A Risk Management Process for Information Security and Business Continuity

João Carlos Gonçalves Fialho
Instituto Superior Técnico - Taguspark
joaogfialho@gmail.com

ABSTRACT

It was from the DNS.PT internship proposal that the theme for this dissertation comes up, the proposal was the creation of a business continuity plan accordingly with ISO 22301 standard. After the standard analysis, the challenge of a risk management process creation has been made.

Since the organization already had a risk management process for information security (ISO 27001), the problem to solve is the creation of a risk management process for both standards.

The problem's relevance is the demonstration of both standards complementarity and the possibility to manage risk from a global perspective.

Both standards refer the ISO 31000 standard as reference for risk management, so I decided to use this standard as base for my work.

By analyzing this standard, I realized that, it states several risk assessment techniques through ISO 31010 standard. The chosen method was BIA, due to be mandatory for business continuity and applicable at information security.

In order to create the process, I used the ISO 31000 suggestion as a high level process architecture and develop a process per activity.

In the end, I was able to demonstrate the complementarity of standards, the global risk management, which is a benefit for an organization that can have all the business points of view in risk management.

Keywords

Business Continuity, Information Security, Risk Management Process, ISO standards, Business Continuity Plan.

1. INTRODUCTION

Almost all organizations nowadays are having the need to implement a system to manage the information security as well a system to manage the business continuity. In order to implement this kind of system the organizations usually adopt well known frameworks such as ISO family, COBIT or ITIL.

The growing concern about these areas isn't only a concern for the organizations, in many areas regulators or the government are creating laws and best practices that obligates organizations to comply to this needs. This happens because when an organization complies with this recommendation it transmits trust to the market and to the consumer, and trust is one of the most important assets nowadays.

In both areas, information security and business continuity, is becoming mandatory the existence of a process that manages the risks that are relevant to that specific domain. This need can be found in every framework, as all of them in one way or another describes ways to manage your risk.

It has become very clear to me the how much this concerns of manage the risk, assure business continuity and information security. Furthermore, the relevance of this themes today helped in finding the motivation to answer the needs of both areas in the matter of risk management, by proving their complementarity.

To accomplish my goal, I will analyze the ISO family framework, specially the ISO 22301 for business continuity, ISO 27001 for information security and ISO 31000 for risk management. The option for the ISO framework is due to the fact that the organization were this work will be developed has already implemented the ISO 9001 and ISO 27001 frameworks, this way it is possible to use some of the work that has been done by the organization to achieve the certification of the mentioned standards.

2. STATE OF ART

In this section I shall expose what is the state of art of business continuity and information security regarding the ISO standards of this domains.

2.1 Business Continuity

The business continuity concept is a result of the need that organizations have to develop formal mechanisms to allow the continuation of business in case of catastrophe or unusual interruption of its normal activity. According to ISO 22301: "*capability of the organization to continue delivery of products or services at acceptable predefined levels flowing disruptive incident*". [1]

As the organization already has the certification in some management system of ISO, it is of my interest to analyze what are the common requirements between the ISO standards.

Requirements	ISO 9001:2008	ISO 22301:2012	ISO 27001:2005
Management System Objectives	5.4.1	6.2	4.2.1
Management System Policy	5.3	5.3	4.2.1
Commitment of Management	5.1	5.2	5
Documental Requirements	4.2	7.5	4.3
Intern Audit	8.2.2	9.2	5
Continual Improvement	8.5.1	10	8
Improvement	5.6	9.3	7

Table 1 - Mapping between ISO standards. [2]

As we can see there is a strong relationship among ISO standards for management systems, this relationship is one of the biggest advantages of implement these standards once you are sparing some work by using the documents produced for the another ISO standard. This becomes a great encouragement to implement and

merge the business continuity standard with the information security standard.

2.1.1 ISO 22301 Standard

This standard has a huge focus on establishing objectives, monitoring and continual improvement along the life of the company. The main points of this standard are: [3]

- Point 4 – Organization Context;
- Point 5 – Leadership;
- Point 6 – Planning;
- Point 7 – Support;
- Point 8 – Operation;
- Point 9 – Performance evaluation;
- Point 10 – Improvement.

At point 4, this standard explains the importance of establishing the context of an organization. First of all, belongs to the company the definition of business continuity inside scope and all the external factor that may have an impact or interest on business continuity. [3]

The leadership role is the organization guidance through the process. It must be an example of commitment, and be capable to motivate and involve all the workers on the process. The planning step is where we must define all our planning. This planning must be detailed, consistent, flexible in order to facilitate the adaptation as new circumstances arises, measurable and allow the monitoring. Only with a plan and objectives that has these characteristics we are in accordance with the ISO standard. [2]

At point 7, it's said that "*The day-to-day management of an effective business continuity management system relies on using the appropriate resources for each task*". [2]

This puts the responsibility of providing all needed resources on the management.

