Risk Data Management:
A case of a Risk Register developed in OutSystems technology

Extended abstract

Diogo Miguel Galhardas Pinto Gonçalves
Instituto Superior Técnico
diogo.p.goncalves@ist.utl.pt

Abstract

Risk management strategies consist of the process of recognizing, observing and preventing threats to the organization, and additionally a framework to support this process. The structure required to support will result in a risk management framework, which information can be managed with the support of a risk register.

Here we report the results of a project that developed a risk register constrained by the mandatory use of a specific technology, OutSystems, and motivated by a real case of a real organization.

The organization that motivated this case is a public company in the business of mint and printing of materials with security features, such as citizen cards and passports.

Key Words

Risk, Risk Management, Risk Registration, ISO Standards, OutSystems.

1 Introduction

Risk is “deviation from expectations, which can be positive, negative or both and can address, create or result in opportunities and threats”, [1], “from different aspects and categories”, [1].

With the evolution of technology, also systems and the entire process that encompasses the smooth running of an organization evolve, increasing the risks associated which can impose challenges to meeting its goals.

In order to achieve the goals, there are several assets that need to be taken into account in the business, such as skilled workers, new technologies that make the organization architecture more complex. To control this complexity, organizations use tools to manage their architectures, making it easier to understand their structure and facilitating business decisions [2].

For risk management to be effective and efficient, it is important to understand, analyze and address risks to ensure that organizations are protected and therefore achieve their objectives. For this reason, many organizations now have their own risk management structures where they identify risks, analyze and take the necessary preventive measures and should be in accordance with the ISO 31000 standard, [1], which was currently considered as the main reference for risk management structures.

To maximize gains and minimize losses when trying to achieve the organization's goals, it is important to use the appropriate methods to address the risks associated with those goals [1]. The way to manage these risks will be the focus of this project, with the objective of implementing a tool capable of meeting the needs of the organization.

1.1 Problem Description

There is a problem when organizations, in this case INCM, we have the need to use tools that assist in this management.

In the specific real case of motivation, which addresses a risk management strategy, it needs ancillary tools. Nowadays organization is using an excel with a number of procedures as an aid, however this practice is not only excellent, it is not intuitive to use.

In order to help the organization of this case, INESC-ID started by developing a tool called HoliRisk, however due to constant changing requirements it became difficult to finalize, in agile development, the tool so that organization could use it during risk management.

So, it is necessary to design, implement, demonstrate and validate a risk register taking into account the requirements used by the real case.

1.2 Objectives of the work

The objective of this work was to gather all the requirements and specifications necessary to develop a risk registration application using OutSystems technology that can support risk management.

The requirements that was used for the development of a risk management tool correspond to the real case functional requirements, for confidentiality reasons it was not possible to use the real case data, however an artificial case of pizzeria was provided, resembles organization for demonstration of the solution.

1.3 Document Structure

This document follows a very simple model where each section represents a different subject of the project.

In the Introduction, we begin by introducing the risk theme, describing the problem with this project and the objectives of the report.

The Fundamental of Risk Management gives some theoretical context about risk, presents the fundamental concepts of risk management, and then explains the whole process of risk management.

In the Technology and Development Method section, OutSystems technology is presented as related project work. This chapter gives an overview of the application concept and benefits of using this agile development tool. Also in this section is presented the method used for application development, which corresponds to the method used in development with OutSystems technology.

Problem Analysis is dedicated to problem analysis, contextualizing the current state of organization's real case.

Next, Domain Model Analysis presents the domain model on which application development is based.

In the Requirements Analysis and motivation case design, we present the requirements that were developed during the dissertation, as well as the use cases that result from these same requirements. Finally we present the development made in this dissertation.

With Demo section of the solution, the artificial case provided by the organization is presented in order to validate the developed application with data that could be tested as real case data, since for confidentiality reasons it was not possible to use real case data.

The last section concludes with the conclusions about the work done and presents ideas for following up this dissertation.

2 Risk Management Fundamentals

This section describes the main concepts of risk management for a better understanding of the problem.

Risk management is the "coordinated activities to direct and control an organization with regard to risk", so, it is a cyclical management process where the objective is to identify, analyze and mitigate risks that may interfere with the organization's objectives and operations.

2.1 Main Concepts

All concepts described below are taken from ISO Guide 73[3].

To better understand what risk management is, it is important to first understand what a **risk** is. The "uncertainty effect", [1], the achievement of an organization's objectives is called **risk** and the effect can either have a positive or negative change in the organization. A risk **owns the risk** and is characterized by potential **events, consequences and causes**, and is often expressed as a combination of consequences related to an event and its likelihood.

Risk owner is the organization people who may affect or be affected by the risk, or consider themselves affected by a decision. One **cause** is what results from the uncertainty of changing the normal behavior of the artifact. An **event** is a situation that occurs from one or more causes that leads to an impact on an organization's goals. The fact that nothing happens can also be considered an event. The impact of an event can be described by one or more **consequences**. For example, considering a police station, where an emergency may arise to go out and intervene in a situation and use the service cars. The owner of the risk could be the person who alerted the emergency, an event about this activity could be, the service car not being operational, which was caused by an engine failure, and leading to a consequence of the police not able to intervene in an emergency.

