Defining an Enterprise Architecture viewpoint to support Risk Management

Ruben Carlos Batista Louro
ruben.louro@tecnico.ulisboa.pt

Instituto Superior Técnico, Lisboa, Portugal

October 2018

Abstract

Enterprise Architecture (EA) refers to an alignment between an organization’s IT and business, from which results an architecture description. Risk Management (RM), which is a process of dealing with risks associated with an organization’s assets and finding solutions to prevent or mitigate such risks, can take advantage of these architecture descriptions in order to improve its efficiency. EA on the other hand, can also take advantage of the results produced by RM in order to support its architecture management. In order to combine the process of risk management with enterprise architectures, this aim of this dissertation is to implement a risk management scenario viewpoint in an existing enterprise architecture tool called Atlas. This project is therefore based in the study of good practices and standards that guide organizations through the risk management process and architecture development process.

Keywords: Risk, Risk Management, Enterprise Architecture, ISO Standards, TOGAF

1. Introduction

Every business emerges with the purpose of satisfying a existing need or idea. This purpose is formally defined, in the business organization, as the organization’s objectives. In order to achieve its objectives a set of different assets have to be brought into the business, such as specialized workers, software technologies and hardware, which leads to a continuous increment over time in the complexity of the organization’s architecture. As a way of controlling this complexity, having a better and easier understanding of the organization’s structure and to facilitate business decisions, organization’s use tools for managing their enterprise architectures[6].

Aligned with the need for better management of their systems, for maximizing efficiency, effectiveness and minimizing losses when trying to achieve the organization’s objectives brings the necessity to take into account a proper way for handling with risks to those objectives[2]. In order to combine risk management and enterprise architecture, this dissertation will focus in the implementation of risk management capabilities into one of today’s tools for managing an organization’s enterprise architecture, called Atlas.

1.1. Thesis proposal

Enterprise Architecture and Risk Management are two subjects which have different overall objectives. Enterprise Architecture is focused in the architecture of an organization and how to deal with its changes, while Risk Management is focused in identifying threats to the organization and how to deal with them. This project aims to analyze both subjects and find an alignment between them, in order to create a Risk Management scenario which supports both parts. This scenario will be implemented into an enterprise architecture platform. The data that will be used as a risk management scenario during the development of this project will be from an example case study.

The platform which will be used is Atlas, which is a tool that was developed to support an efficient management of Enterprise Architectures, where any organization can configure it’s contents and analyze it through different types of customizable visualizations. One of the tool’s big capabilities is that it can be easily used to define forms which hide the complexity of dealing with relations when inserting information. The tool also provides an easy to use configurable navigation between it’s visualizations. Another of it’s big capabilities is that it allows to see how to see how the content evolves through time within a certain representation. This is achieved since the tool allows to manage information regarding the future state of the organization, this is, the organization’s To-Be state.
2. Related Work
This section describes the core concepts of Risk Management and Enterprise Architecture, in order to support a better comprehension of both the problem and the solution.

2.1. Risk Management Concepts
In order to provide a better interpretation of what is Risk Management, it must first be understood the concept of Risk. At any given time, the activities executed by an organization to achieve its objectives are susceptible to occurrences which, due to their intervention, change those objectives reachability, for example by delaying its accomplishment. The prevention against the impact of such occurrences is therefore essential. The uncertainty associated with the effect of occurrences over the accomplishment of an objective is what is defined as a Risk according to [2] and [1].This definition supports that a risk is represented by the composition of a cause, an event and a consequence over an asset[1], which can be seen as the risk’s properties. A cause is the uncertainty resulting from the change of the normal behavior of an artifact. An event is a situation that does not occur, as a result of at least one cause, which leads to an impact on the organization objectives. This impact can be described as one or more consequences.

ISO 31000 defines Risk Management as a set of “coordinated activities to direct and control an organization with regard to risk”[2]. This leads to the understanding that the overall intention when managing risks is to control their severity, which can be done by implementing practices that are able to, for instance, minimize their likelihood or their consequences[1]. Such practices are defined as controls[1] and further on, it will be detailed how they appear.