The point 8 is dependent of the previous point, because it is impossible to accomplish a correct operation without a good support, it is on this point that we have definition of the risk management process. Although, before we can manage the risk according to this standard it's mandatory the execution of Business Impact Analysis (BIA) inside the established scope on the context. After completed the BIA we finally can enter on the risk management process, the recommendation given is to implement a process accordingly to the ISO 31000 standard, it's crucial that we understand that both BIA and risk management process are the base of business continuity. [2]

There are many ways to evaluate the performance of our system and belongs to the management the task of choosing which best alternative. Finally we enter on the review and monitoring phase, here we must do a regular checking on our system in order to detect improvement opportunities. [2]

2.1.2 Risk Management in Business Continuity – ISO 31000

As we could see it's mandatory for the standard ISO 22301 the creation and maintenance of risk management process, this process must meet the requirements of the ISO 31000 standard, accordingly to the business continuity standard.

The ISO 31000 standard states some guidelines and principles that help us create and maintain such important process. Before go further it's important state some concepts:

- Risk management creates and protects value, helps in achieving goals and better performance;
- Risk management is always dependent of the context;
- Risk management must be included in all scope process;
- Risk management helps the decision maker;
- Risk management quality depends of the information quality.

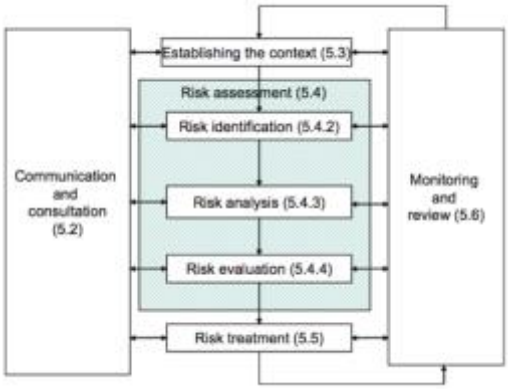

Figure 1 - Risk management process. [4]

As we can see in figure 1, the process is cyclic and aims the continual improvement.

The point 5.2 (Communication and Consultation), states that must exists a way of communicate with stakeholders either for seeking some consulting or for demonstrate and inform what has been done. This can be done in any time, as we can see by the process proposal. [4]

At point 5.3 (Establishing the Context) we can do a direct mapping with point 4 of ISO 22301, since the risk management process must be applied to all scope. Here is expected to produce a risk policy and risk criteria for the organization, as the definition of the chosen method for risk evaluation. [4]

After establish the context, we enter in phase of risk assessment, point 5.4, here we must identify all risks and controls that already exists in the organization, in addition to identify all risks we must identify causes, consequences and impact on business process, also must enter in our analysis the systemic risk. [4]

The next task is the risk analysis, here we have to analyze the all the risk information gathered, the objective of this analysis is to understand risk probability, risk frequency, risk cause, risk impact and consequences on business and what factors may influence this attributes. [4]

In risk evaluation is given to each risk a level, according to some scale created by the organization, this level must be coherent with the analysis done in the previous step and using the already chosen method. After that we enter at point 5.5 (risk treatment), here each risk level is compared with the risk criteria and for the risks above this threshold a risk treatment plan is developed, this plan consists in a set of controls design to mitigate the risk level to below the risk criteria. The final step is the monitoring and review were we aim to improve and review the process over time. [4]

2.2 Information Security – ISO 27001 standard

The main objective of information security is to preserve the accessibility, confidentiality and integrity (CIA) of information. It may also involve protection and preservation of information

authenticity, assuring the trustworthiness of information. An organization that implements an information security management system broadcasts an image of trust to the outside, which is fundamental nowadays. [5]

There are some concepts that we need to keep in mind:

- **Threat**: Potential cause of an unwanted incident.
- **Vulnerability**: Asset or control weakness that can be explored.
- **Event**: Change in a set of circumstances.
- **Consequence**: Outcome of an event that affects objectives.
- **Control**: Measure that modifies risk.
- **Impact**: Negative change on the achieved business objectives.
- **Asset**: Anything that has value for the organization.

The ISO 27001 standard specifies some requirements to implement, establish and maintain through time a management system for security information. [6]

As the rest of the management system standards of ISO, the points 4 and 5 (about establish context and leadership commitment) is a direct mapping of the others (see table 1). [6]

The point 6 can be interpreted at the light of the ISO 31000 standard, since this standard applies the same logic of the ISO 22301 standard in referencing the ISO standard for a generic risk management process. The point 7, 8 and 9 are a direct mapping of points 7, 9 and 10 of ISO 22301. [6]

This logic that was applied to ISO 27001 could be applied to ISO 22301, once few things changes besides the context.