Having the concept of risk clarified it is now possible to speak of **risk management.** Risk management is a set of coordinated activities to direct and control the risks of an organization. There is a continuous and constant application of management policies, procedures and practices for communication, consulting, context setting, identification, analysis, assessment, treatment, monitoring and risk review activities, which correspond to the **risk management process.** Being a complex process, the **risk management framework**, through a set of components, provides the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continuously improving the **risk management process**.

For risk management there are frameworks, which can be divided into two concepts, **risk register** and **risk report**. **Risk register** is a document detailing all risks resulting from the risk management process. **Risk report** consists of some kind of report that can result from the tool, and contain all the knowledge about the existing information.

2.2 Risk Management Process

The Risk Management Process is described by ISO 31000, [1], as presented by **Figure 1**, and "involves the systematic application of policies, procedures and practices in communication and consultation activities, context setting and appreciation, treatment monitoring, reviewing, recording and reporting ", [1], and can be divided into three main activities.

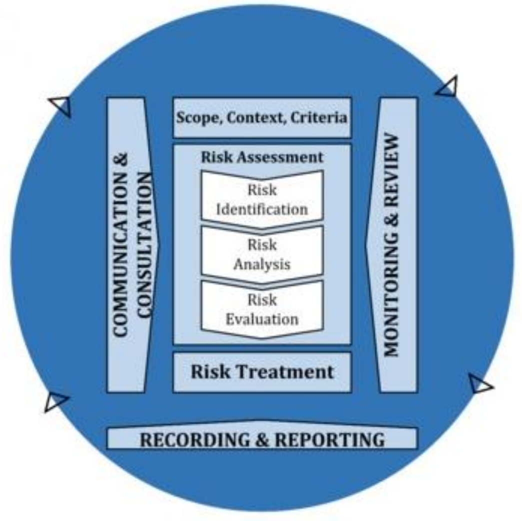
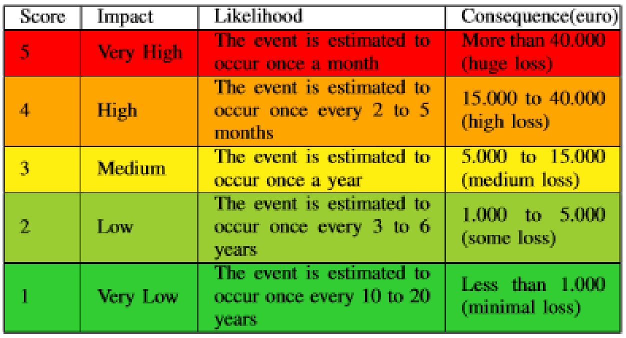


Figure 1. Risk management process

The first activity consists in **establishing the context** and involves understanding external factors related to the activities performed by the organization to try to achieve its objectives and factors related to the internal environment of the organization itself. Visto que todas as organizações diferem umas das outras, o processo da gestão de risco deve ser adaptado [1]. This stage also defines the organization's risk criteria, which includes the level of each risk, the impact associated with each risk, and the level at which the risk can be accepted. Even though risk criteria are defined at the beginning of the process, “they are dynamic and should be continually reviewed and, if necessary, modified” [1].

The second activity is **risk assessment**, where the objective is to identify the risk, analyze it and finally assess whether it is possible to proceed to the treatment of it or not. Following this line of thought it is possible to divide this activity into 3 phases as described by ISO 31000, [1]:

- **Risk identification**, at this stage, after the context has been established, a list is created where all risks are identified. Each risk is described according to a cause, event and consequence and must be associated with an owner who will be responsible for managing the risk. In this process any event that influences the organization's objectives, whether positive or negative, is taken into account for risk selection, so in this process it is important to give importance to the human factor for risk identification
- **Risk analysis**, on the list of risks identified in the previous step, and uses all the information gathered to determine the likelihood of the consequences, their impact and the combination of the two to know the level of the risk. If controls are in place for certain risks, they should also be considered in this analysis. In this analysis, it is possible to classify likelihood and impact quantitatively and / or qualitatively. Qualitative is to separate the scale by categories (Very High, High, Medium, Low, Very Low), and quantitative is to divide the scale by numerical values (1,2,3,4,5), as shown in **Figure** 2**.** At this stage there may be difficulty in analyzing risks with high uncertainty and “this can be a problem when analyzing events with severe consequences”, [1], and in these cases the need to use techniques to facilitate this analysis becomes evident.
- Risk assessment, finally, in this phase, the results of the previous phase are evaluated in order to support decision making. It involves assessing the level of risk according to the organization's risk criteria to better understand which risks need to be addressed or whether controls that exist to stop a certain risk are sufficient In this way it is possible to define in what order the risks should be treated, depending on their severity. “The outcome of the rich assessment should be recorded, reported and then validated at the appropriate levels of the organization.” [1].



