Risk Management in Business Continuity

João Pedro Cabral Teixeira
joao.c.teixeira@tecnico.ulisboa.pt

Instituto Superior Técnico, Lisboa, Portugal

May 2018

Abstract

Uncertainty is everywhere, it is a dangerous condition to be in, not being able to foresee what the future may hold, or the consequences of actions in the long term. But it can also be that some new and unforeseen opportunities may arise from that uncertainty. Nonetheless, the risk is there, companies, and any kind of organization, must make preparations so that they can best manage that uncertainty. Management Systems provide frameworks and processes so that organizations can better reach their goals and reduce the likelihood of any calamity or disaster. These Management Systems directly affect the capacity that an organization has of enduring negative impacts and the amount of time and resources that it takes to recover, therefore, it is important that these Management Systems have appropriate technological support to back them up. With this project we propose to analyze the current risk management application implemented in Associação DNS.PT with the goal of understanding the overall business context on which it is used, identifying the other components from the organization that interact with it and provide a documented appreciation of the tool, which will point towards new developments. Having concluded these objectives, we were able to provide this specific organization with necessary documentation to further optimize and develop this application according to their requirements and needs.

Key-words: Management Systems, Risk, Business Continuity, Enterprise Risk Management.

1. Introduction

Any organization, be it a startup or a multinational company, is exposed to risk. Unexpected events such as natural disasters, loss of capital, injuries to employees, among others, have a profound negative impact on the organization, which can lead to a halt to its activities or even permanent closure. It is imperative that organizations develop processes and tools that ensure the conditions to not only support these events but also quickly recover from the damage caused.

This need that the organizations have motivates the study of the theme of Business Continuity, that is to say, the development of methods that allow a business to continue to function within normality and recover in case of occurrence of harmful events.

An important tool and component of Business Continuity is Risk Management, because it allows companies to identify in a structured way the events that produce disruptive consequences in the business and helps to manage and to prevent them properly.

Risk Management helps organizations achieve their goals, for without the definition of procedures to indicate what actions to take in the face of negative events, the organization would be vulnerable to uncertainty, increasing the likelihood of losing its course.

The process of identifying risks, analyzing them, defining measures and implementing them is complex, and can become difficult to manage if there isn't an adequate support and meets the needs of the organization. In order to maximize the performance of these tools, there must be a broker aligning the various components of the organization involved in the process, and this is only possible if there is adequate documentation of all the components. In this context, an internship was carried out in the Association DNS.PT with the objective of analyzing and implementing a new version of the software application that supports its risk management process.

2. Related Work

In this chapter the concepts and themes used throughout the work will be discussed. The three main concepts of this project are Management Systems, Business Continuity and Risk Management, with a special focus on the latter due to its

relation to the process supported by the application.

2.1. Management Systems

Management Systems expand across a wide range of industries and when properly contextualized can help organizations become more competitive in their area. The International Organization for Standardization (ISO) defines a Management System as being "...the way in which an organization manages the inter-related parts of its business in order to achieve its objectives". The standards of Management Systems created by ISO help organizations to improve their performance by specifying a set of steps that organizations can implement.

The Management Systems implemented according to these standards follow the PDCA (Plan-Do-Check-Act) methodology (Figure 1) for the control and continuous improvement of their products and processes.

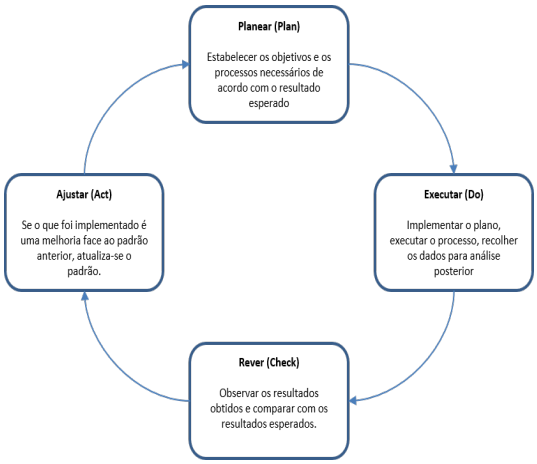

Figure 1: PDCA Method.

