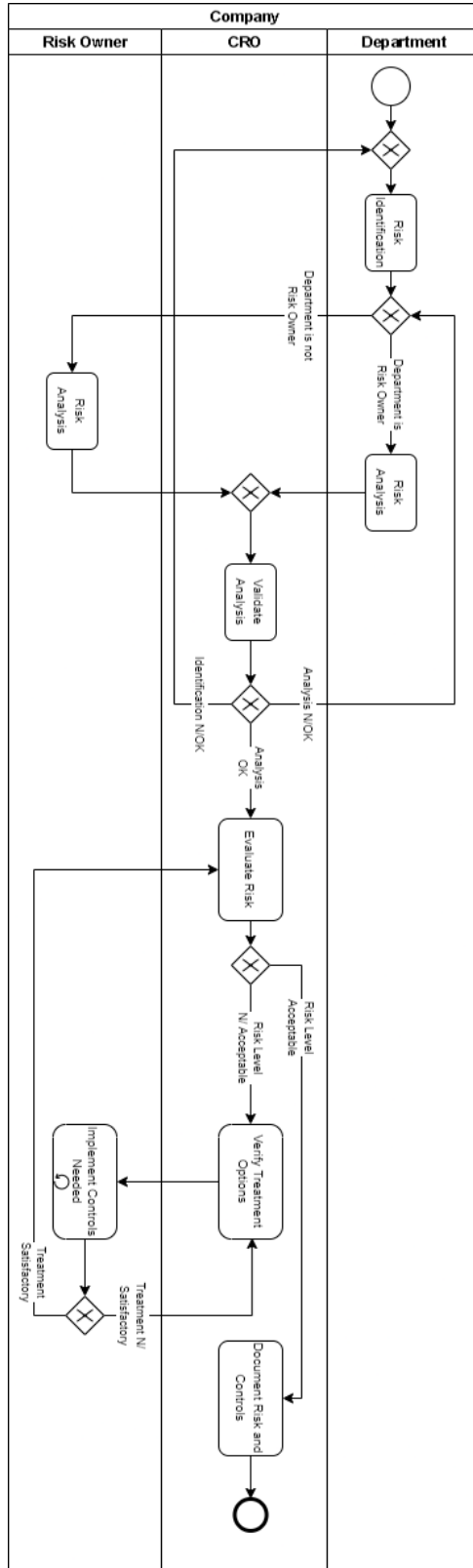


Figure 4.2: BPMN Model of ERM workflow To Be Implemented

At the beginning of the process, the departments where the event occurred would have to fill out a form to give the CRO as much detail as possible. This information could belong to both the identification phase and the risk analysis phase. When obtaining this data, the CRO would have to assess whether everything complies or if the risk owner's analysis is necessary (i.e., if the department is not the risk owner already). This step can easily be reduced, as the CRO does not need to be the intermediary but evaluates the final data as shown in Figure 4.2.

When a risk was identified in the previous model, the CRO would add it to the respective department's file and send it by email to the responsible parties. In JIRA, this segregation and reporting can be done automatically. The department that first identifies the risk also identifies the risk owner when creating a ticket in JIRA. The identified department will be notified and will be responsible for responding to the risk analysis. If the department identifies itself, then it can proceed with the analysis. In the end, the CRO will verify the identification and analysis data; if a change is necessary, he will send it to the respective department; otherwise, the process will enter the evaluation phase.

During the evaluation phase, the CRO will verify the risk level and the existing controls. If the risk is not at an acceptable level, the CRO, based on the impact of the event on the assets, and its likelihood, may meet with the areas and propose new controls to be implemented. These areas will have the responsibility to implement the necessary controls that mitigate the risk in question. The CRO and the risk management department will constantly monitor this implementation. When the implementations are finished, the risk should be reevaluated by reducing the impact or the likelihood of the event, thereby lowering the level of risk. This evaluation process will iterate until the risk level is acceptable. The risk will then be documented and accepted when this happens, allowing further monitoring and reviewing whenever necessary.

With this new model, we can reduce the number of tasks related to communication between areas previously centralized on the CRO. Furthermore, by deploying it in JIRA, the solution will be a considerable advantage for **reporting, communication** and **consultation**, as these were the most significant limitations of the previous process, reducing DPR's efforts considerably. We managed to get the information to go directly from one area to another in an enlightening way while allowing each area to manage and collect reports on all their risks, opportunities, and controls autonomously. Since it means a paradigm change within an already existing process, people will require training to avoid resistance to change and ease their learning curve.

In the case of the ERM process at INCM, we carried out the dematerialization following weekly interviews with the CRO. These interviews granted the constant monitoring of a risk management specialist given the developments made.

The platform structure had to follow the rigor of the ERM process established in the state of the art while following the company's rules. Using the previous list of functional requirements and considering

the tool's limitations, we developed a prototype that tried to meet as many points in the requirement's modules as possible.

JIRA has a user and group management system built-in that allows integration with the organization's Active Directory. This system enables the reuse of corporate login names and passwords, and lets system administrators manage the user's access to the platform. Hence, all the requirements of the first module present in Section 3.2.1 are fulfilled by default.

To achieve a consistent solution, we followed a specific order of configuration that we found to be the best practice when creating new projects in JIRA. First, we defined the issue types of the project. Issue types in JIRA differentiate an object from another and allow different configurations to be associated with different types. These are comparable to the elements that requirement **R4.2** of Section 3.2.4 mentions. In order to maintain the cohesion of the existing process in the company and follow the ERM guidelines, the application needed to have 3 issue types as shown in figure Figure 4.3: **Controls, Opportunities, and Risks**.

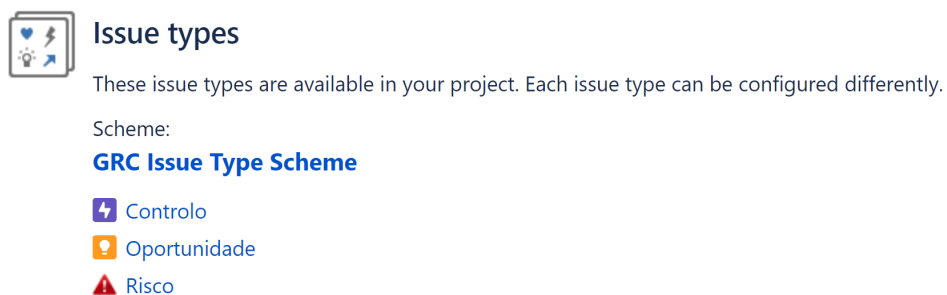


Figure 4.3: Risk Management Project Issue Types

Each type will have an associated workflow dictating their progress and defining what states they must go through before reaching the end of the process.

Then, we defined the screens for each transition and the fields to populate each form. Statuses and transitions are fully configurable, allowing to define conditions in which the transition can be performed, the person allowed to it, the fields that need to be filled in each transition, and what should happen when the transition occurs. These transitions will be used to perform the Risk Analysis and Evaluation, allowing users to fill the fields needed without needing support or meeting with the CRO, contrary to what would happen in the previous model.

In this case we will use state machines to model JIRA's workflows. The first version had a simpler state machine, where the risk assessment was divided into three steps: identification, analysis, and evaluation. The last one worked as a standby step where it waited for the CRO's verdict on the treatment strategy, which could be accepting, mitigating, avoiding, or pursued (in the case of an opportunity). Since we could obtain that treatment strategy from a field, the final statuses were divided into "risk controlled"

if the risk was mitigated, pursued, or accepted; and "risk closed" if the risk was avoided.

We realized later that the transition between the analysis and evaluation step did not need interaction and could be removed. In this way, since the risk evaluation is a decision point more than a status, it would be transformed into an area where only the CRO could progress.

A new status were later added where users could distinguish already evaluated risks that were waiting for treatment. In addition, the CRO wanted an additional step to set a duplicated or mistaken risk that needed to be deleted, finally reaching the final risk state machine depicted in Figure 4.4

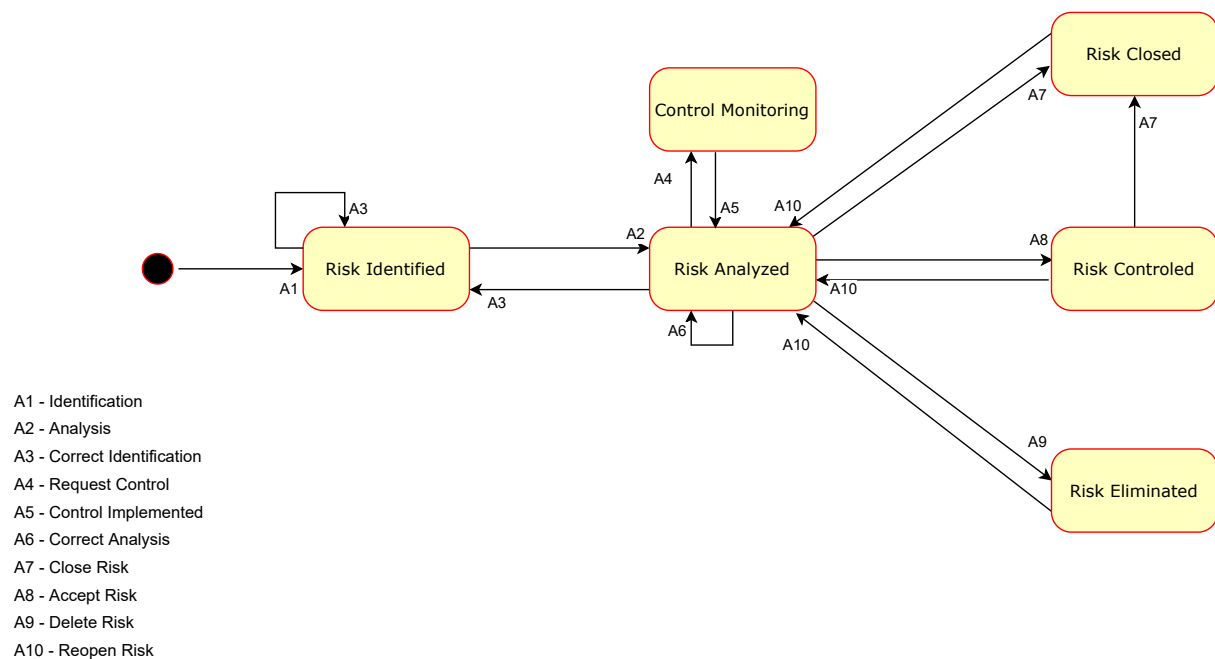


Figure 4.4: Risk State Machine

We also implemented a transition from and to the same status if a user needs to correct the issue instead of enabling the system "Edit" button³ which will help us to select who can edit the issue and in what stage of the process.

When a department receives the email that a Control is needed, the department is responsible for implementing and creating it in the platform.

The control state machine was more straightforward as it was identical to one previously made in INCM concerning action monitoring. The requirements only described four steps: To Implement, In Progress, Implemented, and Not Implemented, and that a control should always be associated with a risk at the creation phase, which was also easy to implement thanks to the JIRA's linked issue field.

³This is a workaround for one of the limitations shown before, where if we enable a group or a person to edit an issue, it lets them edit the fields from all transitions independently of how ahead those fields are on the workflow; this led people to be able to fill fields that were not supposed to yet.

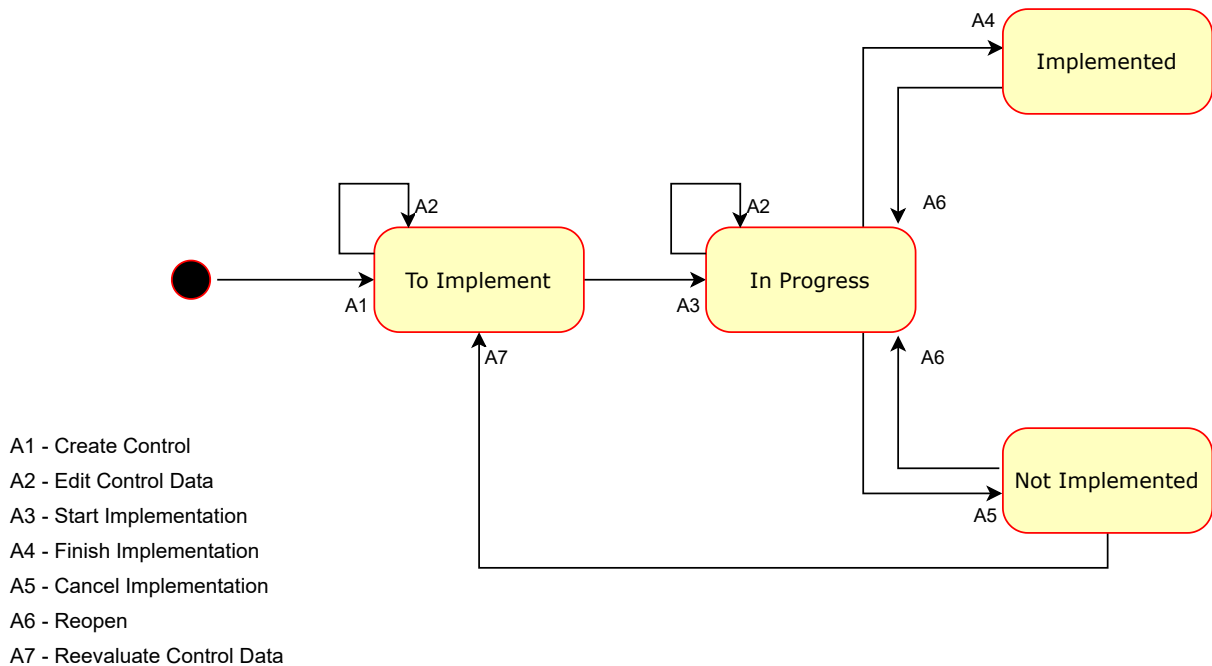


Figure 4.5: First Control State Machine

Regarding Opportunities, the structure, workflow, and transitions should be the same as Risks, except for the metrics and calculations of risk level present in the INCM framework that will also be translated into the project.

Looking at the requirements, specifically for the Data Management Module in Section 3.2.4, the vast majority were fulfilled. JIRA provides a way to configure each field placed in the project, making requirements like **R4.8**, **R4.9** and **R4.10**, easily achievable as shown in Figure 4.6.

