SERIES	TIMBUS WHITE PAPERS

TIMBUS WHITE PAPER:

A Risk Management Approach to Preservation of Business Processes

Publication Date: 20.09.2014

Dissemination Level: PU

SERIES	TIMBUS WHITE PAPERS

TIMBUS is supported by the European Union
under the 7th Framework Programme
for research and technological development and demonstration activities (FP7/2007-2013)
under grant agreement no. 269940

SERIES	TIMBUS WHITE PAPERS

Authors		
Name	**Organisation**	**e-mail**
Ricardo Vieira	INESC-ID	rjcv@tecnico.ulisboa.pt

Contributors		
Name	**Organisation**	**e-mail**

Internal Reviewer		
Name	**Organisation**	**e-mail**
José Barateiro	LNEC	jose.barateiro@gmail.com

Disclaimer

1 Executive Summary

According to the Digital Preservation Handbook from the Digital Preservation Coalition, digital preservation can be defined as “a formal endeavour to ensure that digital information of continuing value remains accessible and usable”. In a different perspective, digital preservation can be understood as identifying implementing the necessary controls to mitigate risks that threaten the long-term availability of digital information. In fact, in recent years, the digital preservation community has been researching on how to use risk management as a mean to achieve a proper digital preservation. This is verified by references such as ISO16363:2012 and DRAMBORA that use risk management to identify and mitigate risks that a digital repository is subject to.

The EU co-founded TIMBUS project innovates by focusing on the execution and preservation of organizations business processes. The project goal is to use traditional digital preservation approaches to eliminate and mitigate possible threats to business sustainability. The goal is pursued by analysing existing business process in order to identify and mitigate possible risks. In other words, risk management is used in TIMBUS as: (1) a motivation to preserve business processes, and (2) a framework to manage existing business risks.

In this white paper we introduce a generic risk management process to assess and mitigate business processes risks using digital preservation techniques. Additionally, the paper describes a risk management tool developed in TIMBUS that can support the aforementioned process.

2 Risk Management Concepts

Risk is defined as the “effect of uncertainty on objectives” [6]. Risk management goal is to support the identification, assessment and mitigation of risks. Due to the holistic definition of risk, risk management is present in different domains such as the financial, healthcare, and insurance sectors. Furthermore, risk management approaches and techniques greatly vary according to the specific goals of organizations. To ease the understanding between different areas of expertise, ISO 31000 [4] provides a generic framework for risk management. The standard defines the main concepts and principles used in risk management along with a generic risk management process. The definition of the concepts in the standard is taken from ISO Guide 73:2009 [6]. With a similar goal, ISO 31010 [5] lists and describes different methods and techniques that can be used on the different risk management activities.

Figure 1 provides an overview of the main risk management concepts. As illustrated, risk management considers that assets have vulnerabilities that can be exploited by specific events (threats) causing specific consequences [1]. Therefore, risk can be seen as the combination of the potential events and their consequences [6]. In other words, risk can be expressed in terms of a combination of the consequences of an event and the corresponding likelihood of the event [6].

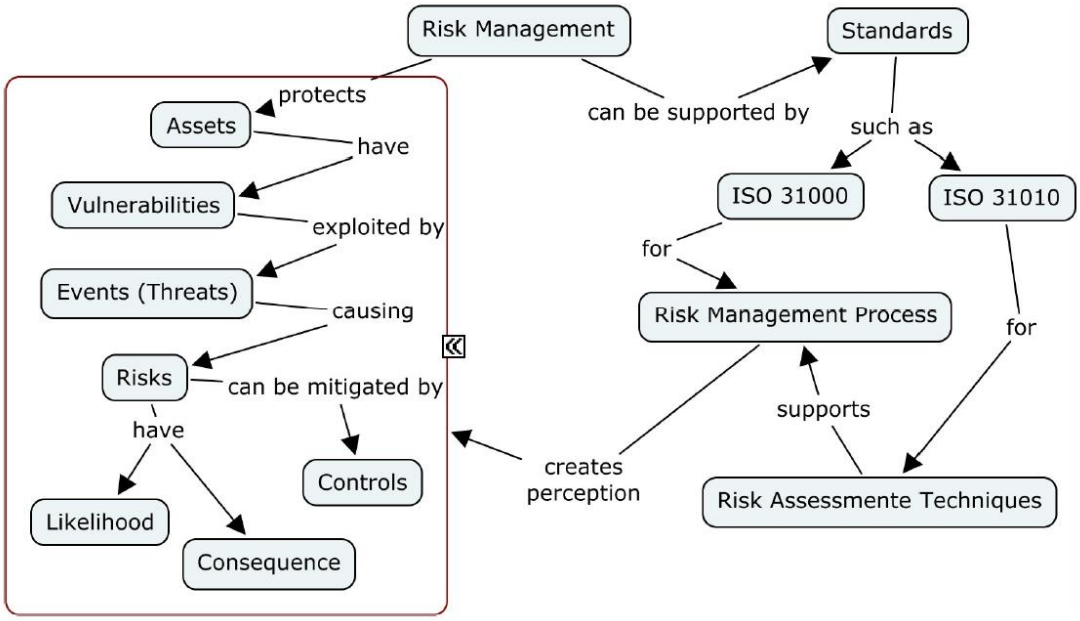

Figure 1 Risk management main concepts and references [2].