The main functions of each of the activities of this methodology are:

- Plan: Define the objectives and the necessary processes according to the desirable goal;
- Do: Implement a plan, execute it and retrieve data for further analysis;
- Check: Compare the output with the desirable;
- Act: If it is an improvement, update the pattern.

2.2. Business Continuity

Business Continuity is defined as the capability of the organization to continue delivery of products or services at acceptable predefined levels following disruptive incident [3]. These events can take the form of natural disasters, accidents at work, loss of technological support, negative media campaigns or even vertiginous falls in the stock market, among others.

In turn, Business Continuity Management is the holistic management process that identifies potential threats to an organization and the impacts to business operations, those threats, if realized, might cause, and which provides framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities " [4].

ISO 22301:2012 is the international standard for the implementation of a business continuity management system and is designed to help organizations minimize the risk of negative events. Specifies the requirements for "... plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise " [4]

2.3. Risk Management

As previously defined, the effect of uncertainty on the objectives and strategies of an organization is called "risk" and in turn Risk Management is defined as *"... set of coordinated activities to direct and control an organization with respect to risk and whose main goal is to define prevention and control mechanisms to address the risk attached to specific activities and valuable assets. "* [2].

Finally, the development, implementation and continuous improvement of a system for the integration of the risk management process with the other processes of governance, strategy and planning, allows the development of an effective risk management and aligned with the context and strategic objectives of the organization.

2.3.1 ISO 310000:2009

The ISO 31000:2009 aims to establish standards, principles and guidelines for effective and efficient risk management, which in turn helps organizations to achieve their objectives, improve the identification of opportunities or threats, and improve the allocation and use of resources for the treatment of risks.

Despite providing guidelines and general principles that organizations can use, it is not intended to promote uniform risk management. The plans and structures of risk management must be implemented, taking into account the specific needs of

each organization.

2.3.2 Risk Management Process

The Risk Management Process, defined by ISO 31000:2009 is represented in Figure 2 and includes the following activities:

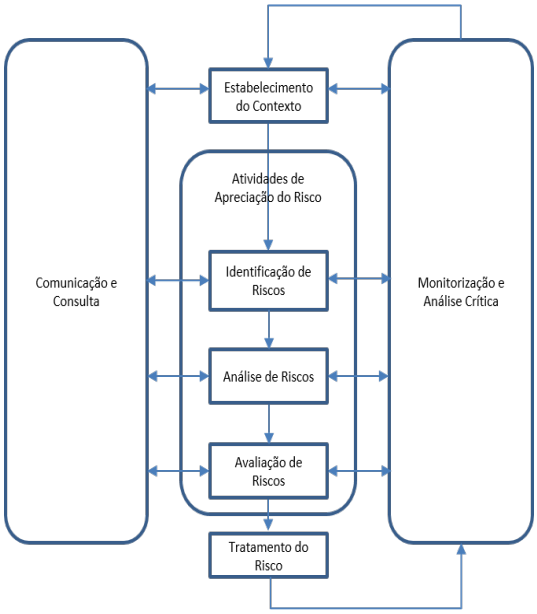

Figure 2: ISO 31000:2009 Risk Management Process.

