HoliRisk – Risk Assessment Framework

Carlos Martins
Instituto Superior Técnico
Av. Cavaco Silva, Taguspark, Oeiras, Portugal
carlos.filipe.martins@ist.utl.pt

Abstract – HoliRisk is a generic platform that gives support to risk assessment in multiple organizational contexts, such as departments, projects or activities. HoliRisk will allow a holistic point of view of the risks involving assets instead of a fragmented vision, diluted in various contexts.
Keywords – Risk Register, Risk Assessment, Risk, Risk Management, Web Application, Decision support system, Framework

I. INTRODUCTION

Risk management define and manage policies and controls to address the risks that affect assets in various organizational contexts, for example, within a department; a project; an activity; throughout the organization. This diversity is the biggest challenge in risk management within an organization, being made in very specific and focused silos, oriented features and disjoint risk management activities. As a direct consequence we find an idea of fragmented risk, with different words, parameterization and measures that lead to highly complex solutions that can not be reused. For example, within the same organization, it may be the case of a financial manager and a marketing manager use a definition, or different risk measure on the same asset - the first individual measures likelihood to break a glass with the range of values [low, medium, high]; already the second measures the same probability with the values [very low, medium, high, very high]. The management of the organization needs to perform extra work to cross the two views and then take results.

This paper proposes a framework flexible and generic enough to integrate the identified risk data for further analysis and mapping, designed taking into account the risk management principles of ISO 31000 [1], which will give support to stages of the risk process assessment in the risk management process.

The paper is organized as follows: section II describes related work; in section III the framework requirements and, in section IV, the implementation; the evaluation of the platform is described in section V and, the conclusions, in section VI.

II. RELATED WORK

A. Principles

The ISO 31000 standard defines risk as "the effect of uncertainty on objectives" [1, p. 1], and defines the principles that an organization must have to effectively manage risks. Risk management:

1. It creates and protects value;
2. It an integral part of all organizational processes;
3. It is part of the decision process;
4. Explicitly addresses uncertainty;
5. It is systematic, structured and timely;
6. It is based on the best available information;
7. It is adapted;
8. It takes human and cultural factors into account;
9. It is transparent and inclusive;
10. It is dynamic, iterative and responsive to change; and
11. Facilitates continuous improvement of the organization;

The process described in ISO 31000 standard is based on the premise that risk management is an iterative process with several stages, as shown in Figure 1.

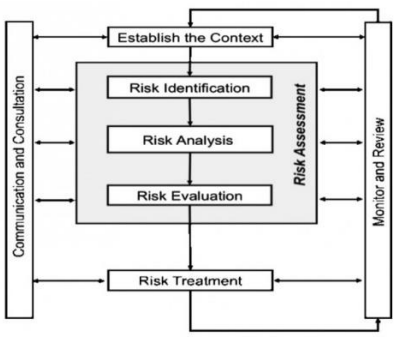

Figure 1 - Risk management process

The first phase is to establish the context. This requires identifying strategic objectives and criteria to determine which the acceptable consequences of this context are. After setting the context, we can begin to identify, analyse and assess the risks. This is called risk assessment. Ending the evaluation, we spent the treatment of risks, if necessary. There are techniques that lead to mitigate, transfer or avoid risk.

The phases that make up the **risk assessment** are: Risk identification; Risk analysis; Risk Assessment (see Figure 1). The identification is necessary to identify the threats and vulnerabilities that can affect the organization and its assets. In the analysis, we examine the nature of the identified risks and not only qualify but also quantify the impact on the organization that risk may have to check. After this we evaluate and define whether the risks are acceptable or tolerable, or if you need to define techniques to control them.

Risk Register, sometimes called in the literature by Risk Log is defined in ISO Guide 73 standard for recording information of identified risks [2, p. 12]. The Risk Register is an information system to record all identified risks, which will support the various stages that make up the assessment of risks, and serves not only to register, but if it is implemented in a technology platform that enables, report information through risk reports. It is a support tool considered essential for the consultation, communication and monitoring of the identified risks.

B. Risk Management Tools

There are many tools in the market not only to register, but also to report risks. ENISA, European Union Agency for Network and Information Security, has generated an inventory[1] with a total of twelve Risk Management / Risk Assessment tools. For this paper there were selected the most relevant tools, as they have interesting characteristics to it.