3 Risk Management Approach to Preservation of Business Processes

The goal of digital preservation is to assure that digital information can be preserved allowing their use and interpretation through time. Using risk management terms we can define digital preservation as the field responsible for protecting digital information (the asset) vulnerabilities from the events (threats) that may affect their proper use and interpretation (consequence) [1]. Therefore, digital preservation is about identifying, assessing and mitigating the risks associated with digital preservation. The association between digital preservation and risk management it is not new and different works regarding this relation have already been published. ISO 16363:2012 [3] and the Digital Repository Audit Method Based on Risk Assessment (DRAMBORA) [7] provide a risk management process for assessing the trustworthiness of digital preservation. Additionally, DRAMBORA also identifies typical threats and vulnerabilities that can be mitigated using Digital Preservation techniques.

TIMBUS proposes a risk management process for the preservation of business processes. The process is based on ISO 31000 and takes into consideration ISO 16363 and DRAMBRORA. Figure 2 illustrates the process that is explained in detail in the next sections.

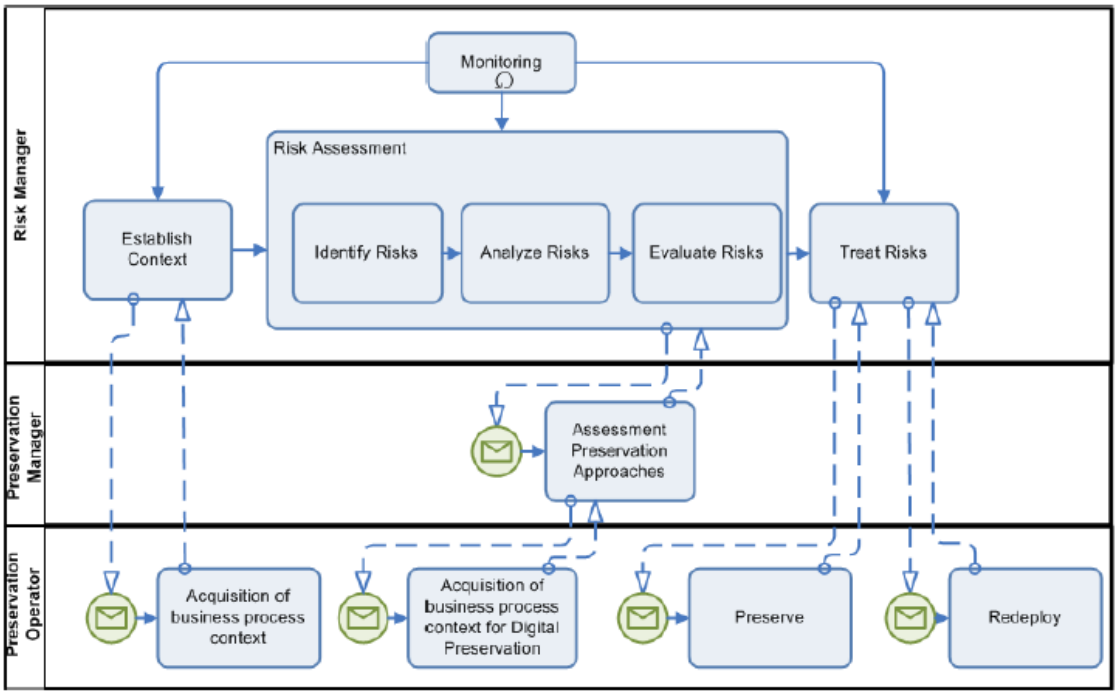

Figure 2 Risk management process for the preservation of business processes[1].

[1] For more information about the risk management process please refer to TIMBUS deliverable D4.6 – Use Case Specific DP & Holistic Escrow that can be found at http://timbusproject.net/component/docman/doc_download/143-d46m24use-case-specific-dp-a-holistic-escrowpdf

3.1 Establish Context

To proper assess risk, one must know the goals and objectives of the organization. Establishing the context consists on identifying all the elements that are associated with the assets we wish to protect and also all the elements that may influence the risk assessment. Additionally, establishing the context includes defining the organization risk criteria. Risk criteria should be based on the context of the assessment and it is the "terms of reference against which the significance of a risk is evaluated" [6].

In TIMBUS, part of the context is established through the acquisition of the business process context. The business process context is a context model instance that describes the process and its context through a Domain Independent Ontology and a set of Domain Specific Ontologies. For more information about this specific activity please refer to TIMBUS deliverable D4.6 – Use Case Specific DP & Holistic Escrow[2]

3.2 Risk Assessment

Risk assessment can be divided into three sub-activities: risk identification, risk analysis and risk evaluation. As the name suggests, risk identification is about identifying, for all assets we which to protect, the associated risks. In other words, risk identification consists on identifying: (1) assets vulnerabilities, (2) events that might exploit those vulnerabilities, (3) the possible consequences if the event occurs, and consequently (4) the associated risks.

