D5.1: Architecture for Intelligent ERM

WP5 – Software Architecture for Digital Preservation

Delivery Date: 30/03/2012

Dissemination Level: RE

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**
Ricardo Vieira	INESC-ID	rjcv@ist.utl.pt

Internal Reviewer		
Name	**Organisation**	**e-mail**
Michael Nolan	INTEL	michael.nolan@intel.com

Disclaimer

Table of Contents

List of Figures

List of Tables

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
PRR	Preservation Recommendation Report
RACI	Responsible, Accountable, Consulted and Informed
RM	Risk Model
S&C	Strategy and Cost
SCM	Strategy and Cost Model
URM	Unified Risk Model

1 Executive Summary

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, it still centres on information and lacks the perspective on business processes. The main innovation of TIMBUS project is therefore its focus on the risk assessment based digital preservation of business processes, thus not only bringing together but also advancing 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.

This deliverable aims to outline the high level architecture of the iERM system, and is the output of the Task 5.1 ("Intelligent Enterprise Risk Management Architecture"). According to the Description of Work, the objective of this task is to establish reference architecture for the development of an intelligent ERM system that interfaces with other organisational systems typically used as inputs into risk analysis. This task is part of workpackage 5, which aims to develop a set of architectures to support the major technical components and prototypes in TIMBUS. As part of this workpackage, the iERM architecture was developed in close relation and is therefore compliant with the Service Architecture for Preservation developed in Task 5.2 and reported in (Galushka, 2012). In this respect, 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 iERM a state and model of the organisational business processes running in 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 in designing iERM architecture 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 *for* risk management.

In designing the architecture of the iERM system we take an iterative approach: to date the first iteration of the iERM architecture was developed and is reported in the current deliverable, as part of project milestone 6 (TIMBUS Architecture Iteration 1). The second iteration of the iERM architecture will be developed as part of milestone 7 (TIMBUS Architecture Iteration 2) and will be reported in deliverable 5.4 ("Refined Architecture for iERM").

2 Introduction

The objective of this deliverable is to establish reference 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 first iteration of the iERM architecture. In TIMBUs we follow the traditional systems engineering approach: identifying functional requirements, design of architecture, specification, implementation, testing, integration, deployment, and evaluation. The present deliverable therefore contains 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, from which we then select a set of functional use cases designed to support the validation of the final system against core functionality (section 5). Section 6 describes an initial data model for risk-aware preservation, while section 7 describes a first, high-level version of the iERM system architecture.

3 Risk Management in TIMBUS

3.1 Risk management stakeholders

Risk Assessment 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 (Burda, 2012).

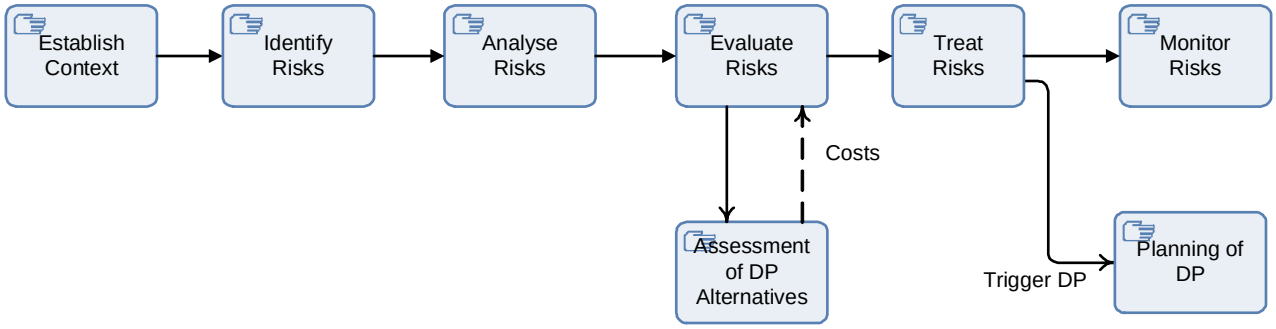

Figure 1: Risk management process in TIMBUS

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:

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 Management; Risk Management; Business Unit Manager; and 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
	Establish risk criteria and risk classification
	Output of "Establish Context"
	Comprehensive list of Risks
	Risk Management; Auditor; and Business Unit Manager;
Input(s)	Checklist
Output(s)	Brainstorming
Main Stakeholders	Interviews
Examples Techniques	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 Controls		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 controls" 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 controls" 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 controls" 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

Functional requirements are a way of capturing the intended behaviour of the system (Malan and Bredemeyer, 1999). 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:
1. to allow the user to define the context for risk management activities (i.e. organisational, financial, process and people related context),
2. to select the specific risk types targeted by the risk management process, and
3. 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 Owner) 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	This includes the propagation of the impact

	business objective at organisation unit level or company level	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 an-other 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 re-quirements
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, preserve
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 realtime.

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 KRIs to monitor multiple types of data sources	Examples: enterprise application, traffic, weather, etc.
R4.3	Define business rules to correlate and monitor	

	multiple KRIs	
R4.4	Monitor KRIs associated with multiple risks	
R4.5	Monitor external and internal context	Defined in (Neumann, 2012)
R4.6	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 realtime 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 Response 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 Use cases

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 are thus different from the 'use cases' defined in the TIMBUS workpackages 7, 8 and 9, which address TIMBUS – level (and not only iERM level) functional validation of the overall TIMBUS objectives, by instantiating the system to industry and application specific domains.

The following use cases show the interaction of the different types of users (here called 'actors') with the system. As the main goals of the iERM system are to support the different steps of the risk management process (presented in section 3), the use cases are documented below according to 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 15: "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 16: "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 17: "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 cases 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 18: "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 19: "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 20: "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.

6 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, three types of information:

1. information entities related to risk management (section 6.1),
2. information entities related to digital preservation (section 6.2), and
3. information entities related to business process modelling (section 6.3),

thus supporting the innovative aspect of this project.

The central relationships between the three 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 7.4). The data model only outlines the main entities and relations between them, with details on the meaning and usage of each entity; however at this stage we do not specify a mapping between these entities and relations and the different data stores, that is, how this model is implemented at database level, as this will be part of a subsequent iteration of this deliverable.

