An Information Management Tool to Support Enterprise Risk Management

Miguel Silveira
Instituto Superior Técnico
Lisbon, Portugal
miguel.da.silveira@tecnico.ulisboa.pt

***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*—Risk, Risk Management, Enterprise Risk Management, Functional Requirements, JIRA Software, Process Dematerialization.**

I. Introduction

Risk Management is focused on creating value for the organization, securing the identification of threats, and management systems.[1][2] 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.[3]

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.

Imprensa Nacional Casa da Moeda (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 analyzed a set of tools that could dematerialize its risk management process, choosing JIRA Software, since acquiring other risk management systems could require adapting the process, which was not desired. Also, 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 uses the INCM case study and 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.

II. Related Work

Given the relevance and diversity of risk management, there is a wide variety of references, standards, and guidelines on this topic. This section 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.

A. Fundamental Concepts

Risk management corresponds to the "*coordinated activities to direct and control an organization with regard to risk.*"[4] It is a decision-making process with action implementations to increase the likelihood of achieving the objectives pursued,

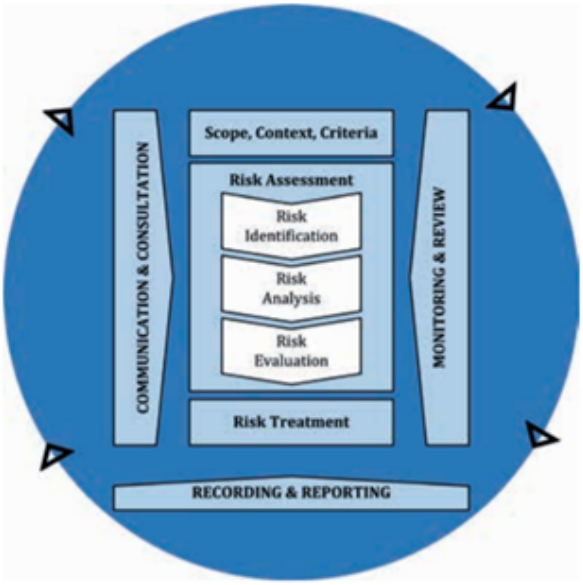

Fig. 1. Risk Management Process - ISO31000

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.[5]

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*"[3], taking into account every risk interdependency.

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 [3]. 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.[3]

B. 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 [4], 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.

This process described in the Standard is shown from a holistic perspective in Figure 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.

TABLE I
RISK TREATMENT STRATEGIES

Decision	Actions
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

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.

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 assets[1], 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.

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 I we describe each of the risk treatment strategies.

[1]An 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.

C. 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.

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.[6]

In general, the definition and concepts of risk management mentioned in Section II-B 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. The process describes an iterative approach based on risk decision points where the process can roll back to a particular activity if the criteria do not meet satisfactory needs.

D. COSO

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.

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.[7] 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 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.

- **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.
- **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.
- **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.
- **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.
- **Information, Communication, and Reporting:** It focuses on information systems, the quality of risk information communication and the risk, culture and performance reporting, aiming to reach a concise result.

III. Problem Analysis

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 section 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.

A. Enterprise Risk Management Process Structure at INCM

Although the INCM's framework is well-structured, its implementation 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.

The process starts when an event occurs leads to a risk. A person from the department identifies it by filling a form and sends it to the Chief Risk Officer(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.

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.

B. Requirement Analysis

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.

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.

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. The requirements are shown in Table II

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. The requirements are shown in Table III

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. The requirements are shown in Table IV

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. The requirements are shown in Table V

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. The requirements are shown in Table VI

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. The requirements are shown in Table VII

IV. Solution Design and First Prototype

The implementation of the solution in the tool had several iterative and crucial steps over time. Some were made in the first months of project design, such as the requirements gathering and the analysis of the tool's capabilities.

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.

