D5.4: Refined Architecture for Intelligent ERM

WP5 – Software Architecture for Digital Preservation

Delivery Date: 28/09/2012

Dissemination Level: CO

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

Deliverable Lead		
Name	**Organisation**	**e-mail**
Roxana Belecheanu	SAP	roxana.belecheanu@sap.com

Contributors		
Name	**Organisation**	**e-mail**
Daniel Draws	SQS	daniel.draws@sqs.com
Daniel Simon	SQS	daniel.simon@sqs.com
Ricardo Vieira	INESC-ID	rjcv@ist.utl.pt
Ying Du	SAP	ying.du@sap.com
Michael Nolan	INTEL	michael.nolan@intel.com

Internal & PCC Reviewers		
Name	**Organisation**	**e-mail**
Pedro Miranda	LNEC	pgmiranda@lnec.pt
Hossein Miri	KIT	miri@teco.edu

Disclaimer

The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The above referenced consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law. Copyright 2012 by SAP, INESC-ID and SQS.

Table of Contents

1 EXECUTIVE SUMMARY....8

2 INTRODUCTION....9

3 RISK MANAGEMENT IN TIMBUS....10

3.1 RISK MANAGEMENT STAKEHOLDERS....10
3.2 RISK MANAGEMENT PROCESS....11
3.3 USER ROLES AND RESPONSIBILITIES....13

4 FUNCTIONAL REQUIREMENTS....16

4.1 REQUIREMENTS FOR ESTABLISHING CONTEXT AND IDENTIFYING RISKS....16
4.2 REQUIREMENTS FOR RISK ANALYSIS....17
4.3 REQUIREMENTS FOR RISK TREATMENT....18
4.4 REQUIREMENTS FOR RISK MONITORING....18
4.5 REQUIREMENTS FOR REPORTING....19
4.6 REQUIREMENTS RELATED TO THE PRESERVATION OF BUSINESS PROCESSES....19

5 USER REQUIREMENTS FROM INDUSTRIAL PROJECTS....21

6 FUNCTIONAL USE CASES....23

7 DATA MODEL FOR RISK-BASED DIGITAL PRESERVATION....29

7.1 DATA MODEL FOR RISK MANAGEMENT FOR BUSINESS PROCESSES....31
7.2 DATA MODEL FOR BUSINESS PROCESSES AND RESOURCES....31
7.3 DATA MODEL FOR DIGITAL PRESERVATION....32
7.4 DATA MODEL FOR RISK MONITORING....32

8 IERM ARCHITECTURE....34

8.1 IERM IN THE SCOPE OF THE TIMBUS ARCHITECTURE....34
8.2 IERM ARCHITECTURE OVERVIEW....35
8.2.1 Data Layer....37
8.2.2 Business Logic Layer....38
8.2.3 Presentation Layer....38
8.3 INTEGRATION WITH THE LEGALITY LIFECYCLE MODULE (LLM)....39

9 IERM TOOL DEVELOPMENT SPECIFICATION....40

9.1 IERM CLASS DIAGRAMS....40
9.1.1 Risk modelling and risk annotation....40
9.1.2 Risk Assessment and Preservation Recommendation....43

9.1.3 Risk monitoring 44

9.2 IMPLEMENTATION FEATURES 45

9.2.1 Risk model definition 45

9.2.2 Risk annotation 46

9.2.3 Risk impact assessment 50

9.2.4 Preservation recommendation 53

9.2.5 Risk Monitoring 58

10 CONCLUSIONS AND OUTLOOK 62

List of Figures

Figure 1: Risk management process in TIMBUS 11
Figure 2: Data model for risk management for business processes....30
Figure 3: Data model for preservation of business processes and resources....32
Figure 4: Data model for risk monitoring....33
Figure 5: iERM module in the scope of the overall TIMBUS architecture 34
Figure 6: iERM architecture overview....35
Figure 7: MVC view of the iERM architecture 36
Figure 8: Mapping between business processes and events....37
Figure 9: Class diagram for risk modelling and risk annotation 42
Figure 10: Class diagram for risk assessment....44
Figure 11: Risk monitoring class diagram....45
Figure 12: Risk annotation interaction diagram....46
Figure 13: Annotating risk impact values to a resource 47
Figure 14: Risk assessment interaction diagram....50
Figure 15: Mock-up of Risk assessment view....53
Figure 16: Interaction diagram for preservation recommendation 53
Figure 17: Mock-up for preservation recommendation view....58
Figure 18: Mock-up for definition risk indicators for risk events 60
Figure 19: Mock-up for risk indicator scheduling....61
Figure 20: Mock-up for risk indicator evaluation 61

List of Tables

Table 1: Risk management stakeholders 10
Table 2: Establish Context 12
Table 3: Identify Risks 12
Table 4: Analyse Risks 12
Table 5: Evaluate Risks 13
Table 6: Treat Risks 13
Table 7: Monitor Risks 13
Table 8: Roles and responsibilities 14
Table 9: Requirements for establishing context and identifying risks 16
Table 10: Requirements for risk analysis 18
Table 11: Requirements for risk treatment 18
Table 12: Requirements for risk monitoring 19
Table 13: Requirements for reporting 19
Table 14: Requirements for business process preservation 19
Table 15: Functional requirements from industrial use cases 22
Table 16: “Establish Context” use case 24
Table 17: “Identify Risks” use case 25
Table 18: “Analyse Risks” use case 26
Table 19: “Evaluate Risks” use case 27
Table 20: “Treat Risks” use case 27
Table 21: “Monitor Risks” use case 28
Table 22: Packages and classes for risk modelling and risk annotation 41
Table 23: Packages and classes for risk assessment and preservation recommendation 43
Table 24: Packages and classes for risk monitoring 44
Table 25: Example risks and risk impact 47
Table 26: Risk Annotation API – Annotate resource with risk 48
Table 27: Risk Annotation API – Annotate activity with risk 49
Table 28: Business Processes and Associated Preservation Requirements and Costs 50
Table 29: Risk Assessment API- Calculate Risk Impact for Business Process 51
Table 30: Risk Assessment API- Rank Business Processes by Risk Impact 52
Table 31: Risk Assessment API- Rank Risks for Business Process 52
Table 32: API – Check Technical Preservation Requirements for Activity 54
Table 33: API – Check Technical Preservation Requirements for Business Process 54
Table 34: API - Check Preservation Cost for Activity 55
Table 35: API - Calculate Preservation Cost for Business Process 55
Table 36: Suitability of preservation activities for preservation costing in TIMBUS 56
Table 37: API- Categorise Processes By Preservation Recommendation 57
Table 38: Risk Monitoring API – Get all Risk Indicators for a Risk Event 58

Table 39: Risk Monitoring API – Get Risk Indicator Status for a Risk Event and a Business Process.................59

List of Acronyms

API	Application Program Interface
BP	Business Process
BPRM	Business Process and Resources Model
CRUD	Create, Retrieve, Update, Delete
DP	Digital Preservation
ERM	Enterprise Risk Management
GUI	Graphical User Interface
HR	Human Resources
iERM	Intelligent Enterprise Risk Management
ISO	International Standards Organisation
IT	Information Technology
ITIL	Information Technology Infrastructure Library
KPI	Key Performance Indicator
KRI	Key Risk Indicator
LLM	Legalities Lifecycle Model
MVC	Model-View-Controller
RACI	Responsible, Accountable, Consulted and Informed

1 Executive Summary

This document describes the revised and internal version of the iERM architecture. It constitutes a revision and extension of the previous document, D5.1 ("Architecture for Intelligent ERM"), and is the output of Task 5.1, which establishes the reference architecture for the development of the iERM system in TIMBUS.

The iERM architecture presented here has been aligned with the revised TIMBUS architecture (described in deliverable D5.5 -"Refined Preservation Architecture"), has been updated to take into account user requirements from industrial projects (WP8 – "Civil Engineering Infrastructures" and WP9 – "eScience and Mathematical Simulations"), and has been further detailed to include a development view of the iERM system which will be the basis for the implementation specification.

From a general architectural point of view, the iERM system offers two types of input interfaces:

1. A risk interface through which the DP acquisition services and agents provide to the iERM a state and model of the organisational business processes running in an enterprise system.
2. A legality interface through which a Legalities Lifecycle Module provides information about the impact of risk on legal aspects, as well as information on preservation obligations, preservation specific IT contracting, data protection and IP issues.

The iERM system also offers output interfaces to the digital preservation components of TIMBUS, through which iERM delivers recommendations for what business processes to preserve.

The design of the iERM architecture is based on the output of the Task 4.1, which establishes the conceptual framework that brings together Digital Preservation with Enterprise Risk Management, and represents an input for the Task 6.1, which will carry out the implementation of the iERM system. The main outputs of the Task 4.1 used here (including ongoing work which will be reported in D4.8 due Month 24), are: an analysis of how digital preservation for timeless business processes and services can be linked into current Risk Management frameworks; and an outline of the phases of risk management which have to be covered in TIMUBS, based on the ISO standard #31000 (ISO 31000:2009) for Risk Management, and a proposal for a Digital Preservation Costing model used by iERM in supporting the user to make decision trade-offs between the economic factors versus the benefits of preserving a business process.

D5.1. discussed the risk management process, different users of the iERM module as well as requirements and requirement descriptions/examples. That deliverable ended with a draft sketch of the architecture of the iERM system which was accepted by the project reviewers with the comments that the "requirements and the architecture the M18 should both be detailed and complete in order to allow the development of implementation guidelines from the deliverable." This has been addressed in D5.4 in section 9 (iERM Tool Development Specification).

2 Introduction

Digital Preservation as an academic discipline and organisational practice aims to ensure the availability of information over a long period of time and is essentially motivated by the business and legal risks incurred by information loss or damage. Risk Management is traditionally addressed as a management discipline and performed typically in an isolated fashion in organisations. While Enterprise Risk Management breaks the "silo" approach and establishes a holistic enterprise wide management of risk through focus on business processes and other enterprise assets, Digital Preservation centres on information and lacks the perspective of business processes. The main innovation in TIMBUS is therefore its focus on the risk assessment based digital preservation of business processes, thus not only bringing together but also advancing the traditional digital preservation, risk management and business process management disciplines.

The iERM system is central to this innovation and a core component of the TIMBUS system. The role of the iERM system in TIMBUS is in the expediency phase of digital preservation, by enabling the monitoring and assessment of risks on business processes, and the cost-benefit analysis of various preservation actions that can be taken in response to a particular risk event for a particular business process. The iERM system supports the user in making the decision on whether a business process should be preserved and how, thus making the decision process more systematic and transparent.

The objective of this deliverable is to establish the software architecture for the development of an intelligent ERM system that interfaces with other organisational systems typically used as inputs into risk analysis. The present deliverable describes the second iteration of the iERM architecture, and is structured as follows: section 3 introduces the risk management process defined for the purpose of the TIMBUS project, the main stakeholders and the user roles involved in this process. In section 4 we outline the most important user requirements for the iERM system, and in section 5 we review requirements from the industrial scenarios from work package WP8 and WP9. A set of functional use cases are then selected to support the validation of the final system against core functionality (section 6). Section 7 describes a data model for risk-aware preservation, section 8 presents the reviewed iERM architecture, and section 9 gives a technical level guideline for the implementation of the iERM components.

3 Risk Management in TIMBUS

Section 3 is adopted from D5.1 for completeness, so that this document can standalone as a complete record of the final status of the iERM architecture work. This material was reviewed between M12-18, but no major changes were deemed necessary.

In order to understand how TIMBUS should address risk management in the iERM system, a detailed look at standard risk management concepts is necessary. In this section, we describe the TIMBUS approach to risk management, with respect to stakeholders (section 3.1), risk management process (section 3.2) and user roles and responsibilities (section 3.3).

3.1 Risk management stakeholders

Risk Management is embedded into major business processes, such as strategy development, performance management and business planning. It is important to address risk management not as a standalone activity or within a business unit, but to incorporate it in all business planning, operational processes and lines of business. An organisation implementing a risk management process and/or application must therefore assign responsibilities for managing the various phases of the risk cycle. These responsibilities could, for example, be defined as part of the risk policy of that organisation, or at the level of local organisational units as part of their tactical and operational management. The iERM system, consequently, must allow the definition of these responsibilities and must build functionality targeting these responsibilities. Table 1 below shows a list of stakeholders and their main responsibilities.

Table 1: Risk management stakeholders

Risk Management Stakeholders	Main Responsibility
Strategic Management	Responsible to determine the strategic direction of the organisation and for creating the environment and the structures for risk management to operate effectively.
Risk Management	Responsible for developing the risk management policy and coordinate all risk management activities across the enterprise, including the collaboration and consensus required to support enterprise risk management (ERM) activities and decisions.
Business Unit Management	Responsible to manage specific business unit processes. Concerning risk it must promote risk awareness within their operations.
Risk Owner	Person or entity with the accountability and authority to manage the assets in risk.
Risk Operator	Responsible for understand, accept and implement risk management processes. Responsible for reporting inefficient controls, loss events and near miss incidents.
Auditor	Responsible for developing a risk-based audit programme and to execute that programme across the organisation.

Regulator	Responsible for external imposing rules concerning the organisation environment such as legislation and standards. These can apply to the organisation, the system's technology, or the system's usage.

3.2 Risk management process

The iERM system aims to assess the impact of risks on business processes in an enterprise context, in order to identify and recommend business processes or process parts that need to be preserved, thus acting in the expediency phase of Digital Preservation. The risk management process adopted in TIMBUS and constituting the basis for the iERM design is illustrated in Figure 1 below, and was developed and explained in detail in TIMBUS Deliverable 4.1

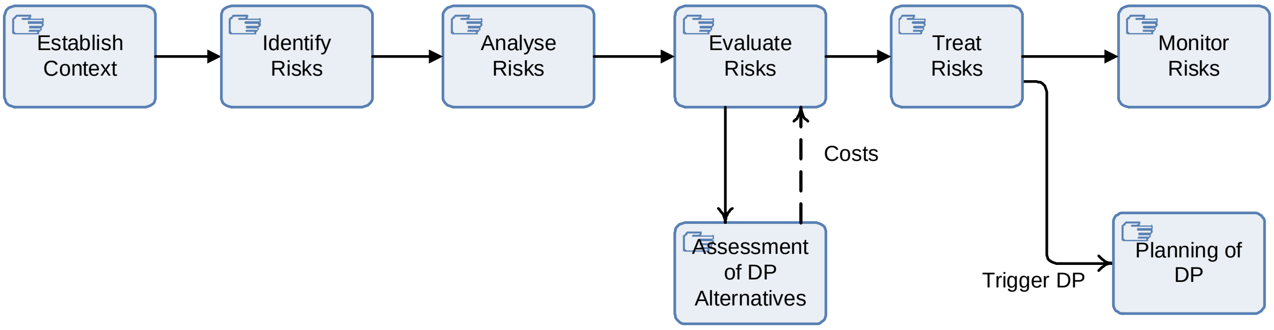


Figure 1: Risk management process in TIMBUS

Today's organisations are continuously exposed to several threats and vulnerabilities that may affect their normal behaviour. Once the business and organisation context for risk management is defined, in terms of, identifying strategic objectives and criteria for assessing the impact of risks, the risk identification step defines the scope of the risk management by selecting the risks that are going to be addressed; the analysis step examines the nature and level of the identified risk; and the evaluation step compares the severity of risk with the defined risk criteria, to decide if the risks are acceptable, tolerable or define the appropriate techniques/controls to handle them. After these steps all the risks should already be classified according to the possible impact, exposure, consequence, likelihood and level of risk. In TIMBUS, the selection of DP alternatives considers a cost/benefit analysis that is used by the risk evaluation process. Risk treatment then defines appropriate techniques to handle the assessed risks. In the particular case of TIMBUS, risk treatment can be a decision towards or against a particular digital preservation action and trigger the planning of the digital preservation process.