The process of Risk Management described in ISO 31000[2], which can be seen as a whole in Fig. 1, is composed of three main activities:

1. Establish the context
2. Risk Assessment
3. Risk Treatment

The first activity is to Establish the context where risks will be analyzed. This means defining a scope that includes external factors related to where the organization executes its activity and tries to achieve it’s objectives plus factors of the environment inside the organization itself, since every organization is different and the process of Risk Management should be adapted to each organization’s strategy and concerns[2]. This activity also includes the definition of the organization’s risk criteria, which includes how the risk level and impact level are measured, and the level at which a risk can be accepted (Risk Acceptance level)[2].

The Risk Assessment activity concerns with identifying the risks, analyzing them and then evaluating if they should be treated or not. Therefore it can be split into three steps respectively and described according to ISO 31000[2] as:

- **Risk Identification**: In this step, an event that has an impact in the organization’s objectives, whether it is to enhance, degrade, delay or accelerate, is considered and, its causes and consequences are identified.

- **Risk Analysis**: Determines what is the likelihood of the identified consequences, what is their impact and, from a combination of these, what is the risk level. When undergoing this analysis, existing controls have to be taken into account, consistency with the organization’s risk criteria has to be maintained and factors that influence the impact and likelihood of consequences should be considered[2]. This analysis is expressed in a way that better suits it’s processing, meaning that it’s likelihoods and impacts can be qualitative or quantitative[1], or even a combination of these two[2]. When using qualitative values, the scale consists in categories, such as {Very High, High, Medium, Low and Very Low}. When using quantitative values, the scale consists of numeric values which can be for example \{1,2,3,4,5\}.

- **Risk Evaluation**: An evaluation is done over the risks level against the organization’s risk criteria, allowing for a better understanding of which risks have to be treated or if their existing controls over that risk are sufficient. This
step also defines in which order the risks must be treated, depending on their severity.

The final activity in this standard's process for Risk Management is **Risk Treatment**. This activity consists mainly in modifying the risks[1] by applying at least one treatment to each of those risks. The treatments can include the following different types of actions according to ISO 31000[2]: the risks can be accepted when the organization is willing to face it (*Risk Acceptance*[1]); the risks can be avoided by not executing activities and processes related to their causes (*Risk Avoidance*); the risks likelihoods and impacts can be minimized through the application of controls (*Risk Mitigation*); After a risk is treated, the risk that remains is designed as **residual risk**[2], which should also be considered for further treatment or otherwise accepted.

Through all of these activities the **communication and consultation** with the stakeholders involved is maintained in order to have a better understanding of their perspectives, as well as helping them comprehend the need for certain actions resulting from this process[2]. A continuous **monitoring and revision** of each activity is needed in order to keep all of the information, regarding the process Risk Management, accurate and updated.

ISO 31010 Standard addresses several tools and techniques than can be used for Risk Assessment[4]. This standard not only describes how to apply each technique, as it also provides a comparison between the techniques in conjunction with guidelines. A few of them will be explored and therefore described, according to this[4] standard:

- **Consequence/probability matrix** is a technique that can be applied in all phases of Risk Assessment. This technique is used to calculate what is the risk level of risks, risk sources or treatments, as the result of combining the consequence and probability represented through a qualitative scale[4]. From the positioning of risks in the different cells of a matrix, it can be interpreted which of them can be accepted, which have to be prioritized to receive a treatment and which require a deeper analysis. This is achieved since each cell of the matrix has a unique value assigned, that represents the risk level of risks in that cell. The output of this technique is either the rating of each risk or a list with the risk's rank and level[4].

- **Check-lists** is a technique that can be applied in the Risk Identification phase. This technique is used to identify new hazards or risks, or to check if the existing controls are efficient. For this, it uses information from previous risk assessments such as hazards, risks, or controls that failed, to produce check-lists that will be applied to check if everything was covered by another technique, while or after it was applied[4]. The result of this technique can be a list of new risks or a list of improper existing controls.