- Communication and Consultation: Identification, recording and taking into account in the decision-making process the various perceptions that stakeholders have, since their views have a significant impact on decision-making;
- Establishment of the Context: The establishment of the context allows an organization to "...articulate their objectives, define the external and internal parameters to be taken into account in risk management and establish the scope and risk criteria for the remaining process" [1];
- Risk assessment process:
  - Risk identification: Registration of sources of risk, areas of impact, events, their causes and consequences in the context of the organization's objectives. It is a critical step because a risk that is not identified at this stage can be excluded in a later analysis;
  - Risk analysis: Remove meaning from the data collected earlier and define the negative consequences, or impact, of the risks and their likelihood. The combination of these two factors determines the level of risk and provides the information needed to assess the need for the risks to be addressed and which strategies and methods are most effective;
  - Risk assessment: Decision aid taking into account the results of the risk analysis, the risks that need to be addressed and the priority that must be taken in the treatment;
- Risk Treatment: Selection of one or more different strategies. that organizations can take on how they deal with different types of risk;
- Monitoring and Critical Analysis: The monitoring focuses on the constant improvement of the risk management process, through the documentation and registration of the information;

2.4. Enterprise Risk Management

Enterprise Risk Management (ERM) is a risk management framework that emerged from the recognition by several entities that risks should not be managed in isolation but rather identified, analyzed and controlled within a single structure.

Classical approaches to risk management, based on statistical experiences, do not capture all the changes that may exist in the markets and in the structure of the organization itself. In the figure 3 we can see the main differences between these two approaches [5].

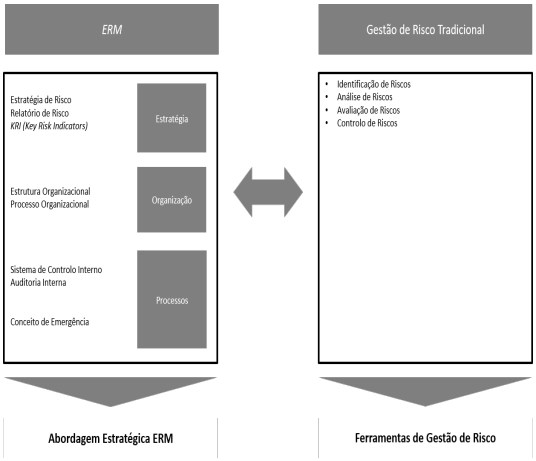

Figure 3: Comparison between ERM and Operational Risk Management.

The goal is to bring together all components and systems and develop an integrated, organization-wide risk management system with dynamic structures to guide not only the objectives but also the organization's strategy and culture.

There is currently no single framework defined and internationally recognized for ERM, however, there are already some frameworks that can be used as a starting point for their implementation. One example of these kind of frameworks is the Risk Maturity Model (RIMS).

This framework is defined as "...an assessment tool ... to develop and improve sustainable enterprise risk management programs" [6] allowing organizations to assess their risk management process according to a set of indicators and produce a report with key points for future improvements (4).

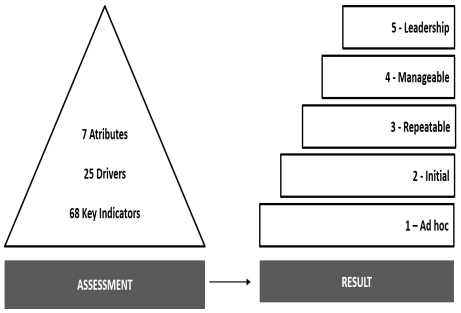

Figure 4: Risk maturity model (RIMS) [6].

This structure defines behavioral motivators for the creation of an ERM structure that creates value and maintains the integrity of the organization. The attributes that define this structure are:

- Focused process management;
- Management of the organization's risk appetite;
- Effective risk identification;
- Performance management;
- Resilience and organizational sustainability;
- Discipline in the search for the main problem of the process.

3. Analysis of the Problem

This chapter will describe the context of where this project came about, what were the challenges encountered, and explain the change of direction of the project from what was initially defined.

3.1. Context of the Problem

Associação DNS.PT, formally established on May 9, 2013, aims to manage, operate and maintain the registration of the top level domain corresponding to Portugal (.PT) complying with the law, the principles of transparency and publicity, its statutes and the best national and international technical, administrative and strategic recommendations applicable to it.