1) *Verinice* – It is a tool licensed by IT-Grundschutz for information security management, replacing the discontinued GSTOOL tool. With this tool you can perform risk analysis in the field of information security, based on ISO 27005 [3]. Of the most interesting features, it allows you to import and export data across multiple file formats, and if the organization holds the paid version allows you to centralize the information on a server, giving the possibility not only of integration as well as collaboration.

2) *Acuity Stream* – Acuity Stream is a risk management tool used in information security. With a very strong focus on the organization's assets, this nicely integrates risk management in the organization. Any identified risk is always related to one or more assets. His greatest quality is the report not only through reports, but also through dashboards, represented in Figure 2, which in real time can be monitored and also interact in order to apply controls to a risk that has exceeded the desired level.
It runs through a central system where operators collaborate in the recording of identified risks and can trigger alerts to interested parties through email or on the dashboard.
Contains data specific risk in the context of security information that can be used to load the domain model, which makes the initialization and configuration of a simple tool.

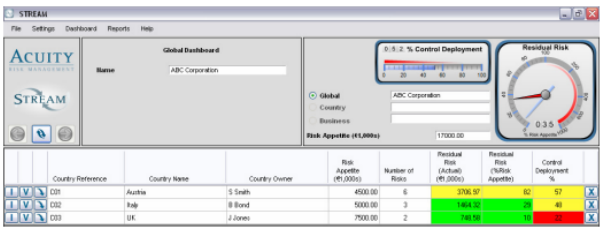

Figure 2 - Auity Stream dashboard

3) *EBIOS* – Ebios is a tool developed by the Central Information Systems Security Division which belongs to the French Ministry of Defence. It is a tool to support the five phases of EBIOS method 2010 [4], also developed by them. This method analyses, evaluates and takes actions related to risks in information systems, with the aim of generating security policies tailored to the needs of organizations. This tool is used not only by the French government, but also by organizations that somehow need to interact with the defence ministry.

4) *Spreadsheets* – Spreadsheets are currently the most used tool when referring to management and risk management is no exception. Spreadsheets have several

[1] https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools

problems not only for large and medium-sized enterprises, but also small. From the outset there are organizational problems from the point of view of information, such as storage, versioning, sharing, collaboration, communication or integration, but also a spreadsheet, being a general purpose tool, not even provide a good interface for a more specific analysis of risk management. It is a tool that with some ingenuity can be used for this, and presents some challenges for other tools, since it is basic knowledge of use, with limited but simple capacity to implement and above all reading and writing easy due to the aspect tabulate.

III. FRAMEWORK REQUIREMENTS

The requirements of this platform can be divided into: access management; domain management; domain model management; and domain data management.

- *[R1] Access Management* – According to the ISO 31004 standard information a risk register is sensitive. It is necessary not only to ensure confidentiality, security and privacy in the information collected and stored on the platform. Access to the platform is done in two steps: user registration; user authentication. A user is defined by the username, email and password. Authentication uses a user mechanism\keyword and authorizes management domains created by himself or domains that are public, but can not do the management of these domains.

- *[R2] Domain Management* – Authenticated users can create new domains, change, or remove domains already created by the same. A domain is a risk register created for a user-idealized context. This is defined by the name, description, whether it is public or shared only with a few users, or private. Additionally you have to define the field the domain model, consisting of concepts, relationships, attributes and values ranges. After defining the domain model, this will register the domain data according to this model.

  - *[R2.1] Attributes Management* – For each domain is necessary to define the attributes that can be used in the domain model. These attributes characterize themselves by name, it is required and the type. The type can be: plain text; text with multiple lines; integer; floating point number; Boolean; date and time; or a range of values (set default values by the user).

  - *[R2.2] Values Range Management* – May be necessary to predefine a set of values for an attribute to be used. A set of values is defined by the name, it is quantitative, qualitative or a table, whether it is public, it is sortable and the respective values.