2.3 Risk Management Technique for Information Security and Business Continuity

After analyze both standards it became very clear to me that in order to manage the completion of the risk management process I would need to find a technique for the risk assessment part. Such technique must be useful for both domains by allowing the aggregation of both views in risk identification and risk analysis.

In standard ISO 31000 exist the reference to another ISO standard, the ISO 31010, this one contains a set of risk assessment techniques to be used in several domains accordingly with the management needs.

One of the referenced techniques is the BIA technique, as we had seen the BIA is mandatory for the business continuity domain, as it must be done with or without a risk management process, and for the information security domain it isn't a mandatory technique, as the standard refers only to ISO 31000, this way I selected the BIA as my technique for the risk management process.

The BIA has 3 key points [7]:

- Identification of the organization key process criticality, activities and associate assets, as well all the key dependencies;
- How the disruption events affect business continuity objectives;
- The needed resources for impact managing and recovering.

The BIA can be divided in 3 steps, scope definition, data collecting and reporting. [8]

In Scope definition we have two phases, at phase one we need to understand where we will implement the BIA, this is very important because it's critical that we apply the BIA only where it is needed and where we are capable of do it, per example chose only critical department or departments that are motivated or understand the BIA importance. [8]

On phase two we have to elaborate the BIA policy and two establish how the BIA will be applied to each part of the scope. [8]

After the policy being completed, we start the data collection step, here we start asking questions to the business in order to gather information. [8]

At this step there is three questions that must be answered [8]:

1. What should be included inside the scope?
2. What should be put aside?
3. How to control the human reaction of considering everything important and critic, and identify what really is critic for the business?

In this part it's truly important that the designed team for the job has a full comprehension of the business, because it is common to drop out an IT system that doesn't belong to the scope but supports a critical process in some way. [8]

There are several ways to gather information, usually in BIA we use personal questionnaires, workshops or discussion tables in order to facilitate the gathering and the comprehension of our objectives by the other part. [8]

On the end we must be able to define some concepts like Recovery Time Objective (RTO), Recovery Point Objective (RPO) or dependencies for each scope's process, system and asset. It's these concepts that will allow us to set a critical level to each process, to establish a recovery order and resource allocation. [8]

Once gather all the needed information it's time to move forward for the reporting step. As the name says, here is where the BIA report is written. However, this isn't straight forward as it seems, first we must check all the information to assure that the information is valid. As soon as we are done with the information check, then we write the report and compare our conclusions with the conclusions of previous years to see if was some improvement or not. Finally, we must put all the values defined for the processes, the RTO and RPO. [8]

3. Problem Analysis

This work was a project proposal that has been made by the DNS.pt organization, the DNS.pt is a service provider that manages the internet domain ".pt" in Portugal. The project that was proposed consisted in the creation of a Business Continuity Plan, since the DNS.pt already were certificated on the ISO 27001 and ISO 9001 standards.[1]

The organization decision what to implement the ISO 22301 standard for business continuity, since this allowed them to use much of the work done, as we have seen by the standards mapping.

Here upon the problem to solve for my dissertation was to create and implement a risk management process for both information security and business continuity, since these standards have the same mandatory risk management process. This process must have in consideration all the requirements of both standards and respect the organizations culture.

[1] https://www.dns.pt/pt/

4. Solution Proposal

My proposal is the creation of a risk management process that allows an organization to bring together the ISO standards for business continuity (ISO 22301) and information security (ISO 27001).

To build this process, I used the process architecture given by the ISO 31000 standard as base for my development.

In order to apply this architecture on the problem domain, I created 5 processes that interact between them as the demonstrated flow of figure 1. These process are:

- Context Establishment;
- Risk Assessment;
- Risk Treatment;
- Monitoring;
- Communication;

In next section I shall describe all my proposals for each process. There are some interactions with some repositories within the process, to facilitate the comprehension, the description of each repository is written in the table 2.

Table 2 - Repositories content.

Repository	Content
BIA	- Stakeholders; - Legal Requisites; - Technological architecture of business; - BIA method;
Registo de Riscos	- Process risks; - Risk probability/frequency; - Risk impacts on business; - Risk level; - Risk controls; - Risk treatment plans;
Monitorização	- Monitoring reports of the processes;

4.1 Context Establishment

The establishment context process objectives are:

- Objective definition for Information Security and Business Continuity;
- Policy definition for Information Security and Business Continuity;
- Internal and external context definition;
- Risk and impact assessment method definition.

It's this process which defines the business, identifies the organization processes, its dependencies and relations, on the processes dependencies it's necessary to obtain the technological architecture, once this has become more and more vital these days. One of the factors to be taken on account is the understanding of processes relationships, how they interact among them and with business, per example if process x is unavailable how business reacts? Which processes become unavailable to?