Score	Impact	Likelihood	Consequence(euro)
5	Very High	The event is estimated to occur once a month	More than 40.000 (huge loss)
4	High	The event is estimated to occur once every 2 to 5 months	15.000 to 40.000 (high loss)
3	Medium	The event is estimated to occur once a year	5.000 to 15.000 (medium loss)
2	Low	The event is estimated to occur once every 3 to 6 years	1.000 to 5.000 (some loss)
1	Very Low	The event is estimated to occur once every 10 to 20 years	Less than 1.000 (minimal loss)

Figure 2. Example of a quantitative and qualitative scale

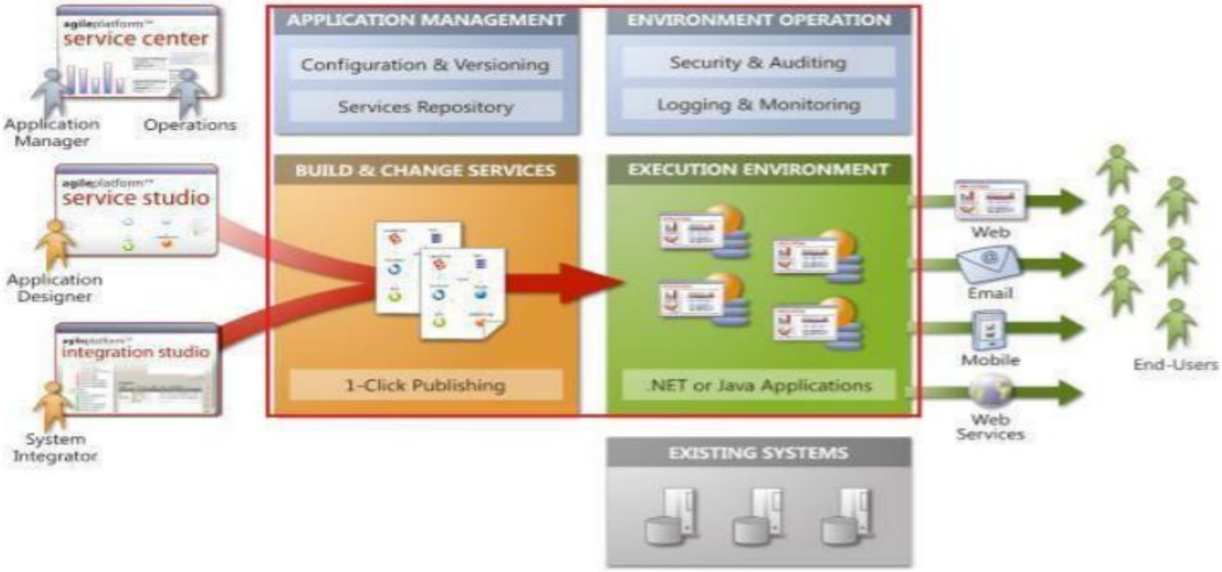


Figure 3. Agile Platform OutSystems

Finally, the third activity of the risk management process is **Risk Treatment**. This activity consists of an iterative process. Start by formulating and choosing treatment options, then planning the implementation of risk treatment. Check how effective the treatment is and decide if the residual risk is acceptable, if not an additional treatment should be. Risk management can take several types of actions: accepting or increasing risk in order to exploit a potential opportunity; avoid risk by stopping activities or processes related to their causes; likelihood and impacts can be minimized through. At the end of the activity all decision makers and stakeholders should be informed of the residual risk, which "shall be documented and subject to monitoring, review and, where appropriate, supplemental treatment", [1].

During these three activities, there are three other activities that occur simultaneously throughout the entire risk management process.

Communication and consultation, one of these activities, aims to help stakeholders gain a better understanding of risk, so, communication seeks to raise awareness of risk, while consultation involves obtaining information to assist in decision-making. All of this stakeholder activity should be "integrated into all stages of the risk management process", [1]. This activity results from not all stakeholders sharing the same point of view.

All processes must be controlled, monitored and reviewed regularly to keep all information on the risk management process accurate and up to date. In this **monitoring and review** activity, in addition to having to occur at all stages of the project, its results should be "incorporated into the organization's performance management, measurement and reporting activities", [1].

Following is the last of these three activities, **Registration and Reporting**, where are documented the results of the risk management process. This activity aims to communicate activities and results, provide information for decision making, support iterations with stakeholders and thereby improve risk management activities, [1].

3 Technology and Development Method

3.1 OutSystems

Outsystems is a Portuguese company providing a platform that enables companies to develop, change and maintain enterprise applications. The platform developed is the number one low-code platform that enables visual development throughout the application, easily integrates with existing systems, as well as adding custom code when needed for proper application operation. With this platform, it is possible to develop applications for both mobile and websites.