Default Configuration Scheme for Nível de Risco

Default configuration scheme generated by Jira

Applicable contexts for scheme: [Edit Configuration](#)

Issue type(s):
Global (all issues)

Default value: Não Analisado [Edit Default value](#)

- Options:
- Não Analisado
 - Muito Baixo
 - Baixo
 - Moderado
 - Alto
 - Muito Alto

[Edit Options](#)

Figure 4.6: Options on risk level field

Requirements like **R4.6**, **R4.7** are also achievable as it is possible with JIRA to configure a workflow,

associate it with an issue type and show its progress at any point in the process as shown in Figure 4.7.

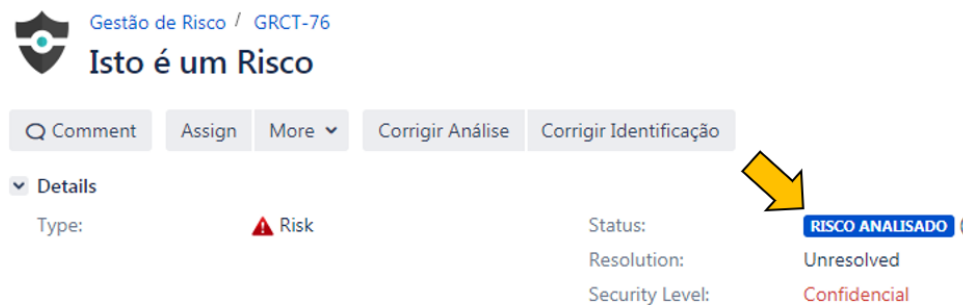


Figure 4.7: It is possible to see the progress in a detailed view of an issue

However, we were also able to identify two requirements of this module that could not be fulfilled. Automation is something that JIRA software does not have by default; therefore, requirements such as **R4.10** and **R4.11** are not possible to achieve. The first one has a significant impact on the process as it implies that the CRO or the DPR need to calculate the risk level in some other way, making the system almost unfeasible. Although requirement **R4.16** is met, it is not done straightforwardly. JIRA's history system is limited, difficult to navigate, forcing the user to check issue by issue to collect the previous data of an issue.

Permissions and notifications are the last ones to be defined⁴, considering they are usually the most challenging parameters to establish when multiple areas interact with a project. This required a list of the departments and their respective promoters (i.e., the person responsible for advising on risks and controls within its department) to create the respective groups in JIRA's system. The permission and notification systems are segregated and are present in the project administration section. Since the tool had these functionalities by default, no additional configuration was necessary to fulfill the requirements of Section 3.2.2 and Section 3.2.3, achieving all the proposed objectives.

In terms of search and reporting, JIRA has an intricate searching mechanism that allows users to search for issues within a project using queries similar to SQL. It also has a more basic search system, providing more straightforward searches based on specific fields. The query provided will then display a list of issues corresponding to the inserted parameters and can be saved to be later used in charts and dashboards. This system fulfills the requirements of Section 3.2.5, except for **R5.19** referring to issue historical features as it is impossible to search previous values of multiple issues unless you search it one by one.

As for the exporting features, the tool finds its biggest weakness. Section 3.2.6 is a small module, but it should support the organization regarding the risk communication between departments. Within

⁴Permissions and notifications can also be granted and set in workflow transitions, allowing to assign who can execute a particular transition and what event should be triggered when that happens.

this module, only the requirement **R6.1**, **R6.2**, **R6.3**, **R6.5** and **R6.6** are fulfilled, showing precisely its limitations. Once again, requirements like **R6.7** and **R6.8**, concerning historical data, are not met, making it challenging to monitor a risk evolution through time.

Although the solution was already in progress, some questions were arising. If the tool did not allow us to perform operations with numerical values, how should the risk level be calculated from the data entered? Was it necessary for the CRO to calculate it based on the likelihood and impact value by hand? This calculation is somewhat complex and is generally supported by a risk matrix. Will we need any external software to do it? If this happens, JIRA would not be so advantageous, considering the effort of using two platforms. It would be inconceivable and would undoubtedly delay the dematerialization process.

Dozens of JIRA add-ons were analyzed, which, as stated, is part of Atlassian's market strategy to solve problems that are not resolvable with JIRA's basic solution. In fact, with this investigation, the most significant milestone of this project was reached, not only solving part of the problems encountered but adding functionality that was previously impossible to achieve, as we will show in the next chapter.

5

Final Solution

Contents

5.1 Automation System	60
5.2 Usage	61

In the previous chapter, we explained briefly the structure of the application where we wanted to deploy our reformulated process. The outcome resulted from several iterations by gathering new requirements from periodic meetings with the CRO and sometimes the promoters, aiming to get a pleasing result for both parties. However, some of the functional requirements we built were not achieved by the first draft we made, which proved to be a significant obstacle to achieving the desired functionality.

This chapter will explain the final solution in-depth and the changes required to deliver a platform compliant with the requirement modules created.

5.1 Automation System

Around March of 2020, the organization acquired the plugin **Automation for JIRA**, which, as its name implies, added automation functionalities to the platform. It was found to be extremely helpful because it showed signs that could mitigate our application problems and, at the same time, add value to many projects in JIRA that needed automation in any way. This add-on would become the most significant milestone to the development, as we could differentiate the process "before" and "after" Automation for JIRA was introduced.

Contrary to what happened in the first version, this plugin allowed us to finally create an automated system that calculated the level of a risk based on the quantitative value of likelihood and maximum impact, fulfilling the requirement **R4.10** of the Section 3.2.4. This would happen after a risk is analyzed and did not require any direct actions from the CRO. These calculations were based on the risk matrix represented in the previous process at INCM, which has not been modified.

Although the problem we had with risk level calculations was a dealbreaker for the system, it was not the only reason to acquire this solution. One of the many audit requirements would be monitoring the controls for risk treatment by the risk owner and the risk management department. It required that areas had an accurate knowledge of the status of their controls and the expected dates of implementation. Although essential to establish a forecast, these dates were easily ignored, and the respective treatment would be overdue, in which case it was the CRO's duty to question these same areas about the situation. With the new add-on, we could add two more steps to the control state machine as depicted in Figure 5.1.

- **Overdue**- Status where the controls should automatically pass when the expected implementation date was reached. The department responsible for it gets notified every day until the respective issue gets postponed.
- **Postponed**- Status that the issue should go through if the areas find that the control should be postponed to a later date than the first one established, going back to "Overdue" automatically if the date is once again reached.

With these extra steps, we were able to achieve the requirement **R4.11** concerning automatic transitions, and so, fulfill the entire Data Management Module.

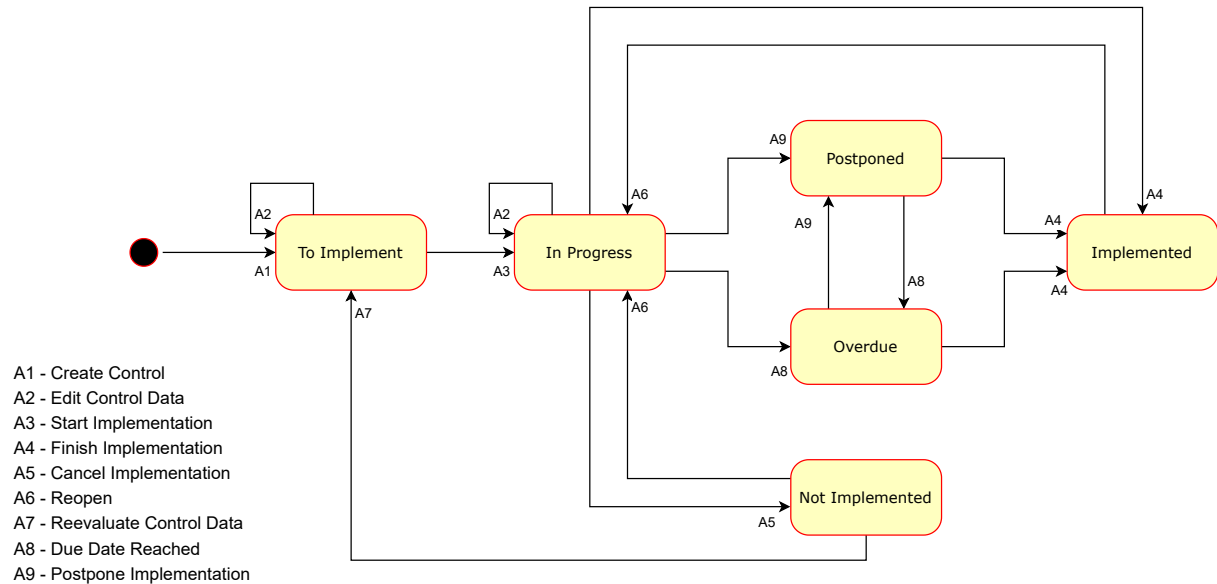


Figure 5.1: Final Control State Machine

Other subtle functionalities and patches could also be added to the platform to improve efficiency by reducing previously performed tasks with user intervention and making them automatic. However, these were not translated into solution requirements, as they were particularities that DPR aspired to have on the platform. One of the extra functionalities was creating a field named "days of delay" which had the sole purpose of incrementing automatically every day that an issue stayed in the "Overdue" status. This would provide an easier way to see how long a specific control stayed overdue and notify the responsible areas every day, compelling them to offer input or postpone the issue, which would later be very effective. If the control was postponed, this field would go back to zero, ceasing the notifications.

Another example is the "Eliminate" status that could now eliminate risks at the end of 30 days, avoiding unnecessary archives of irrelevant data.

5.2 Usage

JIRA supports risk assessment, treatment, recording and reporting, facilitating the communication between departments and allowing easier monitoring and reviewing. However, its effectiveness depends mainly on a scope, context, and criteria that the organization must previously define, as well as the corporate culture about risk management. Although it can help report and monitor each risk, opportunity, and control situation, the application cannot compel those responsible parties to answer for them. The

application is based on a workflow system not meant to create treatment plans or evaluate if a risk meets the acceptance criteria. These decision points are still needed to be evaluated and discussed outside of the application and are the sole responsibility of the CRO, the risk management team, and the department responsible for implementing the treatment plan. For that same reason, and since it is impossible to automate the process enough to execute it without human interaction, good training is still necessary, showing the advantages of the tool and how important it is to respond promptly and adequately to each scenario. Hence, its efficiency is also related directly to the quickness of response of each entity.

Risk assessment, review, and reporting are the stages of the ERM process mainly supported by this application. More than a remainder, JIRA let different entities access updated high-level information about their risks while letting the CRO and the risk management team act on them.

The entire structure of the application can be seen in the user manual presented in Appendix A. The manual will mention, step-by-step, how to create each issue type, assess risk, create and associate controls, and what is expected from the user.

5.2.1 Risk Assessment

Our application follows the process present in ISO/IEC 31000 [1], contemplating in the Risk Assessment stage, the Risk Identification, Analysis, and Evaluation. There are two perspectives, one from the department users; and another from the CRO and the DPR. The first ones should be responsible for identifying and analyzing the risk, and we should assume that they do not have any technical knowledge. Therefore, from their perspective, tasks must be simple, straightforward, and user-friendly since those are the main principles to avoid resistance to change. The second group of people are specialists in risk management and responsible for evaluating, monitoring, reviewing, recording, and reporting risks. They have a deep knowledge of the process, are familiar with the JIRA technology, and know how to act promptly to situations without needing help. Hence they can perform more complex tasks. For this reason, we decided to separate the two perspectives to make this section easier to read.

5.2.1.A Department's Perspective

To identify a risk, a user must access the application with their company credentials and press the Create button on the top panel just as a regular JIRA ticket.

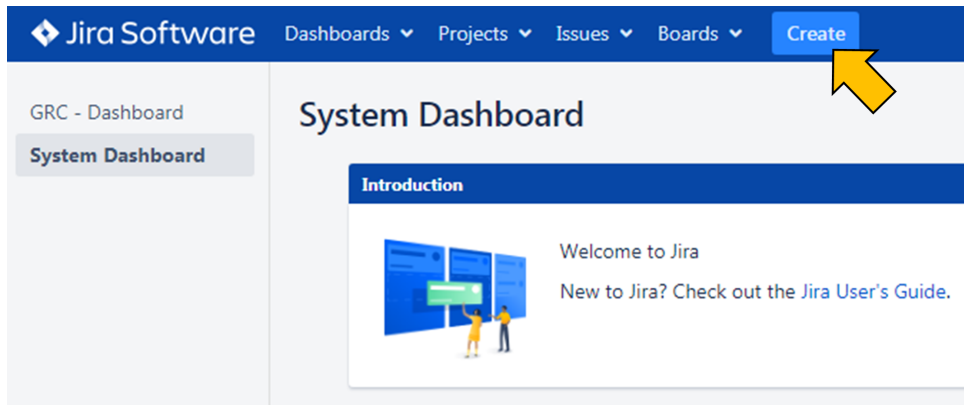


Figure 5.2: Creating a ticket

Then, the user will select the project "GR" and select the "Risk," "Opportunity," or "Control" issue type, depending on what they are trying to identify.

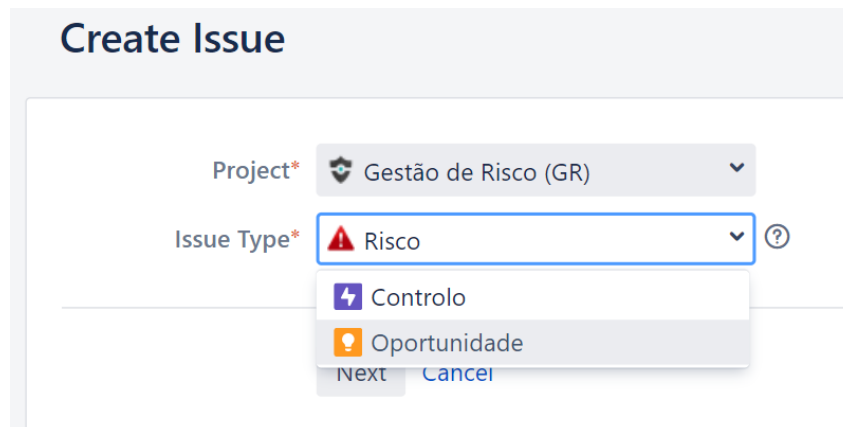


Figure 5.3: Defining the issue type

Let us consider that the user wants to identify a Risk or an Opportunity. In that case, the user needs to fill the fields mentioned on Table 5.1.