    - *Qualitative* – Set of qualitative values that are used to define categories and represent a classification. For example {high, medium, low} or {male, female} are two ranges of qualitative values.
    - *Quantitative* – Set of quantitative values that are numerical values and are used to measure within quantitative scales. The range of values from 1 to 5, or {1, 2, 3, 4, 5, 6, 7, 8, 10} are two ranges of quantitative values.
    - *Tables* – Previous sets are able to define lists of values. However there is a need to create even more complex assemblies that resemble sets of sets. These sets were named tables. Examples such as [{1, high}, {2, medium}, {3, down}] or [{event x occurs 10h}, {event y occurs 11h}, {z event occurs 12h}] are examples of such tables.

- *[R3] Domain Model Management* – To set the risk register of the domain model is it required to define the concepts and properties that define the entities and relationships between them. It is intended to build the domain model through a form or from a graphical as a class diagram in UML.

  - *Concepts* – A concept defines an entity in the domain model. This consists of prefix, name, associated attributes and their relationships.

  - *Attributes* – During the construction of the domain model it is necessary to associate attributes to concepts, in order to define the properties of this concept.

  - *Relations* – Relations are defined by the concepts of origin and destination, the cardinality that can be either zero or one

to many; one to many; one or many to many; or many to many; and a caption.

- *[R4] Domain Data Management* – In the domain data management it will be recorded the risk's identified data according to the domain model that has been set. This information will be stored and available for analysis reports later.
  - *[R4.1] Integration with spreadsheet* – Since most of the risk data information exists today is in spreadsheets, the platform needs integration mechanisms with this format. It must be able to export and import these worksheets. The spreadsheet must respect the structure supported by the platform. Once you define the domain model, you must export a spreadsheet (although with no data) and work on it in order to be able to then import the domain data.
  - *[R4.2] Data Validation* – It is intended that the platform does not impose restrictions, defined in the domain model, during the process of loading the domain data. This means, when creating records we do not validate constraints such as required attributes; relations with cardinality one to many or one or many to many. This will give freedom to the user to fill in the domain data as it will have the necessary information without worrying about the constraints of the model. However, whenever the user so wishes, there must be a mechanism to validate existing domain data and inconsistencies that are presented in accordance with the domain model defined.
  - *[R4.3] Void Objects* – Void objects are objects created by the platform automatically to ensure consistency with the domain model. Whenever you create a record of a concept that has a relationship with cardinality one to many or one or many to many, it creates an empty object of the related concept. Visually these records will be displayed differently than the others, so it is noticeable to the user the existence of void objects. The Id attribute of the void object is automatically generated.
- *[R5] Requirements Graphical Interface* – This platform will have a web-based human interface. The design of this interface takes into account the ten usability heuristics proposed by Nielson [5], where you can set some requirements that the web interface has to take into consideration:
  - *[R5.1] Flexibility and efficiency* – The platform can be used by both inexperienced users and experienced, allowing them to accelerate the performance of tasks.
  - *[R5.2] Visibility* – The platform has to inform the user of the current state and only show the relevant information to fulfill certain task, hiding everything that is not necessary.
  - *[R5.3] Stability* – The platform has to minimize the propensity for errors, helping users avoid, recognize, diagnose and recover them.

The use cases of framework is represented in Figure 3.

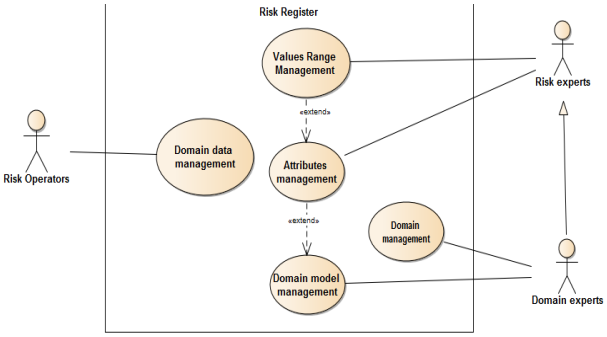

Figure 3 - Framework use cases

HoliRisk makes available the following use cases to the respective actors:

- Risk operators
  - Domain data management
- Risk experts
  - Values range management
  - Attributes management
- Domain experts
  - Domain management
  - Domain model management

IV. IMPLEMENTATION

A. Development Technology

It is intended that the framework is adaptable and changeable in accordance with requirements or features and the inherent cost of developing this condition is as small as possible. So it was chosen to develop stack MEAN: MongoDB[2]; ExpressJS[3]; AngularJS[4]; NodeJS[5]. This allows the web applications development using only JavaScript language.