The tables below describe the six steps of the risk management process in TIMBUS, specifying for each step the objectives, inputs, outputs, stakeholders, and typical techniques and methods that can be applied. The 'Assessment of DP Alternative and 'Planning of DP' steps are non-risk management steps, and therefore external to the iERM system. In TIMUBS, these will be supported by the DP Engine (for details see section 8.1):

Table 2: Establish Context

Process step element	Element description
Main Objectives	Define context (external and internal)
	Align with organisational objectives
	Align with stakeholder expectations
	Establish risk criteria and risk classification
Input(s)	Context Model (D4.5)
Output(s)	Risk Criteria
	Risk Classification
Main Stakeholders	Strategic Manager; Risk Manager; Business Unit Manager; Regulator
Examples Techniques	System Modelling
	Dependency Analysis

Table 3: Identify Risks

Process step element	Element description
Main Objectives	Identify sources of risk
	Identify areas of impacts
	Identify events, causes and potential consequences
	Risk Management; Auditor; and Business Unit Manager;
Input(s)	Output of “Establish Context”
Output(s)	Comprehensive list of Risks
Main Stakeholders	Risk Manager; Business Unit Manager
Examples Techniques	Interviews
	Brainstorming
	Scenario Analysis
	Delphi Studies
	Primary Hazard Analysis

Table 4: Analyse Risks

Process step element	Element description
Main Objectives	Developing an understanding of risk
	Analyse likelihood and consequences
	Determine level of risk
Input(s)	Output of “identify risks”
Output(s)	List of quantified risks
Main Stakeholders	Risk Management; Business Unit Manager; Auditor; and Risk Owner;
Examples Techniques	Decision Tree
	Business Impact Analysis
	Event Tree Analysis
	Fault Tree Analysis
	Hazard and Operability Studies (HAZOP)
	Consequence/Likelihood Matrix

Table 5: Evaluate Risks

Process step element	Element description
Main Objectives	Assist decision making, comparing quantified risks with risk criteria to determine treatment priority.
Input(s)	Output of “analyse risks”
	Digital Preservation alternatives, including costs and risk modification indicators
Output(s)	Prioritized list of risks
Main Stakeholders	Risk Management; Business Unit Manager; Auditor; and Risk Owner;
Examples Techniques	Failure Mode Effect Analysis
	Structure “What-if?” Analysis
	Root Cause Analysis

Table 6: Treat Risks

Process step element	Element description
Main Objectives	Select controls for modifying risks
	Implement controls (triggers planning of DP)
	Calculate residual risk
Input(s)	Output of “evaluate risks” process
Output(s)	List of controls
Main Stakeholders	Risk Management; Business Unit Manager; Auditor; Risk Owner; and Risk Operator
Types of Response	Avoid risk
	Block risk source
	Change consequence
	Reduce risk likelihood
	Share risk
	Accept risk

Table 7: Monitor Risks

Process step element	Element description
Main Objectives	Ensure that controls are effectively and efficient
Input(s)	Output of “treat risks” step
Output(s)	Residual Risk
Main Stakeholders	Auditor
Examples Techniques	Sensors
	System Analysis

3.3 User roles and responsibilities

In order to specify in more detail the responsibilities of the different stakeholders in each step of the risk management process, we use a Responsible, Accountable, Consulted and Informed (RACI) chart (Table 8). In this chart, the following 4 types of involvement are defined:

1. A person Responsible (R) for an activity is in charge of executing the work.
2. A person Accountable (A) answers for the completion and results of a task.
3. A person is Consulted (C) if the process requires his feedback or contribution.
4. A person is Informed (I) when he needs to know of the decision or result of an activity.

Table 8: Roles and responsibilities

Sub-processes	Strategic Management	Risk Management	Business Unit Management	Risk Owner	Risk Operator	Auditor	Regulator
Establish Risk Context	A	R	C			I	C
Identify Risks		A	C		R	R	C
Analyse Risks		A	C	C	R	R	C
Evaluate Risks		A	C	C	R	R	C
Treat Risks	I	A	C	C	R	I	C
Monitor Risks		I	I	I	C	AR	C

R: Responsible, A: Accountable, C: Consulted, I: Informed

A Strategic Manager is accountable for “establishing risk context”. Its main objective is to ensure that all activities of that process are aligned with the organisation objectives. Strategic Management is also responsible for setting the risk criteria that will be used in the remaining process. As the highest decision-maker of the organisation, strategic management also needs to be informed of the controls that are being applied to risk in “risk treatment”.

The Risk Manager is responsible for defining the risk context of the organisation, and report on it to the Strategic Management. It can, for example, define:

- The way in which likelihood is to be expressed;
- How the level of risk will be determined; or
- The risk criteria by which it will be decided when a risk needs treatment or is acceptable and/or tolerable.

It also supervises and controls all the risk assessment (identification, analysis and evaluation of risks) and risk treatment activities. Its main goal is to assure that all risk management activities are running properly without flaws. It is also informed of the results of the “monitor risks” process to assess if it is necessary to re-run any of the previous sub-processes.

The Business Unit Manager is consulted in all sub-processes of the iERM process except for the “monitor risks” stage. As the responsible to manage specific business unit processes, it possesses knowledge about its unit process context and can, for example, identify:

- The elements of context of their unit that need to be captured as part of the “establishing context” step;
- Specific risks of their unit;
- The likelihood and consequence of those risks;
- The efficiency of a specific risk treatment; or
- The cost of a specific risk control.

The Business Unit Manager is also informed of the results of the “monitor risks” process when it is necessary to re-evaluate or re-assess any of their business unit assets.

A Risk Owner is responsible for managing the asset of a risk. Therefore, it is the best qualified actor to assist other stakeholders in activities concerning that particular asset. The Risk Owner is a role that is only established after the identification of the risk and is consulted on the analysis, evaluation and treatment of risk. It is also informed of the results of the monitoring process concerning the risk asset that it is responsible.

The Risk Operator is responsible for executing risk assessment and risk treatment and mainly reports to risk management. This role involves, for example:

- Creating the list of identified risks that will be the result of the risk identification process;
- Creating reports summarizing risk treatment; or
- Implementing a risk control;

The Auditor acts as a control role throughout the entire iERM process, and aims to ensure that all activities are being performed according to what has been planned. The auditor is informed about the context of the organisation in the first step (“establish risk context”) and is responsible to implement monitoring controls. At the end of the process, the Auditor is informed of the controls that were implemented in the risk treatment process and is accountable, and responsible, for monitoring those controls.

The Regulator is responsible for imposing rules, such as legislation and standards, and therefore is consulted in all the iERM steps to ensure that the activities are compliant with those rules.

4 Functional requirements

Section 4 is also adopted from D5.1 for completeness, so that this document can standalone as a complete record of the final status of the iERM architecture work. This material was reviewed between M12-18, but no major changes were deemed necessary.

Functional requirements are a way of capturing the intended behaviour of the system (Malan and Bredemeyer, 1999) as opposed to non-functional requirements that define 'how' a system is supposed to be. Following from the risk management process previously described, the iERM functional requirements are categorised in classes corresponding to the process steps (section 3.2). The following subsections outline these categories of requirements.

In addition, subsection 4.6 will address the category of requirements related to the preservation of business processes, thus supporting the "Assessment of DP alternatives" and the "DP planning" steps in the risk management process (Figure 1).

4.1 Requirements for establishing context and identifying risks

The objectives of this category of requirements are:

- to allow the user to define the context for risk management activities (i.e. organisational, financial, process and people related context),
- to select the specific risk types targeted by the risk management process, and
- to identify their association to various business process and context elements.

This should be done in a flexible way, in order to enable documenting, sharing and assessing risks across multiple dimensions.

Table 9: Requirements for establishing context and identifying risks

Id	Requirement title	Requirement description and/or examples
R1.1	Define the risk hierarchy (as part of the risk catalogue): risk categories and sub-categories, risk events, etc.	Examples of risk categories: IT, Financial, Legal, Operational, etc. Examples of sub-categories of financial risks: market risk, credit risk, etc Examples of risk events: Natural Disaster, Attack, etc.
R1.2	Define risk impact categories	Examples: financial, legal, reputation, environmental
R1.3	Define measurement scales and units for each impact category	Example: reputation measured qualitatively, levels: low, medium, high, catastrophic Example: financial loss measured quantitatively in dollars
R1.4	Define risk likelihood (either qualitative or quantitative)	The likelihood of a risk event can be estimated by:

		• A human expert • Calculating probabilities from historical data from different types of data sources (e.g. traffic, weather, seismic, customer behaviour, financial, etc)
R1.5	Associate risks with corporate objectives	The objective is to enable assessing the impact of the risk on the corporate strategy
R1.6	Associate risks with business objectives	Examples of objective categories: • Financial • Customer o Customer satisfaction • Market o Increase presence in US
R1.7	Associate risks with organisational units	Examples of organisational units: Sales, Human Resources, Controlling
R1.8	Define risk appetite for each organisational unit	The risk appetite can be defined in quantitative and/or qualitative form
R1.9	Define the actual risk impact of a risk event for an organisational unit	This is an estimation given by an expert on the financial loss incurred as result of a particular risk event. Example: the downtime of the main company server causes loss of £100000
R1.10	Define threshold levels for each organisational unit	A threshold level is defined through min and max values of financial loss. A threshold level can be used to associate quantitative loss to a qualitative value (e.g. minor, moderate, major levels, etc).
R1.11	Associate risks with business resources	Examples of resource-related risks: resource unavailability, resource overload
R1.12	Associate risks with elements defined in business process context (as defined in (Neumann, 2012))	Examples: Legal elements, IT components.
R1.13	Associate risks with business processes, activities and business processes categories	Examples of business process categories: HR, IT, Environmental
R1.14	Associate risks to legislation (regulation and category of regulation)	Examples: Financial compliance, IT compliance (e.g. ITIL, ISO
R1.15	Define cause-effect relationships between risks	The objective is to enable assessing the impact of one risk on another (risk propagation)

4.2 Requirements for risk analysis

The objective of this category of requirements is to allow the user (e.g. a Risk Operator) to analyse the impact of a particular risk event on different aspects of the business context, using different qualitative and quantitative methods, and to determine the impact of a risk event on various business KPIs.

Table 10: Requirements for risk analysis

Id	Requirement title	Requirement description and/or examples
R2.1	Measure the impact of a certain risk event on a resource	This includes the propagation of the impact on all dependent resources
R2.2	Measure the impact of a certain risk event on business process activities	This includes the propagation of the impact on all dependent activities and business processes
R2.3	Measure the impact of a certain risk event on a business objective at organisation unit level or company level	This includes the propagation of the impact on all dependent business objectives in the objectives hierarchy
R2.4	Measure the impact of a certain risk event on the corporate strategy	
R2.5	Measure the impact of a certain risk event on another risk	
R2.6	Measure the impact of a certain risk on regulatory compliance	
R2.7	Support for what-if analysis	For a specific risk probability, analyse the risk impact as detailed in the previous requirements
R2.8	Support for Monte Carlo simulations	
R2.9	The tool should be extensible to accommodate other risk assessment methods (Bayesian-trees, fold-trees, etc)	
R2.10	Determine preservation recommendations for a particular risk and a particular business process	

4.3 Requirements for risk treatment

The objective of this category of requirements is to enable the definition and execution of response plans and actions as treatment to a risk event of a particular type, and to measure the efficiency of these plans or actions.

Table 11: Requirements for risk treatment

Id	Requirement title	Requirement description and/or examples
R3.1	Define types of response	Examples: avoid, mitigate, transfer, watch, accept
R3.2	Define cost of response plans (quantitative or qualitative)	
R3.3	Define implementation time for a response plan	
R3.4	Evaluate response plan	Examples: measure plan effectiveness, cost-benefit relation, etc.

4.4 Requirements for risk monitoring

The objective of this category of requirements is to enable the continuous monitoring of the execution of business processes and their context in order to detect risk events in real-time.

Table 12: Requirements for risk monitoring

Id	Requirement title	Requirement description and/or examples
R4.1	For each risk type, define one or more Key Risk Indicators	
R4.2	Define business rules to correlate and monitor multiple KRIs	
R4.3	Monitor KRIs associated with multiple risks	
R4.4	Monitor implementation of preservation action	Monitoring of the risk control execution

4.5 Requirements for reporting

The objective of this category of requirements is to support delivery of aggregated and timely information to the user regarding risks in real-time and on multiple types of devices.

Table 13: Requirements for reporting

Id	Requirement title	Requirement description and/or examples
R5.1	Notification of violation of KRIs to respective user roles	
R5.2	Communicate risk information to different types of stakeholders	Taking in account stakeholders concerns.
R5.3	On-device reporting	
R5.4	On-desktop reporting	

4.6 Requirements related to the preservation of business processes

In addition to the previous requirements specific to a standard risk management process, the iERM tool in TIMBUS must be designed to allow recommendations for the preservation of business processes and associated resource stack. Consequently, the iERM tool must satisfy DP-specific requirements, as below:

Table 14: Requirements for business process preservation

Id	Requirement title	Requirement description and/or examples
R6.1	Functionality for defining "Preservation" as a type of risk mitigation action and for sharing it across risks as 'response template'	Examples of information to be captured: preservation strategy, preservation requirements, etc.
R6.2	Functionality to specify which resource is impacted by the risk and needs to be preserved, and to track the risk assessment(s) that concluded that the resource should be preserved	Annotate resource with the relevant risk assessment information that led to a DP decision
R6.3	Functionality for classifying the digital resources that can be preserved, according to the enterprise model developed in WP6 deliverables (e.g. business processes, software resources, hardware resources, etc.)	Annotate resource with its category / type

R6.4	Support for linking the preservation of a resource with the overall objectives or strategies it helps to achieve, e.g.: Business, Legal, Compliance, or Security. The model has to allow the propagation of risk / preservation impact to the high level objectives in the 4 categories	
R6.5	Support for re-evaluating the costs/benefits of preservation of a resource, if top-level objectives change	If business objectives change, does this impact already preserved resources? Probably they do not have to be kept anymore due to objective change? Not keeping anymore = cost saving?
R6.6	Functionality for documenting and monitoring *preservation effectiveness* (i.e. how well the preservation of a resource helps reduce the Business, Legal, Compliance, or Security risk)	(To be defined if the concept of *preservation completeness*, also an attribute of a regular 'risk response' step in a typical ERM system, has meaning in the context of preservation and how it can be measured)
R6.7	Support specifying or calculating the residual risk of a digital resource (i.e. risk remaining after preserving the resource) and what other risks the preservation does not / cannot address)	The residual risk should probably depend on: 1. Preservation information associated to the resource (e.g. preservation lifecycle stage, type of preservation (migration, redundancy, full/partial preservation, etc.) 2. Business-process specific preservation information, e.g. do we preserve the software implementation versus only the interface)
R6.8	Functionality for specifying (or taking as input) new risks introduced by the preservation of a resource / business process	New risks e.g.: the file format used in Archive X, Z and K has been superseded
R6.9	Functionality for identifying which other risks the preservation of a business process reduces or eliminates, which were not the ones triggering the current preservation activity	

5 User requirements from industrial projects

This section highlights specific user requirements derived in Industrial Projects Work packages: WP7 – "Engineering Services and Systems for Digital Preservation", WP8 – "Civil Engineering Infrastructures" and WP9 – "eScience and Mathematical Simulations". From these work packages, the input comes from the M18 versions of deliverables D7.1, D8.1 and D9.1, which aim to define the technical, business and economical contexts and also the user requirements for a digital preservation system applied to the civil engineering, and scientific domains respectively. D5.4 has also worked closely with D8.2 and D9.2 which specifically look at risk analysis within the WP8 and 9 use cases. This chapter specifically addresses some of the reviewer feedback from M12 relating to more detailed and complete requirements to aid the development work in WP6 and the eventual demonstrators when they get implemented in WP8 and 9.

In Table 15 we show how iERM will address the functional requirements captured in deliverables D7.1, D8.1 and D9.1 (both requirements below apply for both the civil engineering and the eScience use cases).

Table 15: Functional requirements from industrial use cases

Industrial requirement	How it is addressed in iERM
Requirement: *" Relevant information"* Goals: This requirement supports the goals: "Preserve the dam monitoring process" (in D8.1) and "Preserve the local analysis process" (in D9.1). Short description: Once information about data, context and tasks has been captured, the system must be able to determine which information is relevant to preserve the local analysis process Additional information: The set of relevant information is the minimum information necessary to preserve the local analysis process	iERM supports the risk-based identification of business processes which need to be preserved
Requirement*: "Preservation-worthy information"* Goals: This requirement supports the goals: "Preserve the dam monitoring process" (in D8.1) and "Preserve the local analysis process" (in D9.1). Short description: Once information about data, context and tasks has been captured, the system must be able to determine which information is preservation-worthy. Additional information: The decision of determining if information is preservation-worthy can, for example, be made through its value of risk loss. In case of data transformations that can be a huge overhead on the system, there should be a risk analysis made a priori to validate if saving all this data is critical or not. If possible, when we only can save data after transformation, we should make use of reversible transformations. In this way, in the future we could derive the initial values from the transformed values.	iERM supports the risk-based identification of business process resources (software, hardware, data, documents) which need to be preserved.
Requirement*: "Discover preservation-worthy business processes"* This requirement was issued by the WP7 industrial usecase "Engineering Services and Systems for Digital Preservation" and document in Deliverable 7.1 (Winkler, 2012) Short description: The system must be able to determine from all identified BPs in FR5, which one are the most critical for DP and assess feasibility of their preservation. Additional information: A decision whether a particular BP is preservation-worthy is made by assessing different risk and cost factors associated with preserving and non-preserving scenarios	iERM supports the risk-based identification of business process resources (software, hardware, data, documents) which need to be preserved.

6 Functional use cases

Section 6 is also adopted from D5.1 for completeness so that this document can standalone as a complete record of the final status of the iERM architecture work. This material was reviewed between M12-18, but no major changes were deemed necessary.