After this form is filled, a ticket is created, and the **Risk Identification** phase is considered complete. This step will notify the Organic Unit identified on the creation form to perform a risk analysis. The DPR and the CRO will also be notified for monitoring purposes, as they do not need to perform any obligatory actions.

Identification Field	Description
Summary	A generic name for the Risk/Opportunity
Risk Category	Category and Sub-category of the risk, defined by the company when the scope and criteria were established
Event	Event that led to the risk
Cause	Cause that led a certain event to happen
Consequence	Consequences of the event in the assets of the company
Risk Source	The reason we are identifying the risk, i.e., if an event occurred, if it is a compliance finding or a governance measure
Organic Unit	Department(s) responsible for the risk. This field will dictate which department should be notified to perform the analysis and track the risk.
E2E Processes	The company's operational process affected

Table 5.1: Risk Identification Fields

Figure 5.4: Risk Identified visualization

All relevant information filled in at the different stages of the process will be transcribed to the ticket as depicted in Figure 5.4. On the right, we have the process actors, such as reporter and assignee, and the creation and update dates of the ticket. Apart from the issue type and its status, the issue has three tabs in the middle. The default one is related to the identification phase, where we can see the identification fields, but also its risk level (since the risk demonstrated in Figure 5.4 is still in "Risk Identified" status, the risk level is still null until an analysis is performed). The second and the third ones are related to the risk analysis and should be empty until further progress.

From this point forward, the departments have two possibilities, correct the risk identification if

needed, or, if they identify their organic unit in the creation form, a button will appear to analyze the risk. By clicking it, the department will see a screen with new fields to fill, required to perform a correct risk analysis:

Analysis Field	Description
Likelihood	chance of the particular event happening again, calculated qualitatively and quantitatively
Effectiveness of prevention Controls	Effectiveness of the control(s) identified. Effectiveness must consider the quality of the control, its monitoring and its redundancy
Existing controls	A list of all existing controls related to this risk
Strategic Impact	Impact on strategy indicating which goals, indicators or objectives may be affected by the event
Operational Impact	Impact on operations indicating which processes or activities may be affected by the event
Financial Impact	Financial impact estimating the financial value that can be lost by the event
Reputational Impact	Impact on the company's reputation indicating the possible extent of the incident
Information Security(IS) Impact	Information security impact indicating which assets may be affected by the event
IS Asset Affected	Type of information security asset affected between confidentiality, integrity and availability, or a combination of those
Regulatory Impact	Regulatory impact indicating what laws, contractual goals or requirements may be affected by the event
Safety at Work Impact	Impact on safety at work estimating the possible losses of the event
Environmental Impact	Impact on the environment estimating the possible losses of the event

Table 5.2: Risk Analysis Fields

By submitting the form, the CRO and the DPR will be notified again, and the **Risk Analysis** ends. The status of the issue becomes "Risk Analyzed", the risk enters the evaluation phase, and the likelihood, impact, and effectiveness of prevention controls will be automatically used to calculate the maximum impact and derived loss likelihood. The technology, translates these two results into a risk level, which in turn will be present in the default tab in the details section, highlighted in different colors based on its value as previously shown in Figure 4.6. The third tab will show all impacts specified in Table 5.2 with the respective description and the maximum impact. On the other hand, the second tab will show the rest of the analysis data.

Identificação	Análise	Impacto
Categoria do Risco:	Danos Pessoais e	
Evento:	Inundação nas Á	
Causa:	Rutura de Canali	
Consequência:	Incapacidade de	
Fonte de Risco:	[Risco] Identifica	
Unidade Orgânica:	UGF - MPA, UMC	
Processos E2E:	Do Planeamento	
Estratégia de Tratamento:	Mitigar	
Nível de Risco Inerente:	3 - Moderado	
Nível de Risco:	3 - Moderado	

Identificação	Análise	Impacto
Probabilidade:	O evento ocorreu ou é previsível qu	Probabilidade
Eficácia do Controlo de Prevenção:	Controlo de prevenção inexistente	
Probabilidade da Perda Derivada:	2 - Baixa	

Identificação	Análise	Impacto
Impacto Estratégico:	Moderado - Impede o cu	cumprimento dos objetiv
Impacto Operacional:	Severo - Impacto severo	negócio
Impacto Financeiro:	Moderado - Impacto fina	
Impacto Reputacional:	Não Existente	
Impacto Segurança de Informação (SI):	Severo - Ativos de segur:	confidencialidade, integri
Pilar SI Afetado:	Disponibilidade do ativo	
Impacto Regulamentar:	Baixo - Ato isolado em in	das partes
Impacto Segurança no Trabalho:	Baixo - Lesões que requere	24horas)
Impacto Ambiental:	Moderado - Impacto aml	
Nível de Impacto:	5 - Severo	

Figure 5.5: An analyzed risk with a moderate risk level

 **Gestão de Risco / GR-398**
Inundação nas Áreas Produtivas

Details

Type: ▲ Risco
 Status: RISCO ANALISADO

Resolution: Unresolved
 Security Level: Confidencial

Identificação	Análise	Impacto
Categoria do Risco:	Danos Pessoais e Materiais - Inundação	
Evento:	Inundação nas Áreas Produtivas	
Causa:	Rutura de Canalização Falhas de Isolamento	
Consequência:	Incapacidade de Produzir Perda Material	
Fonte de Risco:	[Risco] Identificação de Risco	
Unidade Orgânica:	UGF - MPA, UMD - MPA	
Processos E2E:	Do Planeamento à Entrega	
Estratégia de Tratamento:	Mitigar	
Nível de Risco Inerente:	3 - Moderado	
Nível de Risco:	3 - Moderado	

Figure 5.6: An analyzed risk with a moderate risk level

On the example of Figure 5.6, we can see that the status of the risk has changed, and the risk level, represented in orange, has been set to **3-moderate**.

Unless the departments want to correct something from the previous data inserted, they will not have to perform any more tasks. From this moment on, the risk will enter the evaluation phase meaning that

no one except DPR or the CRO can transit the issue. However, the evaluation phase is not translated into a new status but into a "zone" where only these two have access and can manage the information inside, while trusted parties can watch the progress.

5.2.1.B CRO's Perspective

The CRO have now a decision point between the four statuses left in the Workflow: Eliminate, Control Monitorization, Risk Closed, and Risk Controlled. He can deliberate if the previously analyzed risk is redundant or mistaken, sending it to the **Eliminate** status, which will notify the responsible parties with the reason to do so, and delete it after 30 days. If the risk can be avoided, the CRO will define the treatment strategy field to "avoid" and the issue will be passed to the **Risk Closed** status. If the risk is not within the acceptable level, it means it will need some controls to mitigate it. In that case, the CRO will pass it to **Control Monitorization** as Figure 5.7 shows, identifying the group responsible for implementing the control, notifying them, and defining the treatment strategy field to "mitigate", meaning that the risk entered the **treatment** phase.




The screenshot shows a risk management interface. At the top, there is a breadcrumb "Gestão de Risco / GR-525" and a title "Incapacidade de realizar ensaios fiáveis". Below the title, there are several action buttons: "Edit", "Comment", "Assign", "More", "Controlo Implementado", and "Admin". A "Details" section is expanded, showing the following information:

Type:	▲ Risco	Status:	MONITORIZAÇÃO DE...
		Resolution:	Unresolved
		Security Level:	Confidencial

Figure 5.7: A risk in control monitorization waiting for treatment

The issue will stay in this status until a control is implemented to mitigate it. When that happens, the CRO should transition it back to **Risk Analyzed** by clicking the button "Implemented Control", which will oblige him to perform a reevaluation of the risk, reformulating the values present in Table 5.2, reducing the risk level automatically. When the risk reaches an acceptable level, usually a low or very low level, always depending on the CRO assessment, he will change the treatment strategy to "accept" move it to the **Risk Controlled** status as depicted in Figure 5.8.

▼ Details

Type:  Risco

Status: **RISCO CONTROLADO**

Resolution: Resolved

Security Level: **Confidencial**

Identificação **Análise** **Impacto**

Categoria do Risco: Danos Pessoais e Materiais - Incêndio

Evento: Incêndio nas Áreas de Produção

Causa: Elétrica Presença de Materiais Inflamáveis

Consequência: Incapacidade de Produzir Perda Humana e Material

Fonte de Risco: [Risco] Identificação de Risco

Unidade Orgânica: UGF - MPA, UMD - MPA

Processos E2E: Do Planejamento à Entrega

Estratégia de Tratamento: Aceitar

Nível de Risco Inerente: 2 - Baixo

Nível de Risco: 2 - **Baixo**

Figure 5.8: A risk already controlled

5.2.2 Risk Treatment

Generally, the treatment phase is triggered by some risk that enters in "Control Monitorization" status. The department identified by the CRO will receive an email with all the information needed to develop a control plan to mitigate the desired risk. JIRA should act as a pillar of information in this case, where the department must insert all the planning it intends to do to inform interested parties. In this way, the monitoring can be constant, and it will not be necessary to question the areas unless some delay arises that requires justification. When a user wants to identify a control that is meant to be implemented, it must press the Create button in the top panel and pick the "Control" as an issue type as we did with the risk and fill the fields mentioned in Table 5.3. In addition, there is another way to create a control by going directly into the risk that needs to be treated and select "Create Linked Issue", this will show the same fields, but the risk will be already linked, facilitating the form filling.

Control Field	Description
Summary	A generic name for the Risk/Opportunity
Linked Issues	Field to link the risk(s) that should be treated by this control
Organic Unit	Department(s) responsible for implementing the control. This field will dictate which department should be notified to implement and track any updates on the issue
Description	Detailed description of what is meant to be done

Table 5.3: Risk Identification Fields

By finally clicking on create, the control stays on "To Implement" status, until a person from the department identified in the organic unit field starts to implement it, defines it as implemented, or cancels it.

The screenshot displays a web interface for risk management. At the top, it shows 'Gestão de Risco / GR-606' and the title 'Relatório de Avaliação de Documentação Acumulada'. Below the title is a navigation bar with buttons for 'Comment', 'Assign', 'More', 'iniciar implementação', 'corrigir controlo', and 'Workflow'. The main content area is divided into sections: 'Details', 'Attachments', and 'Issue Links'. The 'Details' section shows the control type as 'Controlo', status as 'PARA IMPLEMENTAR', resolution as 'Unresolved', and security level as 'Confidencial'. The responsible group is 'UCF - MPA'. The 'Attachments' section is empty, and the 'Issue Links' section shows a link to a risk item 'GR-605 Contra Ordenação por Indevido Cumprimento de Reten...' with a 'MONITORIZAÇ...' status.

Figure 5.9: Control to be implemented, with a risk associated

In Figure 5.9 we can see the status of the issue, its type, the data filled in the previous form, and on the bottom, we have the linked risks that this control should mitigate.

When the user wants to start the progress, it will need to press on "start implementation", this will ask the user to select an expected due date. The issue stays in "In Progress" status until it finishes or a user cancels its implementation.

The screenshot displays a web interface for risk management, similar to Figure 5.9. The navigation bar now includes 'corrigir controlo', 'planeado', and 'Workflow'. The 'Details' section shows the control type as 'Controlo', status as 'EM PROGRESSO', resolution as 'Unresolved', and security level as 'Confidencial'. The responsible group is 'UCF - MPA'. The 'Issue Links' section is not visible in this view.

Figure 5.10: Example of a control in progress

Suppose the control reaches the due date established. In that case, the control passes automatically to "Overdue" status, which, as said earlier, will notify the responsible area every day, as exemplified in Figure 5.11, until they change its implementation date by pressing the "postpone" button or closing it by setting it as "Implemented".

There are **2 updates**.

Gestão de Risco / GRCT-55 **ADIADO**

Stock de Passaportes e Chips

[View issue](#) · [Add comment](#)

2 updates

Changes by **Miguel Silveira** on 27/Jan/20 11:23 AM

Dias de Atraso: 0

Status: **Adiado** Atrasado

Figure 5.11: Example of an email of an overdue control

Gestão de Risco / GR-186

Código de Ética e Conduta

Edit Comment Assign More reabrir controlo Admin

Details

Type: **Controlo** Status: **IMPLEMENTADO** (View Workflow)

Resolution: Done

Security Level: **Confidencial**

Grupo Responsável: DDP - MPA

Pelo Controlo:

Qualidade de Controlo: 3

Monitorização de Controlo: 3

Avaliação de Controlo: 3

Eficácia do Controlo %: 100

Figure 5.12: Example of an implemented control

When the area finishes the control implementation, besides the status, three fields are automatically set to their maximum value: Control Quality, Control Monitoring, and Control Evaluation. These dictate the efficiency of the representative control and can be edited if the area so desires. Then, every associated issue will have this particular control marked on its key as shown in Figure 5.13.

Issue Links	
é controlado por	
GR-100 Manutenção Preventiva	IMPLEMENTADO
GR-101 Sistema de Gestão de Edifícios (BMS)	IMPLEMENTADO
GR-102 Contrato de Manutenção com Fornecedor	IMPLEMENTADO

Figure 5.13: Implemented controls are marked in every link they have

5.2.3 Review and Reporting

On the Risk Management Dashboard, as stated in the previous section, you can find all the information about the project: maps, graphs, tables, and filters with relevant information about the tasks present in the project. The dashboard, shown in the user manual present in Appendix A, was fully configured based on the representation wanted and data to be shown, adapted to this project's needs.