The goal is to offer technology that allows you to handle applications at any time of the cycle, lowering your delivery costs and streamlining the wreath of web and mobile applications. For this, agile methodologies are used, namely the OutSystems methodology, which was created based on the scrum methodology [4].

OutSystems as an agile platform, has a set of tools and services that automate the application delivery process. These in turn integrate with existing systems and reach users through the web, email and mobile devices. The platform consists of the following modules illustrated in **Figure 3:**

- **Service Studio** – It is a visual development environment for the development of applications that are subject to change in your business processes. The service studio has all the components for building the application without the need to have any code written. It allows you to automatically create, change and publish apps.
- **Service Center** – It is a web console that allows the *OutSystems* developer to manage and monitor the entire agile platform. This allows you to configure access control policies, perform quality control on development teams and applications, a history of all application versions made, and monitor and audit performance and quality issues.
- **Integration Studio** – Work environment for developers to integrate applications and access to external databases from custom components. Includes assistants to map and identify databases, *API* libraries, *SAP* components and you can use *Microsoft Visual Studio* for integration. It also allows you to create connectors to integrate other existing systems that can be reused in any *OutSystems* application once integrated with *Service Studio*.

- **Plataform Server** – In this environment applications are stored, published and run, and provide a set of services for compiling and monitoring applications. This environment is represented in red in **Figure 3**.

The following are the main features that make this platform, the number one platform, and the reasons why it was the chosen technology:

- **Unbeatable Speed**: As applications develop visually, it makes the whole process faster and not final to deploy the solution in the cloud just takes a touch with the mouse.
- **High scalability**: *OutSystems* applications will always perform optimally regardless of number of users, complexity or data volume.
- **Implementation is not breakable**: The *OutSystems* platform only lets you implement solutions that have no errors, so applications will never store faulty solutions in cloud environments and in the environment itself.
- **Integrated Security**: ensures applications are safe from design to deployment, with the latest security features being used.
- **Integration with everything**: You can easily connect applications developed on the platform with any other system.

3.2 Method

Given that the tool would have to be made using OutSystems technology to meet INCM's interests, and that the method that this technology uses for development is scrum, it was necessary to use this method agile for application development.

Considering the methodology that OutSystems uses to develop projects with its platform is the scrum methodology [6], it was decided to use this agile methodology for application development.

Scrum is agile and flexible methodology for the development of a project. A software development methodology utilizes an iterative and incremental practice, so it is possible to have a better understanding of the entire project development over time. This development methodology focuses on delivering the most valuable customer functionality as quickly as possible, so it adapts to projects where requirements can change rapidly.

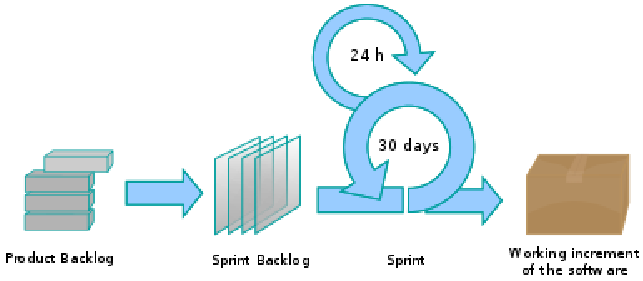


Figure 4. Scrum Method

As **Figure 4** demonstrate, this methodology proposes that the project start with a list of features desired by the customer. This list can be modified by the customer at any time during the project, and is broken down into tasks that are developed over the 30-day sprint cycles.

During a sprint meetings are held between team members to discuss issues about project progress and obstacles. Ideally, these meetings would be held daily, but due to the availability of those involved, and after joint reflection, it was decided that it would be most beneficial for everyone if the meetings were weekly.

Since this project will have only one programmer (report author), it would be difficult to have new features developed every day to be presented and discussed among all. The method remains agile given that contact will be constant during development, thus maximizing existing resources over time. At the end of each cycle, the functionality provided for the customer to be tested is implemented. In this way, it is possible to obtain the customer's opinion, which allows future adjustments of the project. This cycle repeats until the final delivery of the product.

There are three key roles in the scrum methodology:

- Product Owner: person responsible for the product backlog, which defines which features have the highest priority and chooses the tasks to do for the rest of the team. It is the person responsible for defining the sprints until the final product development.
- Scrum Master: Team manager who ensures that tasks are done by different team members without inconvenience, and responsible for the team following good practices. Represents the team in the presence of the product owner.
- Team Member: Member of the product development team whose role is to make sprint backlog tasks functional.

The work team is made up of only one element - author of the report. The work was mediated by another element - organization co-advisor. The role played by this element is to follow the work done by the author, by elucidating questions related to certain components of the project. The supervisor of this project plays the role of scrum master, with the objective of guiding the team to reach the final product.

4 Problem Analysis

This section explains the structure of risk management, which is currently defined in organization.