MongoDB is a NoSQL database, without schema or relations, JSON document oriented, easily querying through a JavaScript framework.

ExpressJS enables the NodeJS with an interface that complies with the HTTP protocol.

AngularJS is a very extensible and versatile framework, stimulating the HTML pages through checks and extensions to the HTML language, which otherwise would have a more complex implementation and also much higher development costs.

NodeJS is a runtime environment for applications. It has an event-driven architecture capable of asynchronous I/O. Such design choices aim to optimize throughput and scalability in web applications.

B. Architecture

The architecture of the HoliRisk framework is represented by Figure 4.

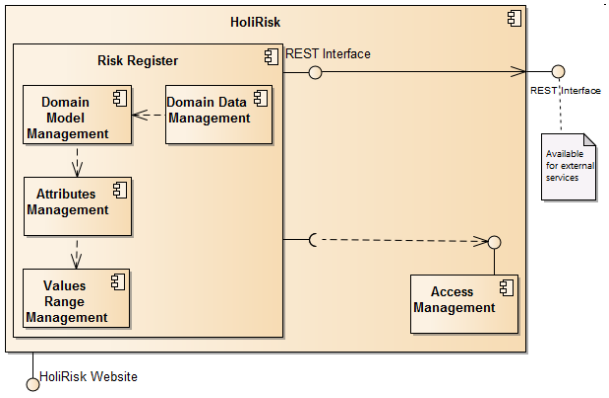

Figure 4 - Framework architecture

The *Access Management* ensures not only registration, authentication and authorization on the framework, but also allows you to add, change or remove users.

The *Domain Data Management* uses the domain model for collecting and storing data using forms dynamically constructed for this purpose.

The *Domain Model Management* models defines the concepts and relationships that will be used as a risk register of the domain model.

Attribute Management allows to add, change and remove attributes of a particular domain using a form designed for this purpose.

Values Range Management allows you to add, change and remove ranges of values using a form designed for this purpose.

C. Proposed solution

The proposed solution is based on the requirements and take advantage of the technology chosen to create a risk assessment framework with a web-based human interface and an API available for external services (e.g.: reporting tools) through a REST interface.

- *[DP1] Authentication and Authorization* – Recapping the ISO 31004 standard to secure access to information collected and stored in the risk register is of utmost importance. To ensure that access to the server are properly authenticated and authorized (the user is holding the correct profile to access a particular resource) uses the standard RFC 7519 industry called JSON Web Tokens.

- *[DP2] Activity and Error log* – Not only for safety but also for any errors analysis that the platform can generate, you must register not only errors, but also all the actions made by users that change the status of any document database.

  - *[DP2.1] Error Log* – All errors are caught at services level (the last layer before returning the response to the client) and are recorded on the server console. Later, they can be exported to a text file if necessary.

  - *[DP2.2] Activity Log* – Traceability of actions, performed by a particular user, all stored documents in the database have the properties: createdBy; updatedBy; createdAt; updatedAt; indicating the user who created the document, who updated it the last time, the date and time it was

[2] https://www.mongodb.com
[3] https://expressjs.com
[4] https://angularjs.org
[5] https://nodejs.org

created and the date and time of the last update, respectively.

- *[DP3] Domain Model Design* – Considering the state of the art tools to support risk management processes, the attribute settings, possible values and the entities or concepts involved, these are done through forms that sometimes become complex. In domain model management we assume a new approach to create the domain model as a UML class diagram it were.

- *[DP4] Integration with spreadsheet* – As previously discussed, spreadsheets are the most used tool in management. Furthermore other risk management tools import and also export to this format, which makes the widely used format.

- *[DP5] View large amounts of information* – In computer graphics the user experience in manipulating and viewing large amounts of information is a problem. The information associated with risk data can be extremely extended, not only the number of attributes and the associated text, as well as the record number (hundreds or even thousands). Bearing in mind that the information is arranged in a tabular form, the problem described raises a number of challenges:

  - *[DP5.1] Expandable Desktop* – The desktop has to adjust (expand) when the width and height of the web browser window for each user, in order to have the greatest visual area possible.

  - *[DP5.2] Partial Load records* – There must be made two partial loads: only loads the records of the concepts that are being worked at the moment; and records must be loaded partly in windows of fifty as you browse. Otherwise the user experience becomes longer.