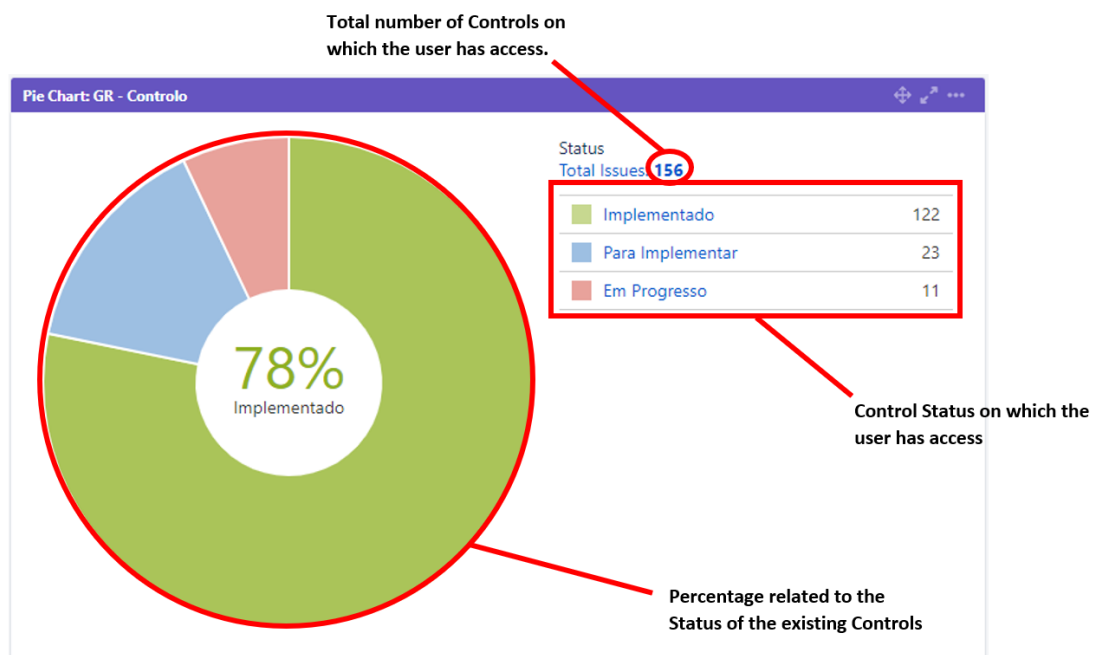


Figure 5.14: Control status pie-chart

By analyzing the previous dissertation made on Reporting and communication of the Risk Management process in INCM [2], we found that most of the information present in their solution proposal cannot be applied directly to JIRA. Especially in terms of timeline tracking, shown earlier to be a limitation that is not built-in and needs an extra add-on to do so. On the other hand, the tool is meant to ease access to the current situation of risks, opportunities, or controls. That's what is expected to get in the end.

Figure 5.14 shows the first chart of the dashboard. This chart presents the controls quantitatively in terms of their status. However, it will not appear equally to every user since it will only show the

controls in which the user's department was held responsible. The chart provides some interactivity by highlighting each section of the wheel on mouse-over, referring to a particular status, and show the respective percentage in the middle concerning the total number of controls to which the user has access. By clicking the wheel or the labels on the right, the application redirects to a list of every control in that particular status, filtering and offering more details about them.

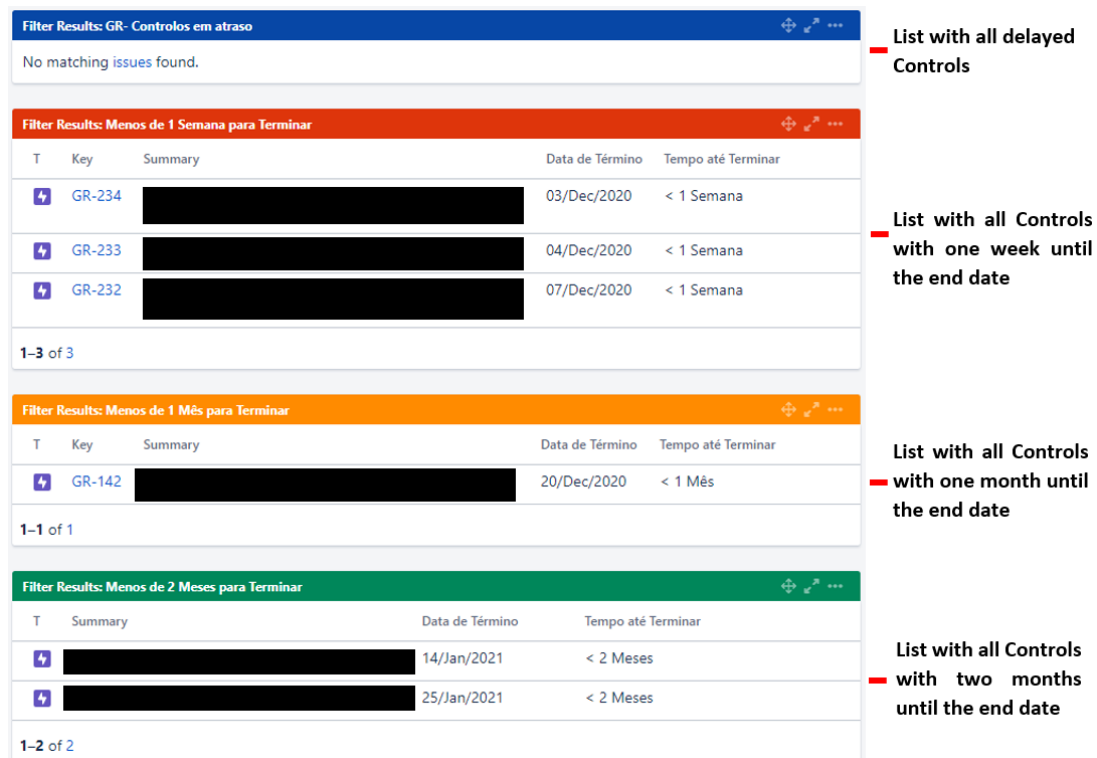


Figure 5.15: Time concerning tables

On Figure 5.15 there are four tables concerning the application's controls. The first table lists every control in the Overdue status, meaning that those particular controls' due date has been reached. As mentioned previously, each of these issues should send a notification every day until the control gets implemented or postponed, thus leaving the table. The table presents the control's key, summary, due date, and overdue days. The tables in red, yellow, and green represent the time until it reaches the control's due date, one week, one month, and two months respectively. As the controls get closer to the due date, they enter these tables, notifying their responsible parties. Each table shows the summary, due date, and time left until the due date.

Concerning Risks, Figure 5.16 shows a table that crosses the risk statuses with their risk level. The lines should represent every risk level shown previously on the organizational ERM framework in Figure 3.5. The line in gray "Não Analisado"(Not Analyzed) means that seven days have passed since its creation, and the risk owner did not analyze it. The columns represent every risk status on the

application. In the case shown, there are no identified risks because everything is either analyzed or controlled. This table is also interactive by clicking on the numbers shown, which will automatically redirect to a filtered list with more detailed information about them. The user can gather information about the progress of certain risks while evaluating their severity and evaluating the most common patterns.

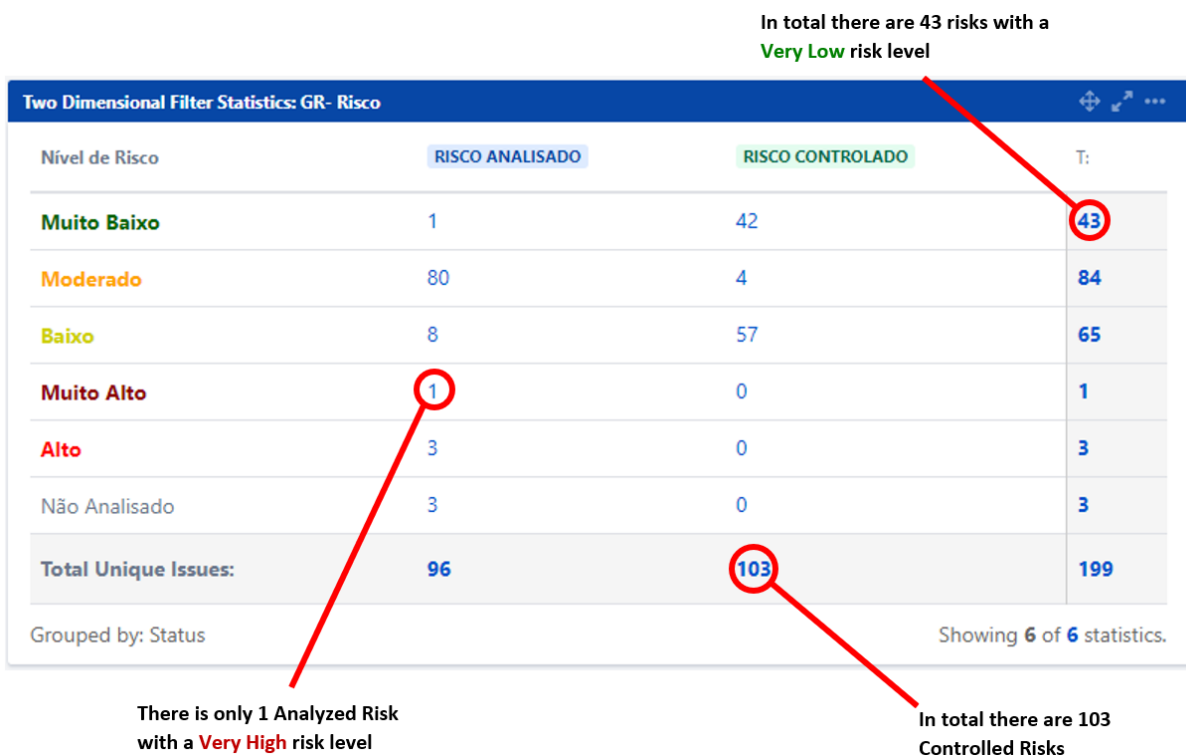


Figure 5.16: Cross table with risk level and status

The table shown in Figure 5.17 shows the percentage of treatment plans chosen for every risk. From this table, it can be concluded that the most used treatment strategy is acceptance; five risks are waiting to be controlled, and one risk to be transferred. However, precisely 90 risks do not have a treatment plan yet, meaning that these risks have not been evaluated.

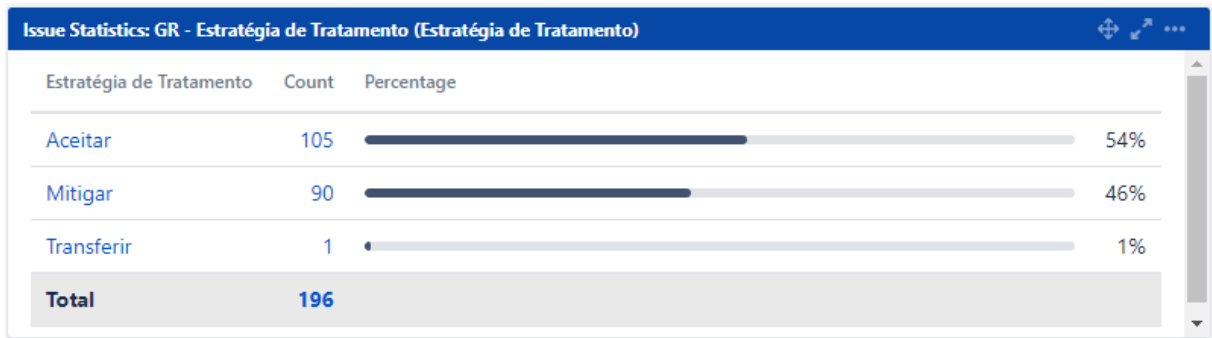


Figure 5.17: Risk treatment table

6

Evaluation

Contents

6.1 Method	76
6.2 Analysis of the Results	77
6.3 Discussion	80

After numerous tests and reviews with the CRO about our application's functionality, it was finally time to deploy the developments made on the production server to test its usability and efficiency with the real future users: risk owners, project managers, and risk managers. Since we cannot perform these testings outside of the organization's environment due to confidentiality and data protection, the results are not being represented on a large scale, being limited to the people responsible for identifying, analyzing, and evaluating risks, that are, in fact, the most meaningful opinions and must be considered.

This section shows the method used to evaluate the answers, the results, and overall opinion of the users, that, should be considered for future adjustments on the application if necessary.

6.1 Method

In order to evaluate the efficiency and how intuitive the application was, we scheduled usability tests with the users mentioned earlier, from different departments within the organization, with different responsibilities, but all related to the risk management process that existed in INCM.

These usability tests involved eight tasks that were carried out with the user manual's help in Appendix A. In Appendix B, we can observe the script of those same tests and each task's content.

We decided to follow an evaluation method to guide us in what questions should we make and have a quantitative way to estimate whether the tool was efficient without requiring too much information from the users. For that reason, we chose the System Usability Scale (SUS). John Brooke invented the System Usability Scale in 1986 to evaluate practically any kind of system. This system has been tested ever since and has proven itself to be a meaningful method for evaluating usability and user experience compared to other standards. [7]

The SUS is based on a Likert Scale that includes ten questions for users to answer and could be applied to every software, application, or website developed. The users must rank each question from **1 to 5** based on the statement mentioned, **5** meaning they **completely agree** and **1** that they **totally disagree**.

The system offers ten pre-built questions that should be adapted depending on the language, complexity, and type of software:

1. I think that I would like to use this system frequently.
2. I found the system unnecessarily complex.
3. I thought the system was easy to use.
4. I think that I would need the support of a technical person to be able to use this system.

5. I found the various functions in this system were well integrated.
6. I thought there was too much inconsistency in this system.
7. I would imagine that most people would learn to use this system very quickly.
8. I found the system very cumbersome to use.
9. I felt very confident using the system.
10. I needed to learn a lot of things before I could get going with this system.

After answering these questions with ranks between 1 to 5, the results must be calculated to offer a proper evaluation scale.

- For each of the **odd-numbered questions**, we need to subtract 1 from the score.
- For each of the **even-numbered questions**, we need to subtract their value from 5.
- Sum all of these values, and **multiply the final number by 2,5**.
- Calculate the average of the total value of all users.

Although it does not provide a qualitative analysis of what went wrong with the solution developed, it gives us a score out of 100 to evaluate how badly our application needs rearrangements.

The average System Usability Scale score is 68. The following values represent the scale:

- ≥ 80.3 - Users are pleased with the development made and will recommend it to their peers.
- ± 68 - The application needs adjustments since it does not fulfill the user's needs.
- ≤ 51 - Usability is low, and the application needs to be fixed or rearranged.

At the end of the survey, we wanted to know the details about the challenges that users faced, their difficulties, what could be improved, and if, in fact, they could carry out their duties related to risk management in the proposed application. Other questions were related to the tool's familiarity since some of the challenges could arise because users are not used to the JIRA software itself, not because of the application developed. Therefore, it would also help to know if JIRA is intuitive enough for people that never looked at it in the first place.