A. Analysis of the JIRA Technology

Many companies acquire JIRA intending to digitize their business to integrate technology in all processes (or at least the organization's possible ones). This 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]

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. [8]

B. 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.

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
Discrepancies in Language Packages
Data migration between servers
Report Exporting
Add-Ons as Solution

[2]Atlassian. (2019) What is JIRA used for?, https://www.atlassian.com/software/JIRA/guides/use-cases/what-is-JIRA-used-for

C. First Prototype

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 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.

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 Table II 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 Table V 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: **Controls**, **Opportunities**, and **Risks**.

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: iden-

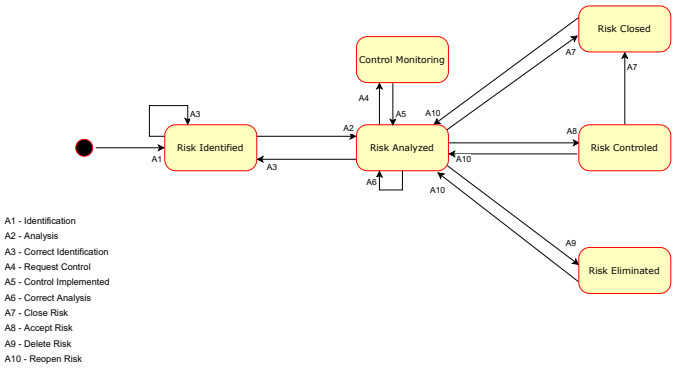

Fig. 2. Risk State Machine

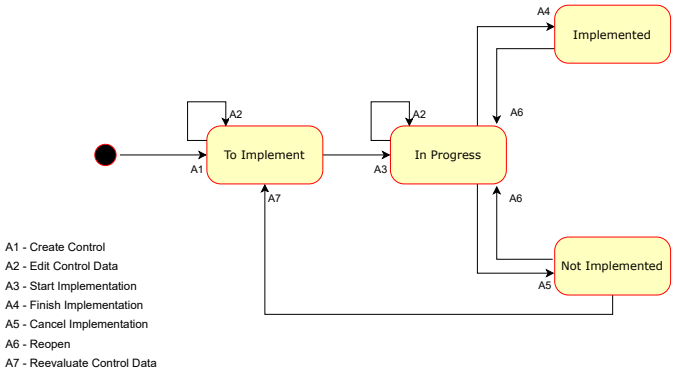

Fig. 3. First Control State Machine

tification, 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.

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 2.

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.

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 Table V, 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.

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

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 defined[3], 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 Table III and Table IV, 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 Table VI, 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. Table VII is a small module, but it should support the organization regarding the risk communication between departments. Within 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.

V. Final Solution

This section will explain the final solution in-depth and the changes required until we delivered a platform compliant with the requirement modules created.

[3]Permissions 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.

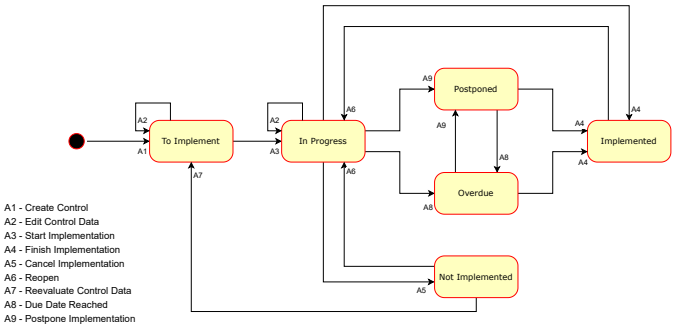

Fig. 4. Final Control State Machine

A. 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 Table V. 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.

With the new add-on, we could add two more steps to the control state machine as depicted in Figure 4.

- **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 in the workflow, and so, fulfill the entire Data Management Module.

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.

VI. Evaluation

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.

A. 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 that was built while configuring the platform.

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). 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**.

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:

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

B. Analysis of the Results

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 5.