Risk analysis involves analysing the aforementioned risks to enable a proper decision regarding whether risks need to be treated or not. Typically, a risk analysis involves, at least, estimating the likelihood of the events and the impact of the consequences. These two indicators allow the classification of risks through their severity, i.e., "the magnitude of a risk expressed in terms of the combination of consequences and their likelihood" [6]. Other risk analysis indicators can be cost, value, dependency factor, etc.

Finally, risk evaluation involves taking the decision about which risks should be treated. The decision should be done according to the previous risk analysis and risk criteria. Risk can be eliminated, mitigated, transferred (e.g. by insuring the asset or outsourcing the risk treatment), or accepted. Risk mitigation can be achieved by (1) eliminating the vulnerability of the asset, (2) reducing the likelihood of the event, or (3) reducing the impact of the consequence [1]. A crucial factor to consider when evaluating risks is the potential treatments that might exist and their respective costs. Therefore, in TIMBUS, risk evaluation considers an assessment of different preservation approaches and their respective costs[3].

[2] Deliverable D4.6 – Use Case Specific DP & Holistic Escrow is available at http://timbusproject.net/component/docman/doc_download/143-d46m24use-case-specific-dp-a-holistic-escrowpdf

[3] For more information about the risk management process please refer to deliverable D4.6 – Use Case Specific DP & Holistic Escrow that can be found at http://timbusproject.net/component/docman/doc_download/143-d46m24use-case-specific-dp-a-holistic-escrowpdf

3.3 Risk Treatment and Monitoring

Risk treatment consists on implementing the controls (treatments) identified at risk assessment. In TIMBUS, the process assumes two possible treatments: to preserve all, or part, of the business process, or to redeploy the business process. An important aspect of risk treatment is to assure that the performance of the controls are measured, i.e. to assure that controls are monitored in order to understand if the risk is being mitigated or if it is necessary additional actions/controls.

In fact, risk monitoring should be present at all risk management activities. The context should be monitored since context changes might reveal new risks or affect the existing ones. The list of vulnerabilities, events, consequences and risks should be monitored to assure that is always updated. The analysis of risk should be periodically checked to assure that estimations to not deviate from reality. Finally, treatment decisions should be reviewed and updated if necessary.

4 Risk Assessment with HoliRisk

As stated before, risk management can be useful in several different contexts. It can be applied in an entire organization, a specific department or area, or even a specific function, project or activity. This multitude of contexts is behind one of the main problems in the field where efforts operate in silos with narrowly focused, functionally driven, and disjointed risk management activities [1]. As consequence, organizations are faced with a fragmented view of risks, with different languages, parameterizations, and metrics that lead to highly complex specific-built solutions that cannot be reuse. This section describes HoliRisk - a flexible generic framework developed in TIMBUS to support the steps of risk assessment. The sections starts by providing an overview of the tool and ends by describing how HoliRisk can be used to support the risk assessment process described in section 3- Risk Management Approach to Preservation of Business Processes.

4.1 HoliRisk – An Overview

HoliRisk framework follows the multi-level conceptual architecture of OMG MetaObject Facility (MOF)[4], as illustrated in the Figure 3.

These definitions apply:

- Layer M0 (domain): **Instances** that contain the actual information structures, which in our case will be the specific data factual objects and the respective association objects created to represent the specific business process being focus of a risk assessment (e.g. the representation of the specific vulnerabilities and events related to a risk fire in an organization that can affect a relevant asset such as a specific computer server).
- Layer M1 (domain model): **Model**, meaning the domain model of a specific view. In this case it contains the collections of concepts that categorize (or classify) the instances at layer M0, meaning only instances of the concepts defined at this level can be created (e.g. the concept of “risk incident” -where “fire” can be included-, the definition of a “resource” -where the “computer server” can be included-, the concept of “risk probability”, etc.). Models can be defined to represent the specific concerns of multiple views of risk management, e.g. Financial, Security, Project Management, etc.
- Layer M2 (domain metamodel): **Metamodel** that defines the schema of elements that can be described in the models (Layer 1). By default the system uses a metamodel with the following risk concepts[5]: **Asset**, **Vulnerability**, **Event**, **Risk**, **Consequence**, **Control**, and **Policy**. However, any other concept can be defined in this layer.
- Layer M3 (domain meta-metamodel): **Meta-Metamodel** corresponds to the data that can be used to define the most generic types and ranges for the domain metamodel (for example: probability, time, integer, custom ranges such as [low, medium, high], or [bad, neutral, goof], etc., so we can define a metamodel stating that “an Event has Probability ranging [0%,100%]”, a Consequence can have an Impact ranging [low, medium, high], etc.).

These layers enable the flexibility that allow the system to be holistic[6], meaning it must allow the support of a risk management process (**Instance level**) using different risk management concepts

[4] http://www.omg.org/mof/

[5] Core concepts taken from the “ISO 31000:2009, *Risk management – Principles and guidelines”*

[6] Thus the motivation for its name, “HoliRisk”!