4.1 Problem Context

INCM assumes risk management as an integral part in order to ensure compliance with the company's objectives. The objectives are to promote risk management value creation, promote a risk management culture, ensure stakeholder awareness, promote the sharing and reuse of risk information and ultimately ensure the compliance of the risk management process.

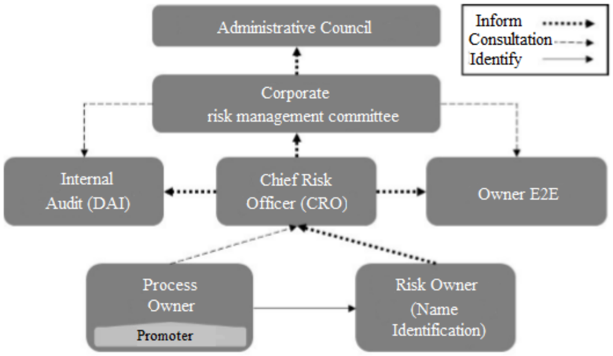


Figure 5. Corporate Risk Management Functions

In functional terms, corporate risk management is represented in **Figure 5**, and the functions of each element are:

- **Administrative Council**: Supported by the corporate risk management committee, it defines the risk management strategy. It also provides and approves resources required for risk management.
- **Corporate risk management committee**: Organ that supports the board of directors, monitors and the risk management structure, suggesting changes, following a strategy of continuous improvement. Guarantees communication with stakeholders.
- **Chief risk officer (CRO)**: defines the risk management structure and has to be approved by the corporate management committee. Supports the implementation of the risk management risk of management framework as a consulting member through the consolidation, aggregation and categorization of risk information.
- **Internal audit**: organ that assess the risk management process, “including proper identification, analysis, assessment and treatment of risks” [4]. Given the associated risks, this body's function is to prioritize the work of the audit plan.
- **Owners E2E**: controls value chain risk information and ensures that changes made to the value chain are reflected and reported.
- **Risk owner**: monitors possible risk changes, quantifies residual risks, ensures, and assesses the effectiveness of controls.
- **Process owner**: organ responsible for risk identification, analysis and assessment.

4.2 Current State Analysis

The risk management process used by organization, represented in **Figure 6**, and incorporates the requirements of ISO 31000 [1].

In general, the main objectives for corporate risk management are established in accordance with organization's strategic objectives by defining the risk categories to be addressed. Thus, at the strategic, governance and environmental responsibility level, the risk is related to the adverse or beneficial change in the environment that results wholly or partially from the environmental aspects of the organization. With regard to social responsibility, the risk of a decision can positively or negatively influence sustainable development and the well-being of society.

The risk of committing any act or its omission, whether lawful or unlawful in this case, against receipt that is not due to oneself or to third parties is corruption or related infringement. In order to ensure the standardization of risk management, the following activities in corporate risk management are established:

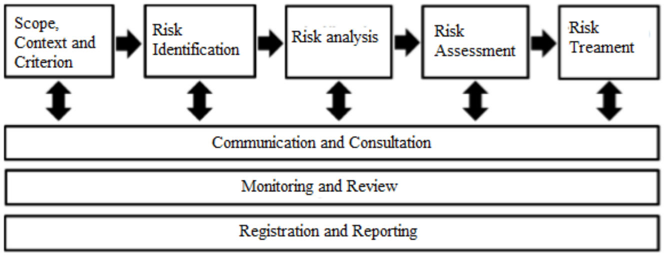

Scope, Context and Criterion
Risk Identification
Risk analysis
Risk Assessment
Risk Treament
Communication and Consultation
Monitoring and Review
Registration and Reporting

Figure 6. Corporate Risk Management Process

5 Requirements analysis and motivation case design

5.1 Domain Model Analysis

The analysis and information gathering of organization's ERM framework allowed the construction of a domain specific model. So, the result of this work is illustrated in **Figure** 7**:**

ERM structures differ from organization to organization to fit their context, so some of the associations, classes, and their attributes and scales result from the context in which INCM fits in and I are defined in [5].

Similarly, the risk has an attribute, the risk state that indicates what stage of its life cycle it is in, and the risk level operation as shown in the following table.

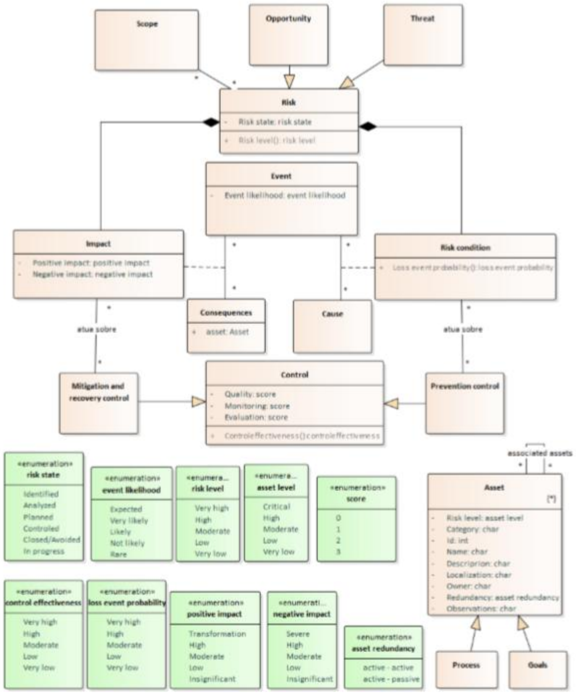


Figure 7. Domain Model from organization ERM Framework

The risk class derives from two classes, the risk condition that is constituted by the probability of loss derivative operation, and the impact that has the positive impact and negative impact attributes.