On the first question, we evaluated the intuitiveness of the tasks performed, and the opinion was consensual by 56% of

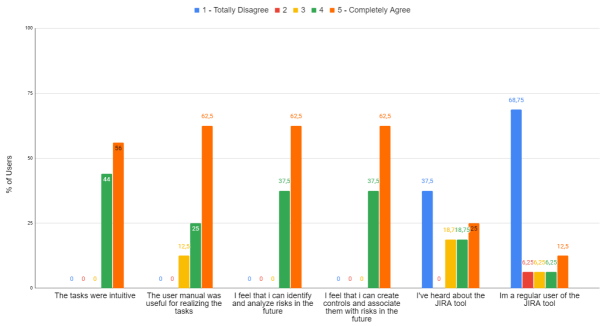

Fig. 5. Questionnaire 2nd part results

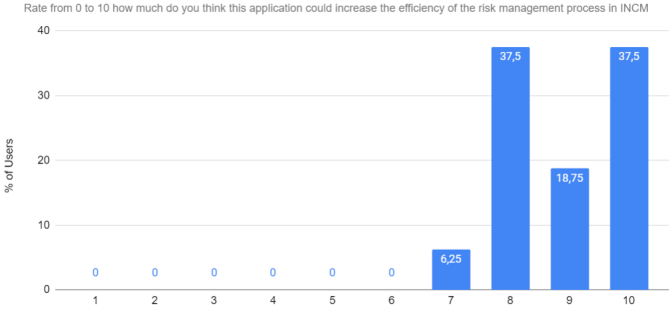

Fig. 6. Efficiency Improvement Questionnaire

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.

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. 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.

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, 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.

VII. Conclusions

This dissertation brings a list of functional requirements 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.

After analyzing ERM processes and JIRA'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. 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**.

VIII. Future Work

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.

References

[1] J. Santos Guilherme; Borbinha, "Enterprise risk management - risk communication and consultation," M.S. thesis, Instituto Superior Técnico, 2018.

[2] M. S. Beasley, "What is Enterprise Risk Management?" *Enterprise Risk Management Insights*, 2016.

[3] PwC, "Enterprise Risk Management - Integrating with Strategy and Performance," Committee of Sponsoring Organizations of the Treadway Commission, Tech. Rep., 2017.

[4] ISO/IEC, "ISO/IEC 31000:2018, Risk Management Guidelines," International Organization for Standardization, International Standard ISO/IEC 31000:2018, Feb. 2018.

[5] P. Hopkin, *Fundamentals of Risk Management, Understanding, evaluating and implementing effective risk management*, 5th Edition. IRM, 2018.

[6] ISO/IEC, "ISO/IEC 27005:2018, Information Security Risk Management," International Organization for Standardization, International Standard ISO/IEC 27005:2018, 2018.

[7] COSO, "Enterprise risk management-integrated framework," *Committee of Sponsoring Organizations of the Treadway Commission*, vol. 2, 2004.

[8] 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.

IX. Appendix

TABLE II
User and Group Management Module

Nº	Summary
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
R1.2	The platform must offer an option for creating new user entities with the properties listed under requirement **R1.1**.
R1.3	The risk is shared with other entity(ies) when its consequences impact more than one department
R1.4	Accepting a risk means that the risk level is within the risk acceptance criteria, meaning no extra actions should be performed
R1.5	When the risk is regarded as an opportunity to achieve objectives, actions should be performed to increase the exposure to the risk
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
R1.7	The platform must offer an option for creating groups or areas with the properties listed under requirement **R1.6.**
R1.8	The platform must offer an option for updating any attributes to reflect changes to the group's details.
R1.9	The platform must offer an option for adding and removing users from a group or an area.
R1.10	The platform must offer an option for deleting a group or area.
R1.11	The platform must offer an option for list the members of a group or area.
R1.12	The platform must offer an option for consulting data of specific users and groups.