(**Metamodel level**) from different risk management domains (**Model layer**). Additionally, we define a context as the focus of execution of a risk management process, which can be an entire organization, a specific department, or even a specific function, project or activity.

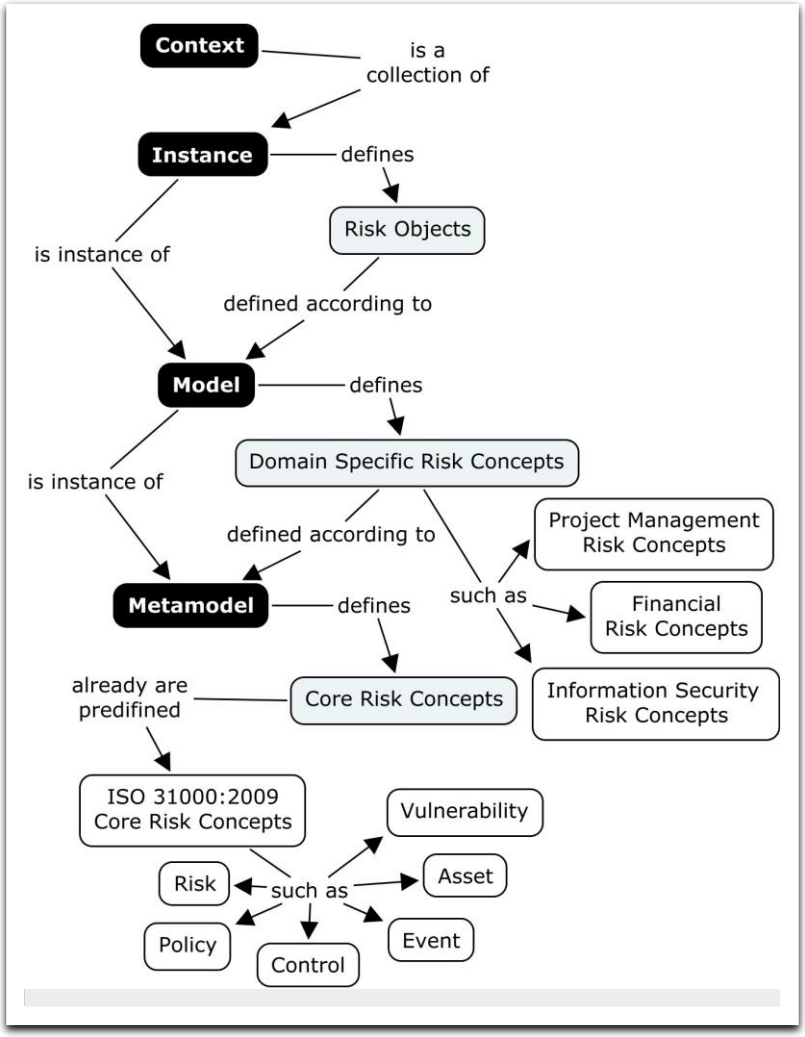

Figure 3 HoliRisk Conceptual Layers.

The HoliRisk framework is composed by two distinct application components: the risk repository where all data is created and managed, and the risk reporter where data from the risk repository can be analysed and evaluated. Those components can also be divided into sub-components that are described in Figure 4.