Is because of this that turns to be extremely important the comprehension of context either internal or external, the identification of all factors that can impact the business, since relationship with stakeholders, key drivers, trends that may affect objectives or adopted standards and guidelines. [4]

On the other hand it's necessary to create an integrated policy for business continuity and information security where it must be stated the organization's risk appetite, furthermore is necessary the business dependencies identification. [4]

After the policy creation and dependencies identification the next step is jumping into BIA, by defining the RTO, RPO of each process, identify each process's criticality by the impact assessment. This process can be observed on figure Figure 2 - Context Establishment Context

.

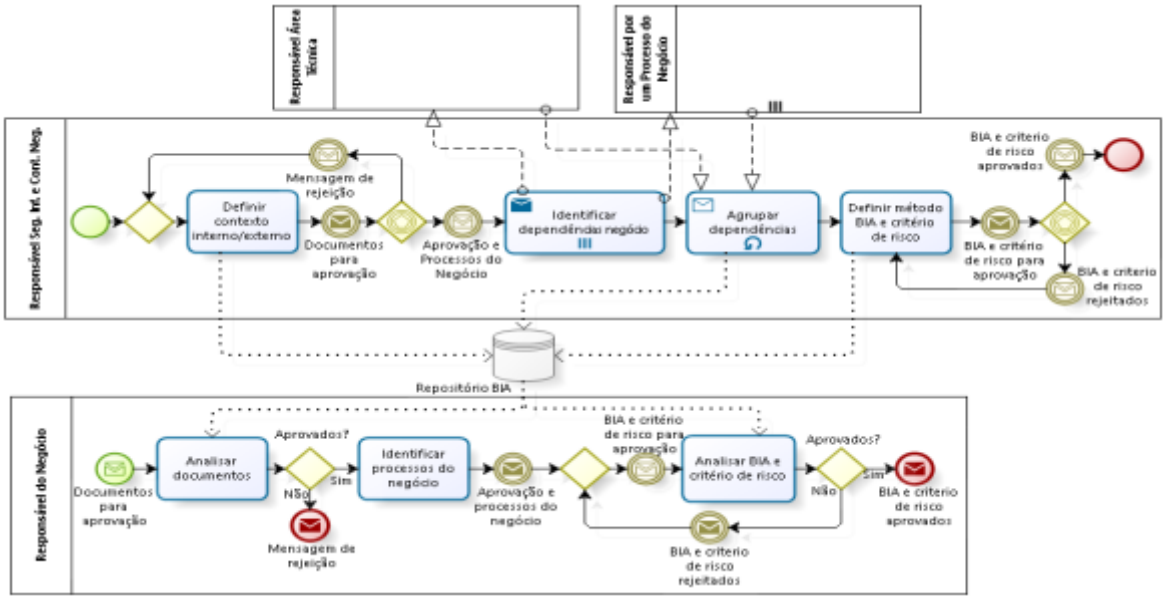

Figure 2 - Context Establishment Context

4.2 Risk Assessment

The risk assessment process has the following objectives:

- Risk identification for Information Security and Business Continuity;
- Control identification for each risk;
- Associate risk with processes;
- Give a coherent level to each risk.

It's in this process where we are going to apply what we have defining at context establishment. Starting with risk identification where all the risk within the scope must be identified, it's very important not overlook any risk, since it may have an impact later.

While the risk identification is going on, we start creating our risk register, the risk register is where we are going to put every information gather about the risks, since events, frequency, probability, controls, pretty much all that is gather and produced on this step belongs there.

We may think that once we are identifying risks we can overlook the controls, although, in order to speed up the process since we are already looking for risks, we also look for the controls, this way we are turning the next step way more easy.

During the analysis phase we must understand which events what more likely to originate risks, estimate with the most possible precision the impacts and consequences associate with a risk, this impact and consequences must be aligned with both problem domains. Another crucial factor to bring to this analysis is the frequency or probability of occurrence during a pre-established period of time (the duration of one period is what the organization considers more suitable to business).

After the analysis we evaluate the risk by giving a level to it. To give this level as said there are several techniques, the one chosen is BIA. The BIA uses several criteria that we already have identified such as impact, consequences, probability or frequency of occurrence to set a level to a risk, by setting this level we are also giving a classification in terms of critically to all risks. This criteria can be used, normalized as we wish, since there isn't a pre-defined rule about which one we have to use and how we have to use it. [1] [7]

We can observe this process modeling in Figure 3 - Risk Assessment Process.