From a service delivery point of view, there are two types of clients that interact with the Registry, Associação DNS.PT: Registrars and Registrants.

- Registrars: Entity that purchases a domain package from the Registry to incorporate them as products to be made available to the end consumer. The aim of the Registry is to have the Registrars remove their workload by providing support to the final consumer;
- Registrants: Final consumer, individual or collective, who seeks to acquire a domain for personal or professional purposes.

In 2013, Associação DNS.PT initiated the implementation of a quality management system as a way of responding to the needs and demands of its business and guaranteeing certain levels of efficiency and effectiveness. The implementation of the quality management system followed the guidelines of ISO 9001: 2008, which is the ISO standard for quality management systems taken as reference at the time. Later, in view of the nature of its function, Associação DNS.PT started in 2015 the process of creating an information security management system following the references defined in ISO 27001: 2013.

In the implementation of the standard ISO 27001: 2013, and according to control A.17 in Annex A of the standard, the need to develop the theme of Business Continuity arose. In this context, a master's degree course was held in 2016, which developed the theme of "Risk Management Process for Information Security and Business Continuity", which resulted in the methodology of the risk management and business continuity process.

Subsequently, the introduction of the topic of risk management in the business came to be strengthened by the new version of ISO 9001: 2015 with an approach stresses more risk than its previous versions. Therefore, in order to support the information security management system, Associação DNS.PT has created a risk management structure in accordance with ISO 31000: 2009 and with the necessary technological support.

3.2. Analysis of the Organization and Application

In order to contextualize the application, the entire architecture of the organization including its processes, applications and technologies was

analyzed. This stage of the work was carried out with the aid of the Archimate nomenclature, and the Archi tool, and allowed to model the organization according to the layers of: Business, Application and Technology.

The main objective was to gain an overview of the entities involved in the entire risk management process. By using the Archimate language and the Archi tool it was possible to represent the various entities over the three defined layers.

Thanks to this project it is possible to visualize for any entity of the organization the relations and dependencies that it has, which allows to assure that the Association DNS.PT has the capacity to quickly realize the impact that each change can have in the organization. The Figure 5 shows all DNS.PT Association entities involved in the FP.02 risk management process.

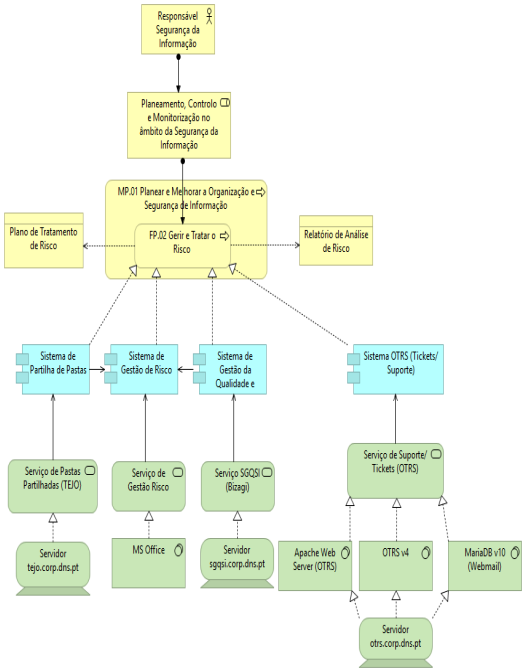

Figure 5: Entities Involved in the Risk Management Process of the DNS.PT Association

The application was analyzed according to three views: Data Model, UML Use Cases and User experience with the tool.