6.2 Analysis of the Results

This evaluation was performed with the collaboration of sixteen volunteers. As mentioned earlier, all volunteers were INCM employees and were related to the organization's risk management process somehow.

SUS Questions	Average Values
1 - I think that I would like to use this system frequently.	4
2 - I found the system unnecessarily complex.	1
3 - I thought the system was easy to use.	5
4 - I think that I would need the support of a technical person to be able to use this system.	2
5 - I found the various functions in this system were well integrated.	4
6 - I thought there was too much inconsistency in this system.	2
7 - I would imagine that most people would learn to use this system very quickly.	4
8 - I found the system very cumbersome to use.	2
9 - I felt very confident using the system.	4
10 - I needed to learn a lot of things before I could get going with this system.	1

Table 6.1: SUS average values for each question

We have evaluated the ten template questions mentioned for the SUS, and the results were straightforward. The SUS scores ranged from **57,5 to 100**, and we reached an **average score of 83,9**, meaning that the application's general opinion was **adequate** and the implementation was **successful**. A more in-depth analysis made us realize that lower scores were often related to the lack of JIRA usage or the lack of people's technical knowledge, but even then, no score was lower than 51, which means that for the generic users, there may be some adjustments to make in order to meet their needs. This problem could also be related to the organization's culture, where the resistance to change is a recurrent issue when dealing with dematerialization processes, as mentioned by some of our volunteers.

Other questions were asked about the difficulty of the tasks, and the user experience when realizing the activity. The results about this section of the questionnaire are shown in Figure 6.1.

On the first question, we evaluated the intuitiveness of the tasks performed, and the opinion was consensual by 56% of the volunteers rating a 5 and 44% rating a 4 out of 5. On the second question, we evaluated if the user manual was useful for realizing the entire activity. 62,5% completely agree that the manual was useful, 25% rated a 4, and only 12,5% rated a 3 out of 5. This is probably due to the fact that some people did not need to look at the manual to reach the objective since some of them already knew how to deal with JIRA, or reached it by trial and error.

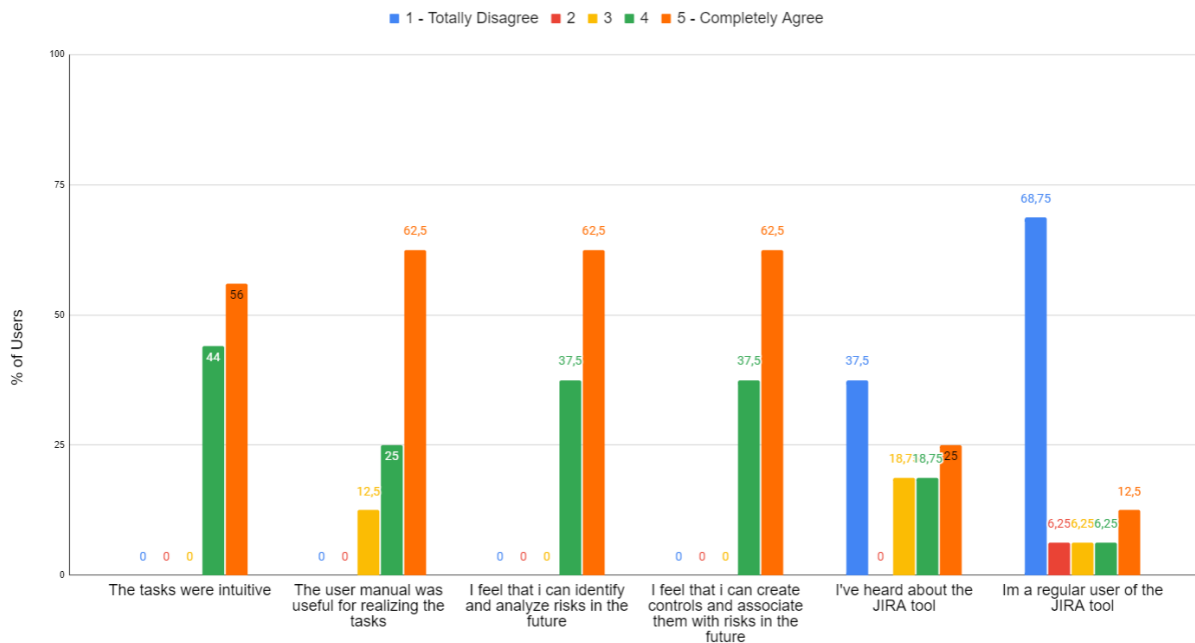


Figure 6.1: Questionnaire 2nd part results

On the third and fourth question, we asked if the users felt that they could identify risks and controls and perform related tasks independently. Both questions had the same results by having 62,5% of the volunteers agreeing that they could, in fact, do it autonomously in the future, and 37,5% rating a 4 out of 5.

Finally, on the last two questions, users needed to mention the familiarity with the JIRA software. In general, most of the volunteers never heard about JIRA, having 37,5% of the volunteers rating a 1 out of 5, and 68,75% also completely disagreeing when questioned about being a regular user of JIRA. Although these last two questions may, at first sight, indicate that the tool is not mature on INCM yet, it shows us that even people who are not experienced with it can perform risk management activities without effort.

Regarding future improvements or necessary adjustments, users showed some difficulties when accessing the dashboard to gather data. Even some experienced users had some trouble to find where the dashboard could be. As soon as they confirmed the dashboard as "favorite," they had no trouble reaccessing it. This challenge is not solvable by any of our developments since the system controls it. We can conclude that the "bridge" between projects and the dashboard data could be slightly simplified, although, with experience and marking the dashboard as the favorite, the learning curve decreases significantly.

The last question tried to evaluate if the users considered the application as an added value to the INCM's risk management process. The question was rated from 0 to 10, being 0 - It will not improve

at all, and 10 - Will improve substantially. As we can see in Figure 6.2, all the results are equal or higher than 7. The opinions were tied between 8 and 10 by 37,5% of the volunteers, concluding that the participants consider it a significant improvement to the organization's existing process, which was precisely our objective.

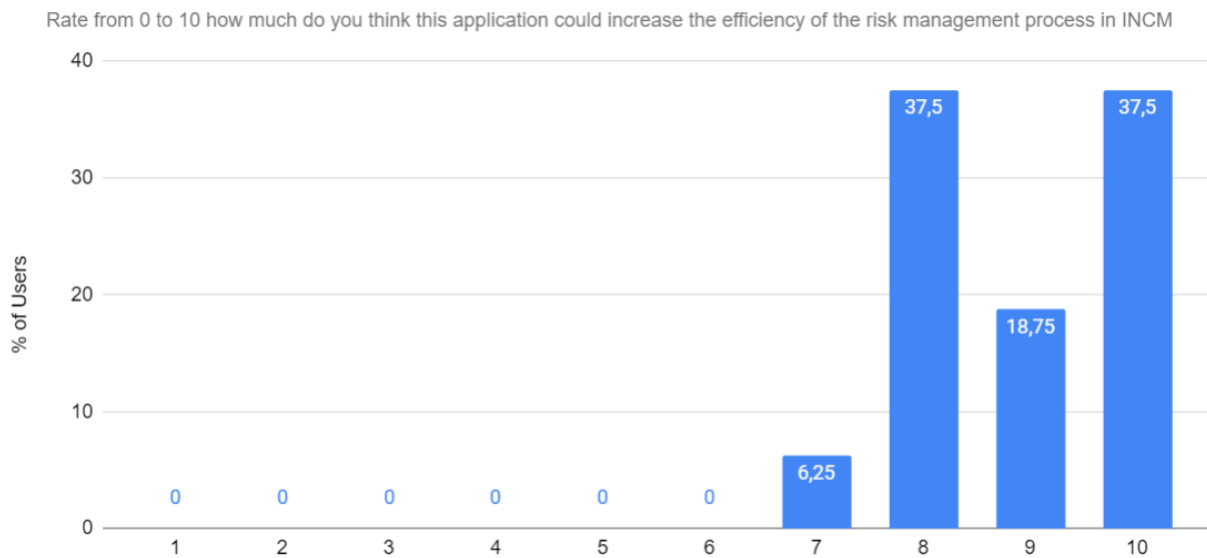


Figure 6.2: Efficiency Improvement Questionnaire

6.3 Discussion

Concluding this evaluation, we found interesting data about our developments.

The overall opinion about the application was positive, although there is room for improvements regarding dashboards and reporting. As we mentioned in the previous chapter, JIRA has some limitations when providing relevant data to users, especially if the process is not software development-based. These limitations proved themselves when testing the dashboard applicability by asking the users to gather data from it. However, these difficulties arose very subtly and were easily overcome by searching the user manual.

Lastly, we found out from the questionnaire that even though most people did not have experience with the tool, they could perform every task. The questionnaire also proves that the manual was a vital variable for achieving the activity's success, and without it, the results would probably not be satisfactory. By meeting most of the requirements created, achieving a high score on the SUS, and getting favorable opinions from the end users, we can denote this implementation as a success in INCM's context.

7

Conclusions and Future Work

Contents

7.1 Conclusions	82
7.2 Future Work	83

7.1 Conclusions

Over the last decades, ERM has been changing, and more complex frameworks have been built to aggregate new company elements that were not previously considered, such as performance, objectives, and mainly strategy setting. This change made several organizations implement new methods to accomplish higher performance and gain a competitive advantage in their markets.

Despite the several normative references, acceptable practices, and frameworks like ISO/IEC 31000, COSO ERM Framework, there is no clear consensus on how risk management systems should be implemented. For this reason, multiple solutions have emerged on the market that, despite serving the same purpose, have distinct features and functionalities that often force organizations to adapt their own ERM processes instead of the other way around.

This dissertation brings a list of functional requirements that are intended to mitigate precisely this problem, generic enough to be used in multiple corporate contexts and markets. In addition, using the INCM use case, which sought to dematerialize its ERM process into a flexible tool but not documented for risk management, we could transpose the requirements created into a solution that satisfied both the identified need for ERM platforms and the challenge of INCM, analyzing the quality of the requirements built.

The tool chosen by the organization was JIRA that already had proven its value in numerous contexts and situations inside the organization when managing work. Despite not having much knowledge of being used in risk management procedures, the tool was expected to be flexible enough to meet the requirements necessary to build a risk management tool. Since this was not taken for granted, its viability was also part of the problem we accepted to research and explore its capabilities and functionalities in-depth.

After analyzing ERM processes and the tool's limitations and capabilities we used the requirements created to reach a solution that suffered several improvements over the months and went through various iterative developments to reach an acceptable level based on the INCM's objectives. Since some of the limitations were "deal-breakers", its accomplishment needed an extra add-on that facilitated every automated mechanism that the process needed. Although it may not be a suitable tool for this purpose, JIRA managed to meet the vast majority of proposed requirements and organization needs, except for those related to export capabilities, which had been identified as one of the main limitations of the tool used.

The feedback from the volunteers that performed the usability tests was very positive. Every task was completed successfully by each user, and, in general, people found the tool to be an added value and an excellent improvement for the risk management process and the organization itself. The results have shown that even people with no technical knowledge or experience with the software could work on the application and perform what was asked. These developments also materialized in a user manual

that the users found very useful to accomplish their objectives.

We concluded that our list of requirements for ERM solutions was a success, having managed to implement a system of this complexity in the JIRA tool from scratch. JIRA could **effectively provide a practical platform to assess treat, and communicate risks** within the entire organization, **covering all business scopes, capable of offering crucial information to act adequately and timely to future risks.**

7.2 Future Work

There are still developments to be done and functionalities that would be interesting to find implemented. The functional requirements described were not all met. **R6.4** concerning metadata exporting was not directly achieved, as there were timestamps and user information that was not possible to be exported, failing to meet this requirement. **R6.7** and **R6.8** related to timeline and history tracking also could not be implemented. This requirement involved functionalities that the base version of JIRA software could not provide. This possibility would increase the value that the dashboards could offer by giving stakeholders the possibility to find the **evolution of a single risk over time.**

Reporting and Communication could also be improved. This issue has been shown to impact strategy setting and decision-making the most, and the theoretical research made on previous dissertations on the organization about this topic could not be fully implemented.

It should be interesting to evaluate the **process's performance** with the developed application outside of a testing scope since performance plays a significant part in the ERM methodology and should be considered.

It would also be interesting to test our functional requirements on a brand new software, developing it from scratch instead of adapting an already built tool. In this way, it would be possible to obtain information on whether the list was sufficient to meet all the needs of an organization or whether it would be necessary to adapt or include new modules to these requirements.