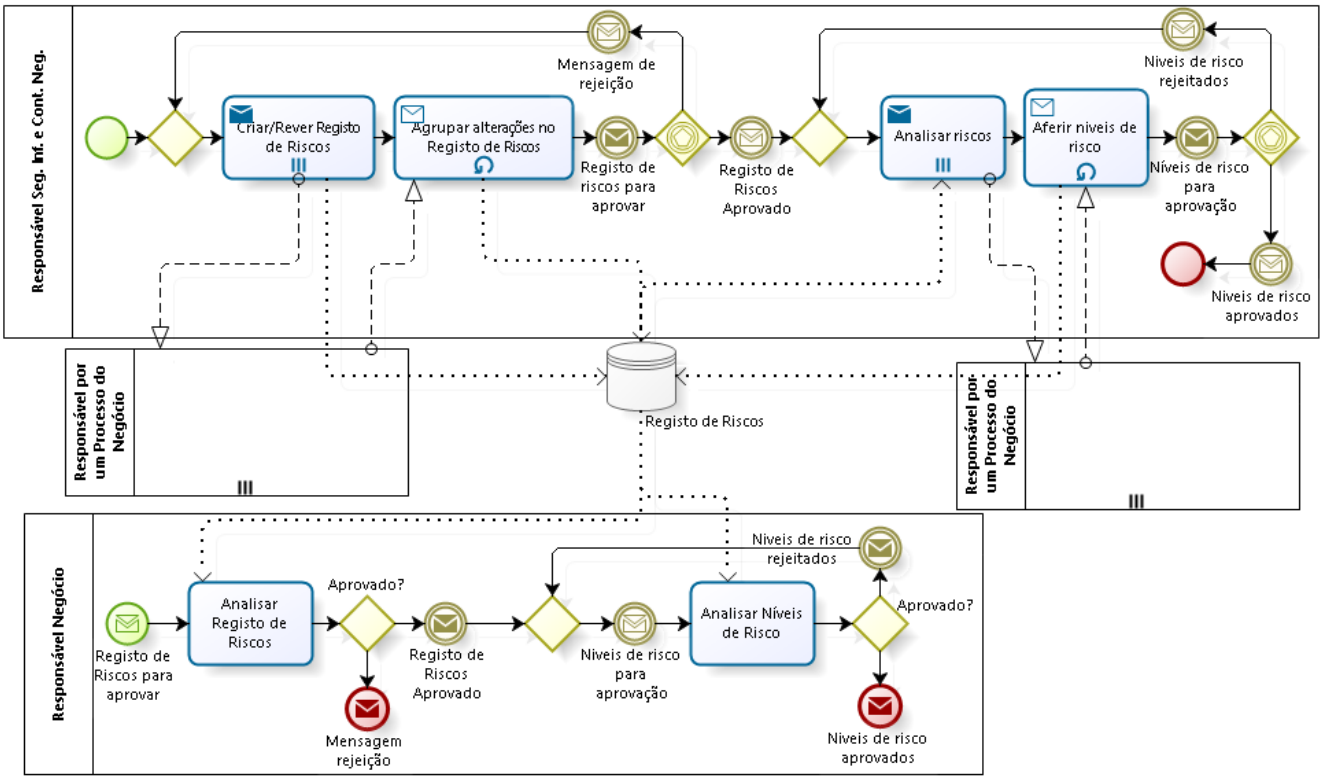

Figure 3 - Risk Assessment Process

4.3 Risk Treatment

The risk treatment process objectives are:

- Control definition for the identified risks;
- Update of old controls;
- Risk mitigation for an acceptable level.

On risk treatment we receive as input the risks level that we gave in last step. With this input we have to create a plan that manages to bring all risks levels below the defined threshold (risk criteria).

This mitigation ca be done in several ways, there isn't any rule about how many controls we need to have in each risk, since we also ca share the risk with a third party. [4]

On this plan we must include the controls that already exists, add new others and delete the obsolete ones. It's important that the control definition, update and deleting, be done with the process owner collaboration, because the process owner has an unique view of the process and can give a value input to the plan.

After defined all controls we need to calculate the cost associated to each control, this cost calculation although appears to be a minor task it isn't, since the cost of a control helps the management on the decision making process by prioritize the controls by impact and cost.

Once finished all the calculations of the costs the plan must be approved, in the approval the management must choose which controls are applicable according with the budget available. This why is so important to know the risk level, the real effect of a control and a cost of a control.

The diagram produced to modeling this process can be observed in Figure 4 - Risk Treatment Process.