Based on the previously described user requirements (sections 4 and 5), a representative set of use cases, covering the major goals of the iERM system and which are architecturally significant have been selected and are presented in this section. The objective is to support, later on, the validation of the implemented iERM system with respect to achieving the main user goals. These use cases show the interaction of the different types of users ('actors') with the system and have been documented according to the 6 risk management process steps:

Use case 1: Establish Context

The goal of this use case is to define:

1. the context where risk management is applied, e.g. in terms of strategic and operational objectives (KPIs)
2. the scope of risk management for that particular organisation, in terms of risk types and risk hierarchy;
3. the criteria for assessing the impact of a risk type (e.g. financial, qualitative) and how the risk impact is measured (i.e. converted from qualitative form to monetary value)

Table 16: “Establish Context” use case

Use case element	Definition
Title	Establish risk management context
Actor	The Risk Manager or Business Unit Manager (i.e. a user with in-depth knowledge about the business and risks affecting it)
Pre-condition	N/A
Post-condition	The Risk Model Store has been populated with business specific information for the purpose of risk management
Scenarios	This use case includes the following scenarios: Scenario 1: Define strategic and operational KPIs Scenario 2: Defining risk categories and risk event types in each category Scenario 3: Define measurement scales for the likelihood of occurrence for each risk event type Scenario 4: Define how risk impact is measured for each risk type, in terms of: a) quantitative or qualitative type; quantitative type represents aspects like time and money, while qualitative type represents aspects like reputation, customer satisfaction, legal impact b) scale and unit Scenario 5: Define threshold levels for linking qualitative and quantitative risk impact for each affected entity (e.g. organisational unit, resource, etc) Scenario 6: Define risk appetite values Scenario 7: Define Key Risk Indicators

Use case 2: Identify Risks

The purpose of this use case is to define which risk events affect which organisational resources (be those IT, people, manufacturing, or facilities level resources).

Table 17: "Identify Risks" use case

Use case element	Definition
Title	Identify risks
Actor	Risk Manager
Pre-condition	A BPRM has been selected by the user.
Post-condition	A BPRM model is annotated with risk information and a Unified Risk Model is generated.
Scenarios	This use case consist of the following scenarios: Scenario 1: For each resource associated with a business process, this use case defines the following information: • Risk Event and the category to which it belongs (e.g. risk event: "contractor gone bankrupt", risk category: "business/commercial risks"). • Risk Driver – the cause behind the occurrence of this risk (e.g. loss of multiple contracts, market crash, etc. could be drivers for bankruptcy) • Risk Impact Value – monetary loss incurred as result of the risk event (in unit and on the scale defined through 'Establishing Context' Scenario 2: The same information can also be associated with a Business Activity, if available. Scenario 3: Assign a Risk Owner to a particular Risk Event.

Use case 3: Analyse Risks

The goal of this use case is to allow the user to assess the impact of a particular risk event (either in real time or through what-if scenarios). To this end, the iERM system will determine and notify the user on the affected business processes and associated resources stack. Based on the consequences and the likelihood of a risk event, the system will also output a ranking of the risks

Table 18: “Analyse Risks” use case

Use case element	Definition
Title	Analyse the impact of a risk event
Actor	Risk Owner
Pre-condition	The Unified Risk Model is generated for a particular BPRM. Cost information exists for different preservation strategies.
Post-condition	N/A
Scenarios	The objective is to assess the risk impact on business process level and on business objectives / KPIs level. In order to achieve this, the Risk Owner must use the iERM tool to run a Risk Assessment. This use case includes the following scenarios: Scenario 1: For a triggered Risk Event, the output is a list of affected business processes. Scenario 2: For a selected business process, determine a ranked list of risks and associated impact values (the ranking of risks is based on the impact value). Scenario 3: For a selected business process and Risk Event, the output is a list of DP alternatives, and associated: a) risk reduction factor (or residual risk); and b) the cost of preserving the business process and stack using that particular DP alternative

Use case 4: Evaluate Risks

For each of the previously identified business processes affected by a risk, the goal is to evaluate the costs and benefits of treating the risk using different digital preservation strategies.

Table 19: “Evaluate Risks” use case

Use case element	Definition
Title	Evaluate risks
Actor	Risk Manager or Line of Business Manager
Pre-condition	For each DP alternative, the following information is available: a. Risk reduction (as a factor or the final residual risk after implementing the DP action) b. The cost of implementing the DP action for a specific BPRM c. The legal impact of the risk event
Post-condition	The system will produce recommend a preservation action Recommendation Report is generated and stored in the PRR store
Scenarios	For a chosen business process, the user explores the costs and benefits of different types of response to a risk event, such as accepting the risk, or preserving the process, before deciding whether DP is an option and if it is, what DP strategy or alternative to select in order to treat that particular risk event

Use case 5: Treat Risks

The goal of this use case to allow the user to select a preservation action and to trigger its execution:

Table 20: “Treat Risks” use case

Use case element	Definition
Title	Treat risks
Actor	Risk Manager or Line of Business Manager
Pre-condition	The costs and benefits of different preservation actions have been explored by the user and a trade-off decision has been made.
Post-condition	The preservation of the business processes is triggered.
Scenarios	The user selects the preservation action for a particular business process and risk event.

Use case 6: Monitor Risks

The goals of this use case are:

1. to ensure that risk events that can be addressed through DP are detected and the user is notified in real time.
2. to ensure that the preservation of a business process stack triggered as treatment is executed efficiently

Table 21: "Monitor Risks" use case

Use case element	Definition
Title	Monitor risks
Actor	Risk Owner
Pre-condition	A Key Risk Indicator is defined and configured to detect the occurrence of a specific risk event.
Post-conditions	A risk event is generated internally in the iERM system. The user is notified on the GUI of the iERM system.
Scenarios	This use cases consist of the following scenarios: Scenario 1: Monitor specific Key Risk Indicators Scenario 2: Monitor the execution of the preservation of a business process.

7 Data model for risk-based digital preservation

This section describes an information model necessary for implementing the risk based digital preservation environment in TIMBUS. The model was designed specifically for the purpose of TIMBUS and aims to bring together, for the first time, four types of information:

1. information entities related to risk management for business processes(section 7.1),
2. information entities related to business processes and resources (section 7.2),
3. information entities related to digital preservation (section 7.3), and
4. information entities related to risk monitoring,

The central relationships between these types of entities are:

1. business processes and associated resources can be annotated with risk information thus allowing the assessment of impact of risk events on business processes and their KPIs, and

2. based on the previously assessed risk impact, the preservation of certain business processes and associated resources is an action aimed to reduce or eliminate this impact on business objectives and legal compliance.

The Entity-Relation diagram in Figure 2 below outlines the main concepts and their relations and represents the basis for designing and implementing a persistence layer in the form of data stores (for details see section 8.2.1).

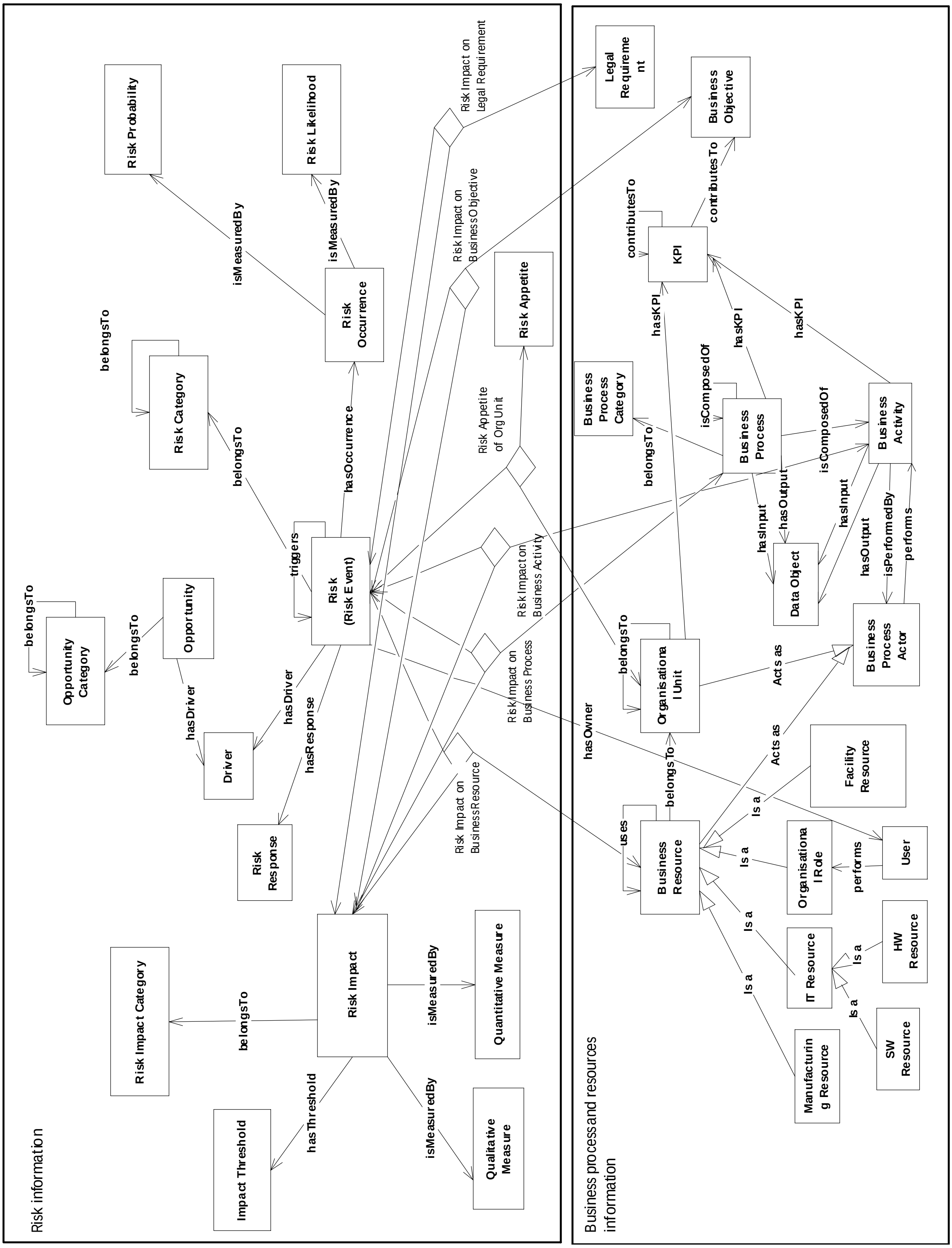


Figure 2: Data model for risk management for business processes

7.1 Data model for risk management for business processes

The *Risk* entity is the central entity in the data model and is the synonymous of a risk event. Causes of risk are modelled as *Drivers*, while consequences are modelled as *Risk Impact*. A *Risk* can *belong to* one or more *Risk Categories* and *Risk Categories* can also *belong to* other *Risk Categories* (thus enabling the modelling of a risk hierarchy).

The *occurrence* of a *Risk* can be modelled either as a *Risk Probability* (when it can be *measured* in a quantitative form) or through a *Risk Likelihood* (when it can only be *measured* in a qualitative form). *Risk Probability* can be defined through e.g. minim of scale, maxim of scale, measurement unit, while *Risk Likelihood* can be defined through a series of values e.g. 'low', 'medium', 'high'.

The *Risk Impact* entity is necessary to allow modelling 3 types of information associated:

1) the type of consequence of a risk event, modelled here through a *Risk Impact Category* (e.g. financial impact, customer satisfaction, etc.);

2) how the impact is measured (i.e. qualitatively or quantitatively) and modelled here through the *Qualitative Measure* and *Quantitative Measure* entities, respectively; for example, financial impact is measured in cost (quantitative), delays are measured in time (quantitative), while customer satisfaction can be measured through ''low', 'medium', 'high' values (qualitative).

3) the entities on which the impact of a risk event is assessed, and therefore the *Risk Impact* is associated to a *Business Resource*, an *Organisational Unit*, a *Business Activity*, a *Business Process*, a *Business Objective* and a *Legal Requirement*.

An *Impact Threshold* entity is also necessary to store the mapping between a qualitative and a quantitative measurement of the impact, e.g. a loss of £30,000 is a quantitative impact that can be mapped to 'high' on a qualitative scale.

The amount of risk an organisational unit can accept before addressing is modelled as *Risk Appetite*.

The model also allows modelling *Opportunities*, as uncertain events that can have a positive consequence, (as opposed to a risk which has a negative consequence), and it similarly allows grouping them into *Opportunity Categories*.

7.2 Data model for business processes and resources

This section describes the information model for business processes and resources. While this is only an initial model outlining the main entities and relations, a more detailed and extended model is presented in (Neumann, 2012), as an ontology of business processes and context.

As shown in Figure 2, the central entity is the *Business Process*, which is *composed of Business Activities*, and *has inputs* and *has outputs* as *Data Objects*. A *Business Process* can also be composed of other *Business Processes* and can be grouped in *Business Process Categories*. A *Business Activity is performed by* a *Business Process Actor,* which role can be taken by a Business Resource or by an Organisational Unit.

Business Resources can be of different types, i.e. *IT*, human, *Manufacturing*, or *Facilities* (i.e. building, electricity, etc) resources, and can belong to *Organisational Units.* A human resource is modelled through an *Organisational Role* (e.g. Unit Manager, Payroll Accountant, etc), which is *performed by* a *User*.

A Key Performance Indicator (KPI) can be associated to an *Organisational Unit*, to a *Business Activity*, or to a *Business Process*, and contributes to a *Business Objective.*

7.3 Data model for digital preservation

The model described in this section is necessary to capture information about the preservation action recommended and/or executed for a particular business process and associated resources stack, and was designed to support the risk-aware digital preservation requirements presented in section 4.6. Figure 3 below shows the main entities and relations of this model.

A *Preservation Recommendation* addresses a particular *Risk* event and *preserves* a *Business Process* and/or its *Business Resources*, and contains information about the *Preservation Requirements* necessary for executing the *Preservation Action.* (These requirements depend on the preservation action *and* the entity to be preserved, and therefore are associated to the *Preservation Recommendation* and not to the *Preservation Action*). The *Preservation Action* should further result in the reduction of *Risk Impact* by a *Risk Factor*.

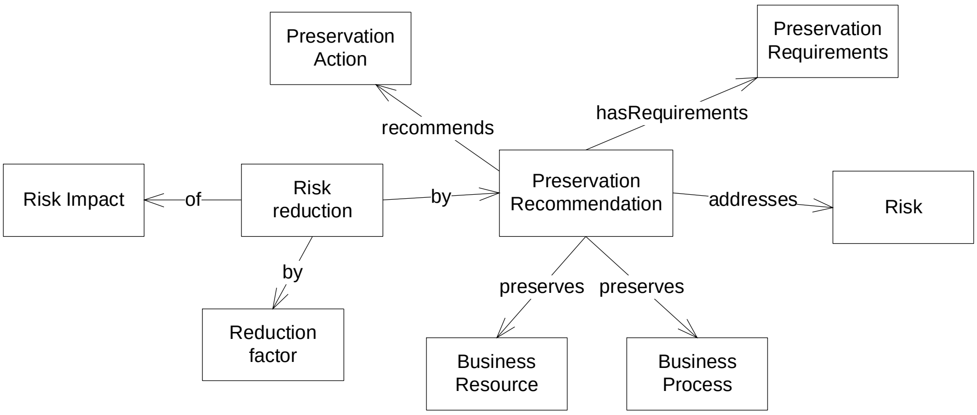


Figure 3: Data model for preservation of business processes and resources

7.4 Data model for risk monitoring

Risk Monitoring is the act of verifying whether a set of conditions occur in order to detect if a risk event is likely to happen. These conditions are named here *Risk Indicators*. A *Risk Indicator* (also sometimes called *Key Risk Indicator (KRI*), or simply *indicator*) is a piece of information that indicates the likelihood of *Risk Event* happening (i.e. supports the prediction of a risk event). Figure 4 below shows the Entity-Relation diagram that will be used for modelling risk monitoring information as part of the Risk Model store. A *Risk*

Indicator is a type of *Risk Driver* which can be checked at a certain point in time (*Timestamp*) and evaluated to have a certain *Value*. Every time a *Risk Indicator* is checked, a *Risk Indicator Instance* is created. A *Risk Indicator* can be used for monitoring multiple *Risk Events*, and one *Risk Event* can be monitored through several *Risk Indicators*. Monitoring means checking, according to a *Schedule*, that a *Risk Indicator* passes over a *Threshold*.