Bibliography

- [1] ISO/IEC, “ISO/IEC 31000:2018, Risk Management Guidelines,” International Organization for Standardization, International Standard ISO/IEC 31000:2018, February 2018.
- [2] J. Santos, Guilherme; Borbinha, “Enterprise risk management - risk communication and consultation,” Master’s thesis, Instituto Superior Técnico, 2018.
- [3] M. S. Beasley, “What is Enterprise Risk Management?” *Enterprise Risk Management Insights*, 2016.
- [4] PwC, “Enterprise Risk Management - Integrating with Strategy and Performance,” Committee of Sponsoring Organizations of the Treadway Commission, Tech. Rep., 2017.
- [5] ISO/IEC, “ISO/IEC 9001:2015, Quality Management Systems - Requirements,” International Organization for Standardization, International Standard ISO/IEC 9001:2015, 2015.
- [6] J. R. Lewis, “The system usability scale: Past, present, and future,” *International Journal of Human–Computer Interaction*, vol. 34, no. 7, pp. 577–590, 2018. [Online]. Available: <https://doi.org/10.1080/10447318.2018.1455307>
- [7] A. Bangor, P. T. Kortum, and J. T. Miller, “An empirical evaluation of the system usability scale,” *Intl. Journal of Human–Computer Interaction*, vol. 24, no. 6, pp. 574–594, 2008.
- [8] P. Hopkin, *Fundamentals of Risk Management*, 5th ed. IRM, 2018.
- [9] R. Ross, “Risk management framework for information systems and organizations: A system life cycle approach for security and privacy,” National Institute of Standards and Technology, Tech. Rep., 2018-12-20 2018.
- [10] N. Gatzert and M. Martin, “Determinants and value of enterprise risk management: Empirical evidence from the literature,” *Wiley-Blackwell: Risk Management & Insurance Review*, 2015.
- [11] R. E. Hoyt and A. P. Liebenberg, “The value of enterprise risk management,” *Journal of Risk and Insurance*, vol. 78, no. 4, pp. 795–822, 2011. [Online]. Available: <https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1539-6975.2011.01413.x>

- [12] D. L. Olson and D. Wu, *New frontiers in enterprise risk management*. Springer Science & Business Media, 2008.
- [13] A. Yazid, M. Hussin, and W. Norhayate, "An examination of enterprise risk management (erm) practices among the government-linked companies (glcs) in malaysia," *International Business Research*, vol. 4, 09 2011.
- [14] P. Saeidi, S. P. Saeidi, S. Sofian, S. P. Saeidi, M. Nilashi, and A. Mardani, "The impact of enterprise risk management on competitive advantage by moderating role of information technology," *Computer Standards & Interfaces*, vol. 63, pp. 67–82, 2019.
- [15] S. Ahmad, C. Ng, and L. A. McManus, "Enterprise risk management (erm) implementation: Some empirical evidence from large australian companies," *Procedia - Social and Behavioral Sciences*, vol. 164, pp. 541 – 547, 2014, international Conference on Accounting Studies 2014, ICAS 2014, 18-19 August 2014, Kuala Lumpur, Malaysia. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S1877042814059643>
- [16] J. R. Fraser and B. J. Simkins, "The challenges of and solutions for implementing enterprise risk management," *Business horizons*, vol. 59, no. 6, pp. 689–698, 2016.
- [17] ISO/IEC, "ISO/IEC 27005:2018, Information Security Risk Management," International Organization for Standardization, International Standard ISO/IEC 27005:2018, 2018.
- [18] COSO, "Enterprise risk management-integrated framework," *Committee of Sponsoring Organizations of the Treadway Commission*, vol. 2, 2004.
- [19] E. Demidenko and P. Mcnutt, "The ethics of enterprise risk management as a key component of corporate governance," *International Journal of Social Economics*, vol. 37, pp. 802–815, 08 2010.
- [20] D. Williamson, "The coso erm framework: a critique from systems theory of management control," *International Journal of Risk Assessment and Management*, vol. 7, no. 8, pp. 1089–1119, 2007.
- [21] R. Vieira, *Framework de gestao de riscos corporativos (restricted)*, Imprensa Nacional Casa da Moeda, November 2018.
- [22] J. Ciervo, S. C. Shen, K. Stallcup, A. Thomas, M. A. Farnum, V. S. Lobanov, and D. K. Agrafiotis, "A new risk and issue management system to improve productivity, quality, and compliance in clinical trials," *JAMIA open*, vol. 2, no. 2, pp. 216–221, 2019.
- [23] J. Fisher, D. Koning, A. Ludwigsen *et al.*, "Utilizing atlassian jira for large-scale software development management," in *14th International Conference on Accelerator & Large Experimental Physics Control Systems (ICALEPCS)*, 2013.

- [24] R. Marques, G. Costa, M. M. da Silva, D. Gonçalves, and P. Gonçalves, "Using gamification for adopting scrum in practice," in *27th Int. Conf. Inf. Syst. Dev*, 2018.



Risk Management User Manual

Gestão de Risco

MANUAL DE UTILIZADOR

2

Índice

Introdução	3
1. Dashboard	3
2. Risco	10
2.1 Como criar um risco	10
2.2 Como editar um risco	13
2.3 Como analisar um risco?	14
2.4 Fluxo de Trabalho de Risco (Workflow)	17
3. Oportunidade	18
4. Controlo	19
4.1 Como criar um controlo	19
4.2 Como editar um controlo	22
4.3 Como associar um controlo a um risco	23
4.4 Transições de Controlo	24
4.4.1 Como iniciar a implementação?	24
4.4.2 Como concluir/cancelar a implementação?	25
4.4.3 Como adiar a implementação?	26
4.4.4 O que fazer quando o controlo está atrasado?	27
4.5 Fluxo de Trabalho de Controlo (Workflow)	28
5.1 – Recebi um email com um Risco em estado de “Monitorização de Controlo”	29
5.3 – Recebi um email com um Controlo em estado de “Atrasado”	31

Introdução

Esta documentação visa oferecer o conhecimento necessário para a utilização da ferramenta Jira, no âmbito da gestão de risco, seguindo o processo descrito no framework do PA18. Nas próximas secções são apresentados detalhadamente os temas relevantes para a utilização da ferramenta.

Siga este link para aceder ao processo : <http://jira.incm.pt/projects/GR>

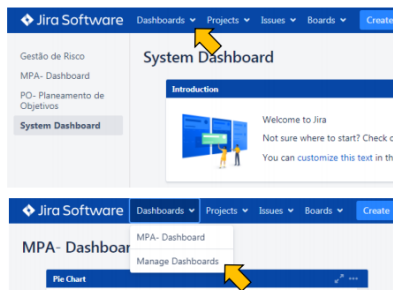
Para dúvidas ou qualquer outra questão que tenha, contacte dpr@incm.pt

1. Dashboard

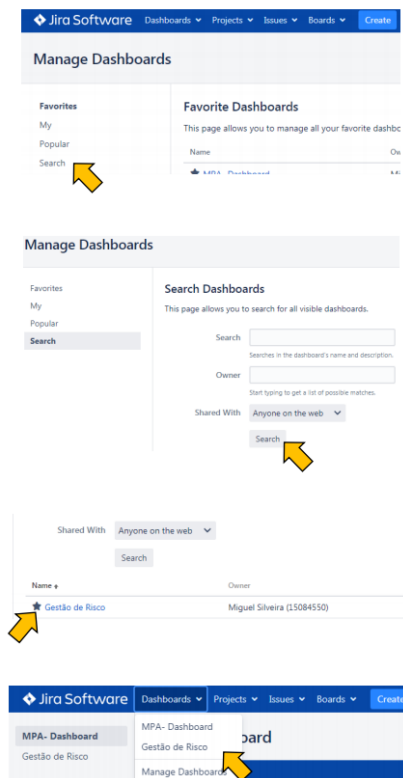
No Dashboard da Gestão de Risco poderá encontrar toda a informação sobre o projeto, podendo visualizar mapas, gráficos, tabelas e filtros com informações relevantes sobre as tarefas presentes num ou mais projetos. Estes dados são totalmente configuráveis a nível de design, tipo de representação e dados escolhidos a serem representados, podendo adaptar-se às necessidades de cada projeto ou utilizador.

As permissões para cada dashboard poderão ser definidas, dando ou restringindo o seu acesso a vários utilizadores, singularmente ou dependendo do seu papel e grupo na ferramenta. Para esta visualização deverá seguir os seguintes passos:

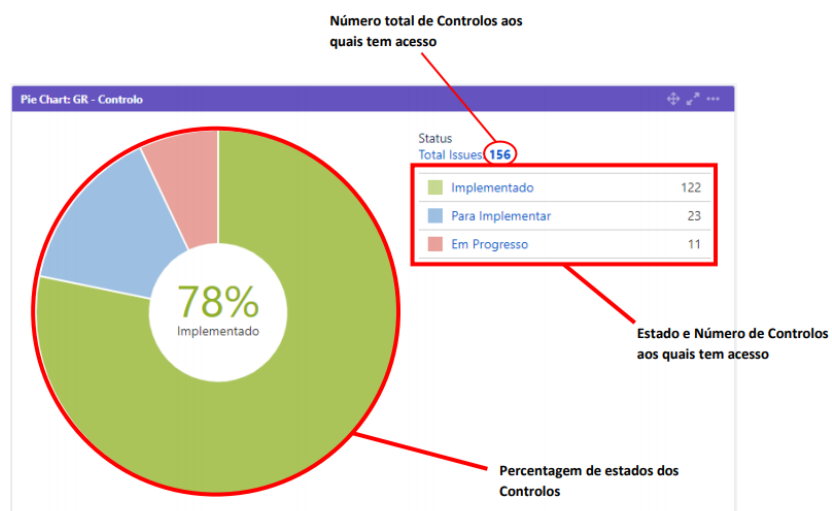
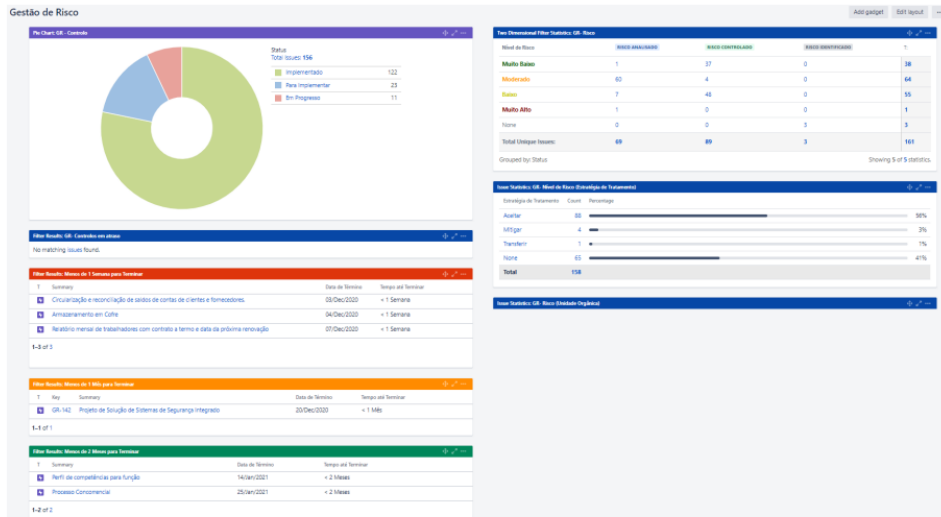
Dashboard -> Manage Dashboards -> Search -> Search -> Gestão de Risco -> Favorito



4



Terá então acesso às tabelas e estatísticas dos riscos que identificou e aos controlos criados pela sua UO, e qualquer caso que lhe tenha sido designado. Vamos ver com mais atenção:



Este é um gráfico de percentagens referente aos estados dos controlos sobre os quais foi identificado como responsável. Se pretender abrir a lista de controlos respetivos de cada segmento, basta carregar numa das secções da roda e escolher *View in Issue Navigator*.

Lista de todos os controles em atraso

Filter Results: GR- Controles em atraso				
No matching issues found.				
Filter Results: Menos de 1 Semana para Terminar				
T	Key	Summary	Data de Término	Tempo até Terminar
	GR-234	[REDACTED]	03/Dec/2020	< 1 Semana
	GR-233	[REDACTED]	04/Dec/2020	< 1 Semana
	GR-232	[REDACTED]	07/Dec/2020	< 1 Semana
1-3 of 3				
Filter Results: Menos de 1 Mês para Terminar				
T	Key	Summary	Data de Término	Tempo até Terminar
	GR-142	[REDACTED]	20/Dec/2020	< 1 Mês
1-1 of 1				
Filter Results: Menos de 2 Meses para Terminar				
T	Summary	Data de Término	Tempo até Terminar	
	[REDACTED]	14/Jan/2021	< 2 Meses	
	[REDACTED]	25/Jan/2021	< 2 Meses	
1-2 of 2				

Lista de todos os controles a uma semana de terminar o prazo

Lista de todos os controles a um mês de terminar o prazo

Lista de todos os controles a dois meses de terminar o prazo

Nesta tabela poderá encontrar o número de Riscos aos quais o seu departamento tem acesso divididos por Nível de Risco e Estado de Risco

Existem no total 38 Riscos com um nível de risco **Muito Baixo**

Two Dimensional Filter Statistics: GR- Risco				
Nível de Risco	RISCO ANALISADO	RISCO CONTROLADO	RISCO IDENTIFICADO	T:
Muito Baixo	1	37	0	38
Moderado	60	4	0	64
Baixo	7	48	0	55
Muito Alto	1	0	0	1
None	0	0	3	3
Total Unique Issues:	69	89	3	161

Grouped by: Status

Showing 5 of 5 statistics.

Existe 1 Risco apenas com um nível de risco **Muito Alto** e no estado Analisado

Existem 3 Riscos que foram Identificados mas ainda não foram Analisados

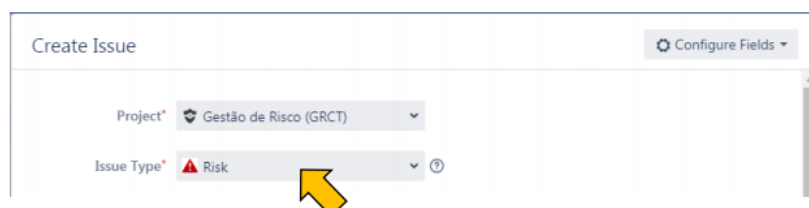
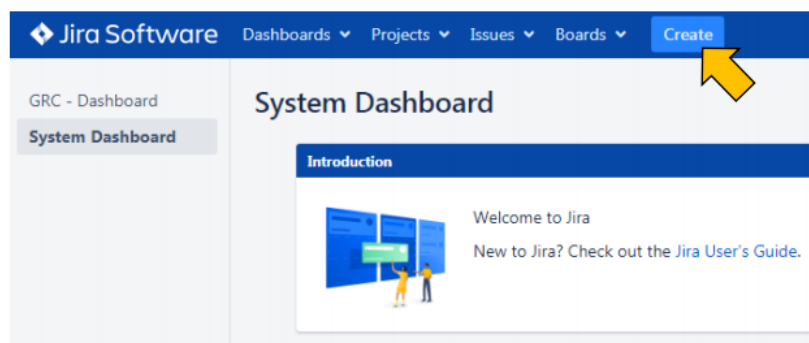
Nesta tabela poderá encontrar o número de Riscos aos quais o seu departamento tem acesso divididos pela Estratégia de Tratamento Adotada.

Issue Statistics: GR - Estratégia de Tratamento (Estratégia de Tratamento)		
Estratégia de Tratamento	Count	Percentage
Aceitar	88	95%
Mitigar	4	4%
Transferir	1	1%
Total	93	

2. Risco

2.1 Como criar um risco

Para criar o risco basta carregar no botão da barra superior **Create** e preencher os campos que surgem no ecrã como mostrado nas figuras seguintes.