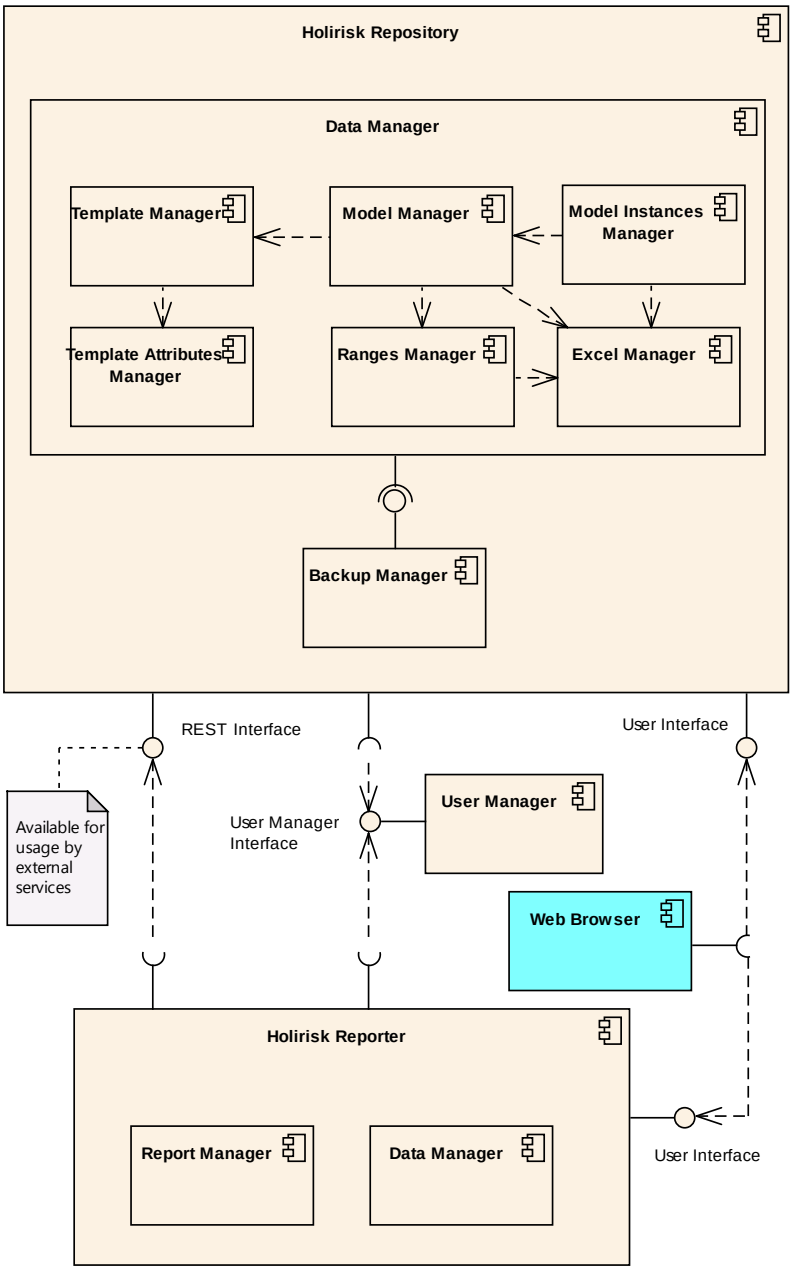

Figure 4 HoliRisk application components.

4.2 Risk Assessment with HoliRisk

As described above, before risk assessment it is important that we establish the context of assessment. In HoliRisk, establishing the context implies defining the *risk model* we are going to use for the assessment. The model will define: (1) which elements are going to be used to assess the risk, (2) which metadata will characterize the elements of the model. Both goals are achieved in the tool through the *template manager component*. The component provides a set of default elements (asset, vulnerability, event, consequence and risk) and attributes (metadata) that are considered essential to

the assessment (Figure 5). However it is possible to create and associate different attributes to the existing elements. An attribute is defined by its name, its description, its type, and an optional flag that indicates whether the attribute is optional or mandatory. The attribute can be of the type text, i.e. it allows free text as the value of the attribute, or of the type range. Ranges can be qualitative or quantitative. One important aspect to note is that attributes and models can be shared between different projects allowing the stakeholders to have a flexible and extendable repository of attributes and models.

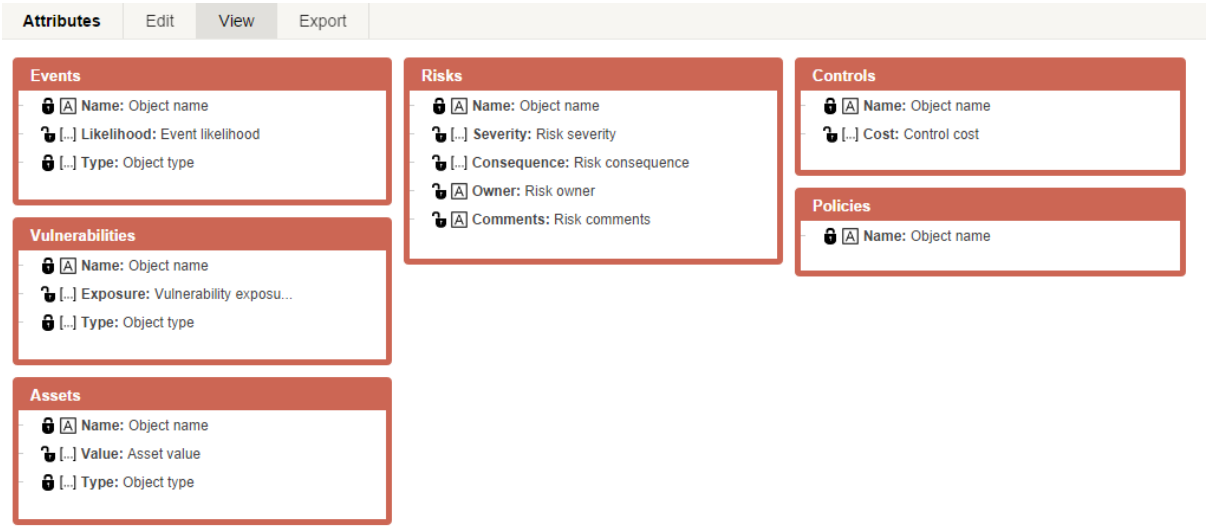

Figure 5 HoliRisk default model template.

Risk identification is done through the *data manager component* and involves defining the instances of the risk elements defined in the previously defined risk model. For each created object, stakeholders are requested to provide information on the attributes previously defined. Figure 6 shows an example of creating a risk. Note that some of the requested information already includes essential attributes (e.g. severity and consequence) for risk analysis.