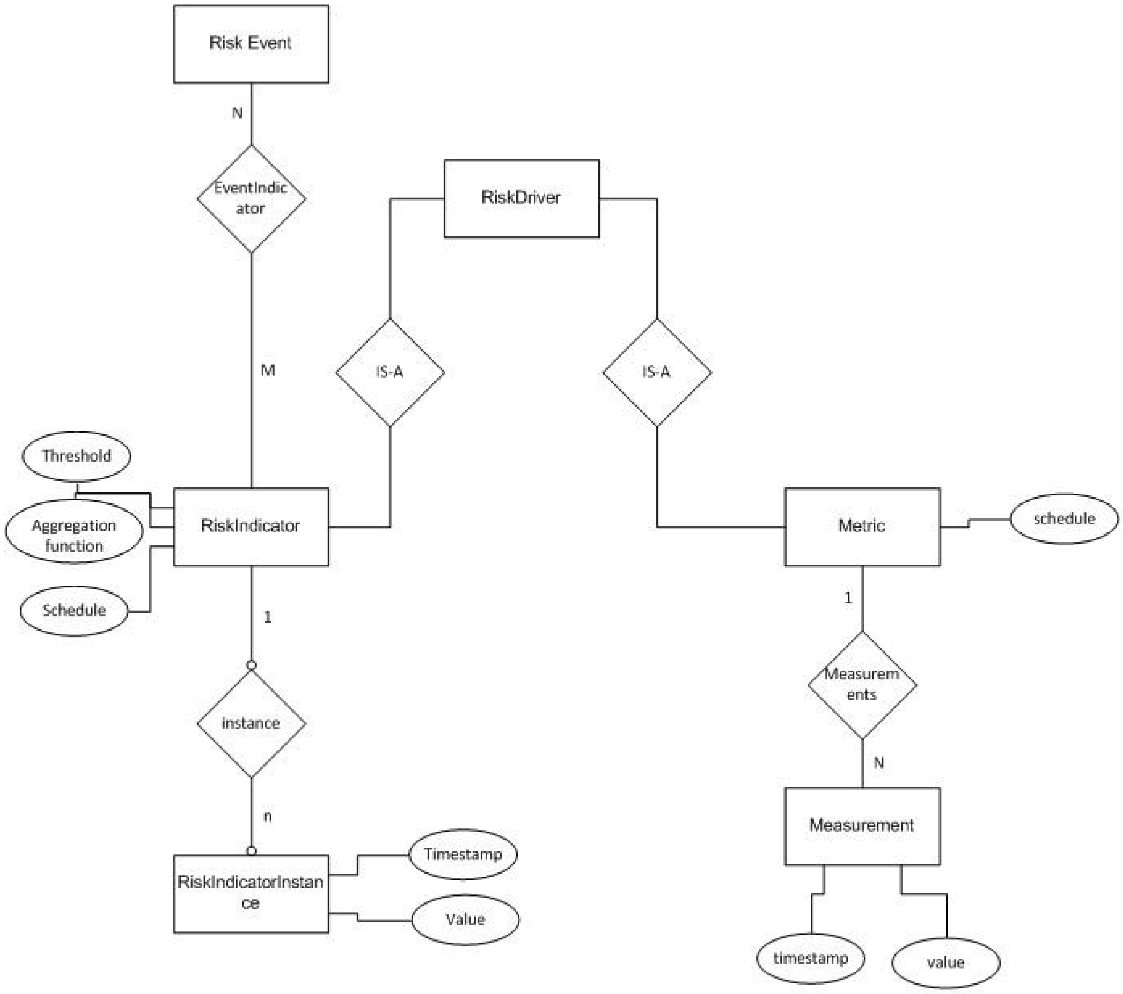


Figure 4: Data model for risk monitoring

8 iERM Architecture

This section presents a high level architecture of the iERM tool, which reflects the changes made since the original M12 deliverable. The objective is to build a more detailed and realistic reference architecture based on the previous work and thus to establish a strong foundation for the development of an intelligent ERM system, which allows to assess the impact of risks on business processes and associated context and to recommend a Digital Preservation action aimed to counteract the effects of these risks.

8.1 iERM in the scope of the TIMBUS architecture

The place of the iERM tool within the overall TIMBUS system and how it interfaces with other TIMBUS components is briefly covered in Deliverable 5.5 (Galushka, 2012, pp. 26), section 5.1, and shown in Figure 5 below. The iERM tool receives as input information about the business processes running in the organisation and the associated resource stack (as part of the internal organisational context), from the formalism-compliant meta-model component in the DP Acquisition Module (and defined in Neumann, (2012) – TIMBUS Deliverable 4.5). Assessing the risk impact on legality aspects is delegated to the Legality Lifecycle Module, of which results are merged with business process impact results into a final preservation recommendation. The preservation recommendation information is then taken and acted upon by the Preservation Expert Suite.

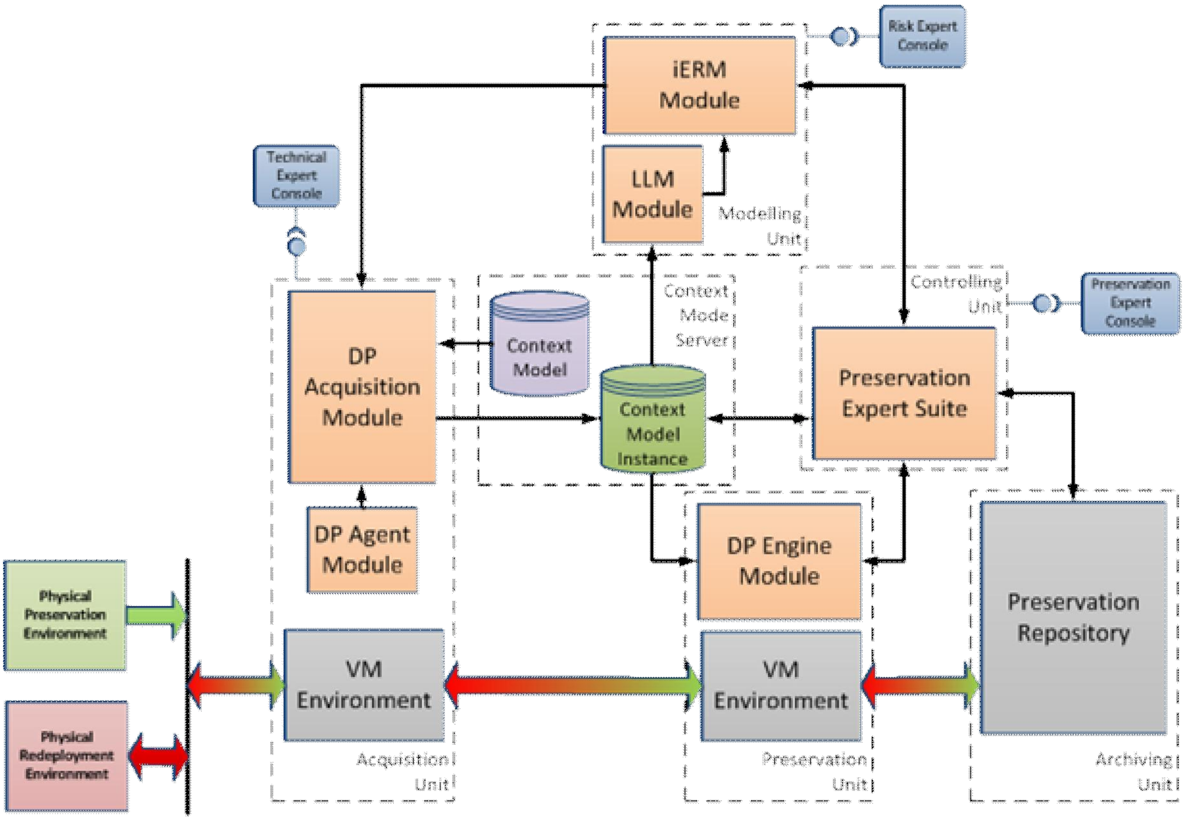


Figure 5: iERM module in the scope of the overall TIMBUS architecture

8.2 iERM Architecture Overview

The overall iERM architecture has been revised and updated as result of work carried out in Task 5.1 during months 12-18. Figure 6 below shows the main iERM components, data flow and APIs:

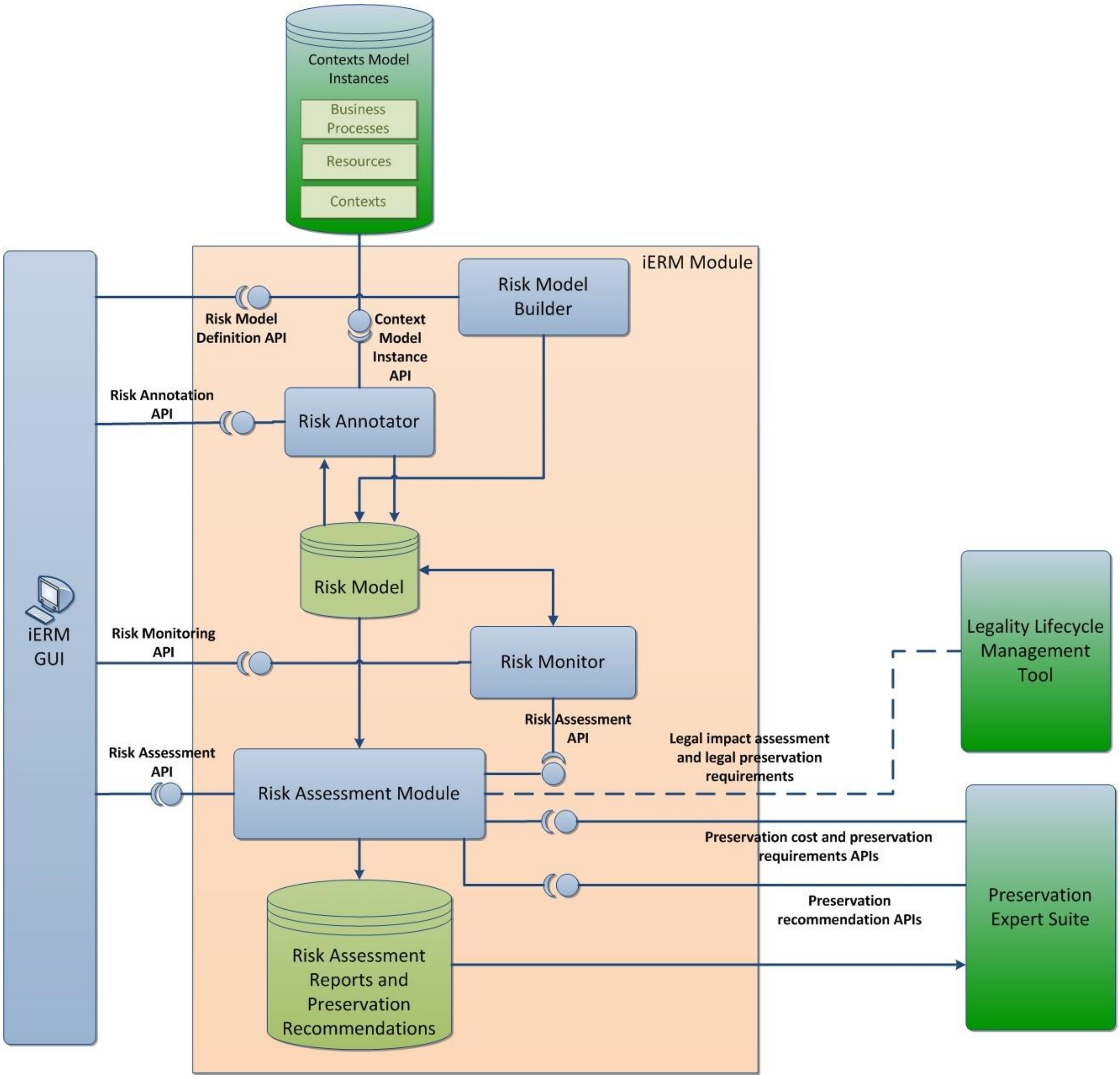

Contexts Model Instances
Business Processes
Resources
Contexts
iERM Module
Risk Model Builder
Risk Model Definition API
Context Model Instance API
Risk Annotation API
Risk Annotator
Risk Model
iERM GUI
Risk Monitoring API
Risk Monitor
Risk Assessment API
Risk Assessment API
Risk Assessment Module
Legal impact assessment and legal preservation requirements
Legality Lifecycle Management Tool
Preservation cost and preservation requirements APIs
Preservation recommendation APIs
Preservation Expert Suite
Risk Assessment Reports and Preservation Recommendations

Figure 6: iERM architecture overview

Once models of business processes and resources have been captured by the DP Acquisition Module and stored in the Context Model Instances store, business process models can be extracted, visualised and annotated with risk information using the Risk Annotator in iERM. For this purpose, the Risk Annotator uses risk information from the previously defined Risk Model, such as risk categories, risk events, risk impact measurement scales and units. The Risk Annotator also allows the user to attach estimations of risk impact such as resource unavailability duration, cost impact to the business, strategic, customer impact, etc. and to store these in the Risk Model. The Risk Assessment Module uses this information to calculate a ranking of risks by overall impact per business process and a ranking of business processes per risk type by overall risk impact. The Risk Assessment Module will also retrieve from the Preservation Expert Suite information about the technical requirements and costs of a preservation solution and make a recommendation for preservation for a given business process and risk event. Risk assessment results and preservation information are displayed via iERM GUI and stored in the Risk Assessment Store, from where they are taken later by the Preservation Expert Suite and used in the preservation planning.

Conceptually the iERM architecture can be described using a Model-View-Controller (MVC) pattern (Burbeck, S., 1987) and is shown below:

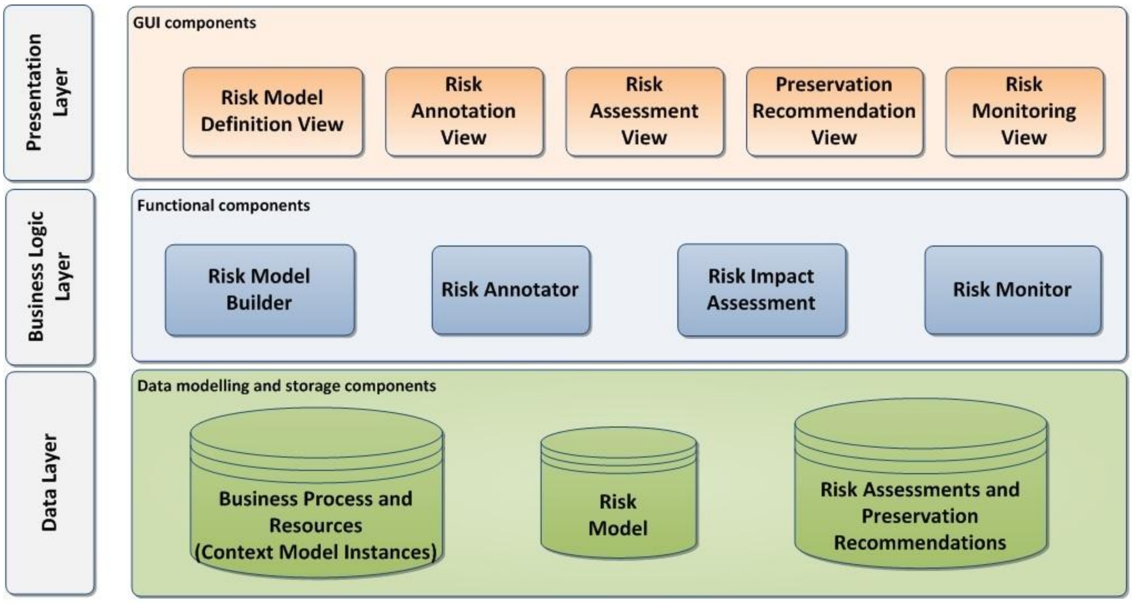


Figure 7: MVC view of the iERM architecture

In the MVC paradigm, the user input, the modelling of the domain and the visual feedback are explicitly separated and handled by three different specialised components, according to the 'separation of concerns' principle. The view manages the graphical and/or textual output to the portion of the bitmapped display that is allocated to its application. The controller interprets the mouse and keyboard inputs from the user, commanding the model and/or the view to change as appropriate. Finally, the model manages the behavior and data of the application domain, responds to requests for information about its state (usually from the view), and responds to instructions to change state (usually from the controller).

In iERM, the model (named here Data Layer) consists of the data stores and associated data management classes. The data stores model and store all entities and relations according to the models described in section 7, and are structured into three repositories: Context Model Instances, Risk Model store and Risk assessment Reports and Preservation Recommendations. These stores are managed by data access components, which implement the basic Create-Read-Update-Delete (CRUD) operations (for more details, see the class diagrams in section 9.1).

The controller (named here Business Logic Layer) consists of the main functional components in iERM, Risk Model Builder, Risk Annotator, Risk Impact Assessment and Risk Monitor.

The view (named here Presentation Layer), consists of GUI components designed to allowing the user to create, update and view results of the iERM workflow, and to access the iERM functionality.

In the following sub-sections we describe in more detail the data stores (section 8.2.1), the business logic components (section 8.2.2), and the user interface components (section 8.2.3) of the iERM tool.

8.2.1 Data Layer

1. Risk Model Store

This store contains information about risk types and their classification, risk appetite for organisational units, risk impact levels. The Risk Model also associates BPRM entities with various risk related information entities, such as risk impact level, mapping between quantitative and qualitative risk impact levels, risk probability, risk appetite, risk assessment formulae, etc. This model contains all the information necessary for assessing the impact of risk events for example, on business process KPIs, organisational KPIs or objectives and corporate strategy.

2. Context Model Instance store

This store contains instantiations of business process models and associated resources and dependencies.

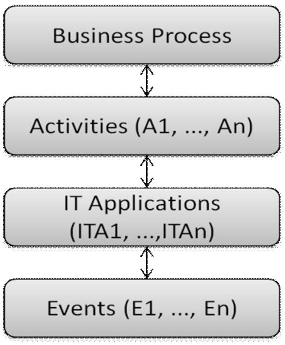


Figure 8: Mapping between business processes and events

The Business Process and Resource Model is a representation of business processes, and the resources they require to execute. These resources could be for example software resources (e.g. web services, application components, etc.), hardware components, human resources, facilities-type of resources (e.g. buildings, electricity, etc.). The model contains also the dependencies between different levels of resources (e.g. a web service ‘uses’ or ‘depends on’ an application component, which in turn ‘uses’ an OS product, etc.). Figure 8 shows these dependencies and was developed as part of TIMBUS Deliverable 4.1 (Burda, 2012). This model is compliant with the formalism developed in Task 4.4 for the purpose of context capturing.