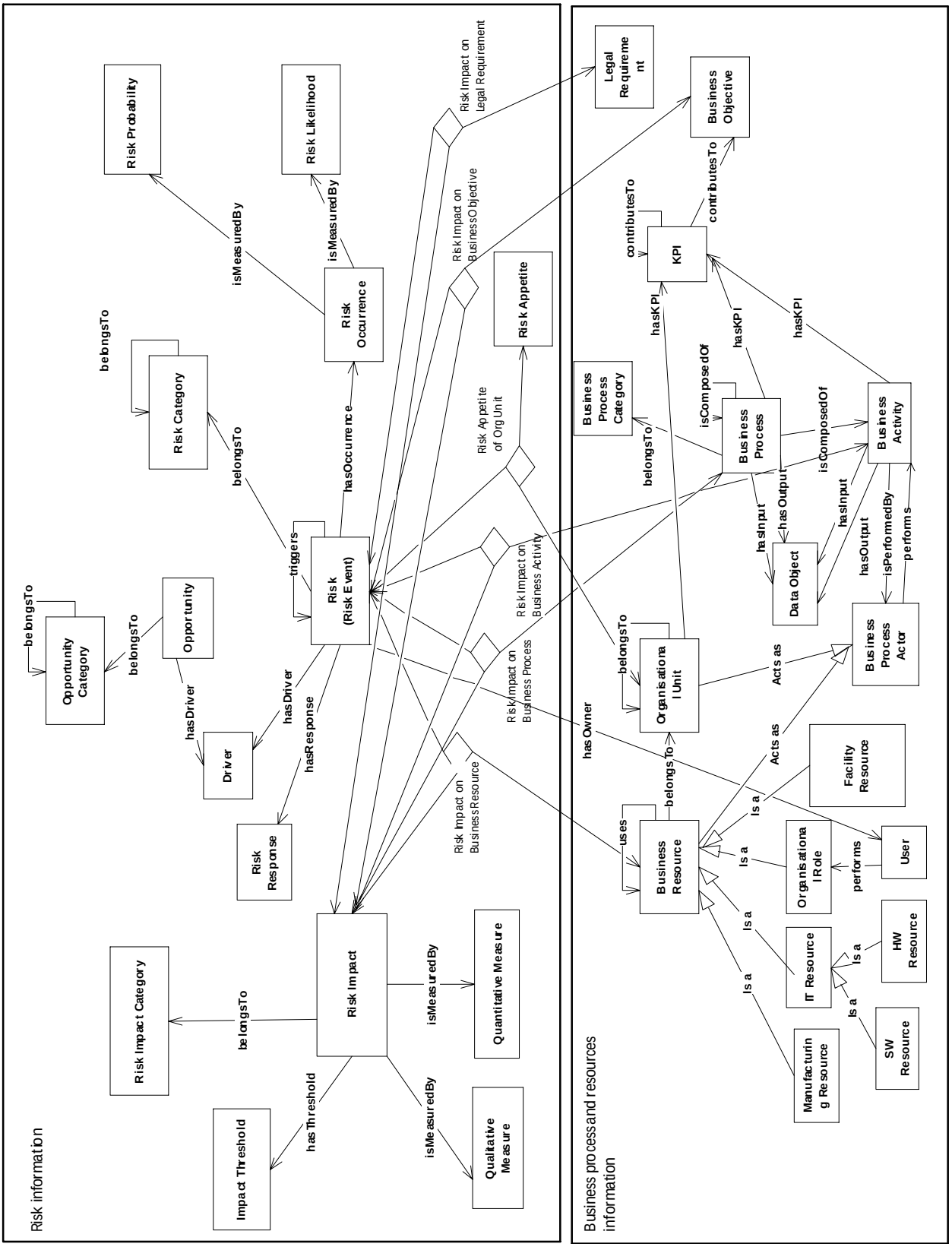

Figure 2: iERM data model

6.1 Information model for risk management

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 measure 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*.

6.2 Information 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.*

6.3 Information 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 Processes* 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*.

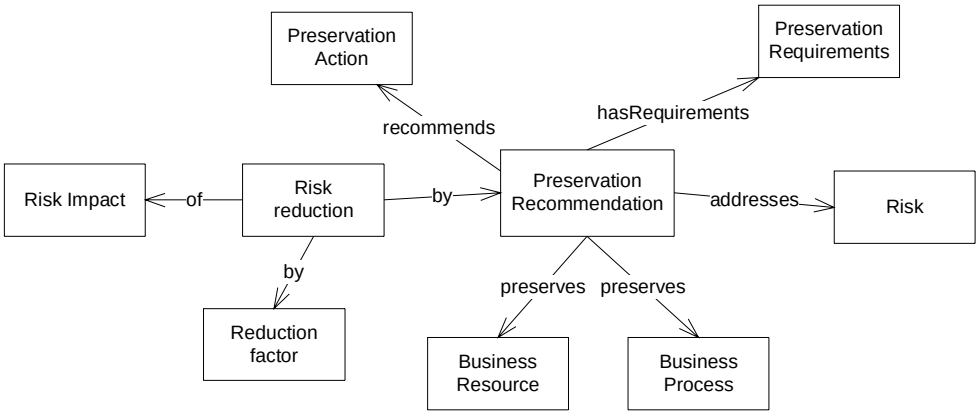

Figure 3: Data model for preservation information

7 iERM Architecture

This section will present a high level architecture of the iERM tool. The objective is to establish a reference architecture 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.