The main entities necessary to support the risk management process and systems identified in the Data Model were:

- **Asset:** Resources that support the information and business of the DNS.PT Association, including, paper and digital data, processes, people and technologies;
- **Information:** Not only electronic support (databases, PDF files, Word, Excel, and other formats), but also on paper;
- **Information System:** Set of assets that interact with one another to produce a product or provide a service;
- **Process:** Set of structured activities that result in the final delivery of a uniform product or service;
- **Risk:** The Effect of uncertainty on objectives; Control: Measure taken against a risk, which may be through: elimination, transfer, mitigation or acceptance of the risk, which are not mutually exclusive;
- **Control:** Measure taken against a risk, which may be through: elimination, transfer, mitigation or acceptance of the risk, which are not mutually exclusive;
- **Responsible:** The ”Responsible” entity corresponds to a user who has been associated with one or more artifacts (Assets, Processes, Risks, Controls, Information and Information System). This user must perform their functions, analyze, evaluate, implement, or validate them by the type of artifacts and responsibilities they hold.

Additionaly the Use Cases that translate the behavior and functionalities of the application, were represented using an UML Diagram as in Figure 6

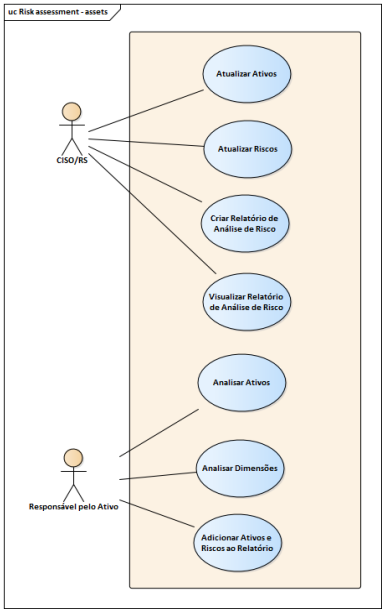

Figure 6: Use Case Diagram - Risk Management (Assets)

Finally we identified some issues in the User Experience regarding the physical constraint of being installed on only one machine which makes it necessary for the system manager to move to perform activities with other users.

From the analysis presented in the previous section, the following conclusions were reached:

- Although the data model used by the application supports the risk management process, its structure and organization makes it difficult to identify the key entities involved in the process, improving the model and capture errors, and not conformities;
- The representation of the current Application layer indicates a need to specify the components of the application layer in addition to changing the definition of ”Information Systems” referenced in the organization’s documentation;
- The requirements raised with Associação DNS.PT identify a wider range of uses cases that have not yet been defined and need to be specified;
- The need to definitively separate the roles of those responsible for the various objects in the application. Another set of user types was delineated from the meetings with the organization, which further increases the degree of complexity of the application.

4. Results & discussion

In this chapter it will be presented and described the improvement proposals prepared to meet the needs of Associação DNS.PT. These have taken into account the operational needs of the organization and the interests of its stakeholders.

4.1. Data Model

It started by revamping the data model, redefining the key concepts and entities to support the risk management process. The following changes to the data model were suggested:

- Definition and simplification of the entities about which the risk will be analyzed through the agglomeration of the entities ”Process”, ”Information System” and ”Information”, under the ”Asset” entity, thus simplifying the structure of the model;
- Identification for each type of ”Asset”, of which performance indicators to be analyzed, defining the entity ”Indicator” as a separate entity and characterizing each type of ”Asset”. Indicators are to be a set of defined metrics, oriented to the organizational strategy, that aim to define the goals to be achieved;
- Association of a ”Responsible” to each ”Asset”, ”Risk”, ”Control” and ”Indicator”, since each user can be associated with one or more of these entities;
- Definition of entities ”Risk Analysis” and ”Risk Treatment Plan” as the result of the ”Asset” - ”Risk” and ”Risk” - ”Control” relationship respectively;
- Definition of the relationship of the ”Stakeholder” with the other entities, so as to ensure communication with stakeholders in the process.

The final version of the Data Model proposed to Associação DNS.PT for their risk management process is represented in Figure 7.