Operation	**Parameters - Class**	**Return Type**
Risk level	- Impact - Likelihood of Derived Loss	Risk Level
Likelihood of Derived Loss	- Event likelihood - Control Effectiveness	Likelihood of Derived Loss
Control Effectiveness	- Quality - Monitoring - Evaluation	Control Effectiveness

Table 1. Operações das classes do modelo de domínio

5.2 Functional Requirements

In this section are presented the requirements that developed during the dissertation that are defined by [8], even those that were decided that would not be implemented, at least for now.

Turning to the context of Risk Management at organization which is currently characterized by the existence of several Specialized Risk Management Structures, each focused on providing concrete answers to operational (eg for certification) or business (eg , in response to national and international competitions). Thus, the Corporate Risk Management Framework should aim to develop a tool that, taking advantage of existing Specialized Risk Management Frameworks, should provide at a given moment a common and cross-sectional view of operational and business risks of the organization.

To meet these objectives, a contradiction must be resolved: on the one hand, the organization adopts common risk management concepts and principles, while on the other hand it cannot construct the definition of Specialized Risk Management Processes for the various business contexts of the company organization. This contradiction may, however, be apparent if it is possible to design and put in place an infrastructure for common use, this is, a technology solution for managing a Risk Register and capable of generating Risk Reports, which serves the at the same time, each specialized context and the objective of Corporate Risk Management. That is, an infrastructure that can manage all risk information in a uniform and transparent manner to stakeholders in each context, while providing them with support services for their Risk Management Process activities, including Risk Reporting, according to the actual needs of the respective context.

To support the implementation of the Risk Management Process and the domain model common to the organization, an appropriate support infrastructure must be defined. Corporate Risk Management at INCM will be supported by an information system that will support the definition and integration of Risk Registration. A Risk Register is an object where risk information is recorded. In particular, it is a support tool considered essential for risk communication, consultation, monitoring and review - the main objectives of corporate risk management.

The Risk Register is also the basis for information integration. Through the various Risk registers created by the different Risk Management processes, the information system to be implemented must allow the aggregation of all information in a Corporate Risk Register. In order to enable such aggregation it is necessary that all risk registrations created have at least the concepts defined for corporate registration. It is important to note that typically risk governance has only concerns about risks that jeopardize the functioning of the organization. It is therefore necessary for aggregation also allow risk information to be filtered based on stakeholder concerns, which can be obtained by setting the context by objectives. That is, a Risk Register must be designed so that Risks relevant to only one or more specific objectives can be listed and analyzed.

It will be necessary to develop a Back Office, with a “Users and Groups Service”, in order to ensure that the application is only used by previously authorized people to access the system. Good user management must be ensured. To simplify user management, the requirements below introduce the user group concept that allows you to group users by common denominators.

A Front Office with a “Risk Registration Service” was also developed, which corresponds to a risk management process supported by a risk registration - an object where all risk information is recorded. In particular, it is a support tool considered essential for risk communication, consultation, monitoring and review - the main objectives of corporate risk management. Front Office will also consist of a risk reporting service.

5.3 Use Case

This section describes the main use cases that affect the classes in the application domain model. A **Figure 8** shows use cases (UC) identified by following the textual and table description of each of the identified use cases.

The analysis of **Figure 8** identifies seven cases of distinct uses. They all use and/or alter classes present in the **Figure 7** domain model.

Use case **UC01** describes the phase of the process where the CGRC defines the scope of the organization's risk activities, which includes the definition of internal and external contexts. As soon as the scope is defined, it must be registered in the Risk Register application.

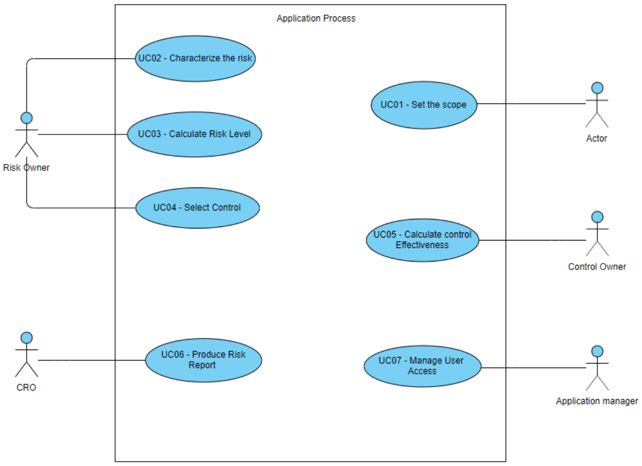

Application Process
UC02 - Characterize the risk
UC01 - Set the scope
Actor
Risk Owner
UC03 - Calculate Risk Level
UC04 - Select Control
UC05 - Calculate control Effectiveness
Control Owner
CRO
UC06 - Produce Risk Report
UC07 - Manage User Access
Application manager

Figure 8. System Use Cases

Use case **UC02** corresponds to the phase of the process where the Risk Owner characterizes the new risks that have been reported. This characterization of the new risks is associated with existing events, consequences, causes and controls.