7.1 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 5.2 (Galushka et al., 2012, pp. 26 – 29), section 4.4, and shown in 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 Metamodel component in the DP Acquisition Module. 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 Digital Preservation Engine.

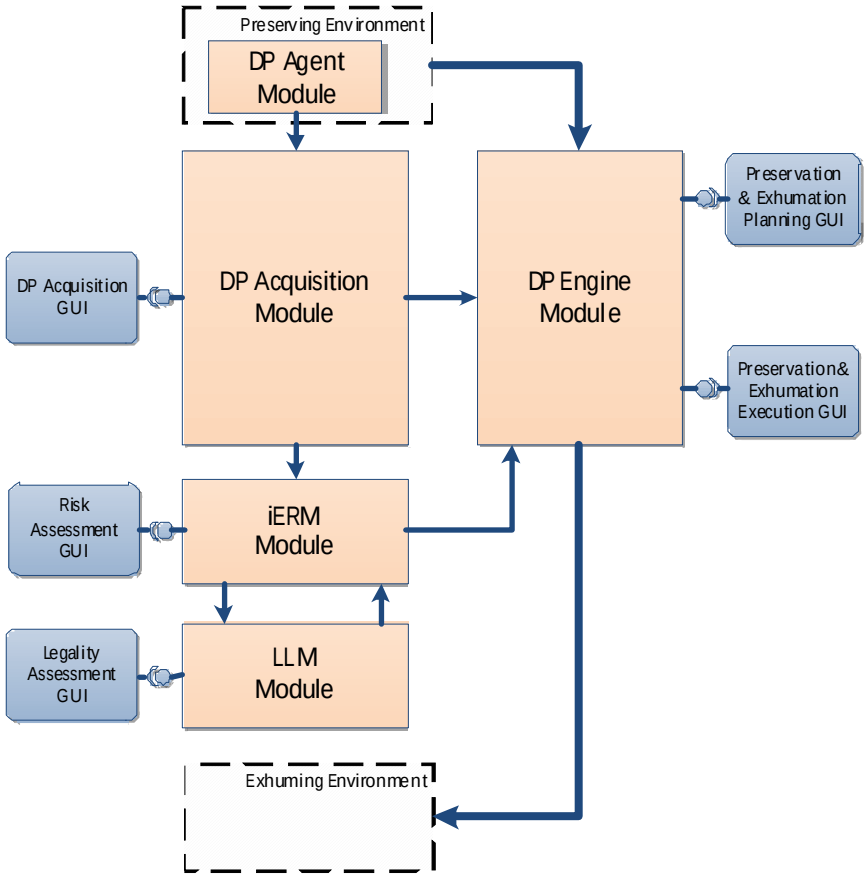

Figure 4: iERM module in the scope of the overall TIMBUS architecture

7.2 Model-View-Controller design of iERM architecture

Conceptually the iERM architecture can be described using a Model-View-Controller (MVC) pattern (figure Figure 5 below):