TABLE III
Permissions Module

Nº	Summary
R2.1	The platform must provide a permissions system to define user authorization.
R2.2	The platform must allow at least one authorized user with high privileges to define the system **R2.1** permissions.
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**.
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**.
R2.5	The platform must offer an option for defining who can identify a risk, opportunity, or control under the system **R2.1**.
R2.6	The platform must offer an option for defining who can edit a risk, opportunity, or control under the system **R2.1**.
R2.7	The platform must offer an option for defining who can delete a risk, opportunity, or control under the system **R2.1**.
R2.8	The platform must offer an option for defining who can analyze a risk or an opportunity under the system **R2.1**..
R2.9	The platform must offer an option for defining who can evaluate a risk or an opportunity under the system **R2.1**.
R2.10	The platform must offer an option for defining who is responsible for risk treatment under the system **R2.1**.
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**.

TABLE IV
Notifications Module

Nº	Summary
R3.1	The platform must provide a notification system to notify a group of users through email or others when an event occurs.
R3.2	The platform must allow at least one authorized user with high privileges to define the system **R3.1** notifications.
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**.
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**.
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**.

Continues on the next page

Nº	Summary
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**.
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**.
R3.8	The platform must offer an option of notifying users, groups, or areas indicated by other authorized users throughout the workflow.
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**.
R3.10	The platform must offer an option of bundling notifications to send instead of several repeated notifications.

TABLE V
DATA MANAGEMENT MODULE

Nº	Summary
R4.1	The platform must allow an authorized user to create new elements with at least the following system attributes: - Unique ID - Descriptive Name - Detailed Description - Creation Timestamp - Last Update Timestamp - Creator ID/Name - Responsible Person or Group - Event History
R4.2	The platform must support the creation of at least the following elements: - Risks - Controls
R4.3	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.
R4.4	The platform must offer an option for creating new fields to be filled in.
R4.5	The platform must offer an option for adding new fields to transitions.
R4.6	The platform must offer an option for defining different statuses and transitions in workflows and associate them with the platform elements.
R4.7	The platform must offer an option for showing the progress of a particular issue.
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)
R4.9	The platform must allow the organization to define the levels and values of every property used to calculate the risk level.
R4.10	The platform must offer an option for risk evaluation that calculates the risk level automatically based on the properties of **R4.8**.
R4.11	The platform must offer an option to automatically move an issue through a workflow based on certain criteria.
R4.12	The platform must offer an option to close risks that have already been treated.
R4.13	The platform must allow authorized users to assign issues to other users, giving them the needed access.
R4.14	The platform must allow authorized users to correct their inputs on each issue.
R4.15	The platform must allow authorized users to input information on their issues at any given point of the workflow without editing them.
R4.16	The platform must offer an option of showing historical element values such as risk level, likelihood, and impact.

TABLE VI
SEARCH AND REPORTING MODULE

Nº	Summary
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.
R5.2	The platform must allow users to restrict searching results, under **R5.1**, to issues of the types described in **R4.2**.
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.
	Continues on the next page

Nº	Summary
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.
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.
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.
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
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**.
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.
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.
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.
R5.12	The platform must allow a user to specify a search criterion, under **R5.4**, that returns only open or closed issues.
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.
R5.14	The platform must provide the ability to order every column alphanumerically, sorting in an ascending or descending way.
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.
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**.
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.
R5.18	The platform must allow authorized users to save, modify, delete and share search queries.
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.
R5.20	The platform must allow authorized users to show any issues in the form of charts or any other type of graphic report.
R5.21	The platform must allow authorized users to create dashboards with charts chosen by them to illustrate a specific set of data.

TABLE VII
EXPORTING MODULE

Nº	Summary
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.
R6.2	The platform must allow an authorized user to export only the data that he has access to.
R6.3	The platform must only allow exporting issues chosen by the user.
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.
R6.5	The platform must allow an authorized user to export any data in the form of a chart.
R6.6	The platform must allow an authorized user to export any dashboard that he has access to.
R6.7	The platform must allow an authorized user to export the history of one or multiple entities under **R5.19**
R6.8	The platform must allow an authorized user to export data from one or multiple entities from a particular point in time.