3. Risk Assessments and Preservation Recommendations Store

This store contains reports describing the results of the risk assessment and the information of available preservation strategies for the affected business processes and associated costs. This store contains information about: the risks associated with a particular business process, a prioritisation and categorisation of these risks based on their impact, and the preservation strategies and associated costs available for each risk type. Such a report can be generated for a selected business process, showing all the relevant risks and their priorities, preservation costs, etc., or can be generated in response to a risk event, and in this case it will contain a list of all affected business processes and resources, and their relevant preservation options and costs. This report contains all information necessary to make trade-off decisions and cost/benefit analysis on what to preserve.

8.2.2 Business Logic Layer

This layer consists of the following functional components:

1. Risk Model Builder

This is a data management component which provides APIs for managing Risk Model information. These APIs will allow creating, retrieving, updating and deleting (CRUD) risk entities, such as Risk Event, Risk Category, risk impact information, etc. The Risk Model Builder APIs will be used by an editor component (e.g. the Risk Model Editing view of the iERM GUI) to allow the user to define or modify the Risk Model in the design stage.

2. Risk annotator

This component provides APIs for annotating a Business Process and Resources Model with risk information and for storing them in the Risk Model.

3. Risk Impact Assessment Module

The Risk Impact Assessment module uses the in conjunction with preservation requirements and costs from the Preservation Expert Suite to generate preservation recommendations, which encapsulate the information required to support the preservation process. This module aims to give an insight into the impact a risk event has on business process KPIs/ corporate objectives.

8.2.3 Presentation Layer

The iERM tool will implement a number of Graphical User Interface (GUI) components (views) to enable user level access to iERM functionality and data models. These views are:

1. Risk Model Definition View

This is an editing component of the iERM GUI which allows the user to graphically manage the Risk Model entities. However, the Risk Model and Risk Model Definition View are not of critical importance to delivering the core TIMBUS functionality and innovation (risk-based business process preservation), and therefore their implementation is optional in TIMBUS. This is also because off-the-shelf, generic database management tools and editors can also be used to define and manage the data entities, and no dedicated graphical editor is necessary to be implemented.

2. Risk Annotation View

This is an editing component of the iERM GUI which allows the user to graphically associate a BPRM model with risk information, such as risk likelihood and risk impact.

3. Risk Assessment View

This component of the iERM GUI allows the user to carry out two types of actions:

Define and edit risk assessment scenarios.

View results of the risk assessment in the form of reports or analytics dashboards.

4. Risk Monitoring View

This GUI component will allow the user to define Key Risk Indicators and associate them with the data sources to be monitored, and to enter results of monitoring controls evaluation for specific business processes and risk types (‘manual monitoring).

8.3 Integration with the Legality Lifecycle Module (LLM)

As shown in Figure 6, a loose integration (represented as a dotted line) is foreseen between iERM and LLM at this stage. We propose a ‘logical’ (i.e. non-technical) integration, whereby at a minimum level the user interface of each tool allows the user to invoke / connect to the other tool (via button or hyperlink), without any data and workflow (i.e. state) persistence or transfer between the two modules. The context and activities in which the LLM should be invoked from iERM are:

1. Once risk impact has been assessed and risks classified for a business process, the user can call LLM to check the legal impact of each risk.
2. Once preservation requirements, costs and recommendations have been given, the user can call LLM to check the legal requirements for a given preservation alternative.

9 iERM Tool Development Specification

Having outlined in previous sections the functional requirements, functional use cases and the main architectural components of the iERM architecture, we now present a developmental view of the iERM in which we seek to provide a high level implementation specification and guidelines for software development. This section again specifically addresses the M12 feedback from the reviewers relating to providing a detailed enough architecture to be of value to the tool development. As such, this section contains:

1. Class diagrams for the main implementation modules, showing software classes and packages
2. Interaction diagrams showing the sequence of invocations between software modules as result of specific user actions
3. API specifications for the main functionality of iERM
4. Mock-ups for some of the UI-level components (views)

9.1 iERM Class diagrams

The diagrams in Figure 9 and Figure 10 show how the architectural components in can be implemented using software packages and classes. The following packages are recommended for implementation, grouping classes corresponding to the three layers of the Model-View-Controller architectural pattern (data, business logic and presentation layers), as follows:

9.1.1 Risk modelling and risk annotation

Packages and classes in Figure 9 are explained in Table 22 below:

Table 22: Packages and classes for risk modelling and risk annotation

Layer	Package	Content and purpose
Data	*ierm.risk.model*	Contains classes implementing the Create-Read-Update-Delete (CRUD) operations on entities from the Risk Model data store data stores. The *Risk, RiskCategory, RiskImpact, RiskOccurence, ImpactThreshold and RiskImpactCategory* classes and the relations between them are based on the Entity-Relation model presented in section 7, Figure 2, while the *RiskModelConfiguration* class is neecessary be used to allow the user e.g. to define and maintain his/her own risk events and risk categories, to define the type of impact a particular risk will have, and how risk impact will be measured.
Business logic	*ierm.risk.annotator*	Contains classes implementing business logic or controller-type of functionality. For example, the *BPResourceFactory* in the *ierm.risk.annotator* package will extract from the Context Model Instance store (external to iERM) information about existing business processes and resources and will pass that on to the *MainView* class for graphical visualisation. Similarly, the *RiskFactory* class will establish the connection between the *RiskModelConfiguration* and the *RiskModelDefinitionView* classes, for the purpose of defining e.g. risk categories, risk impact categories, acceptable values for risk impact etc. The *RiskFactory* class will also be used for processing annotated risk data entered by users through the *RiskAnnotationView*. The *RiskClassCalculator* class in the *ierm.risk.impactAssessment* package will implement the classification of a risk event impact for a particular business process, (e.g. into 'Low', 'Medium', 'High').
Presentation	*ierm.risk.gui*	Contains classes implementing the presentation layer modules: *RiskModelDefinitionView, RiskAnnotationView and MainView*.

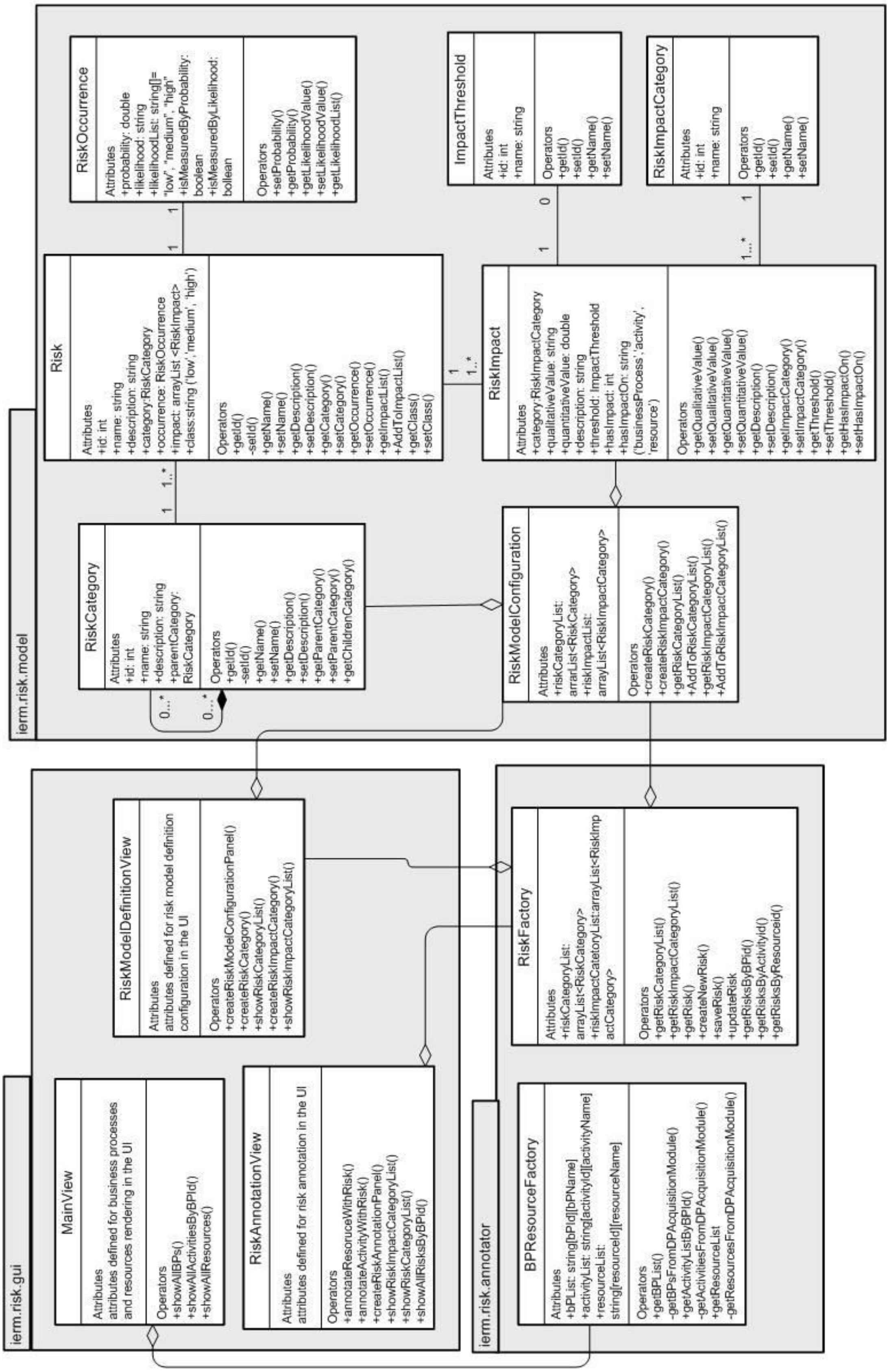


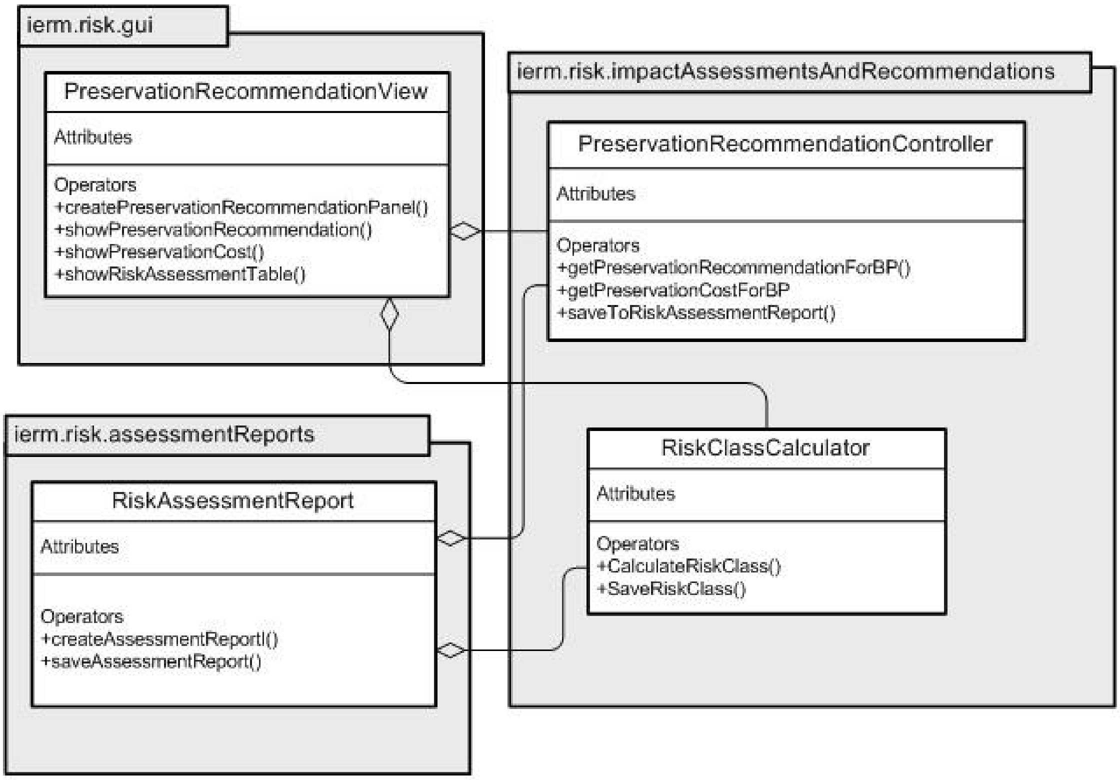
Figure 9: Class diagram for risk modelling and risk annotation

9.1.2 Risk Assessment and Preservation Recommendation

Packages and classes in Figure 10 are explained in Table 23 below:

Table 23: Packages and classes for risk assessment and preservation recommendation

Layer	Package	Content and purpose
Data	*ierm.risk.assessmentReports*	The *RiskAssessmentReport* class implements methods for storing, updating and deleting information about results of risk impact assessments and associated preservation recommendations and costs, into the Risk Assessment Reports store.
Business logic	*ierm.risk.impactAssessment*	The *RiskClassCalculator* class implements methods for classifying the level of risk impact of a particular risk event on a particular business process (e.g. low, medium, high) and saving this information in the Risk Assessment Report store. The method will also determine a ranking of possible risk events for a business process based on the previously determined class, in combination with the associated costs of treating that risk. The *PreservationRecommendationController* class implements methods for requesting from the Preservation Expert Suite information about whether a business process or resource should be stored ('yes' or 'no') and technical and cost requirements for preservation for a particular preservation strategy. This information will be saved together with the risk assessment results in the Risk Assessment Report store.
Presenta-tion	*ierm.risk.gui*	The *PreservationRecommendationView* class contains methods for displaying preservation recommendations from the Preservation Expert Suite The *RiskAssessmentView* class implements methods for displaying risk impact values and risk ranking and classes for risk events and business processes and resources.



ierm.risk.gui
PreservationRecommendationView
Attributes
Operators
+createPreservationRecommendationPanel()
+showPreservationRecommendation()
+showPreservationCost()
+showRiskAssessmentTable()
ierm.risk.impactAssessmentsAndRecommendations
PreservationRecommendationController
Attributes
Operators
+getPreservationRecommendationForBP()
+getPreservationCostForBP
+saveToRiskAssessmentReport()
RiskClassCalculator
Attributes
Operators
+CalculateRiskClass()
+SaveRiskClass()
ierm.risk.assessmentReports
RiskAssessmentReport
Attributes
Operators
+createAssessmentReportl()
+saveAssessmentReport()

Figure 10: Class diagram for risk assessment

9.1.3 Risk monitoring

Packages and classes in Figure 11 are explained in Table 24 below:

Table 24: Packages and classes for risk monitoring

Layer	Package	Content and purpose
Data	*ierm.risk.model*	Contains classes for storing risk monitoring information, such as indicators used for monitoring, monitoring instances, and reports containing the results of monitoring
Business logic	*ierm.risk.monitoring*	Contains classes connect the graphical views implementation with the data handling classes, in terms of risk indicator evaluations and risk monitoring reports.
Presenta-tion	*ierm.risk.gui*	Contains classes implementing the monitoring views that allow the user to define risk indicators, enter values obtained from checking (manually) the indicators, and requesting and visualising monitoring reports.