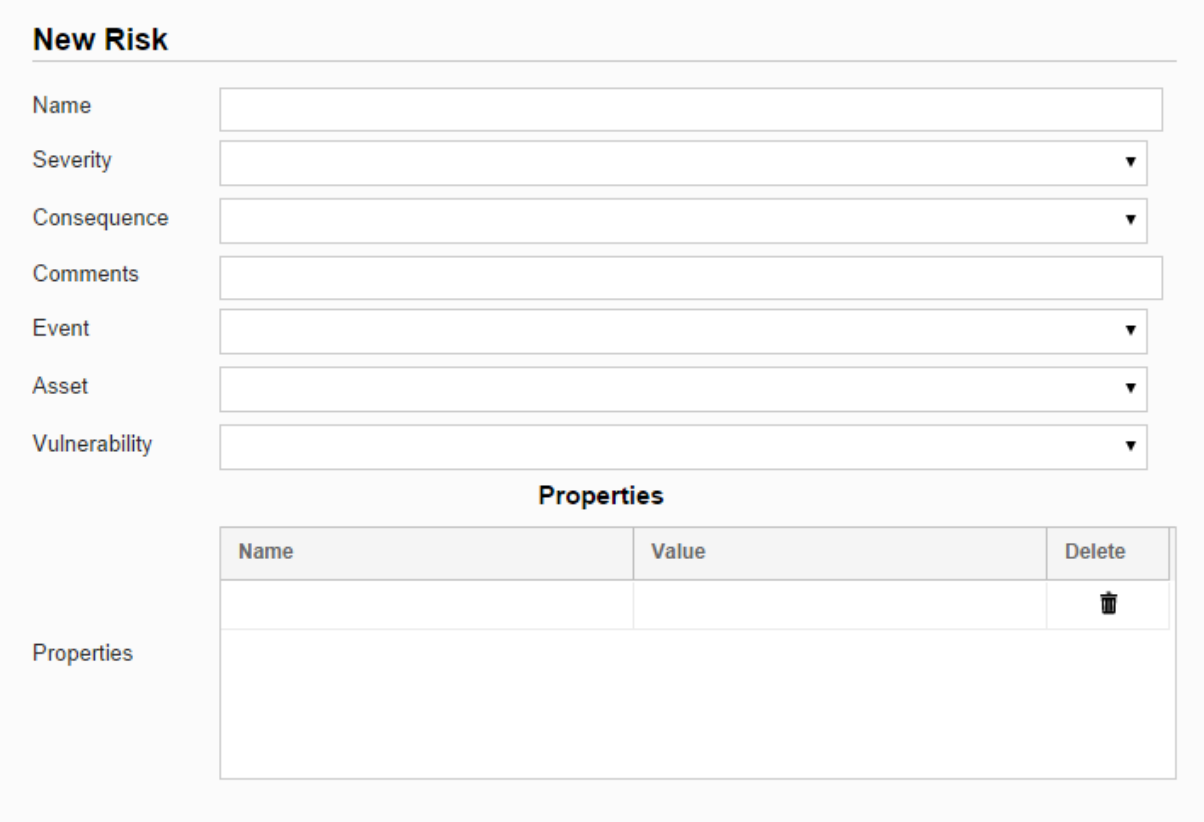

Figure 6 Adding a new risk using HoliRisk.

Additionally, risk analysis can be performed in HoliRisk by defining a risk matrix. A risk matrix is a coloured matrix that supports an overall view of the risks and their severity. Figure 7 shows an example of a risk matrix.

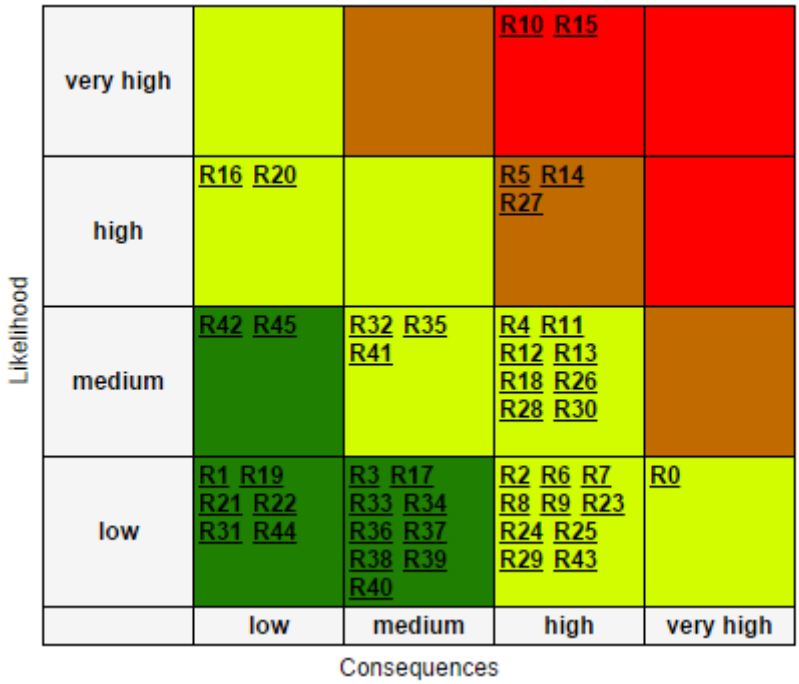

Figure 7 HoliRisk Risk Matrix.