Create Issue Configure Fields

Project: **Gestão de Risco (GR)** 1- Escolher Gestão de Risco

Issue Type: **Risco** 2- Escolher Risco como Issue Type

Summary: 3- Descrever sucintamente o risco

Categoria do Risco: **None** 4- Identificar Categoria e Sub-Categoria do Risco

Evento: 5- Descrever Evento

Ocorrência ou alteração de um conjunto particular de circunstâncias que, caso se manifeste, impacta (de forma negativa ou positiva) o âmbito da gestão de risco. Por exemplo: incêndio.

Causa: 6- Descrever Causa do evento

Elemento que, por si só ou em combinação com outros, tem o potencial intrínseco de originar o evento acima.

Consequência: 7- Descrever Consequência do evento

Resultado do evento acima que afeta objetivos, processos ou ativos.

Fonte de Risco: **[Risco] Identificação de Risco** 8- Identificar Fonte de Risco

[DBRGAT0R0C] Identificar que fonte de risco deu origem à identificação de risco. Caso a identificação não seja motivada por nenhuma fonte de risco indicar "Identificação de risco".

Descrição da Fonte de Risco: 9- Descrever fonte de risco

Descrever detalhadamente a fonte de risco. Por exemplo, caso a fonte seja uma constatação de auditoria indicar qual a constatação.

Unidade Orgânica: **DIJ - MPA** 10- Identificar Unidade(s) Orgânica(s) Responsável

Escolha uma ou mais unidades orgânicas.

Processos EZE: **Da Aquisição ao Abate** 11- Identificar Processo(s) EZE

Processo ao qual a ação está associada.

Create another

Depois de preencher os campos e pressionar **Create**, poderá ter acesso ao risco que criou e às informações que o compõem ficando no estado de **Risco Identificado**:

Gestão de Risco / GRC7-76

Isto é um Risco

Comment Assign More Analisar Corrigir Identificação Aqui poderá inicializar o processo de Análise de Risco

Details

Type: **Risk** Aqui poderá designar uma pessoa da Unidade Orgânica identificada para Analisar o Risco

Status: **RISCO IDENTIFICADO** (View Workflow) Aqui poderá corrigir a Identificação feita

Resolution: Unresolved

Security Level: Confidencial

Identificação Impacto

Fonte de Risco: [Governance] Monitorização de Objetivos

Descrição da Fonte de Risco: Isto foi a fonte de Risco

Unidade Orgânica: DPC

Processos EZE: Da Aquisição ao Abate. Do Recrutamento à Saída/Reforma. Estratégia, Gestão e Orçamentação

Evento: Algo Ocorreu

Causa: Isto Causou algo a ocorrer

Consequência: Depois de Algo ocorrer, algo aconteceu

Activity

All Comments Work Log History Activity

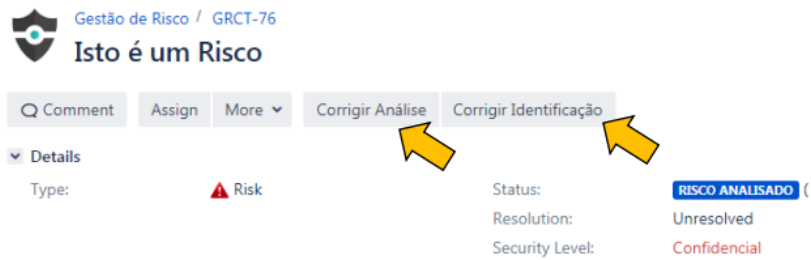
There are no comments yet on this issue.

Analisar: Para poder progredir e analisar o risco é necessário pertencer à unidade orgânica identificada aquando da identificação do mesmo, ou pertencer à GRC.

Corrigir Identificação: Para corrigir os campos inseridos anteriormente na identificação do Risco

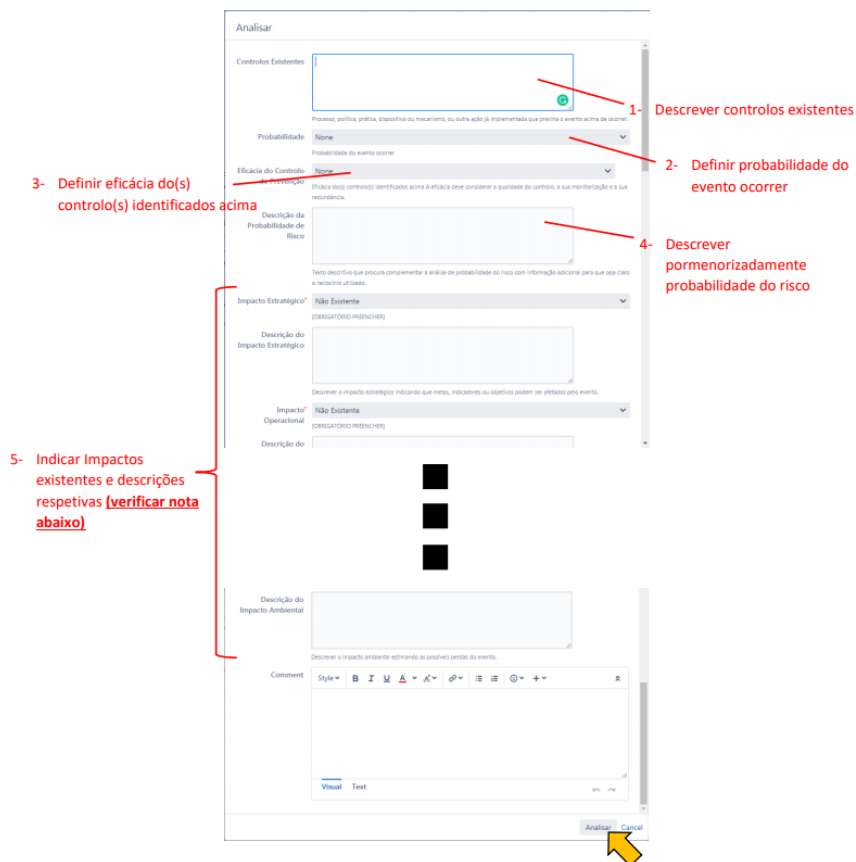
2.2 Como editar um risco

Todos os utilizadores, desde que tenham acesso, poderão corrigir os valores anteriormente inseridos ao utilizar as transições: **Corrigir Identificação** ou **Corrigir Análise**, visto que são os únicos estados do fluxo de trabalho em que podem trabalhar.



Depois do risco progredir no fluxo de trabalho, o utilizador não terá mais a possibilidade de alterar os valores

2.3 Como analiso um risco?



Para prosseguir deverá preencher obrigatoriamente todos os campos do ecrã:

- Para os controlos existentes deverá indicar resumidamente os controlos associados ao risco especificado, se não existir nenhum aparente, deixar o espaço em branco
- Na probabilidade e eficácia do controlo de prevenção, escolher a opção que se adequa mais à realidade. Se não existir controlo, escolher opção “**Controlo de prevenção não existente**”
- Para o tipo de impactos e descrição dos mesmos, preencher pelo menos um que se adequa à situação e selecionar o valor do mesmo. Por omissão, cada impacto será descrito como não existente.

NOTA: É sempre uma boa prática deixar um comentário a explicar os detalhes ao se transitar para estes estados.

Depois de analisar o Risco passará para o estado de **Risco Analisado**:

Será possível navegar pelos separadores do Risco, sendo observável todos os indicadores presentes na Identificação, Análise e Impacto [Tab.3].

Identificação	Análise	Impacto
Fonte de Risco: [Governance] M	Probabilidade: O evento ocor	Impacto Estratégico: Elevado - Impede o cumpri
Descrição da Fonte de Risco: Isto foi a fonte c	Eficácia do Controlo de Prevenção: Controlo de p	Descrição do Impacto Estratégico: Este risco impede o cumpri
Unidade Orgânica: DPC	Descrição da Probabilidade de Risco: O evento é pc	Impacto Operacional: Não Existente
Processos EZE: Da Aquisição ac		Impacto Financeiro: Não Existente
Evento: Algo Ocorreu		Impacto Reputacional: Baixo - Incidente com publi
Causa: Isto Causou algo		Descrição do Impacto Reputacional: Não trará reputação quasi
Consequência: Depois de Algo		Impacto Segurança de Informação (SI): Não Existente
Nível de Risco: Moderado		Pilar SI Afetado: Não Existente
		Impacto Regulamentar: Não Existente
		Impacto Segurança no Trabalho: Não Existente
		Impacto Ambiental: Não Existente

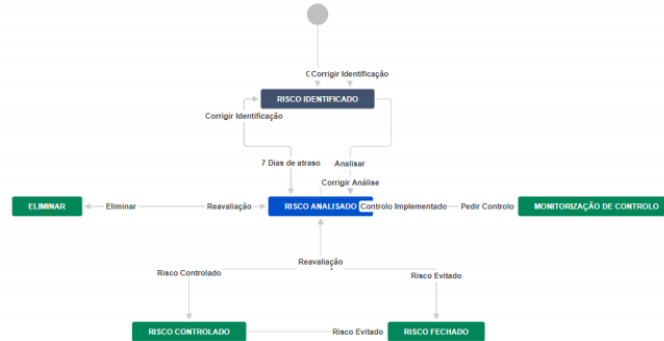
Tab.3 – Separadores

A partir deste ponto, todas as informações serão validadas pelo grupo de GRC, pelo que se pede que se verifique se todos os valores estão corretos antes do Risco passar para Avaliação. Poderá continuar a observar o progresso e a comentar sempre que ache necessário. Continuará também a ser notificado sobre qualquer alteração efetuada nesse risco.

NOTA: A pessoa que executar esta transição ficará automaticamente “assigned” (designada) para o risco, sendo a partir desse ponto notificada sobre qualquer alteração feita.

2.4 Fluxo de Trabalho de Risco (Workflow)

Esta é uma imagem do fluxo de trabalho existente para o Risco:



Aqui estão presentes todos os estados existentes para o risco assim como as suas transições possíveis.

Além das transições anteriormente mostradas, existem algumas extra apenas para reabrir o caso ou voltar ao estado anterior.

3. Oportunidade

A oportunidade tem exatamente o mesmo funcionamento que o risco.

- Para criar uma oportunidade deve seguir a secção [2.1 Como criar um risco](#) seleccionando oportunidade ao invés de risco.



- Para editar uma oportunidade deve seguir a secção [2.2 Como editar um risco](#)
- Para verificar as transições de uma oportunidade deve seguir a secção [2.3 Transições de Risco](#)

Em comparação com o risco, na oportunidade apenas alguns campos e representação gráfica são alterados.

Gestão de Risco / GRCT-88

Oportunidade

Edit Comment Assign More Pedir Controlo Risco Controlado Workflow

Details

Type: Oportunidade Status: RISCO ANALISADO
(View Workflow)

Resolution: Unresolved

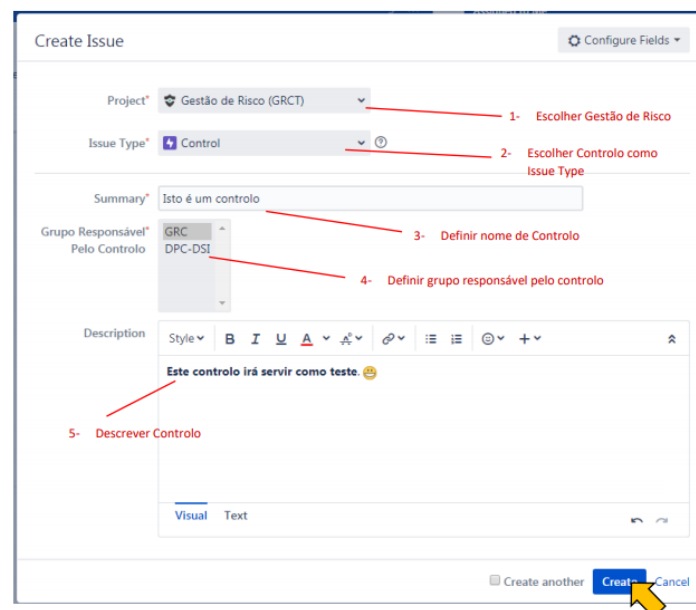
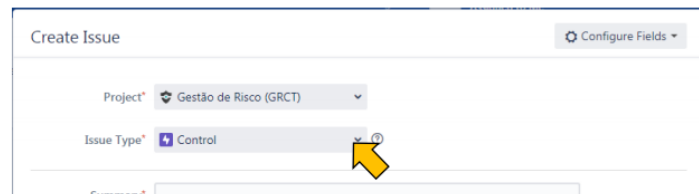
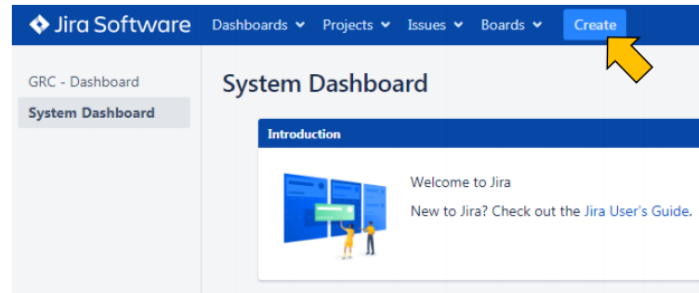
Security Level: Confidential

Identificação	Análise	Impacto
Fonte de Risco: [Risco] Identificação de Risco Descrição da Fonte de Risco: asdadad Unidade Orgânica: GRC Processos EZE: Da Ideia ao Produto Evento: Nova release version para a ferramenta Jira Causa: A nova release foi feita de forma a atender às necessidades dos seus clientes Consequência: Possibilidade de migrar dados de um servidor para outro sem perder informação Nível de Oportunidade: Alto	Controlos Existentes: A ferramenta está constantemente a ser monitorizada pelo departamento responsável Probabilidade: O evento ocorreu ou é previsível que possa ocorrer uma vez nos próximos 6 meses 80-90% Probabilidade Eficácia do Controlo de Potenciação: Controlo de potenciação redundante, com eficácia avaliada e verificada Descrição da Probabilidade de Risco/Oportunidade: Esta nova versão poderá corrigir uma falha existente na migração de dados entre servidores	
Impacto Estratégico da Oportunidade: Moderado - Superação de um ou mais indicadores estabelecidos. Sem impacto no cumprimento dos objetivos Impacto Operacional da Oportunidade: Baixo - Baixa melhoria na eficiência dos processos. Pode originar antecipação de prazos Impacto Financeiro da Oportunidade: Insignificante - Melhoria financeira insignificante (<250m€), <1% redução no custo do projeto Impacto Reputacional de Oportunidade: Não Existente		

4. Controlo

4.1 Como criar um controlo

Para criar o controlo basta carregar no botão da banda superior **Create** e preencher os campos que surgem no ecrã como mostrado nas figuras seguintes.