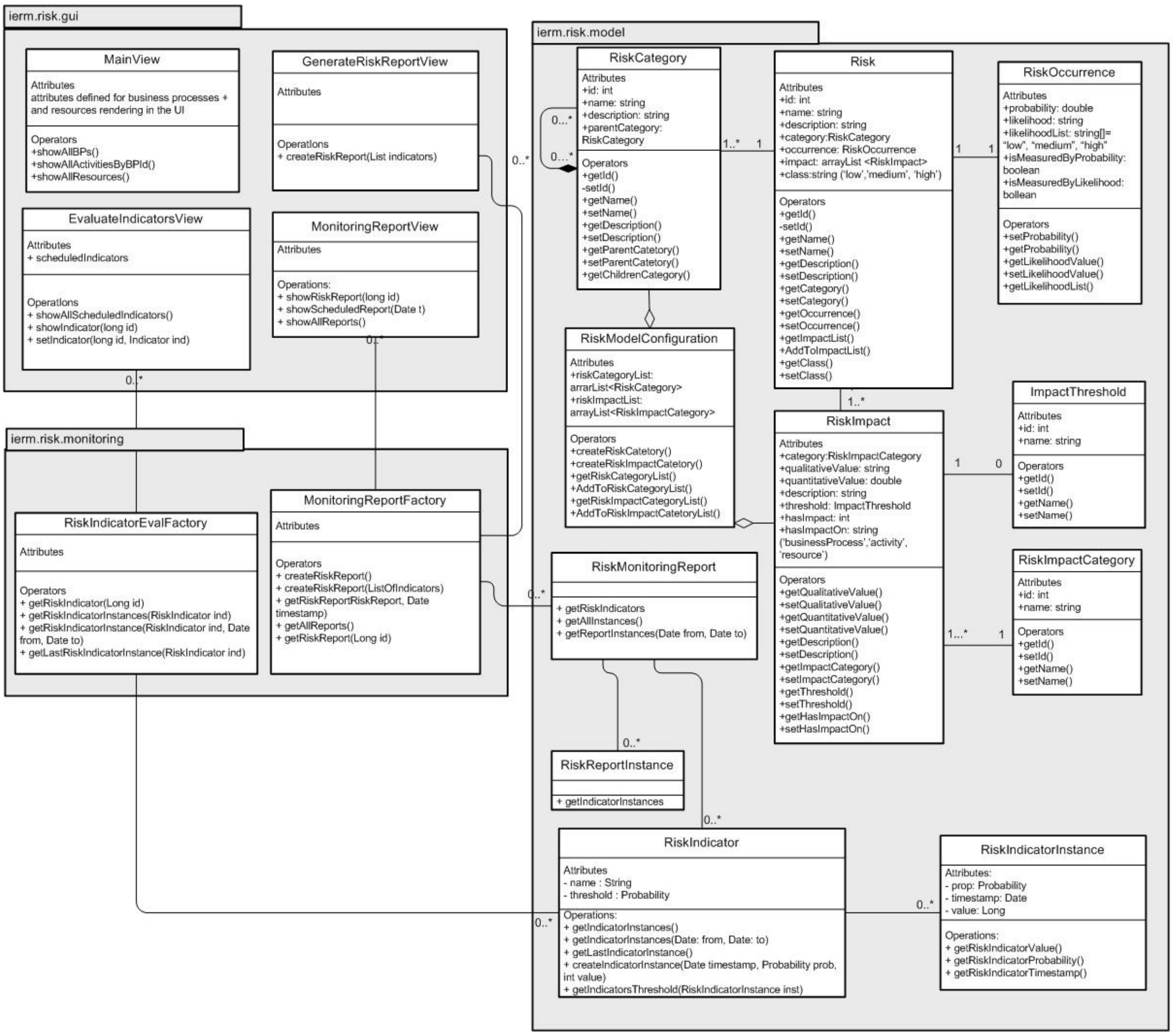


Figure 11: Risk monitoring class diagram

9.2 Implementation features

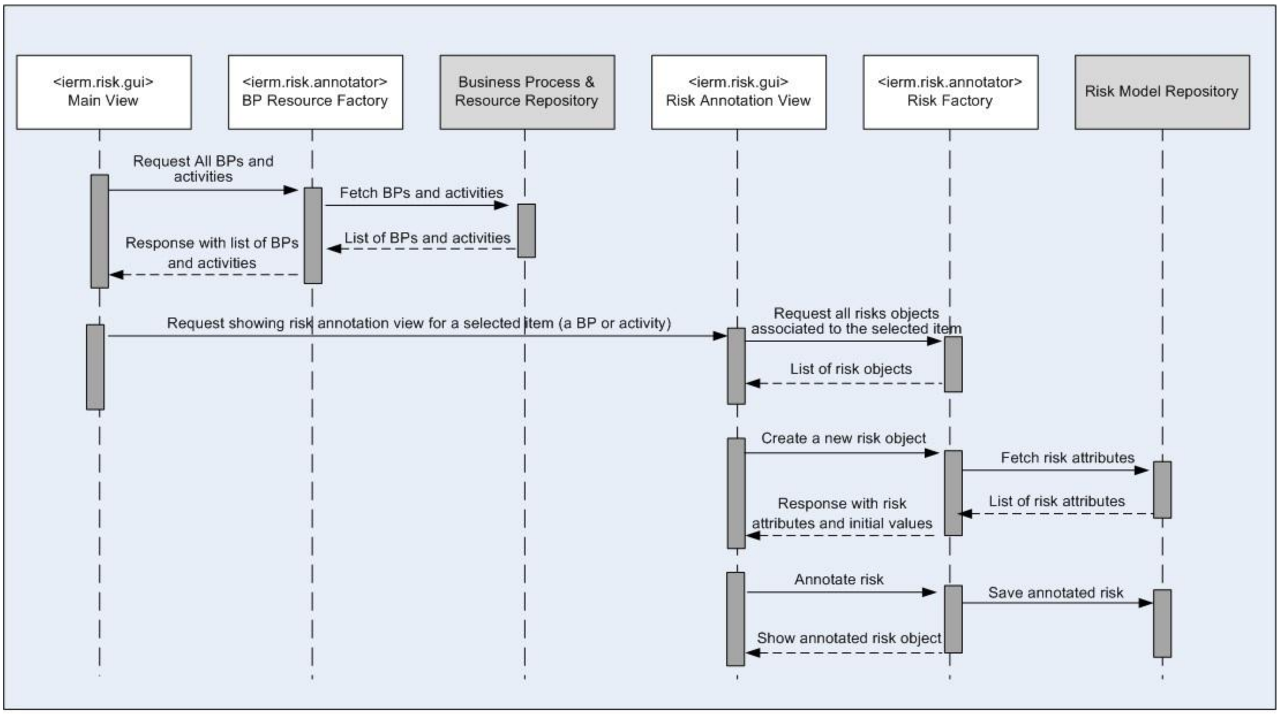
The following are the main, high-level features iERM will implement, each corresponding to one of the use cases presented in Section 6, "Functional use cases".

9.2.1 Risk model definition

This is a design-time feature implementing the "Establishing Context" use case. The user will create risk categories, risk events in each category, define how risk impact is measured for each risk event in terms of quantitative/ qualitative, possible values and scale, for each of the pre-defined categories of risk impact: financial impact, customer satisfaction, legal, and strategic. The user can do this using a database management tool or, if implemented, using a risk modelling graphical view of the iERM.

9.2.2 Risk annotation

This is a design-time feature implementing the “Risk identification” and part of the “Risk analysis” use cases. The user interaction of risk annotation is triggered when a user creates a risk object in the iERM tool (Figure 12). After the risk annotation, a risk object should have the attributes and user-entered values as shown with the example in Table 25.



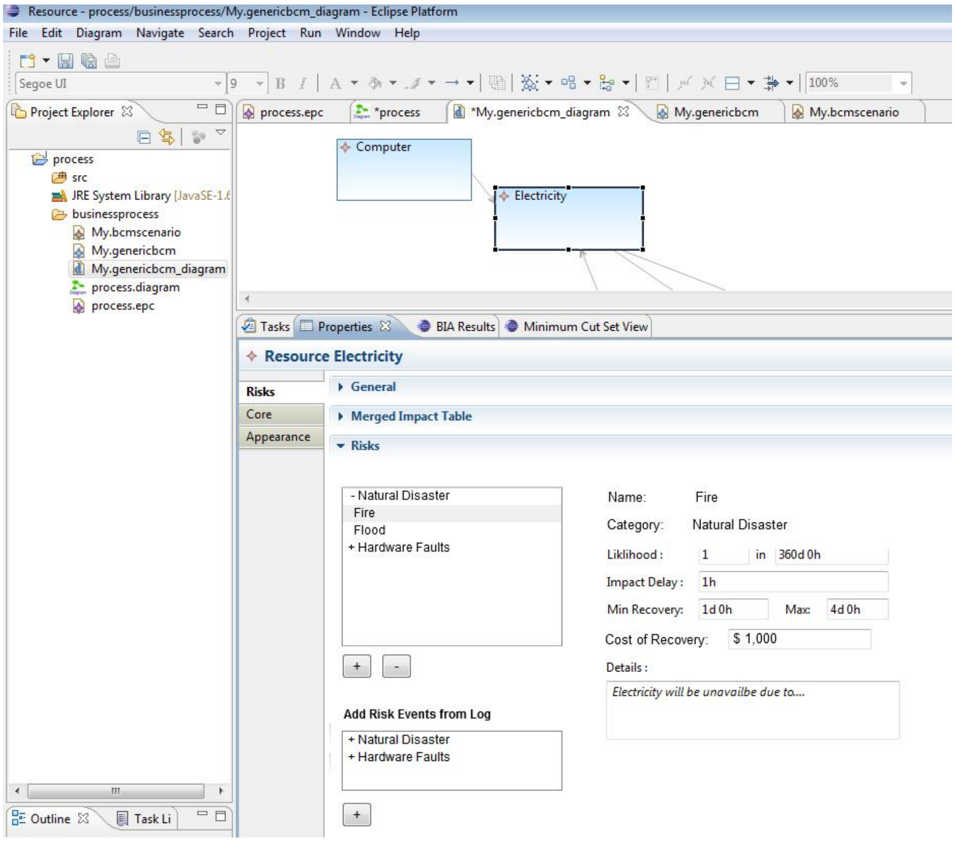
<iferm.risk.gui> Main View
<iferm.risk.annotator> BP Resource Factory
Business Process & Resource Repository
<iferm.risk.gui> Risk Annotation View
<iferm.risk.annotator> Risk Factory
Risk Model Repository
Request All BPs and activities
Fetch BPs and activities
List of BPs and activities
Response with list of BPs and activities
Request showing risk annotation view for a selected item (a BP or activity)
Request all risks objects associated to the selected item
List of risk objects
Create a new risk object
Fetch risk attributes
List of risk attributes
Response with risk attributes and initial values
Annotate risk
Save annotated risk
Show annotated risk object

Figure 12: Risk annotation interaction diagram

The screenshot in Figure 13 below shows a mock-up for the Risk Annotation View, where the user has selected the ‘Electricity’ resource attached to a ‘Computer’ resource, and annotates this resource with a risk event of type ‘Fire’. The user enters the following information:

- How likely the event is to happen (number of times in a given period). This value of the risk likelihood can also be computed by the system
- How long it takes for the impact to be effect on the resource, from when the event happened
- Minimum and maximum time needed to recover the resource after the event happened
- Cost of recovery

The user can also create new risk event types, assign them to risk categories, and associate them and their impact values to the selected resource (in this example new ‘Natural Disaster’ or ‘Hardware Fault’ risk-type of events can be created).



- Natural Disaster
  Fire
  Flood
+ Hardware Faults

Name: Fire

Category: Natural Disaster

Liklihood : 1 in 360d 0h

Impact Delay : 1h

Min Recovery: 1d 0h Max: 4d 0h

Cost of Recovery: $ 1,000

Details : Electricity will be unavailbe due to....

Add Risk Events from Log

+ Natural Disaster
+ Hardware Faults

Figure 13: Annotating risk impact values to a resource

The Table 25 below shows examples of values entered by the user through this mock-up screen, as estimations of the different types of risk impact.

Table 25: Example risks and risk impact

Risk ID	Financial Impact	Likelihood	Strategic Impact	Impact on customers	Legal impact	Impact Duration
R1	450.000 €	Medium	Noticeable strategic impact	Major significant impact on >100 customers	Minor breach of legal/ regulatory requirements	10 days
R2	393.750 €	Very low	Major impact on important business objectives	Noticeable impact on customers	No breach of legal/ regulatory requirements	2 days

The APIs required to be implemented for the risk annotation scenario are specified in Table 26 and Table 27 below, to allow annotating a risk resource and risk activity, respectively, with risk impact information.

Table 26: Risk Annotation API – Annotate resource with risk

API	AnnotateResourceWithRisk				
Summary	Attach risk information to a resource defined in the Context Model				
Implemented by	UI component (Risk Annotation View)				
Pre-conditions	Context Model extracted and Risk Model defined				
Postconditions	The Unified Risk Model is created or updated				
Inputs	Information entity	Semantic	Entity elements and / or formats	How it is determined	Comments
	RiskType	Type of risk event which can affect a resource	integer (risk type identifier)	user-selected from risk taxonomy	type of risk defined in the risk taxonomy in the Risk Model
	Resource	E.g. IT applications, web services, hardware resources, facilities resources, people.	integer (resource identifier)	selected graphically by the user	resources taxonomy defined in the Context Model
	RiskLikelihood	The likely occurrence frequency of the risk for the given resource	a. quantitative (double, representing %) or b. qualitative (text, e.g. Low, medium, high), as defined in the Risk Model	computed	The measurement unit and scale for all risk impact types have been defined in the Risk Model
	CostImpact	Cost incurred by not addressing the risk (quantitative)	Value: double	value estimated by user	
	StrategicImpact	Impact on strategic level (qualitative)	Level: text, (e.g. low, medium, high), and Description: text	selected by user from available options	
	CustomerImpact	Impact on customer satisfaction (qualitative)	Level: text, (e.g. low, medium, high), and Description: text	selected by user from available options	
	ImpactDuration	Duration of unavailability of resource	Value: integer e.g. Minutes, Hours, Days, Weeks, Months	value estimated by user	
	LegalImpactValue	Impact on regulatory compliance (qualitative)	Level: text, (e.g. low, medium, high), and Description: text	selected by user from available options or returned by LLM API (to be decided)	
Outputs	None				

Table 27: Risk Annotation API – Annotate activity with risk

API	AnnotateActivityWithRisk				
Summary	Attach risk information to a process activity				
Implemented by	UI component (Risk Annotation View)				
Pre-conditions	Context Model extracted and Risk Model defined				
Postconditions	The Unified Risk Model is created or updated				
Inputs	Information entity	Semantic	Entity elements and / or formats	How it is determined	Comments
	RiskType	Type of risk event which can affect a process activity	integer (risk type identifier)	user-selected from risk taxonomy	type of risk defined in the risk taxonomy in the Risk Model
	Activity		integer (activity identifier)	selected graphically by the user	
	RiskLikelihood	The likely occurrence frequency of the risk for the given activity	a. quantitative (double, representing %) or b. qualitative (text, e.g. Low, medium, high), as defined in the Risk Model	computed	The measurement unit and scale for all risk impact types have been defined in the Risk Model
	CostImpact	Cost incurred by not addressing the risk (quantitative)	Value: double	value estimated by user	
	StrategicImpact	Impact on strategic level (qualitative)	Level: text, (e.g. low, medium, high), and Description: text	selected by user from available options	
	CustomerImpact	Impact on customer satisfaction (qualitative)	Level: text, (e.g. low, medium, high), and Description: text	selected by user from available options	
	ImpactDuration	Duration of unavailability of resource	Value: integer e.g. Minutes, Hours, Days, Weeks, Months	value estimated by user	
	LegalImpactValue	Impact on regulatory compliance (qualitative)	Level: text, (e.g. low, medium, high), and Description: text	selected by user from available options or returned by LLM API (to be decided)	
Outputs	None				

9.2.3 Risk impact assessment

The Risk Assessment GUI should list all the available business processes and their associated legal and technical preservation requirements and cost of preservation as the example shown in Table 28. When the user clicks on a business process, the iERM tool will show its associated risks with risk impact ranking classes (e.g., low, medium, or high) calculated by the Risk Impact Assessment Module (*RiskClassCalculator* class). The user interaction for determining the risk class is shown in Figure 14.

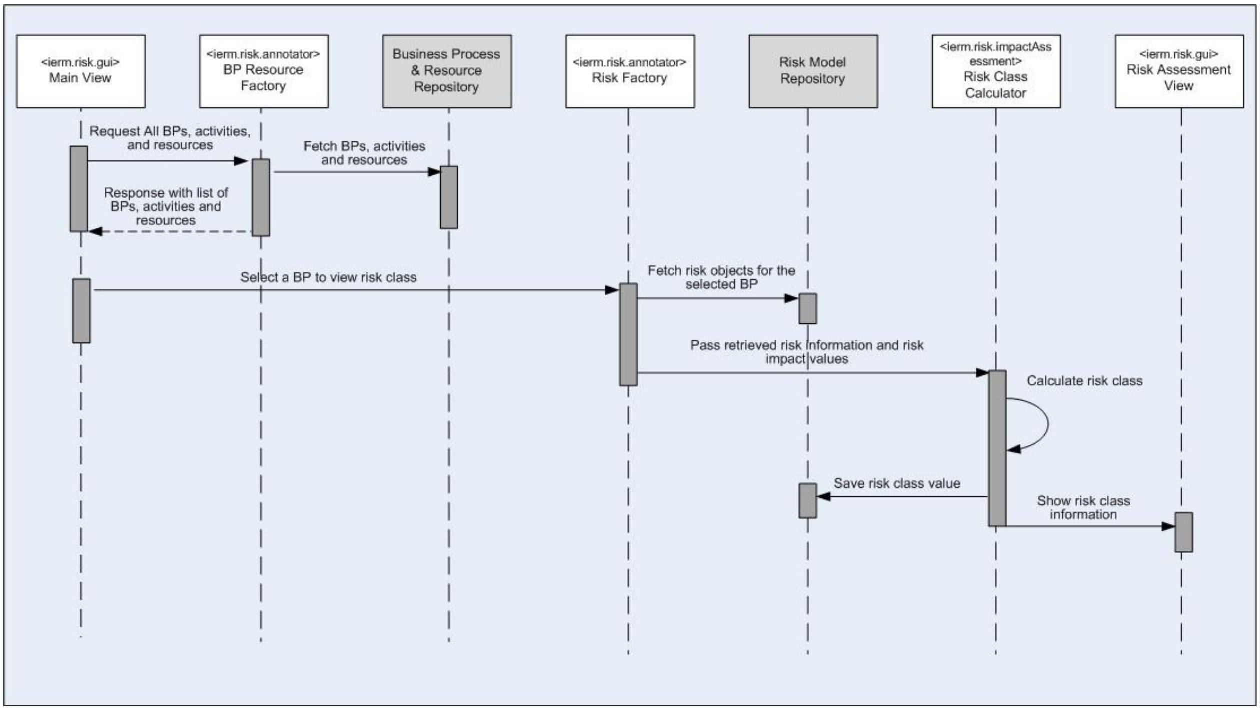

<iermrisk.gui>
Main View
<iermrisk.annotator>
BP Resource
Factory
Business Process
& Resource
Repository
<iermrisk.annotator>
Risk Factory
Risk Model
Repository
<iermrisk.impactAssessment>
Risk Class
Calculator
<iermrisk.gui>
Risk Assessment
View
Request All BPs, activities, and resources
Fetch BPs, activities and resources
Response with list of BPs, activities and resources
Select a BP to view risk class
Fetch risk objects for the selected BP
Pass retrieved risk information and risk impact values
Calculate risk class
Save risk class value
Show risk class information

Figure 14: Risk assessment interaction diagram

Table 28: Business Processes and Associated Preservation Requirements and Costs

Business Process	Technical Preservation Requirements	Legal Preservation Requirements	Costs of Preservation	Preservation Recommendation
BP1	Name and description of technical preservation requirements	Name and description of legal preservation requirements	1050.000 €	Yes
BP2	...	...	...	...