  - *[DP5.3] Set displayed information* – Give the hypothesis only see what you want to see and how they want to see, that is, it must be possible to hide or display columns and you can move them in position within the table.

  - *[DP5.4] Sort* – Be possible to sort the values of a particular column.

  - *[DP.5.5] Filter* – So the number of records is not too extensive that it becomes difficult to search what we need, the operation of filtering by text a specific column is extremely useful.

- [DP6] Collect domain data - As the domain model is completely configurable by the user, the form that collects field data for each concept has to be created depending on the type of associated attributes and relationships present.

- *[DP7] Validate domain data* – In order the expert in risk does not have to carry all the information to comply with the restrictions imposed by the domain model, the domain data management module allows records to be created with missing data. At any time you may need to validate the consistency of the information that has already been inserted. This framework confronts domain data with the domain model and informs the user of inconsistencies found, so they can be corrected as soon as desired.

- [DP8] REST API – This API will allow third parties to consult the registered domain data. It was designed taking into account the REST architecture. This architecture communicates over HTTP, taking advantage of the verbs that implements this: GET; POST; PUT; DELETE. The messages exchanged are in JSON format. This format is lighter than XML for two reasons: you can send the same information in shorter messages; and platforms currently already have very efficient parsers for JSON format.

- *[DP9] Technical Documentation* – It is necessary to produce technical documentation, not only to include in this work, but also to be used by those who need to use the platform API. This challenge is achieved by placing comments directly in the source code, using the standard JSDoc[6], and creating documentation in HTML format via the JSDoc tool.

V. EVALUATION

It is intended with this development framework to provide its users not only efficiency but also efficiency in the tasks that need to be performed

[6] http://usejsdoc.org/

during the risk management process. To assess this, a usability study was conducted on the framework.

Data for this study was collected from a population of:

- three experts in risks: a PhD finalist; and two Master's finalists in wich the scope of their thesis is to develop a risk register of corruption and information security, respectively;
- two Masters finalists whose dissertations fall within the HoliRisk framework, and already had knowledge about the framework when conduct the evaluation;
- an expert in user experience in web applications and mobile devices;
- four experienced users, more specifically web applications.

For this study it was defined a guide with a set of tasks (see Annex A), which attempted to guide the participants from the process of setting up the domain data editing.

At the end of the tasks being performed, each participant answered a questionnaire of satisfaction.

Performing a post-hoc analysis of the tasks execution times during the evaluation it was build the chart shown in Figure 5. This chart shows the average time and the standard deviation (σ) of the execution of tasks.

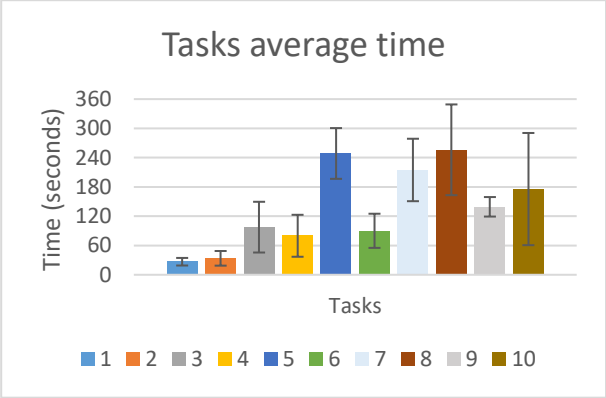

Figure 5 - Tasks average time and standard deviation

We can conclude that the creation and configuration of a new domain (task 2 to 6) on average take nine minutes. Importing data and validating it take no more than three minutes.

The answers to the questionnaire of satisfaction were collected on a scale of 1 to 5, where 1 indicates “strongly disagree” and 5 “fully agree”.

The overall satisfaction of participants was 4.5, which can be seen in the chart represented by the Figure 6. Participants were divided between the note 4 and 5 equitably.