Risk evaluation is mainly performed using the *Risk Reporter application component*. The component provides a set of analysis and visual aids that can support decision-making. In particular, it allows sorting and filtering the different risk elements (Figure 8), it provides an overall view of the relations between the different risk elements; it allows the definition of risks reports that can be shared among users of the tool or exported to PDF, etc.

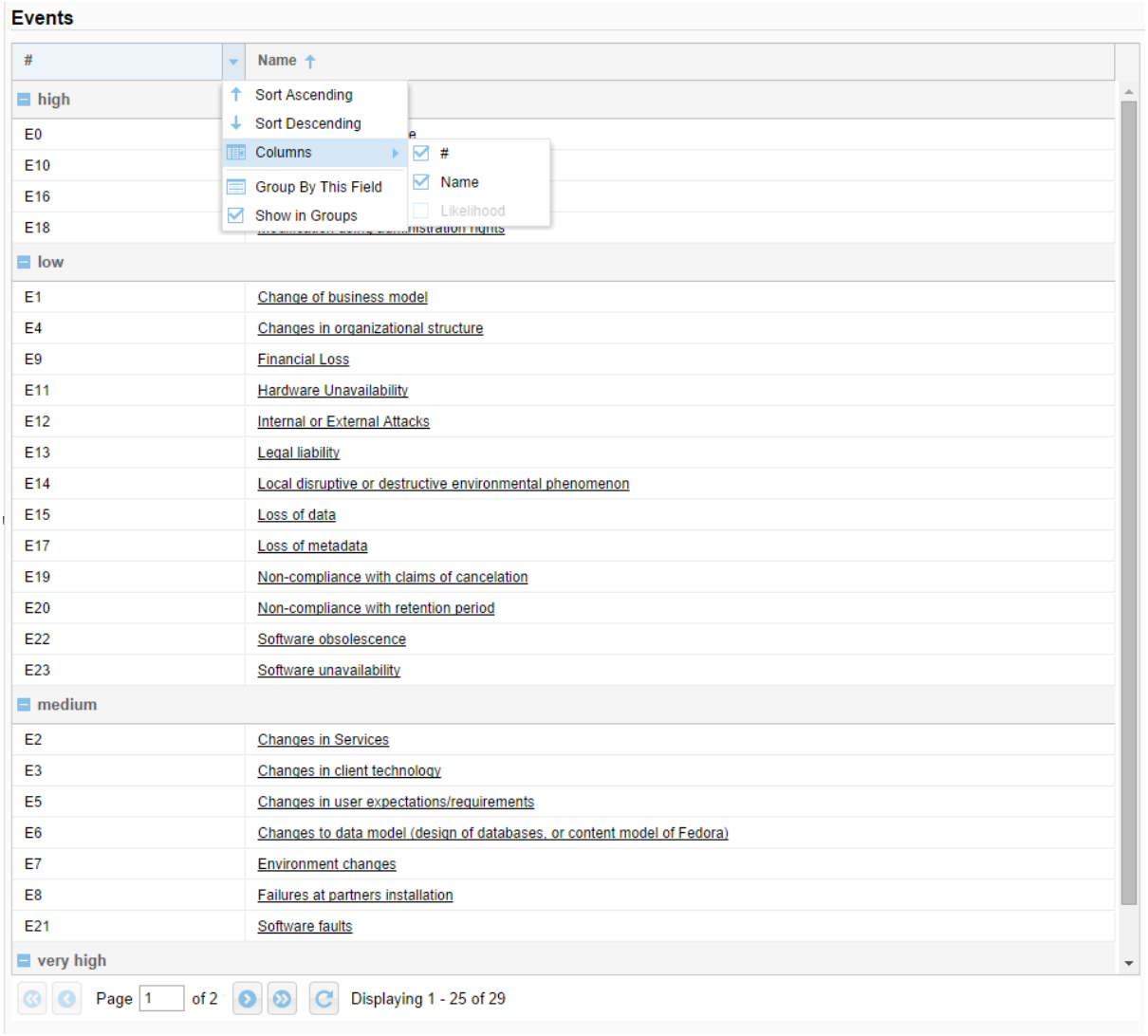

Figure 8 HollRisk representation of events. Events can order, filtered and/or grouped by a specific attribute.

One important concept for risk evaluation is the concept of policy – a set of controls that can be applied to mitigate risks. By defining alternative policies, it is possible to see a risk matrix representation of how the policy will impact the risks allowing a better comparison of different policies. For example, in Figure 9 it is easy to understand that by applying the policy entitled “TIMBUS policy” the severity of the risks is greatly reduced (e.g. Risk R10 consequence is reduced from high to low).