Table 30 and Table 31 describe the APIs used to support the risk assessment scenario. The objective is to determine the level of risk impact on business processes and thus identify the processes the might require preservation.

Table 29: Risk Assessment API- Calculate Risk Impact for Business Process

API	**CalculateRiskImpactForBusinessProcess**			
Summary	Determine the overall level of impact of a given risk on a given business process			
Implemented by	Risk Impact Assessment Component			
Pre-conditions	Unified Risk Model defined			
Post-conditions				
Inputs	**Information entity**	**Semantic**	**Entity elements and/ or formats**	**Comments**
	Risk Type	Type of risk event which can affect a process	Integer (risk type identifier)	Type of risk defined in the risk taxonomy in the Risk Model
	Business Process		Integer (process identifier)	Business processes defined and modelled in the Context Model
	RiskLikelihood	The likely occurrence frequency of the risk of the given activity	a. quantitative (double, representing%) or b. qualitative (text, e.g., low medium, high, as defined in the Risk Model)	The measurement unit and scale for all risk impact types have been defined in the Risk Mode
	CostImpact	Cost incurred by not addressing the risk (quantitative)	Value: double	
	StrategicImpact	Impact on strategic level (qualitative)	Level: text, (e.g., low medium high), and Description: text	
	CustomerImpact	Impact on customer satisfaction (qualitative)	Level: text, (e.g., low medium high), and Description: text	
	ImpactDuration	Duration of unavailability of resource	Value: integer e.g., Minutes, Hours, Days, Weeks, Months	
	LegalImpactValue	Impact on regulatory compliance (qualitative)	Level: text, (e.g., low medium high), and Description: text	
Outputs	Overall Risk Class	Used to finally rank several business processes by risk impact level	Level: text, (e.g. low, medium, high)	

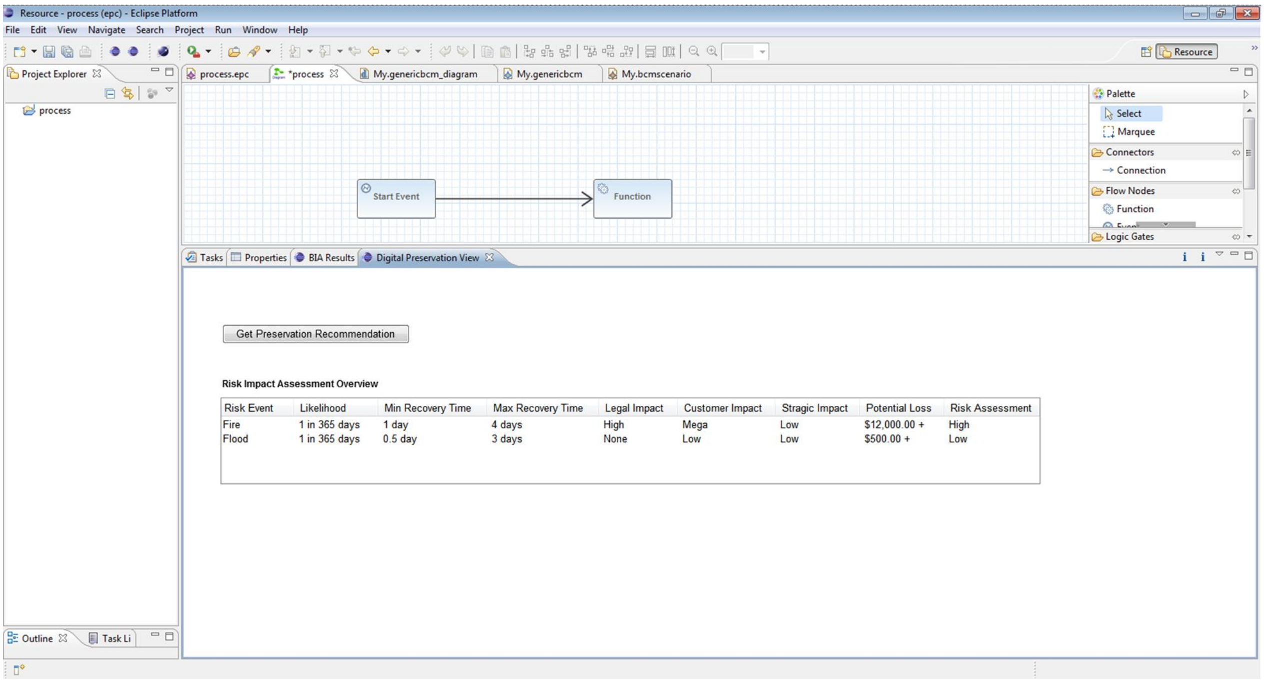
Table 30: Risk Assessment API- Rank Business Processes by Risk Impact

API	RankBusinessProcessesByRiskImpact			
Summary	Order business processes by overall risk class for a given risk type			
Implemented by	Risk Impact Assessment component			
Pre-conditions	Unified Risk Model defined Risk impact assessed for each business process for the given risk event type			
Postconditions	Ranked processes are stored as risk assessment report in the Risk Assessmen Repository and displayed on GUI			
Inputs	Information entity	Semantic	Entity elements and / or formats	Comments
	RiskType	Type of risk event which can affect a process	integer (risk type identifier)	type of risk defined in the risk taxonomy in the Risk Model
	BusinessProcessesList		list of integers (process identifiers)	business processes defined and modelled in the Context Model
Outputs	OrderedBusinessProcessesList	Ordered by overall risk impact class	list of integers (process identifiers)	

Table 31: Risk Assessment API- Rank Risks for Business Process

API	RankRisksForBusinessProcess			
Summary	Order the risk event types relevant for the given process by the overall risk class			
Implemented by	Risk Impact Assessment component			
Pre-conditions	Unified Risk Model defined Risk impact assessed for each risk event type for the given process			
Postconditions	Ranked risk event types are stored as risk assessment report in the Risk Assessmen Repository and displayed on GUI			
Inputs	Information entity	Semantic	Entity elements and / or formats	Comments
	BusinessProcess		integer (process identifier)	business process defined and modelled in the Context Model
	RiskTypesList		list of integers (risk types identifiers)	types of risk defined in the risk taxonomy in the Risk Model
Outputs	OrderedRiskTypesList		Ordered list of risk even types and associated risk impact assessments, by overall risk class	

The screenshot in Figure 15 below shows a mock-up of the Risk Assessment view, whereby risk events have been ranked by overall impact on a given business process and the user can request a recommendation whether the preservation is cost-worthy.



Risk Impact Assessment Overview

Risk Event	Likelihood	Min Recovery Time	Max Recovery Time	Legal Impact	Customer Impact	Stragic Impact	Potential Loss	Risk Assessment
Fire	1 in 365 days	1 day	4 days	High	Mega	Low	$12,000.00 +	High
Flood	1 in 365 days	0.5 day	3 days	None	Low	Low	$500.00 +	Low

Figure 15: Mock-up of Risk assessment view

9.2.4 Preservation recommendation

Recommending a preservation strategy for a particular busniess process and/or resource is necessary in order to support the Risk Treatment use case. The iERM tool interacts with the Preservation Expert Suite to get information about technical preservation requirements and cost of preservation, for a particular business process and preservation strategy. This information is displayed in the Preservation Recommendation View, to allow the user to decide what processes and/or activities to preserve by providing together information about risk impact and preservation costs and supporting the trade-off between the costs of not preserving (i.e. risk cost) and the cost of preserving a given business process and/or associated resources. Figure 16 shows the interaction diagram for this purpose.

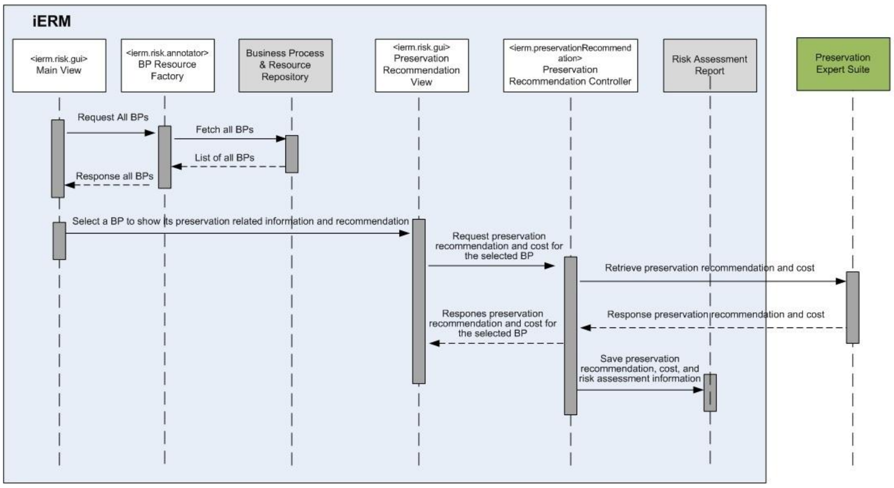

iERM
<ierm.risk.gui> Main View
<ierm.risk.annotator> BP Resource Factory
Business Process & Resource Repository
<ierm.risk.gui> Preservation Recommendation View
<ierm.preservationRecommendation> Preservation Recommendation Controller
Risk Assessment Report
Preservation Expert Suite
Request All BPs
Fetch all BPs
List of all BPs
Response all BPs
Select a BP to show its preservation related information and recommendation
Request preservation recommendation and cost for the selected BP
Retrieve preservation recommendation and cost
Response preservation recommendation and cost
Respones preservation recommendation and cost for the selected BP
Save preservation recommendation, cost, and risk assessment information

Figure 16: Interaction diagram for preservation recommendation

Tables 32, 33, 34 and 35 below describe the APIs required by iERM from the Preservation Expert Suite in order to obtain information about the technical requirements for and cost of preserving a business process and its resources, respectively.

Table 32: API – Check Technical Preservation Requirements for Activity

API	CheckTechnicalPreservationRequirementsForActivity			
Summary	Get back from the DP Engine the list of technical preservation requirements for given activity			
Implemented by	DP Engine			
Pre-conditions	PreservationRequirement entity defined in the DP system			
Postconditions				
Inputs	Information entity	Semantic	Entity elements and / or formats	Comments
	BusinessProcess		integer (process identifier)	business process defined and modelled in the Context Model
	Activity		integer (activity identifier) (?)	
Outputs	List of PreservationRequirements entities		A PreservationRequirements entity could contain: EntityToPreserve: integer (identifier of process), EntityType: text ('process'), RequirementDescritpion: text, RequirementType: text ('technical')	These are technical preservation requirements which need to be checked and complied with before deciding to preserve (i.e. not legal)

Table 33: API – Check Technical Preservation Requirements for Business Process

API	CheckTechnicalPreservationRequirementsForBusinessProcess			
Summary	Get back from the DP Engine the list of technical preservation requirements for given process			
Implemented by	DP Engine			
Pre-conditions	PreservationRequirement entity defined in the DP system			
Postconditions				
Inputs	Information entity	Semantic	Entity elements and / or formats	Comments
	BusinessProcess		integer (process identifier)	business process defined and modelled in the Context Model
Outputs	List of PreservationRequirements entities		A PreservationRequirements entity could contain: EntityToPreserve: integer (identifier of process), EntityType: text ('process'), RequirementDescritpion: text, RequirementType: text ('technical')	These are technical preservation requirements which need to be checked and complied with before deciding to preserve (i.e. not legal)

Table 34: API - Check Preservation Cost for Activity

API	CalculatePreservationCostForBusinessActivity			
Summary	Get back from LLM the cost of preserving the given activity			
Implemented by	LLM			
Pre-conditions	Preservation cost model defined in the DP system			
Postconditions				
Inputs	Information entity	Semantic	Entity elements and / or formats	Comments
	Activity		integer (activity identifier)	
Outputs	Cost		double	Cost unit (currency) defined in the DP system

Table 35: API - Calculate Preservation Cost for Business Process

API	CalculatePreservationCostForBusinessProcess			
Summary	Get back from LLM the cost of preserving the given process			
Implemented by	LLM			
Pre-conditions	Preservation cost model defined in the DP system			
Postconditions				
Inputs	Information entity	Semantic	Entity elements and / or formats	Comments
	BusinessProcess		integer (process identifier)	business process defined and modelled in the Context Model
Outputs	Cost		double	Cost unit (currency) defined in the DP system

The cost of preserving a business process and its associated resources can be determined by examining the cost incurred during the different presevation lifecycle acitvities: Acquisition, Disposal, Ingest, Archive Storage, Preservation Planning, First Mover Innovation, Data Management, Access, Administration and Common Services. As it is currently being documented in Deliverable 4.8 - “Refined DP & Intelligent Enterprise Risk Management”, a preliminary version of the cost model for business process preservation in TIMBUS is a revision and adaptation of the “Keeping Research Data Safe” (KRDS) cost model (Stanger, 2011) driven by an analysis of the suitability of including the different preservation activities in the costing. Table 36 below shows the rationale for including these activities in the preservation costing model for business processes in TIMBUS.

Table 36: Suitability of preservation activities for preservation costing in TIMBUS

Main phases and activities of KRDS Activity Model		*Suitability*	*Rationale*
Pre-Archive Phase	*Outreach*	*No*	*In TIMBUS, preservation is seen as a risk mitigation action therefore there is no need to account costs for Producers.*
	Initiation	*No*	*Same as above.*
	Creation	*No*	*Same as above.*
Archive Phase	*Acquisition*	*Yes*	*The activity involves selection of the information, negotiating submission agreement and depositor support.*
	Disposal	*Yes with revision*	*In TIMBUS the business processes need to be preserved in a way that allows re-running in a later time (using business process virtualization). Therefore the sub-activities of this activity are different.*
	Ingest	*Yes*	*The activity involves receiving the information, assuring quality, generating a package for archiving, generating metadata, etc.*
	Archive Storage	*Yes with revision*	*Same as Disposal activity.*
	Preservation Planning	*Yes*	*The activity involves monitor technology, develop preservation strategies, develop and monitor SLAs, etc.*
	First Mover Innovation	*Yes*	*The activity involves pre-anticipating a change in the context and developing a new strategy to preservation.*
	Data Management	*Yes with revision*	*Same as Disposal activity.*
	Access	*Yes with revision*	*Same as Disposal activity.*
Support Services	*Administration*	*Yes*	*The activity involves general management, customer accounts, administrative support, etc.*
	Common Services	*Yes*	*The activity involves network services, software and hardware licenses maintenance, utilities, etc.*
Estates		*No*	*This activity involves costs of space management and maintenance that are out of the scope of TIMBUS.*

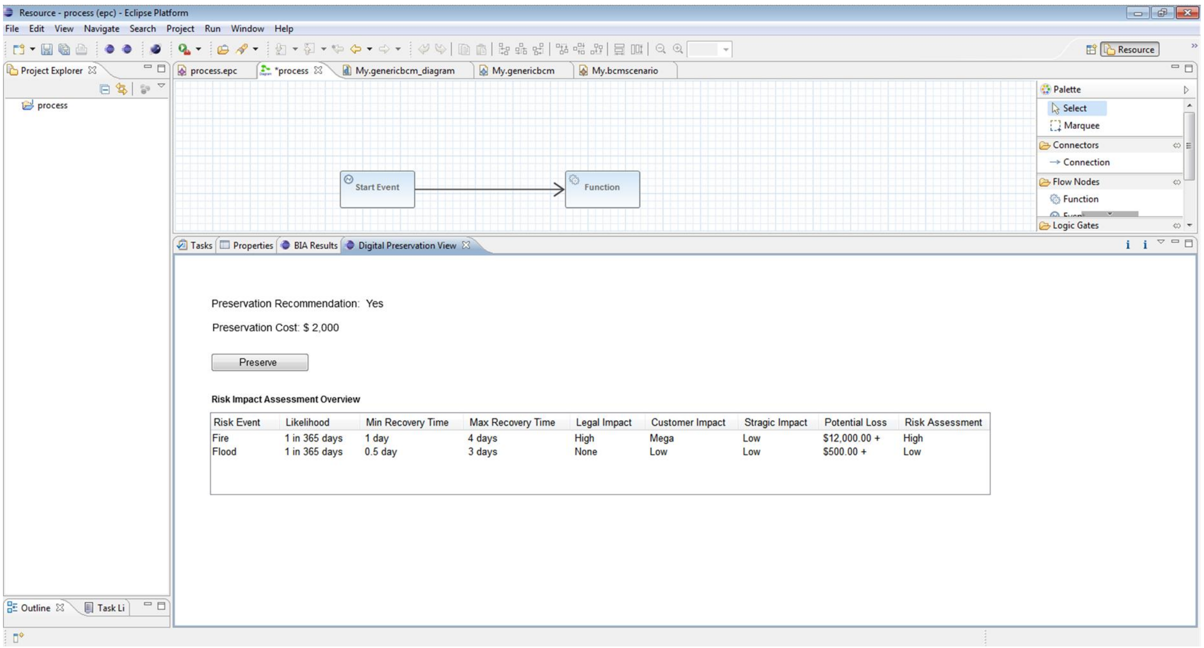
Assuming all technical preservation requirements are met for a given risk type and preservation strategy, the system will give preservation recommendations by categorising processes into:

a. 'Yes' - processes with high risk impact and low preservation cost, hence recommended to be preserved
b. 'No' - processes with low risk impact and high preservation cost, hence not to be preserved
c. 'Trade-off' - all the rest of the processes, where the user has to decide

Table 37: API- Categorise Processes By Preservation Recommendation

API	CategoriseProcessByPreservationRecommendation			
Summary	Assign a 'yes','no' or 'trade-off' value to a given process, meaning respectively: 'it should be preserved', 'it should not be preserved', and 'to be decided by the user'			
Implemented by	Risk Assessment Tool			
Pre-conditions	All risk and cost information has been derived for the given process			
Postconditions	Preservation recommendation stored in the Risk Assessment Report			
Inputs	Information entity	Semantic	Entity elements and / or formats	Comments
	BusinessProcess		integer (process identifier)	business process defined and modelled in the Context Model
Outputs	PreservationRecommendation flag associated to the process is: 'yes', 'no' or 'trade-off'			

Figure 17 below shows a mock-up of the Preservation Recommendation View, where the preservation recommendation is given together with the cost of preservation.