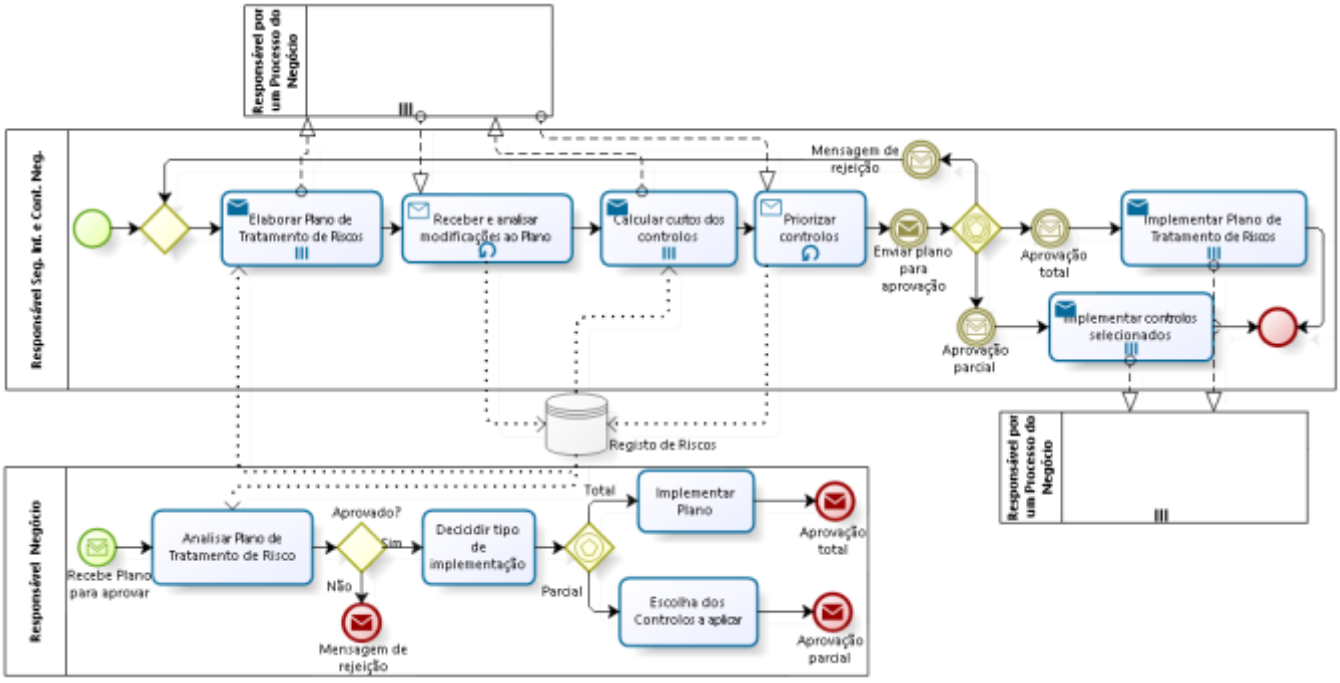

Figure 4 - Risk Treatment Process

4.4 Monitoring

Analyzing the ISO 22301 and ISO 27001 standard we realize the importance of the review and monitoring process, happens that as we can see by **Error! Reference source not found.** this process is also included on the risk management.

This process intents to respond to the ISO 31000 standard requirements for monitoring and reviewing, it responds to the need of review all the work done on the previous steps in order to check if everything goes as planned, if is necessary to modify something and if exists an improvement opportunity. [4]

In order to accomplished the objective of monitoring all processes I divided the monitoring process in 3 sub-processes, context establishment, risk assessment and risk treatment.

4.4.1 Context Establishment

On the context monitoring the objective beyond the review of all work done, is to understand if something within the internal or external context of the organization has changed, like new guidelines by the regulator, new stakeholder, some kind of political change, or internally some technological change in the IT systems.

The BPMN modulation for this process can be observe at Figure 5 - Monitoring Context Process.

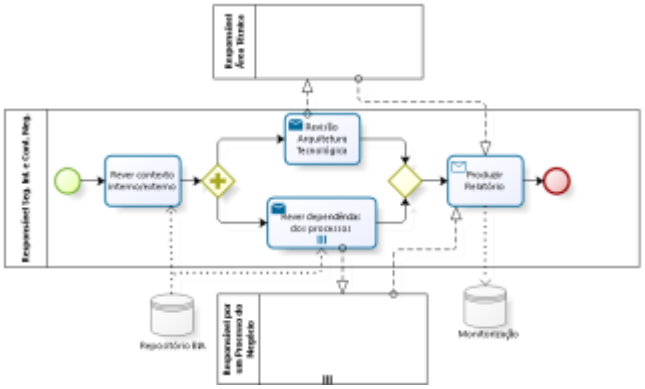

Figure 5 - Monitoring Context Process

4.4.2 Risk Assessment

On risk assessment monitoring we need to have present that a change on the context usually implies a change at risk assessment, because new risks arise, old ones disappear, change in risks impact, consequences, frequency or probability, all of this can happen after a change in context. So usually after review the context we should review our risk assessment.

It's usually that standards like ISO 27001 have a recommendation to re-assess the risks in a periodic way, the one-year period is the more common. With this process that I purpose instead of start the

risk assessment process all over again we can first do this one and only re-assess the risks if needed.

The BPMN modulation for this process can be observe at Figure 6 - Monitoring Risk Assessment Process.