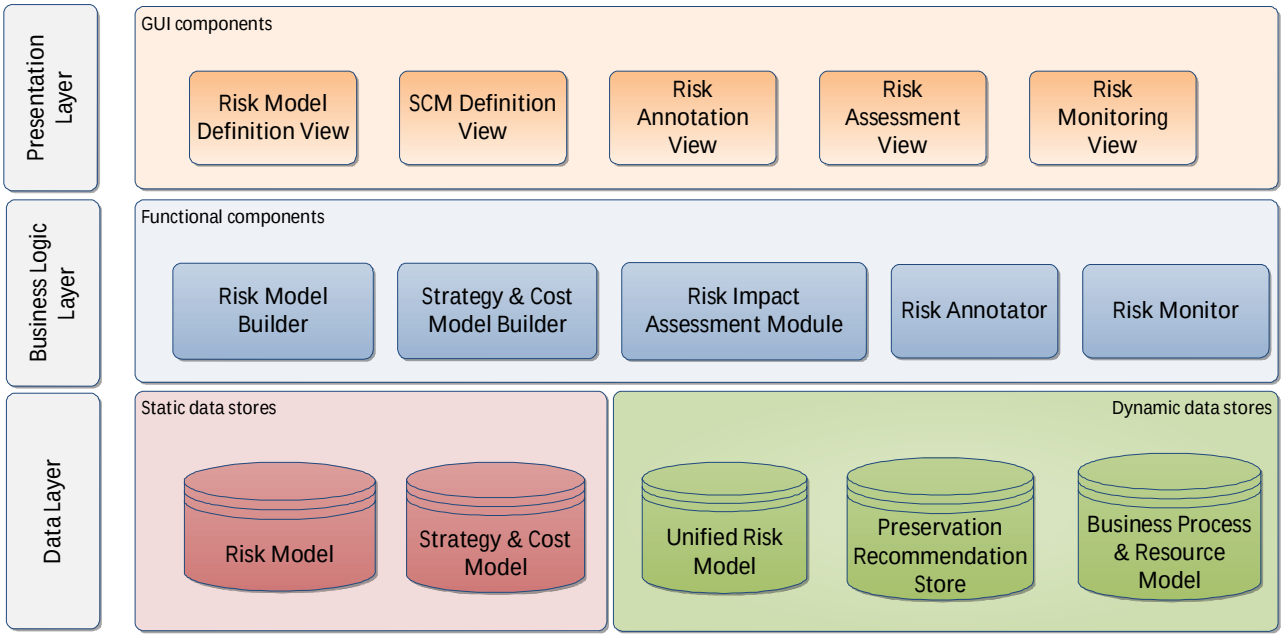

Figure 5: MVC view of the iERM architecture

The "Model", represented by the Data Layer, consists of the main data stores in iERM, which can be divided into:

1. Static data stores (Risk Model and Strategy and Cost Model), which are mainly created by the user using the respective access components
2. Dynamic data stores (Unified Risk Model, Preservation Recommendation Store and BPRM Store)

The "Controller" represented by the Business Logic Layer, consists of the main functional components in iERM, which can be divided into:

1. Data access components: Risk Model Builder and Strategy and Cost Model Builder, which allows read / write operations on the respective model entities
2. Application type of components: Risk Impact Assessment Module, Risk Annotator and Risk Monitor, which implement the main functionality of the iERM tool.

The "View", represented by the Presentation Layer, consists of GUI components allowing the user to create, update and view results of the iERM workflow.

7.3 iERM workflow view

Figure 6 below shows represents another view of the iERM architecture showing the general workflow:

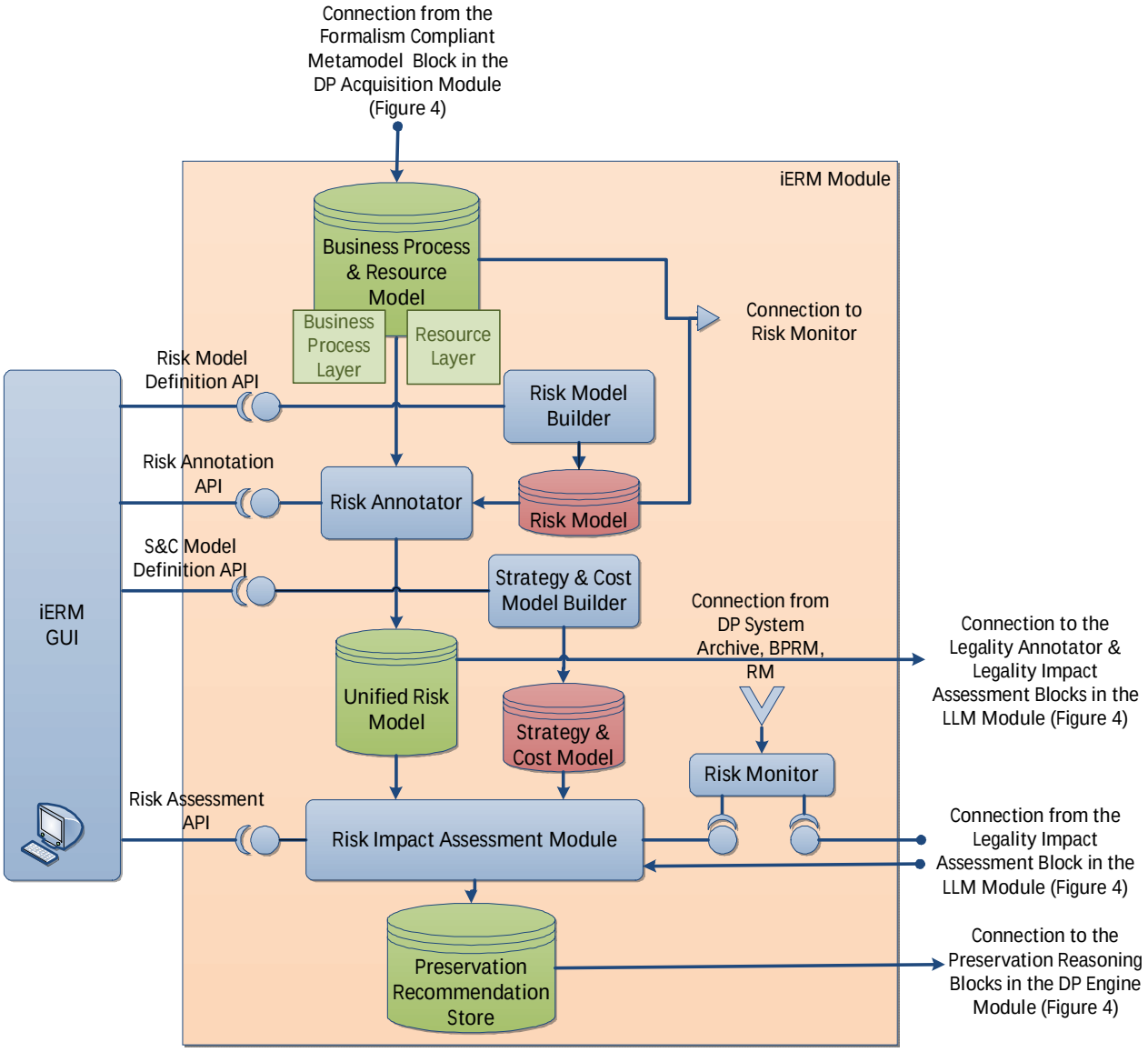

Figure 6: Data flow and APIs in iERM

In the following sub-sections we describe in more detail the data stores (section 7.4), the business logic components (section 7.5), and the user interface components (section 7.6) of the iERM tool.

7.4 Data Layer

7.4.1 Static data stores

Risk Model Store

This store contains information about risk types and their classification, risk appetite for organisational units, risk impact levels.

Strategy and Cost Models Store

This store contains a model of the digital preservation strategies and associated costs, preservation requirements.

7.4.2 Dynamic data stores

Business Process and Resources Models Store

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

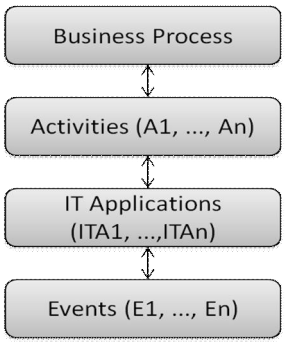

Figure 7: Mapping between business processes and events

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 7 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.

Unified Risk Model Store

The Unified Resource Model 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.

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, in the form of Preservation Recommendation Reports (PRR).

A PRR 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.

A PRR 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.

7.5 Business Logic Layer

This layer consists of the main functional components of iERM, which are:

Risk Model Builder

This is a data management component which provides APIs for managing Risk Model information. These APIs will allow creating, retrieving, updating, 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.