Use case **UC03** describes the phase of the process where the Risk Owner after having characterized the new risk (s) that has been reported calculates the risk level. To calculate the risk level the Risk Register first calculates the probability of loss arising using the event probability and effectiveness of the prevention control metrics, and then the maximum impact. The level of risk is calculated through the intersection between the probability of loss derived and the maximum impact. All results are recorded in the Risk Register.

Use case **UC04** describes the phase of the process where the Risk Owner selects existing controls for the risks. This requires that the effectiveness of controls has already been calculated.

Use case **UC05** describes the phase of the process where the Control Owner calculates the effectiveness of the control applied. At this stage of the process, the Control Owner will plan and implement the selected controls. Control planning includes the activities of estimating the cost/benefit of control and the expected date of completion of control implementation, among others. The use case ends by checking the quality of the control and recording these metrics in the Risk Register, which will use them to calculate the effectiveness of a control.

Use case **UC06** describes the phase of the process where CRO prepares risk reports. This use case triggers at the beginning of the report production, which will later be shared with stakeholders.

Use case **UC07** describes the phase of the process where Application Manager gives/withdraws permissions to application users by defining the profiles each user has.

5.4 Development

For this development was divided in 3 cycles, each one with 3 weeks, where two weeks correspond to development, and the last week corresponds to tests with the client.

In the **first cycle**, the service was developed to manage user access (use case UC07 - **Figure 8),** was also created entities for the domain model, created pages to define scope, create relationships between entities, and build risk arrays (use case UC01 - **Figure 8).**

In the **second development cycle**, screens were created to register new and edit controls (use case UC05 - **Figure 8**), a screen listing the various details of a risk where you can edit each of these details (use case UC02 – **Figure 8**), including consequences, causes, events and assets.

For the **third and final phase of development**, a risk register screen was created (use case UC03 - **Figure 8)**, where the risk level is calculated from the matrices defined within the scope, and a Dashboard with general management information, and a report that you can export on the Dashboard page (use case UC06 - **Figure 8**).

6 Solution Demo

As noted throughout the document due to confidentiality reasons it was not possible to have access to real case data to demonstrate the solution, although the motivation case corresponds to the real case.

Alternatively an artificial case was provided so that the solution could be demonstrated with the same success as the organization data would have. The artificial case will therefore be described in a first step and then demonstrated how the data from this practical case is used in the developed tool.

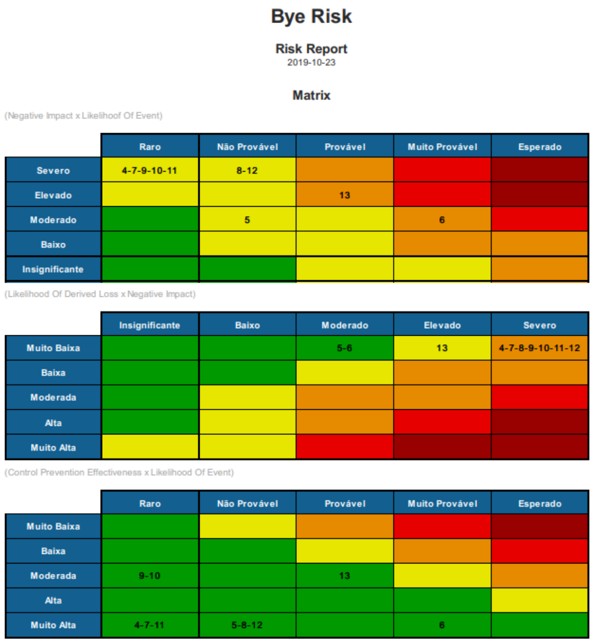
6.1 Description of the artificial case

The case depicts a scenario of a pizza restaurant serving food both in the dining room and on home delivery. The roommate assisted by an employee guarantees room service. The employee also guarantees home delivery with a pizza parlor motorcycle.

Home delivery requests are received by site, and the principal receives an sms from the site itself. The pizzeria has a kitchen, run by a chef, responsible for all orders he receives from the director. The head chef has an assistant who performs tasks under the head of the head chef. When an order is completed the boss informs the director, if it is a home order the employee proceeds for delivery.