Depois de preencher os campos e pressionar "Create", poderá ter acesso ao seu Issue e às informações que o compõem estando em estado de **Para Implementar**:

Aqui iniciará o processo de implementação de Controlo

Se não estiver em vista a implementação do controlo

Se o controlo já se encontrar implementado poderá passar-se o estado diretamente para **Implementado**

Aquando a criação poderá transitar para os seguintes estados do processo:

iniciar implementação: Aqui será iniciado o processo de implementação de Controlo, será necessário inserir a data de início e de término do mesmo e o estado passará para **Em Progresso**.

concluir: Se o controlo já se encontrar implementado deverá então transitar o estado diretamente para **Implementado**, completando assim o processo.

cancelar implementação: Na eventualidade da implementação do controlo não estar em vista, deverá então transitar para o estado de **Não Implementado**.

reabrir controlo: Se houver a necessidade de reabrir o controlo enquanto estiver no estado de **Implementado/Não Implementado**, poderá transitar para o estado de **Em Progresso** novamente.

4.2 Como editar um controlo

Apenas será possível editar o controlo estando o mesmo no estado de **Para Implementação** ou **Em Progresso**.

A partir do momento em que saem destes estados serão impossibilitados de alterar qualquer valor presente.

Ecrã de Controlo -> corrigir controlo

4.3 Como associar um controlo a um risco

Para criar um controlo e associá-lo a um risco deverá então seguir os seguintes passos:

Ecrã de Risco -> More -> Create Linked Issue

Gestão de Risco / GRCT-76
Isto é um Risco

Q Comment Assign More

Details
Type:

Identificação Análise

Fonte de Risco:
Descrição da Fonte de Risco:
Unidade Organizativa: NDR

Status: **MONITORIZAÇÃO DE...**
Resolution: Unresolved
Security Level: Confidencial

Link
Clone

ção de Objetivos

Preencher:

- **Issue Type:** Control
- **Created Issue:** "serve de controlo a"
- **Summary:** <Nome do Controlo a ser criado>
- **Description:** <Descrição do Controlo>
- **Grupo Responsável pelo Controlo:** <Indicar grupo a que pertence>

A partir deste ponto deverá seguir o processo normal de implementação de Controlo.

4.4 Transições de Controlo

4.4.1 Como inicio a implementação?

iniciar implementação

Data de Início:

Aqui será definido qual a data real de início de Ação.

Data de Término:

Aqui será definido qual a data para o término da ação.

Comment

Style B I T A -

Visual Text

Iniciar implementação Cancel

Para prosseguir deverá inserir a data em que deverá ser dado início à implementação do controlo e a data de término prevista para o mesmo.

A qualquer momento poderá acrescentar um comentário que sinta necessário.

Estas datas vão ser utilizadas para calcular o tempo passado e os dias de atraso de cada controlo. Se passar do dia da data de término então o controlo entrará no estado de Atrasado e notificará as entidades responsáveis como veremos mais à frente.

O estado passará então para Em Progresso.

Gestão de Risco / GRCT-67
Isto é um controlo

Edit Q Comment Assign More Iniciar concluir cancelar implementação

Details
Type: Control
Status: **Em Progresso** (New Workflow)
Resolution: Unresolved
Security Level: Confidencial

Grupo Responsável: GRC
Qualidade de Controlo: 3
Monitorização de Controlo: 3
Avaliação de Controlo: 3
Eficácia de Controlo %: 100

Description
Este controlo irá servir como teste

People
Assigned: Unliador Testes
Reporter: Unliador Testes
Votes: (0)
Watchers: (1) Start watching this issue

Date
Created: 28/Oct/19 5:56 PM
Updated: Just now
Data de Início: 29/Oct/15
Data de Término: 29/Nov/15

4 of 13

4.4.2 Como concluir/cancelo a implementação?



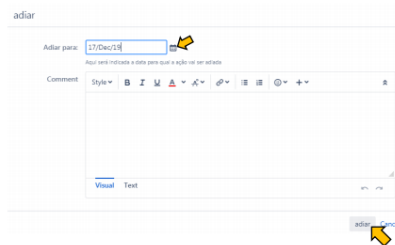
Ao executar estas transições o controlo passará para o estado de **Implementado** e **Não Implementado** respetivamente. Nenhum ecrã surgirá ao transitar para estes estados, e **não poderá mais editar o controlo** nestes pontos.

Poderá no entanto **reabrir controlo** caso exista algo que necessite de ser reavaliado.

NOTA: É sempre uma boa prática deixar um comentário a explicar os detalhes ao se transitar para estes estados.

GRC: Neste estado é calculada a percentagem da **Eficácia de Controlo** com base nos valores de **qualidade, monitorização e avaliação** do controlo. Ao transitar para o estado **Implementado**, estes valores estão no máximo, e a eficácia é respetivamente 100%. Ao longo do tempo, caso a GRC verifique que existe alguma anomalia no controlo mencionado, alterará os valores, e o cálculo será atualizado.

4.4.3 Como adio a implementação?

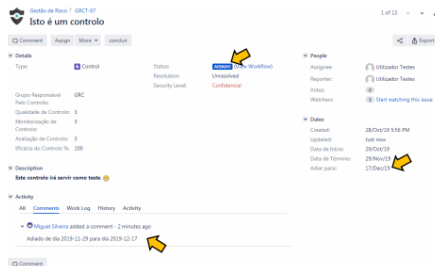


Para prosseguir terá de indicar a data para o qual quer adiar o término da implementação do controlo.

NOTA: É sempre uma boa prática deixar um comentário a explicar os detalhes ao se transitar para este estado.

Ao utilizar esta transição o estado passará para **Adiado**, e o **cálculo de dias em atraso continuará a ser feito mas desta vez em relação à data especificada nesta transição** em vez da data original de término.

Será acrescentado ainda um comentário automático a definir a data para o qual o controlo foi adiado.



4.4.4 O que faço quando o controlo está atrasado?

Gestão de Risco / GRC-67

Isto é um controlo

Comment Assign More adiar concluir

Details

Type: Control Status: **ATRASADO** (New Workflow)
 Resolution: Unresolved
 Security Level: Confidencial

Grupo Responsável: GRC
 Pelo Controlo:
 Qualidade de Controlo: 3
 Monitorização de Controlo: 3
 Avaliação de Controlo: 3
 Eficácia do Controlo %: 100

Description

Este controlo irá servir como teste. 😊

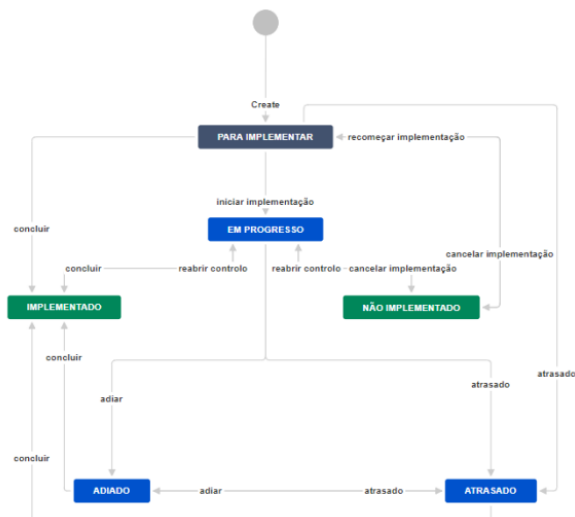
Quando a data de término ou de adiamento for ultrapassada, o estado do controlo passará automaticamente para **Atrasado** e será enviada uma notificação à entidade responsável pelo controlo.

Todos os dias de manhã serão atualizados os dias de atraso, sendo o responsável pelo controlo, notificado todos os dias até passar o estado para **Implementado** ou **Adiar** o controlo.

Como foi mostrado, no Dashboard será possível ver os controlos aos quais tem acesso e os detalhes mais relevantes, como por exemplo os dias em atraso e o estado em que o mesmo se encontra.

4.5 Fluxo de Trabalho de Controlo (Workflow)

Esta é uma imagem do fluxo de trabalho dos controlos:

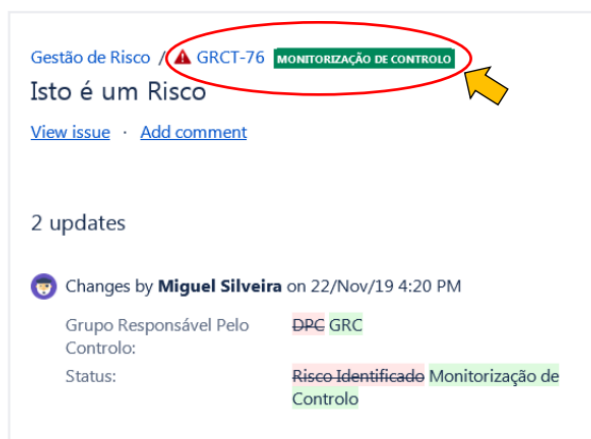


Aqui estão presentes todos os estados existentes para os controlos assim como as transições possíveis para os mesmos.

Além das transições anteriormente mostradas, existem algumas extra apenas para reabrir o caso ou voltar ao estado anterior.

5. Casos Práticos

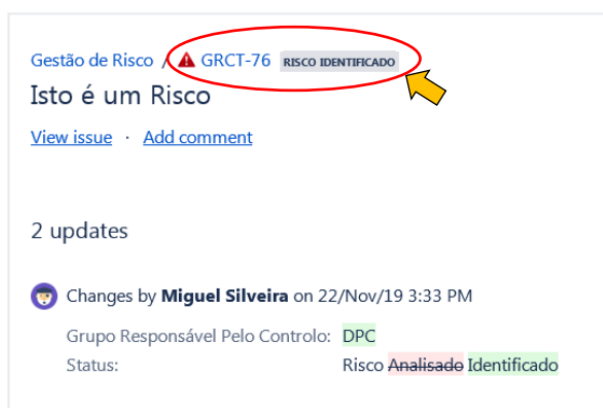
5.1 – Recebi um email com um Risco em estado de “Monitorização de Controlo”



Se receber um email sobre um risco que se encontre no estado de **Monitorização de Controlo**, significa que o seu grupo foi designado para implementar um controlo que o mitigue.

Deverá portanto aceder ao mesmo e seguir o procedimento como explicado no setor [4.3 Como associar um controlo a um risco](#).

5.2 – Recebi um email com um Risco em estado de “Risco Identificado”



Se receber um email igual a este, significa que a sua Unidade Orgânica foi designada para analisar o Risco indicado.

Deverá portanto aceder ao mesmo e seguir o procedimento como explicado no setor [2.3.1 Como analiso um risco?](#).

5.3 – Recebi um email com um Controlo em estado de “Atrasado”



Se receber um email igual a este, significa que um controlo sobre o qual é responsável está **Atrasado**.

Deverá portanto seguir os procedimentos de acordo com o setor [4.4.4 O que faço quando o controlo está atrasado?](#)

B

Usability Test Guide

Usability Testing Guide

Introduction

Thank you very much for the availability and for accepting to test our project in JIRA.

This project's development comes within the scope of a master thesis in Computer Science and Engineering, where it was intended to monitor and develop the dematerialization of the INCM Risk Management process for the JIRA tool.

The following activity is composed of 8 tasks and questions that only have academic purposes, aiming to test the application's efficiency and intuitiveness and never the user itself.

Before this activity begins, you should open the user manual of the sent email attached to the email previously sent. That manual should be consulted whenever you have doubts.

These tasks should take approximately 20 minutes, and some questions will be asked at the end. We remind you that we ask that you answer the questions sincerely for the results to be reliable.

In this activity, no confidential data will be collected, and no interaction will be recorded.

Requirements

- Computer
- Mouse and Keyboard
- Internet Connection
- Microsoft Teams Installed
- User Manual Open

Procedure

- This activity will be carried on Microsoft teams with screen share.
- The user manual should be an active resource to support the activity.
- The manual structure will be explained before the activity starts.
- The tasks described will then be mentioned, one at a time until completion. No task will be timed so you can do it calmly and carefully.
- You will be asked at the end of all tasks to answer a questionnaire regarding the activity.

Tasks

Task 1

- Open the [link in the manual](#) and enter your [INCM credentials](#). Then open the [Risk Management Project](#).
-

Task 2

- [Create a risk](#), and input the following data:
 - **Summary:** Flooding risk
 - **Category:** Personal and Property Damage
 - **Sub-category:** Flooding
 - **Event:** Toilet flood
 - **Cause:** Burst of a pipe from the Department's bathroom
 - **Consequence:** Toilet flooded
 - **Risk Source:** [Risk] Risk Identification
 - **Department:** <your department>
 - **End-to-End Process:** From planning to delivery
 - Refresh your page by clicking F5 and tell the **risk key** of the risk (**Ex: GR-999**) you just created and what's its **Status**.
-

Task 3

- Now [Analyze](#) the Risk you created earlier with the following data:
 - **Likelihood:** The event has occurred or is expected to occur once in the next 18 months.
 - **Effectiveness of Prevention Control:** No Prevention Control
 - **Financial Impact:** Insignificant
 - **Environmental Impact:** Low
- Once you're done, press F5 and indicate the **Risk Level** assigned to it.

Task 4

- Now create a control associated with the risk you created previously with the following data:

- **Summary:** Preventive Verification every 6 months.
- **Serves as a Control to:** <Risk you created earlier>.
- **Group responsible for control:** <your department>

- Once you're done, press F5 and say the control key of the control you just created and its **Status**.

Task 5

- From the list of risks on the left, indicate the Risk Level of Risk **GR-434**.

Task 6

- How many controls are associated with the risk **GR-399**?
 - What about **GR-422**?
-

Task 7

- Open the **Risk Management Dashboard** and explore it.
 - How many risks are in the **Risk Controlled** status and at the same time with a **Very Low** Risk Level?
 - How many risks in total are in **Moderate** Risk Level?
 - How many controls are yet to be **Implemented**?
 - How many risks are there in total **related to your department**?
-

Tarefa 8

- From the Dashboard, show the list of all Controls that are **Implemented**.