### 2.2. Enterprise Architecture concepts

TOGAF is the most reliable standard for Enterprise Architecture[5] and it's main comprehensive source, resulting from an evolutionary development by The Open Group which started in 1995 and led to the most recent version 9.1, launched in 2011[3].

![Figure 2: TOGAF ADM](image)

The Open Group Architecture Framework (TOGAF) combines a detailed method and a set of tools for supporting the development of enterprise architectures[3]. Before further describing the content of TOGAF, the different domains of architecture that are part of an enterprise architecture and whose development TOGAF supports[5], should be first understood. According to [3], there are four types of architecture: **Business Architecture**, which handles business strategy, governance, organization and key business processes; **Data Architecture**, which handles the structure of logical and physical data assets, within an organization, as well as assets regarding the management of data; **Application Architecture**, which handles applications that will be deployed and their relations to the business processes; **Technology Architecture**.
tured, which handles software and hardware that is required to support services in the previous architectures[3].

The Architecture Development Method (ADM) (seen in Fig. 2) is the core component from TOGAF and consists in an iterative and cyclic process that describes how an enterprise architecture’s lifecycle should be developed and managed[3].

As Fig. 2 shows, the ADM is a step-by-step method, where the steps correspond to different architecture phases that interact with each other, which cover the development of architecture domains[5]. Each of this phases has guidelines established on TOGAF[3], regarding the phase’s objectives, approach, inputs, steps and outputs.

3. Methodology

This section will analyze the problem, understand the requirements and then show how the solution was achieved.

3.1. Problem Analysis and Requirements

As mentioned in section 2.2, an Enterprise Architecture consists in the representation of an organization’s structure, where all of the organization’s information is modeled through a set of components, properties and relations. This provides valuable information to improve the efficiency of the Risk Management Process, since it can analyze the architecture layers in order to identify risks. Since risks will be associated to assets which are part of the organization’s architecture, they will need to exist in the domain model. This implies that firstly, the domain model an organization to be supported, must be clearly defined in Atlas to form its architecture with its specific domain. Secondly, the concepts that are handled through the process of risk management should be also modeled, if they are not already present, while having the appropriate connection to the architecture’s components, in order to support the risk management scenario. These concepts should include: objectives of the organization, assets, events, consequences, cause and controls.

From what we analyzed in subsection 2.1, having a risk associated to causes, events and a consequences, implies the existence of different likelihoods and impacts which combined will result in the risk’s level. Processing these values, across all existing relations to all risks, in an automated way, is essential to understand which risks have to be dealt with and thus supporting the Risk Evaluation activity. The necessity of this automation is enhanced when controls are introduced as a mean of Risk Mitigation, which can modify the existing values of either likelihood or impact, resulting in a different risk level. Another concern is that if the values are all qualitative, or a combination of qualitative and quantitative, before proceeding to any calculation, the values of impacts, likelihoods and control reductions must be converted to a universal qualitative scale.

The impact of architectural changes, resulting from the transformation from a plateau into another is identified as a source of risks by [3]. For example, introducing a new component in the architecture could raise new risks, which could have impact on other components. When introduced, this component could also be affected by another risk’s consequences, which would modify the impact value of those consequences. As stated by standard ISO 31000 (explored in subsection 2.1), one of the objectives of the risk monitoring and revision activity is to deal with changes in the environment and understanding whether they result in new risks or not[2]. This type of concern is also expressed in one of the steps from the Architectural Change Management phase [3] of TOGAF’s ADM (seen in Fig. 2). In order to support both of them, it should be possible to analyze entity’s relations through a set of views, to be able to determine which components they influence, overall improving risk identification efficiency. Atlas also provides a key feature for this type of analysis, with its time analysis, where it is possible to see the different plateaus of the organization, therefore further improving risk identification capabilities when used.