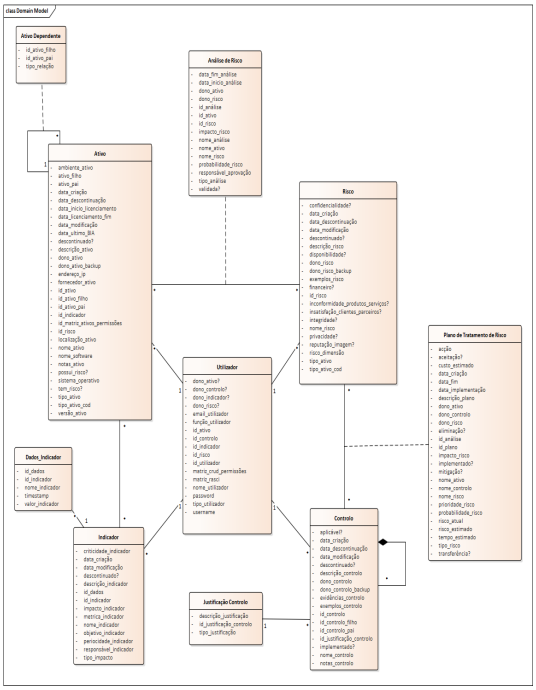

Figure 7: UML Diagram - Data Model Proposed

After analyzing the various representations of Associação DNS.PT created in Archimate, an alternative architecture was developed for the various diagrams created based on the rules defined by the nomenclature Archimate. The changes suggested were:

- Full adoption of Archimate nomenclature and Change the designation of ”Information Systems” to ”Application Services”;

- Adding missing Archimate components, such as the list of ”Application Interfaces” components through which Business Processes access Application Services;
- Specification of the Functionality of the Application Service ”Serviço de Gestão de Dados”.

The Use Cases for this application were also redefined taking into account the DNS.PT Association.

- Asset Management;
- Risk Management;
- Control Management;
- Indicator Management;
- Report Review;
- Authentication;
- Notifications;
- Upload and Download of Files
- Traceability

5. Conclusions

During this work it was possible to deepen my knowledge of ISO standards, more closely to ISO 22301: 2012 and ISO 31000: 2009. The internship in the DNS.PT Association allowed me also to have privileged access to information, such as the structure and processes implemented in the organization.

It was equally important to have been able to watch the operation first-person application and to be able to study how the organization's employees used it as well as the main needs.

This was only possible with the help and support of the DNS.PT Association. The initial objective of the work was to effectively develop a new version of the computer application, however as already described, this scope was eventually adjusted to the reality of the effort that would be necessary to achieve the expected objectives. The main value that this work added to the organization was to allow it to have greater documentary support on which to base future developments of the application.

Although the aded value of this work does not contain a presentation of alternative technologies to support the application, it establishes views that will make it easier to choose these technologies.

The review, analysis, representation and creation of documentation performed are a good basis of work in order to proceed to the next phase, the proposed objectives for this work were reached culminating in the preparation of the analysis report delivered to the DNS.PT Association.

The literature often describes risk as the possibility of suffering damage or loss. Despite this seemingly so negative and pessimistic definition, we all face risk in our day to day, and these risks can have consequences that manifest in the following moment like a few years.

Uncertainty makes the use of this type of tool more and more useful and rewarding. I hope that with this project you have been able to contribute to give the DNS.PT Association a less uncertain and secure future

References

[1] International Organization for Standardization. ISO / FDIS 31000 Risk Management - Principles and Guidelines, 2009.

[2] International Organization for Standardization. ISO Guide 73:2009: Risk Management Vocabulary, 2009.

[3] International Organization for Standardization. ISO 22300:2012 Societal Security — Terminology, 2012.

[4] International Organization for Standardization. ISO 22301:2012 Societal Security — Business continuity management systems — Requirements, 2012.

[5] Prof. Dr. Olaf Passenheim. *Enterprise Risk Management*. 2013.

[6] Risk and Insurance Management Society Inc. RIMS Risk Maturity Model (RMM) for Enterprise Risk Management.