Strategy and Cost Model Builder

This is a data management component which provides APIs for creating and managing the Strategy and Cost Model (SCM). This model contains information about the costs and requirements of different Digital Preservation strategies, and generally draws upon Value Engineering knowledge on the economic and financial data that affects Digital Preservation. These APIs will allow creating, retrieving, updating and deleting (CRUD) entities and relations defined in the S&C model. The S&C model builder APIs will be used by the SCM definition view of the iERM GUI (section 07.6) to allow the user to define or modify the S&C model in the design stage.

Risk annotator

This component provides the APIs for annotating a Business Process and Resources Model with risk information and thus for generating the Unified Risk Model.

Risk Impact Assessment Module

The Risk Impact Assessment module uses the URM in conjunction with DP Strategy & Cost Model (DP SCM) and with compliance results from the LLM tool to generate Preservation Recommendation Reports (PRR), which encapsulate the information required to support the preservation process. This module aims to give an insight into the impact a risk event has not only on business process KPIs/ corporate objectives, etc., but also on legal aspects.

Risk Monitor

This component monitors the DP System Archive of the DP Engine Module (Figure 4, also detailed in (Galushka, 2012) pp. 32-49), the Risk Model and the Business Process Resource Model to detect risk events. When a risk event is detected, this component will trigger the execution of the Legality Impact Assessment Module, in order to assess the impact of that risk event on legal issues and will trigger the execution of the Risk Impact Assessment Module, to assess the impact of that risk event on business process KPIs.

7.6 Presentation Layer

The iERM tool will implement a number of Graphical User Interface (GUI) components to enable user level access to iERM functionality and data models. Data level interfaces supported by these components will support create, retrieve, update and delete (CRUD) operations on the different entities of the risk model – for those models which are statically created by the user. The iERM GUI will contain the following views:

Risk Model Definition View

This is an editing component of the iERM GUI which allows the user to graphically manage the Risk Model entities.

Strategy and Cost Model Definition View

This is an editing component of the iERM GUI which allows the user to graphically manage the Strategy and Cost Model entities.

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.

Risk Assessment View

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

1. Define and edit risk assessment scenarios.
2. View results of the risk assessment in the form of reports or analytics dashboards.

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 visualise through dashboards and charts results of the risk monitoring over these data sources, as well as be notified of the status and efficiency of the implementation of a preservation action for a particular risk event and business process.

8 Conclusions and Outlook

This deliverable presented the progress made to date towards the design of the iERM system architecture and represents the output of Task 5.1 (Intelligent Enterprise Risk Management Architecture). The purpose of this deliverable was to give a high-level overview of the iERM architecture, the detailed and refined architecture remaining to be presented in the Deliverable 5.4 ("Refined Architecture for Intelligent ERM"). We first covered the risk management process, stakeholders and user roles, the functional requirements and use cases, a data model for risk-aware digital preservation, and finally the iERM Architecture, within which an account of the different functional, persistence and visualisation components was given.

The second version of the iERM architecture will be introduced in Deliverable 5.4 and will cover the design of the different iERM components in higher level of detail to support their implementation, including definition of non-functional requirements, definition of the APIs exposed by iERM components, interaction workflows between these components, selection of implementation technologies and a deployment view of the iERM system.

References

1. Burda, D. (2012) Deliverable 4.1 – DP and Intelligent Enterprise Risk Management, TIMBUS deliverable, pp. 61-74.
2. Galushka, M. (2012) Deliverable 5.2 – Service Architecture for Preservation, TIMBUS deliverable.
3. Malan, R. and Bredemeyer, D. (1999) Functional Requirements and Use Cases, Bredemeyer Consulting Report, June, http://www.bredemeyer.com/pdf_files/functreq.pdf
4. Neumann, A. (2012) Deliverable 4.5 - Business Process Contexts, TIMBUS deliverable