Since Enterprise Architecture by definition supports the existence of different types of stakeholders where not everyone shares the same view and knowledge of the architecture, the need to accommodate a user which is not familiar with the domain model of this risk management scenario is expected. Atlas provides the ideal solution for this problem through the use of forms, for managing and assigning data automatically. Thus, all of the domain model’s entities should have this management option.

A main concern of this dissertation’s problem is how to be able to provide valuable information from the domain model to the Risk Management process. This can be achieved through the use of reports based in one or more Risk Management techniques, such as the ones explored in subsection 2.1. Since this will be applied on an enterprise architecture tool such as Atlas, that was not developed to be able to provide risk specific reports over the information of the architecture on a repository, new types of report, that are configurable to adjust to each organization, need to be added to the tool.

Regarding the subject of inserting data in the risk management scenario, the concern of scalability must also be raised. What happens when, for example, instead of having a blueprint (view) dealing with about twenty risks and suddenly the scenario
scales up, leading to that blueprint having to deal with two-hundred risks or more, is that it creates the necessity to categorize information, in order for it to be able to be filtered. This also allows for the creation of customized views that better suit the concerns of stakeholders. The filtering capability should therefore also be a feature of any report.

A different set of requirements emerged from the need to incorporate Risk Management Capabilities combined with Enterprise Architecture on Atlas platform, in order to support the risk management scenario.

The architecture to be supported by the risk management scenario case study called Pizzeria Under Risk, whose key components can be seen in Fig. 3. From analyzing this domain model it is possible to see that one single risk can be the result of multiple events and consequences. Since both events and consequences will influence the risk's level, the solution must be prepared to process the components of each relation in order to find out the correct risk level. It is also possible to see that the consequences of the risks are related to one or more assets which belong to one or more objectives.

![Figure 3: Pizzeria Under Risk domain model](image)

Requirements raised as important to have for each component of the case scenario were forms, for risk registration purposes and data properties to be able to use the time travel analysis.

The requirements that were set by the stakeholders of Atlas platform regarding new types of reports that it should be able to produce as a consequence of data analysis in the models and that would support the risk management viewpoint are:

- **Risk Matrix**: Based in the Probability/Consequence matrix technique, where risks will be assigned to a specific cell in the matrix after their risk levels are calculated by a job.

- **Filtered List**: Based in the Check-Lists technique, where all information (instances or instance’s properties) that is associated, by one or more selected relations, to a certain class instance.

These types of reports would be used and managed by the risk owners of the organization, which should also have such information available from their own entry points when accessing the platform.

The requirements that were identified as calculations or automatic behaviors are:

- **Qualitative/Quantitative conversion**: Although the case study provides a qualitative scale (seen in fig:PUResencial), a quantitative alternative is required for calculations, thus the combination of both types of value, while on the same context, also being required to manage.

- **Risk level calculation**: The process of calculating a risk level should be automatic and based on all of the risk’s events and consequences. This is required since as we can see in the case study on fig:PUResencial, one risk can have more than one event or consequence.

- **Impact, likelihood and risk level after controls calculation**: The process of calculating a risk level on a risk with existing controls, should take into consideration its existing controls. All events or consequences that have one or more controls, must have their likelihood and impact level updated respectively. The change should then be propagated to each risk level.

- **Configuration Category filter**: When allowing for a user to operate within a set of chosen categories and being able to save such configurations to use at a later time or to use with a desired report, the filtering of the different set of options which the user may or may not choose to use has to be done in a job. The options provided to use as filters should be adequate to the case study and provide the possibility of filtering by key categories such as assets and objectives (based in the information seen in fig:PUResencial).

3.2. Solution Analysis

This section will analyze how each component of the solution for the problem was achieved.