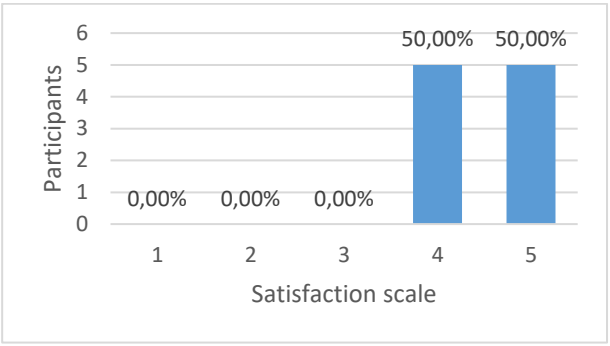

Figure 6 - Overall satisfaction graph

Participants, in general, whether or not experienced found the framework consistent, effective and easy to use, as we see in Table 1.

Question	Satisfaction
At any time, I knew what was happening on the platform	4,3
I realized all expressions or linguistic terms used in the platform	3,9
I found it easy to use platform	4,2
I found the platform consistent	4,3
I always had the information needed available	4,4
I found the platform effective	4,6

Table 1 - Participants satisfaction

However, according to participants, there was some difficulty understanding some expressions and linguistic terms. Analysing the comments that were left during the evaluation and even the questionnaires, the icons used to perform some operations left some doubts and only after consulting the manual realized its significance.

VI. CONCLUSION

Risk management is a complex process, which can become very subjective and particularly within each organization, department or project. The HoliRisk platform aims to support this process, iterative and evolving within the organization in order to provide a holistic view of it, arming the experts and management tools able to make decisions, mitigating risks and exploiting opportunities. In the current conjecture of markets, increasingly this can dictate the success or failure of a business.

The evaluation concluded that it is necessary to make some corrections\changes to the platform

becomes a product with increasingly potential of usability:

1. Redesigning the creation and editing of values ranges;
2. Correct graphics and functional aspects of the graphic design and some buttons;
3. Improve visibility aspects and ensure that the user knows what state the server is in;
4. Improve graphic aspects and define real-world standards both in language and in the icons used so that the user has no doubts during navigation;
5. Equip the domain registration data with best shortcuts and tools in order to make it more efficient (if able to make as efficient tool as a spreadsheet, this will no longer be an excuse as Risk Register).

Furthermore it is necessary to integrate a risk reporting platform that is being developed under another Master's thesis and also improve the authorization mechanism, defining user profiles at each domain.

It should be created a versioning mechanism at the level of the domain model management and the domain data management. It is important that in case any changes occur in the information, it is possible to go back and redo if needed. It would also be useful a real-time collaboration mechanism graphic designer level to facilitate the review and correction.

REFERENCES

[1] "ISO/FDIS 31000:2009: Risk Management - Principles and guidelines," 2009.

[2] "ISO Guide 73:2009: Risk management - Vocabulary," 2009.

[3] "ISO/IEC 27005:2011 - Information security risk management," 2011.

[4] "EBIOS – Méthode de gestion des risques," 2010. [Online]. Available: http://www.ssi.gouv.fr/uploads/2011/10/EBIOS-1-GuideMethodologique-2010-01-25.pdf. [Acedido em 21 12 2015].

[5] J. Nielsen, "Usability inspection methods," in *Conference Companion on Human factors in computing systems*, New York, NY, USA, 1994.

Annex A

#	Task	Sub-task
1	Register new user and login	
2	Create New Domain	
3	Create the ranges	Create qualitative range "3 Levels" with the values [Weak, Moderate, High]
4	Create attributes	Create attribute "Likelihood", that is the type range of values "3 levels"
		Create "Impact" attribute, which is the type range of values "3 levels"
		Create "Risk Level" attribute, which is the type range of values "3 levels"
5	Create the domain model	Create concepts that are not concept-association
		Create relationships
		Create concepts-association
		Add attributes to the concepts • Risk - risk level • Consequence - impact • Event - Likelihood
6	Edit the domain model	"A risk has only one owner"
		"A risk can affect several assets"
		"A risk ceases to have controls"
		"One consequence can have multiple controls"
7	Edit domain data by importing them (using the supplied spreadsheet)	Import Spreadsheet
		Check the risk R47
		Check the EV17 event
8	Edit the domain data	Change Risk Name R1
		Change Event Likelihood EV1
9	Edit domain data in the worksheet	Export the domain to a spreadsheet
		Edit the worksheet
		Import Spreadsheet
		See the changes in the tool
10	Clone created domain	Check the domain model
		Import provided worksheet domain data