The chef's assistant is responsible for counting the resources in the kitchen, and the chef is responsible for ordering more resources when needed. The assistant also has the function of cleaning the kitchen, and the employee cleaning the dining room and checking the condition of the motorcycle.

6.2 Demostration



Bye Risk

Risk Report
2019-10-23

Matrix

(Negative Impact x Likelihoof Of Event)

	Raro	Não Provável	Provável	Muito Provável	Esperado
Severo	🟨 4-7-9-10-11	🟨 8-12	🟧	🟥	🟫
Elevado	🟨	🟨	🟧 13	🟥	🟫
Moderado	🟩	🟨 5	🟨	🟧 6	🟥
Baixo	🟩	🟨	🟨	🟧	🟧
Insignificante	🟩	🟩	🟨	🟨	🟧

(Likelihood Of Derived Loss x Negative Impact)

	Insignificante	Baixo	Moderado	Elevado	Severo
Muito Baixa	🟩	🟩	🟩 5-6	🟨 13	🟧 4-7-8-9-10-11-12
Baixa	🟩	🟩	🟨	🟧	🟧
Moderada	🟩	🟨	🟧	🟧	🟥
Alta	🟩	🟨	🟧	🟥	🟫
Muito Alta	🟨	🟨	🟥	🟫	🟫

(Control Prevention Effectiveness x Likelihood Of Event)

	Raro	Não Provável	Provável	Muito Provável	Esperado
Muito Baixa	🟩	🟨	🟧	🟥	🟫
Baixa	🟩	🟩	🟨	🟧	🟥
Moderada	🟩 9-10	🟩	🟩 13	🟨	🟧
Alta	🟩	🟩	🟩	🟩	🟨
Muito Alta	🟩 4-7-11	🟩 5-8-12	🟩	🟩 6	🟩

Figure 9. Report first page

The data that was used to demonstrate only refers to the entire tool domain model minus the scope definition, the scope data was used as defined in the domain model, and the matrix construction was done as document [5], describes it.

All of the previously presented use cases that relate to the data provided have been tested and demonstrated, such as UC06, which provides reporting, as shown in **Figure 9**, where you can see the risk matrices, overall risk level and performance indicator, and the start of listing all risks.

7 Conclusion and Future work

In this section, the conclusions of this paper will be presented, as well as a brief summary of the possible future work that can be further developed on this risk register for INCM that is kept up to date with the risk management process.

7.1 Conclusion

Following this report, it can conclude that implementing good risk management has been very beneficial to the success of a company today. Many organizations, such as INCM, have been developing risk management frameworks following the best practices of some standards, such as ISO 31000 [1].

In order to make this risk management strategy effective, organizations tend to use risk management tools to assist in decision-making, turning the results more accurate. Developing this type of tool in Outsystems, taking into account the characteristics of the platform, the development is much faster, allowing the programmer to pay more attention to new requirements, which are requested by the customer.

The success of an organization depends on good decision-making by that same organization. To this end, the ultimate goal of this project is to have a stable and as complete version as possible of the new tool, which supports ISO 31000 [1]. Being easy and intuitive to use is another goal for the application.

7.2 Future work

INCM, like any organization, is undergoing small or major changes to its processes over time, so it is necessary to meet with organization regularly in order to keep the application updated to the risk management process and thus to establish new developments.

Still within the development that was done for the preparation of this dissertation would be a good practice, review with organization if the report that is exported to PDF meets your expectations, as well as if they do not need any other type of report. In the "Dashboard" part create filters to get different types of searches.

Lastly, it would be important to review with organization all the requirements that are defined in the document that were not developed, in order to understand if at this moment it will make sense to develop any of the requirements..

8 Referências

[1] Instituo Português da Qualidade (IPQ). NP ISO 31000. (2018). Gestão do risco. Linhas de orientação. Instituto Português da Qualidade.

[2] Marc Lankhorst; Jan Dietz; Erik Proper; Jose Tribolet; Terry Halpin; Jan Hoogervorst; Martin Op't Land; Ronald G. Ross; Robert Winter. (2013) Enterprise Architecture at Work - Modelling, Communication and Analysis. Second Edition.

[3] International Organization for Standardization(ISO). (2009) ISO GUIDE 73:2009: Risk management Vocabulary.

[4] Denis Premji. (2010) Desenvolvimento em tecnologia OutSystems de Aplicação para gestão de património.

[5] Vieira, R. (2018) "PA18 - Descrição do processo. Framework de gestão de riscos corporativos," Relatório Interno INCM.

[6] Eliza S. F. Cardozo; J. Benito F. Araújo Neto; Alexandre Barza; A. César C. França; Fabio Q. B. da Silva.(2010) SCRUM and Productivity in Software Projects: A Systematic Literature Review.

[7] Committee of Sponsoring Organizations of the Treadway Commission. (2017). ERM - Integrating with Strategy and Performance.

[8] Viera, R. (2018), Requisitos para o Sistema de Gestão de Risco Corporativo da INCM, INCM, Relatório Interno.