3.2.1 Impact, likelihood and risk level management

The capability to deal with the requirements Qualitative/Quantitative conversion, Risk level calcula-
ution and impact, likelihood and risk level after controls calculation, the solution combined this capability into a single job. Within this job, firstly the field which was filled by the user out of three possible value options (qualitative, with a scale of {Very High, High, Medium, Low and Very Low}, quantitative from a scale of {5, 4, 3, 2, 1} or a quantitative percentage scale from 0 to 100) to represent consequence's impact, event's likelihood and control's reduction level is used to fill the other empty fields with the appropriate values. Secondly, each control associated to an event or consequence is taken into account in order to determine the final likelihood and impact respectively by using the values in range from 0 to 100 and applying the following formulas each time:

\[
\text{Final Likelihood} = \text{Likelihood} - (\text{Likelihood} \times (\text{Reduction}/100))
\]

\[
\text{Final Impact} = \text{Impact} - (\text{Impact} \times (\text{Reduction}/100))
\]

Finally, the risk level is calculated, taking into account all of the risk's consequences and events, an by using the default formula of:

\[
\text{Risk Level} = \text{Max (Impact)} \times \text{Max (Likelihood)}
\]

These calculations are therefore applied to each event, consequence and risk from the case study introduced in section 3.1, and are aligned with the relations of the domain model seen in Fig. 3. Both the starter value and current value of these three entities is kept in all of the three value options for analysis purposes, meaning that after these calculations, the percentage value is propagated to the other value options.

3.2.2 Configuration Category filter

In order to allow to filter and customize some view settings when using views like filtered-list or the Probability/Consequence Matrix, some additions were required to the domain model. A Risk Filter Configuration Manager class was introduced for purposes of containing access to all the other classes of the domain model. This was a necessity since in case of a user not wanting to use any of the possible risk filter options, then the filtering process would have to by default use all of the existing objects of such category. The only way to define a universal filtering job, required it to start by filling the missing fields, otherwise it would fail to accomplish its purpose.

Associated to the Risk Filter Configuration Manager, a Risk Filter Configuration class was also introduced into the domain model, in order to contain information regarding that configuration preferences and probability / consequence matrix cells, in order to save the results of previously generated reports. The risk filter options were all of the existing entities in the domain model at the time, although if more categorization entities were to be added to the architecture, they would be easily added into the filtering calculations.

The job used for this effect works as follows: filter out configurations which do not require an update, filter out any entity which is not in the configurations preferences, fill any empty fields and filter everything down to risks.

3.2.3 Filtered List

In order to provide information through all of the relations of a certain instance, the following blueprints were defined based on the existing domain model:

- **Objective assets:** Shows all assets associated with a given objective.
- **Asset Description:** Shows all risks, objectives and consequences associated with a given asset.
- **Risk Description:** Shows the severity level before and after controls were applied and all of the controls, assets, causes, events and consequences associated with a given risk.
- **Cause description:** Shows all events and risks associated with a given cause.
- **Consequence description:** Shows the impact level before and after controls were applied and all of the assets, events and controls associated with a given consequence.
- **Control description:** Shows the reduction level, events controlled, consequences mitigated, and overall all the risks controlled by a given control.

These are accessed through any blueprint which was created to list all of each component of the architecture (it is also possible to use these filtered lists through the use of a desired configuration's category options), by interacting with each other or by interacting with the Probability / Matrix report.

3.2.4 Navigation rules

The navigation rules which were defined for the interaction upon double-clicking an object with and between the filtered lists are described in Fig. 4.

3.2.5 Probability / Consequence Matrix report

This type of report was developed through the use of several blueprints, while taking into account the possibility of its content being restricted to a set of categories previously chosen in a configuration.
The Probability / Consequence Matrix report (seen in fig:RistMatrixReport) consists in a blueprint which shows the scales being used for likelihood and impact, and number of risks present in each cell in combination with the option to explore that cell's content. Due to scalability problems and the fixed size of each object represented in a blueprint, if the solution opted to show all the risks in each cell, such as a normal matrix of this type is usually found, the matrix could become unreadable due to the huge amount of information that would be in each cell. The solution for this was to encapsulate the risks and instead show the number of risks which is present in that cell and allow for the user to analyze a specific cell at a time.