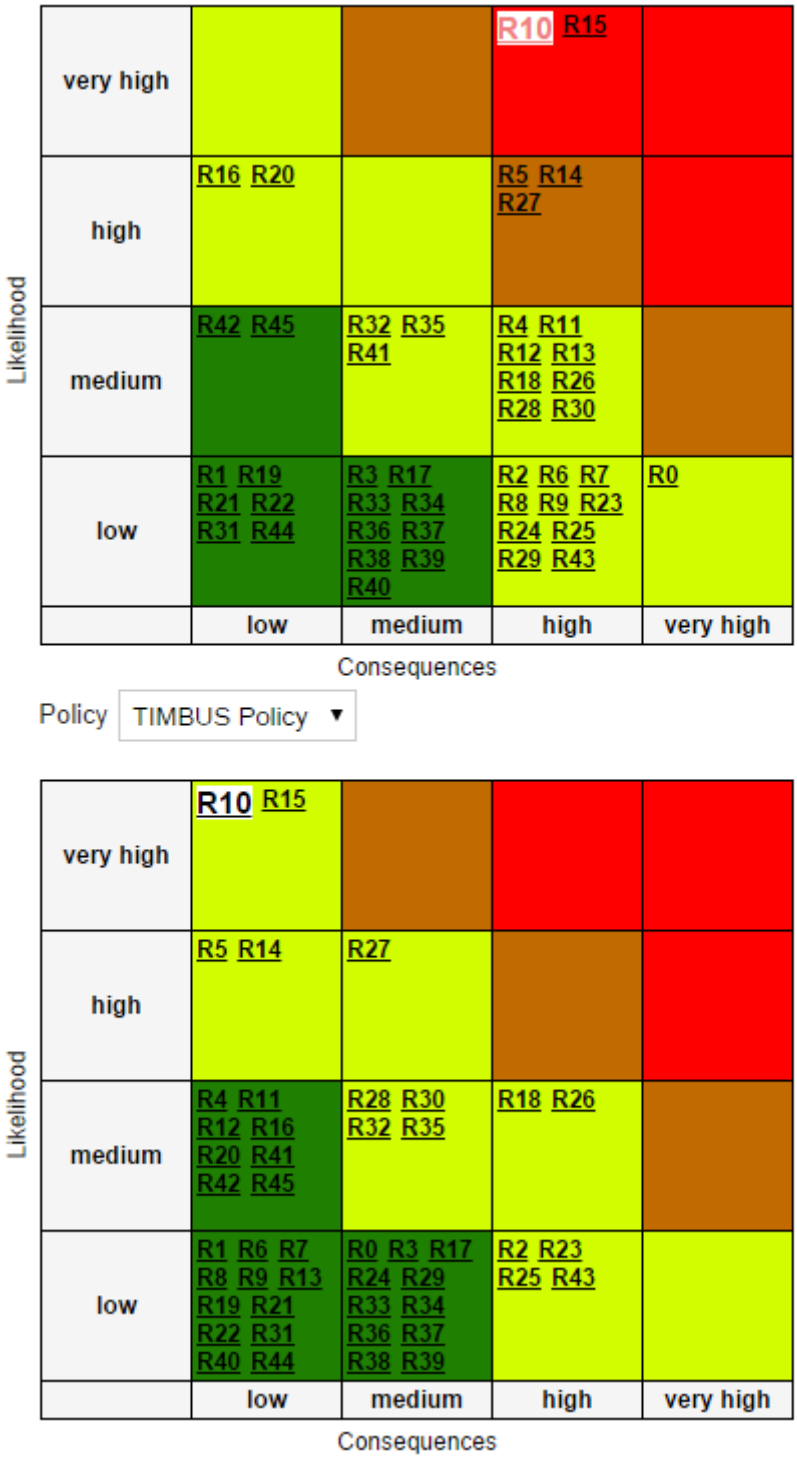

Figure 9 HoliRisk estimation of the result of a policy implementation.

Disclaimer

HoliRisk is a free software program available at https://opensourceprojects.eu/: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

5 References

1. Barateiro, J. (2012) A risk management framework applied to digital preservation, PhD Dissertation, Universidade Técnica de Lisboa, Instituto Superior Técnico, Lisboa.
2. Ferreira, F., Vieira, R., BOrbinha, J. (2014) The value of Risk Management for Data Management in Science and Engineering, Digital Libraries 2014, London.
3. ISO 16363:2012 (2012) Space data and information transfer systems – Audit and certification of trustworthy digital repositories, International Organization for Standardization.
4. ISO 31000:2009 (2009) Risk management – Principles and guidelines, International Organization for Standardization.
5. ISO 31010:2009 (2009) Risk management – Risk assessment techniques, International Organization for Standardization.
6. ISO Guide 73:2009 (2009) Risk management – Vocabulary, International Organization for Standardization.
7. McHugh, A., Innocenti, P., Ross, S.,Ruusalepp, R., and Hofman, H. (2008) DRAMBORA: The Digital Repository Audit Method Based on Risk Assessment, Procedings of the Third International Conference on Open Repositories.
8.