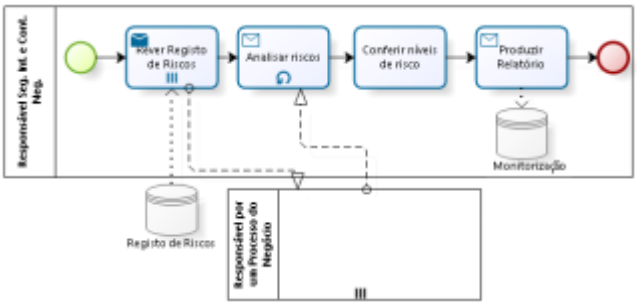

Figure 6 - Monitoring Risk Assessment Process

4.4.3 Risk Treatment

The risk treatment monitoring has two big objectives, the first one is to understand if the controls deployment occurred as planned. The second one is assessing the control efficiency, this is, if the control produced the desired effect on the risk.

By assessing the control efficiency, we are assuring that the process is improving, since we are detecting ineffective controls to replace for new ones. If it is noted that new controls are needed the recommendation is to review the context and the risk assessment to understand if we need to re-start all the process by the context establishment.

The BPMN modulation for this process can be observe at Figure 7 - Monitoring Risk Treatment Process.

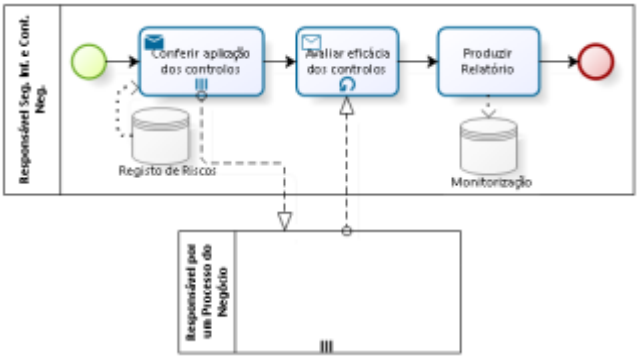

Figure 7 - Monitoring Risk Treatment Process

4.5 Communication

Among all the process it's necessary maintain communication with stakeholders, either by consultation or by reporting.

The organization stakeholder can be used as consultors at any phase, the management may feel the necessity to ask for some expertise or help in order to improve the process. On the other hand, the organization must assure that is responding to the stakeholders concerns with the process, to ensure that these concerns are taken into account the organization can communicate with stakeholders in order to get some input about the work. [6] [1] [4] [5]

Although not every stakeholders input may be applicable, because it's cost-benefit relation not be worth it or by simply doesn't fit the organization culture.

The BPMN modulation for this process can be observe at Figure 8 - Communication Process.

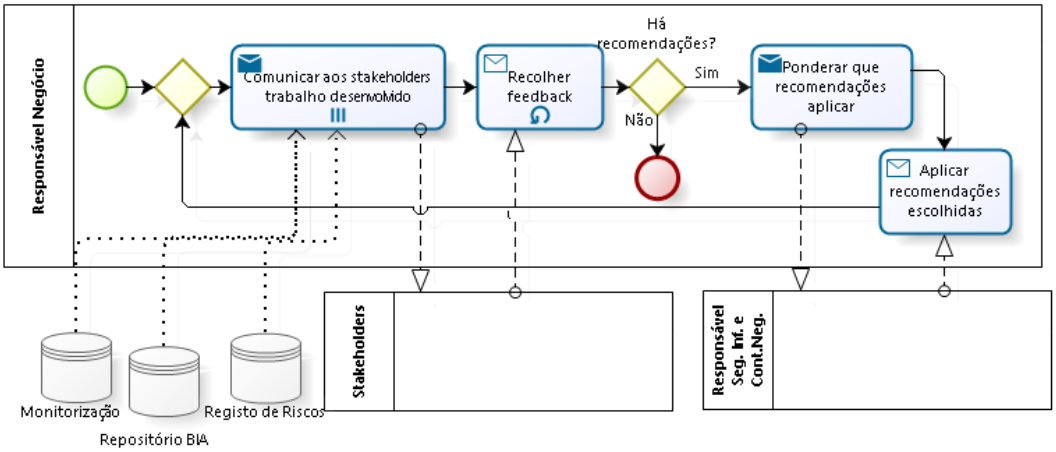

Figure 8 - Communication Process

5. Solution Application

In order to produce a quality work, my first step was the objectives identification:

- Create a Risk Management Plan;
- Integrate my work within the organization culture and processes;
- Get the management approval.

After established my objectives I ask myself what challenges I needed to surpass:

- Understand business;
- Understand organization's culture;
- Adapt my risk management process to organization's culture;
- How to re-use all the done work for the other ISO standards certification.

To understand business, I conducted some interviews with the staff, this interviews were very helpful because allowed me to get more into the business reality and that way I managed the conception about how I should conduct my approach.