Each cell required its own job, where it starts by checking which from all of the existing configurations requires an update and filtering the rest out, then it fetches that specific configuration's risks and filters out the ones that do not belong in that cell, in order to find the number of risks.

The reason for each cell to have two objects, instead of just the object representing that cell’s risk number, is due to Atlas navigation rules between blueprints only being able to be applied to classes and demanding that the object whose properties will be shown is passed as an input. Since the cell risk number is an object which associated to a property of each cell and belongs the class of risk numbers, it was not possible to define navigation through the risks numbers, since there would be no way to specify to which cell to navigate to. Having the cells object represented, allows to navigate by drill-down to that specific cell's blueprint by using a double-clicking. The interaction of that double-click will lead the user to the cell which contains its likelihood, impact and risks, showed in Fig. 6.

This report required the addition to the domain-model of a cell specific class for each existing cell on the matrix, a full matrix class, a likelihood class and an impact class.

### 3.2.6 Forms
In order to avoid mistakes by a stakeholder which is not knowledgeable of the domain model, forms were established to propagate changes when adding, editing and deleting instances of the components (objectives, assets, causes, events, consequences, risks and controls) and configurations.

### 3.2.7 Time slider
For the gap analysis between the different plateaus, or on a single plateau to be possible, each entity of the domain model received four new lifecycle states: NoState (no color), Conceiving/Initial Estimation (gray color) State, Active State (green color) and Dead State (red color). The purpose of these states is to represent when a certain component does not exist yet, when it was estimated to be appear, when it became active and when it disappeared. This is used for example, to see when a certain control is expected to become active or when it is removed. In order to manage the dates of these states, field options for each state are presented when filling each existing form.

On Fig. 7 we can see the lifecycle analysis between two dates, on the existing controls, where
we can see during this period of time: three controls that remained active (full green), three controls which went from the estimated state, into an active state and then disappeared (gray / red color) and four controls which did not exist.

In order to help identify which events, consequences and risks have no controls, the possibility to perform a time analysis on these components with regard to controls was also added. In this type of analysis, the component’s active control’s states are directly shown without requiring to perform a drill-down.

3.2.8 Entry points

An entry point consists in a home page accelerator which allows to create a set of categories, each with its own options to navigate to. In order for the user to interact with the introduced features of this risk management scenario, a set of categorized entry points were defined for the profile "Manager", which included access to all the entity and configurations management, as well as entity lists and filtered lists.

Six categories were createdThe first two categories have lists of elements of each entity and allow a user to navigate to the Filtered lists, with or without having filters. The third category allows access to the Probability / Consequence Matrix report. The fourth and fifth category deal with managing (add, edit or delete) data. The last category allows the user to see which risks he, or another user, is responsible for.

4. Conclusions

After studying how risk management should be done and its implications in the context of developing architectures, some alignments were found and explored in order to create a Risk Management scenario, while following guidelines for managing risk and developing architectures. For this to be achieved some limitations were encountered on the tool Atlas, that needed to be addressed. Ideas were taken from the exploration of a tool similar to Atlas that is focused only in risk management viewpoint. The raised requirements are considered achieved. From these resulted the automation of processes such as formula calculations for risk management, configurable filtering options and ways of analyzing information such as a Probability / Consequence Matrix report.

After the solution developed in dissertation, the possible future steps are:

- Allow for Atlas to be capable of managing single instances based on each of their proper-
- Allow for multiple dates to be assigned to a single state of a class’s life cycle. One of the ideas that was not possible to be explored due to this limitation was to have a category of states which would represent the possible risk levels, thus allowing to analyze the visual change of all the risks level through time on a blueprint which listed risks. For this to be possible, we would have to consider cases where a risk starts in a certain state, changes to another state, but later comes back to a previous state and such feature is not possible.
- Use real case study scenarios with a greater degree of complexity
- Allow for formulas to be a property value, in order to be possible to insert new different ways of calculating risk’s severity levels, or any other type of calculation, in a user friendly way.

References