Preservation Recommendation: Yes

Preservation Cost: $ 2,000

Risk Impact Assessment Overview

Risk Event	Likelihood	Min Recovery Time	Max Recovery Time	Legal Impact	Customer Impact	Stragic Impact	Potential Loss	Risk Assessment
Fire	1 in 365 days	1 day	4 days	High	Mega	Low	$12,000.00 +	High
Flood	1 in 365 days	0.5 day	3 days	None	Low	Low	$500.00 +	Low

Figure 17: Mock-up for preservation recommendation view

9.2.5 Risk Monitoring

For being able to assess the status of a risk event the following API (Table 38) returns the set of all risk indicators defined for a risk. As to be in the position of returning such a list, prior to the call of the API the risk indicators along with supporting metrics and schedules must have been defined in the system and associated with the risk by means of the respective user interfaces in the system.

Table 38: Risk Monitoring API – Get all Risk Indicators for a Risk Event

API	**GetAllRiskIndicatorsForRiskEvent**			
Summary	This function returns a list of risk indicator for a specific risk event.			
Implemented by	Risk Monitor			
Pre-conditions	Risk indicators along with metrics have been defined and associated with the corresponding risk events			
Post-conditions	n/a			
Inputs	**Information entity**	**Semantic**	**Entity elements and/ or formats**	**Comments**
	RiskEvent	Type of risk event which can affect a process	Integer (risk event type identifier)	
Outputs	RiskIndicatorsList		List of integers (risk indicator identifiers)	

The overall assessment of the risk status is done by evaluating the values of the risk indicators associated with the risk event (Table 39). As per business process, risk event and risk indicator the risk indicator value is returned either in terms of “alert levels” (e.g., red, amber, green with red indicating high risk and green indicating low risk) or a probability (0..100% with 0 being a low probability and 100% being the highest probability).

Table 39: Risk Monitoring API – Get Risk Indicator Status for a Risk Event and a Business Process

API	**GetRiskIndicatorStatusForRiskEventAndBusinessProcess**			
Summary	This function yields the status of a risk indicator for a certain risk event in a business process.			
Implemented by	Risk Monitor			
Pre-conditions	Risk indicators have been evaluated and risk indicator values are available in the system.			
Post-conditions	The most recent status of the risk indicator is reported.			
Inputs	**Information entity**	**Semantic**	**Entity elements and/ or formats**	**Comments**
	BusinessProcess		Integer (process identifier)	Business processes defined and modelled in the Context Model
	RiskEvent	Type of risk event which can affect a process	Integer (risk event type identifier)	
	RiskIndicator	Risk indicator that is related to the risk event type	Integer (risk indicator identifier)	
Outputs	RiskIndicatorValue	The result from the last risk indicator evaluation indicating the need for attention to the aspect implemented by the indicator	Alert level (green, amber, red) or Probability (0% to 100%)	Indicators reflect status of an indicator (e.g., certain metrics with respect to threshold specified for the metrics values)

For example, for a “Service unavailability” risk event attached to the “Storage Cloud Service” resource, several risk indicators can be defined, to check e.g. software, hardware, network, power supply availability, etc. The mock-up in Figure 18 shows how these indicators can be associated to the risk event. This mock-up also shows a graph of dependencies between different risk indicators (displayed as discs) and different risk events (displayed as filled squares).

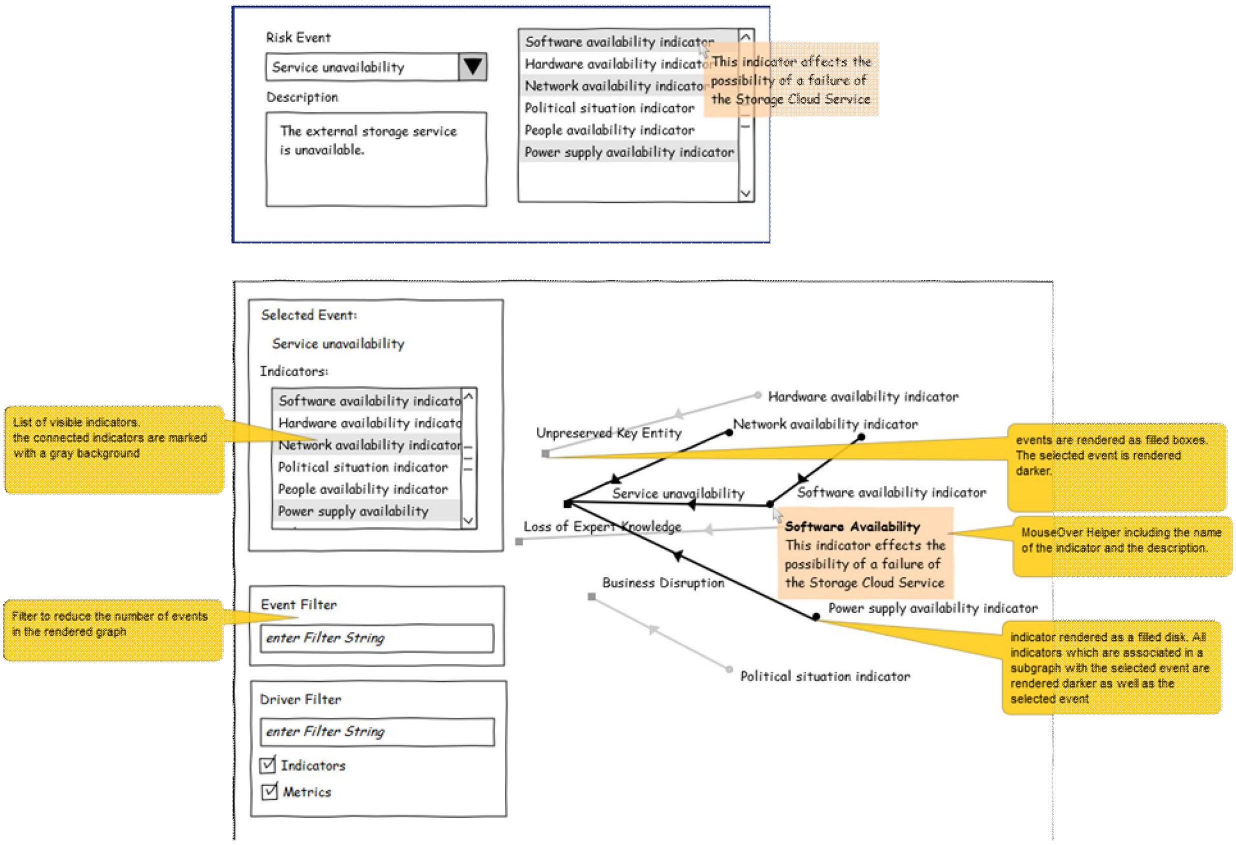
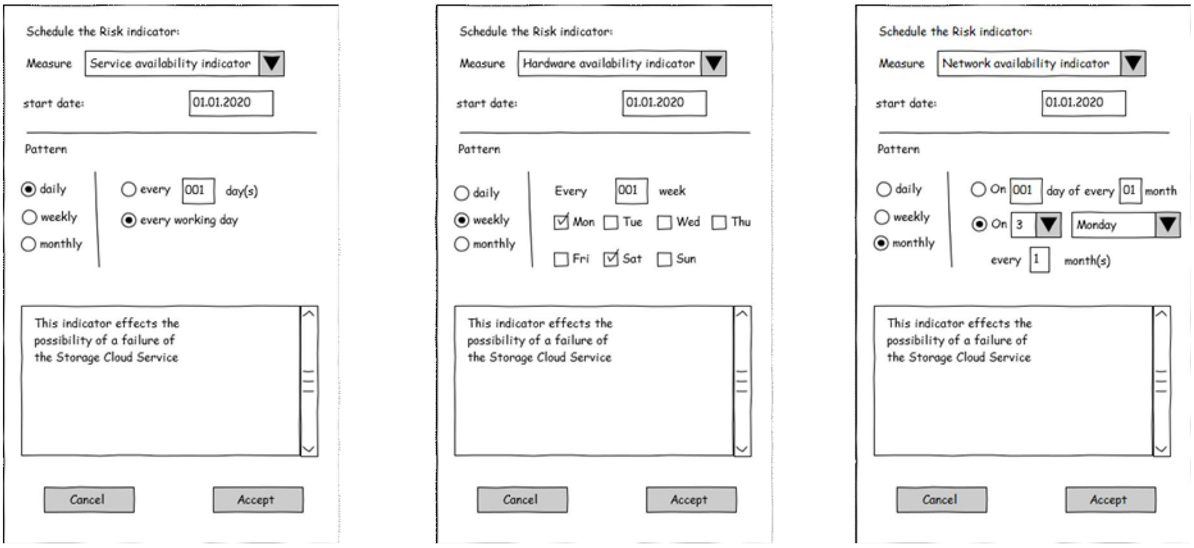

Risk Event
Service unavailability
Description
The external storage service is unavailable.
Software availability indicator
Hardware availability indicator
Network availability indicator
Political situation indicator
People availability indicator
Power supply availability indicator
This indicator affects the possibility of a failure of the Storage Cloud Service
Selected Event:
Service unavailability
Indicators:
Software availability indicator
Hardware availability indicator
Network availability indicator
Political situation indicator
People availability indicator
Power supply availability
List of visible indicators. the connected indicators are marked with a gray background
Event Filter
enter Filter String
Filter to reduce the number of events in the rendered graph
Driver Filter
enter Filter String
☑ Indicators
☑ Metrics
Hardware availability indicator
Unpreserved Key Entity
Network availability indicator
Service unavailability
Software availability indicator
Loss of Expert Knowledge
Software Availability
This indicator effects the possibility of a failure of the Storage Cloud Service
Business Disruption
Power supply availability indicator
Political situation indicator
events are rendered as filled boxes. The selected event is rendered darker.
MouseOver Helper including the name of the indicator and the description.
indicator rendered as a filled disk. All indicators which are associated in a subgraph with the selected event are rendered darker as well as the selected event

Figure 18: Mock-up for definition risk indicators for risk events

The mock-up in Figure 19 shows a graphical view where the user can define the schedule when a risk indicator for a particular risk event should be evaluated or checked (‘manual monitoring’). In this case, three indicators are scheduled, to check the availability of a Service (software component), Hardware and Network respectively.



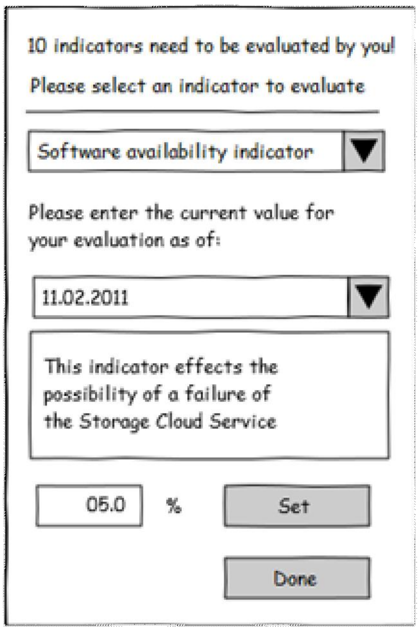
Schedule the Risk indicator:
Measure: Service availability indicator
start date: 01.01.2020
Pattern
● daily ○ weekly ○ monthly
○ every 001 day(s)
● every working day
This indicator effects the possibility of a failure of the Storage Cloud Service

Schedule the Risk indicator:
Measure: Hardware availability indicator
start date: 01.01.2020
Pattern
○ daily ● weekly ○ monthly
Every 001 week
☑ Mon □ Tue □ Wed □ Thu
□ Fri ☑ Sat □ Sun
This indicator effects the possibility of a failure of the Storage Cloud Service

Schedule the Risk indicator:
Measure: Network availability indicator
start date: 01.01.2020
Pattern
○ daily ○ weekly ● monthly
○ On 001 day of every 01 month
● On 3 Monday
every 1 month(s)
This indicator effects the possibility of a failure of the Storage Cloud Service

Figure 19: Mock-up for risk indicator scheduling

The mock-up in Figure 20 shows how a user can enter the result of evaluating a risk indicator, in this case (s)he estimates that there is a 5% chance of the Storage Cloud Service to fail due to software unavailability.



10 indicators need to be evaluated by you!
Please select an indicator to evaluate
Software availability indicator
Please enter the current value for your evaluation as of:
11.02.2011
This indicator effects the possibility of a failure of the Storage Cloud Service
05.0 %

Figure 20: Mock-up for risk indicator evaluation

10 Conclusions and Outlook

This deliverable presented a refined version of the iERM architecture, representing the output of Task 5.1 (Intelligent Enterprise Risk Management Architecture). The purpose of this deliverable was to give a more detailed description of the different logical and implementation-level components of the iERM architecture. This document augments the previous architecture document (Deliverable D5.1) with an updated data model for risk-aware digital preservation, an updated overall architecture, and the tool development specification (section 9) on the development view of the architecture, having the role of an implementation guide. This section contains:

- class diagrams showing how the logical components of the architecture can be implemented into software packages and classes,
- interaction diagrams for the main iERM functions (risk modelling and annotation, risk assessment, risk preservation, and risk monitoring) which show the sequence of control between the different classes triggered by specific user requests,
- specifications for the main APIs necessary to be implemented by iERM, and
- mock-ups which show how the different user interface views can be designed to support the main risk management features.

Implementation of the iERM (which will be part of Task 6.1) should use this deliverable as a recommendation and not strictly as a technical specification, but should focus on the main features needed to deliver the core innovations in TIMBUS, i.e. risk assessment driven preservation of business processes and resources. However, one ‘nice-to-have’, advanced feature which would enhance the core innovations in iERM would be support for visual trade-off analysis. With this, the user could visually specify a financial limit (budget) and obtain from the iERM a recommendation of the possible business processes that can be preserved given a preservation solution. For this feature to be advanced, iERM would need to rely on an advanced cost model with a high granularity to be able to compute the cost of preserving partial business processes and partial resource stacks, in different preservation stages. Variations in this budget (e.g. using a slider) can generate a re-computation of the preservation recommendations. The Task 6.1 could consider such an implementation once the core features have been delivered.

References

1. Belecheanu, R. (2012) Deliverable 5.1 – iERM Architecture, TIMBUS deliverable
2. Burda, D. (2012) Deliverable 4.1 – DP and Intelligent Enterprise Risk Management, TIMBUS deliverable, pp. 61-74.
3. Galushka, M. (2012) Deliverable 5.5 – Service Architecture for Preservation – Refined Version, TIMBUS deliverable.
4. Winkler, U. (2012) Deliverable 7.1 – Process and methods for digitally preservable services, TIMBUS deliverable.
5. Malan, R. and Bredemeyer, D. (1999) Functional Requirements and Use Cases, Bredemeyer Consulting Report, June, http://www.bredemeyer.com/pdf_files/functreq.pdf
6. Neumann, A. (2012) Deliverable 4.5 - Business Process Contexts, TIMBUS deliverable
7. Stanger, N. (2011). Keeping Research Data Safe (KRDS)). Computer and Information Science Seminar Series.
8. Burbeck, S. (1987). Applications Programming in Smalltalk-80(TM): How to use Model-View-Controller (MVC),

   http://st-www.cs.illinois.edu/users/smarch/st-docs/mvc.html
9. ISO 31000:2009 Risk Management – Principles and guidelines,

   http://www.iso.org/iso/catalogue_detail.htm?csnumber=43170