Since the DNS.pt already had the certification in the ISO 27001 and ISO 9001 standards, it was very clear to me that I had to use all this advantages. One of them was that already existed a risk management process for information security and it implied that all the workers were familiar with risk management. This may be one of the biggest advantages I could had, everything became easier.

My first step was review the context, create a new policy to accommodate the business continuity point of view, check the stakeholders list, the legal requirements that needed to be answered with the business continuity accretion.

As soon as I complete the legal stuff, I started the technological architecture mapping with the IT director and the system's owners to understand how the system works and responds to processes and what is within each system.

This time wasn't needed the processes review because it happens that this work coincided with the ISO 9001 certification revision and that part was assigned to the quality team.

In order to create a policy, I reviewed the information security policy and introduced some changes to accommodate the business continuity theme.

Once established the common policy for information security and business continuity, it was time to designed a BIA method to apply on the risk management process.

To create my BIA method I used the recommendation of ISO 31010 [7] and of "*The Definitive Handbook of Business Continuity Management*" [8], of course bearing always in mind the reality of DNS.pt.

The first step on BIA were the objectives establishment:

- Determine the business processes criticality and recovering;
- Identification of the impacts on business due to a process interruption;
- Recovering priorities identification for the business resources.

Once that was already there an impact scale for information security, in order to facilitate the approach, I adopted the same scale used, only changing what each impact level means. This scales combined with the critical times RTO and RPO, defines how much critical a process is.

Beyond the importance that BIA has for a business continuity plan where is core concern knowing how to prioritize the recovering tasks, it's also important for the risk management process because it will have influence upon the risk level of the assets.

After established a method and defined the impacts it's time to spread the impact level for the process dependencies, to do that the responsible team for the process gather some reunions with processes owners in order to understand what assets are critical or not to a process. In order to understand this, we need to use some pre-established questions for focus maintaining, such as:

- It's possible to complete your process without this asset?
- How much time does the DNS.pt endure without this process?

By assigning to each process an impact level, we also assign a RTO and RPO time and by assembling all this factors the concept of criticality arises and is given to each process and asset within the process, if one asset is used by n processes it keeps the most critical level.

Since there was already calendared a risk management review for the ISO 27001 information security annual review, we took the opportunity and added the business continuity risks at risk identification stage. At risk analysis it was asked to put the business continuity concern on the analysis and use the BIA results as an auxiliary.

As the top level domain manager by IANA's recommendation is obligated to ensure the continuity of the service and the organization already complied with the international best practices. All the identified risk didn't produce any effect on the process, this is, it wasn't necessary the implementation of additional controls.

6. Conclusions

During this I seek answering the requirements of two ISO standards the ISO 22301 for Business Continuity and the ISO 27001 for Information Security, these two standards in organization that rely a lot of technology systems and processes are deeply connected, as we have seen there is lots of requirements in both standards that can be used in the other when we talk about technology.

One of the conclusions that I took from this work was the fundamental role of the risk assessment technique, only with the right choice I was able to merge these two standards in only one risk management process. In this specific case, only BIA will allow such integration, since for business continuity it's mandatory and I had to do it anyway.

By thinking in business continuity we have a broader sight on business which allows to think a bit ahead, by thinking in the risk impacts on business. On the other hand, the information security allows that when thinking only in business continuity we remember that we need to ensure the information security in case of disruption.

One disadvantage is that the context establishment as a great influence in all process and if a well-defined and structured context is one more step through a risk management process of excellency. On the other hand, a poorly defined context is also a step through, but this time through a potential problem that may put at risk the business continuity itself. Because we may be dropping out something important that may contain very dangerous risks.

Finally, I think that doesn't make sense think in this two domains separately, since the information security only makes sense if we assure the business continuity and the business continuity only makes sense if we manage to keep the information security.

7. References

[1] ISO, ISO/FDIS 22301, Societal security - Business continuity management systems – Requirements, 2012.

[2] Professional Evaluation and Certification Board (PECB), Whitepaper ISO 22301: Societal security - Business continuity management systems.

[3] BSI, Moving from BS 25999-2 to ISO 22301: The new international standard for business continuity management systems.

[4] ISO, ISO/FDIS 31000, Risk Management — Principles and guidelines, 2009.

[5] G. Mateus, A Risk Register for Information Security - Relatório de Projeto de Dissertação do Mestrado em Engenharia de Telecomunicações e Informática, IST, 2016.

[6] ISO, ISO 27001, Security techniques - Information security management systems - Requirements, vol. 2, 2013.

[7] ISO, ISO/FDIS 31010, Risk Assessment — Risk Assessment techniques, 2009.

[8] D. Andrew Hiles FBCI, The Definitive Handbook of Business Continuity Management, Kingswell International Limited.

[9] ISACA, COBIT® 5, 2012.

[10] N. Gibbs, COBIT 5 for Risk, Vancouver: The Institute of Internal Auditors International Conference, 2015.