



Project Report

Demonstrators of RM/RA in Business Processes

Integration of Risk Management with Operational IT Processes

Conducted by the

**Technical Department of ENISA
Section Risk Management**

and

**BOC Information Technology GmbH
Berlin, Germany**

November 2007

Legal Notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless it is stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004. This publication does not necessarily represent state-of-the-art and it might be updated from time to time.

Third party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external web sites referenced in this publication.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic mechanical, photocopying, recording, or otherwise without the prior written permission of ENISA, or as expressly permitted by Law or under terms agreed with the appropriate rights organisations. Source must be acknowledged at all times. Enquiries for reproduction can be sent to the contact address quoted in this publication.

© European Network and information Security Agency (ENISA), 2008

Executive Summary

This report summarises the results of the ENISA deliverable from the Work Programme 2007 with the title *Demonstrators of RM/RA in Business Processes*. This effort has been conducted by ENISA in cooperation with BOC Germany as external contractor. This effort was initiated with respect to the main task of ENISA: ensuring a high and effective level of network and information security within the European Union. In particular within this and other ENISA efforts the *integration* of IT Risk Management with other relevant disciplines has been addressed. While this deliverable copes with the integration with operational processes, further ENISA deliverables elaborate on integration with Corporate Governance.

The aim of this effort is to identify interfaces between the processes described in the ENISA Risk Management/Risk Assessment Framework and selected operational processes. By having available a comprehensive documentation of such interfaces, an organisation is going to be able to plan the implementation of an integrated IT Risk Management, improve the overall effectiveness of its business processes, and enhance the quality of its IT Risk Management.

The results generated are available in the form of ADOit[®] process models as well as in the form of this report. The developed process models consist of the ENISA RM/RA Framework, selected operational processes, and their interface descriptions (i.e. the integration method). The report includes a short description of the model content, covering the ENISA RM/RA Framework, the integrated operational processes (ITIL IT Service Management, an Application Development Process, PRINCE2^{TM1}, CMMI), and their interfaces. It also provides a generic integration process which aims at supporting an organisation in the process of integrating IT Risk Management with operational processes, i.e. applying the project results.

The present results are mainly targeted to staff members who play a significant role in the area of IT-Security, Risk Management and IT Governance in general, as well as persons accountable for certain operational processes including the handling of operational and IT risks.

The benefits from the delivered result can be summarised as follows: An organisation may expect

- a better guidance along the IT Risk Management integration process,

¹ PRINCE2TM is a Trade Mark of the Office of Government Commerce

- a better quality of IT Risk Management, especially with respect to the handling of risks from IT operations,
- a better protection against disastrous incidents emanating from operations, which may cause severe damage to the organisation,
- an improved alignment with respect to compliance with IT governance frameworks like ITIL, project risks but also Governance Frameworks like e.g. SOX, Euro-SOX and Basel II and
- an overall advantage regarding competitive edge compared to business rivals.

Contact details: ENISA Technical Department, Section Risk Management, Dr. L. Marinos, Senior Expert Risk Management, e-mail: RiskMngt@enisa.europa.eu

Table of Contents

| | | |
|----------|--|-----------|
| 1 | INTRODUCTION..... | 6 |
| 1.1 | SCOPE AND OBJECTIVE OF PROJECT | 6 |
| 1.2 | STRUCTURE OF THE REPORT | 7 |
| 2 | THE ENISA RM/RA FRAMEWORK..... | 9 |
| 3 | OPERATIONAL IT PROCESSES | 11 |
| 3.1 | ITIL | 11 |
| 3.2 | APPLICATION DEVELOPMENT PROCESS..... | 12 |
| 3.3 | PRINCE2™ | 12 |
| 3.4 | CMMI..... | 13 |
| 4 | MODELLING TOOL AND MODELLING LANGUAGE..... | 14 |
| 4.1 | THE MODELLING TOOL ADOIT 3.0® | 14 |
| 4.2 | THE MODELLING LANGUAGE | 15 |
| 5 | THE INTEGRATION METHOD | 18 |
| 5.1 | MODELLING OF THE ENISA RM/RA FRAMEWORK INCLUDING ROLES..... | 18 |
| 5.2 | MODELLING OF THE OPERATIONAL PROCESSES | 19 |
| 5.3 | MODELLING OF THE INTERFACES BETWEEN THE PROCESSES | 20 |
| 6 | THE PROJECT RESULTS: ADOIT® MODELS | 22 |
| 6.1 | NAVIGATION THROUGH THE MODELS | 23 |
| 6.1.1 | <i>Exemplary Navigation through a Risk Management Process.....</i> | <i>23</i> |
| 6.1.2 | <i>Exemplary Navigation through an Operational Process.....</i> | <i>28</i> |
| 6.2 | ROLE MAPPING | 32 |
| 7 | APPLICATION OF RESULTS..... | 35 |
| 8 | EXPECTED BENEFIT | 40 |
| 9 | REFERENCES..... | 42 |

Table of Figures

| | |
|---|----|
| Figure 1: The Risk Management Process (from [5], Fig. 4, p. 13)..... | 10 |
| Figure 2: Screenshot of ADOit [®] 3.0 | 14 |
| Figure 3: Legend of Basic Model Elements | 17 |
| Figure 4: Mapping of Data Elements..... | 20 |
| Figure 5: Browser Window with Model | 22 |
| Figure 6. Example for Context Sensitive Menu..... | 23 |
| Figure 7: Navigational Path through Models – Example 1..... | 24 |
| Figure 8: RM/RA Framework Overview – Example 1..... | 25 |
| Figure 9: Risk Acceptance Process..... | 26 |
| Figure 10: Risk Acceptance Process with Interfaces to ITIL Service Support..... | 27 |
| Figure 11: ITIL Release Management | 28 |
| Figure 12: Navigational Path through Models - Example 2 | 29 |
| Figure 13: RM/RA Framework Overview - Example 2 | 30 |
| Figure 14: Selection of Operational IT Processes..... | 31 |
| Figure 15: ITIL Overview..... | 32 |
| Figure 16: The Integration Process..... | 36 |

Table of Tables

Table 1: Role Mapping 34

1 Introduction

This report is describing the ENISA deliverable *Demonstrators of RM/RA in Business Processes* which was conducted by the European Network and Information Security Agency² (ENISA) according to the ENISA Work Programme 2007. This deliverable contributes towards the main task of ENISA: ensuring a high and effective level of network and information security within the European Union, and developing a culture in this area, thus contributing to the smooth functioning of the Internal Market (see [9]). The following paragraph 1.1 explains the motivation, scope and aim of the project in detail, whereas paragraph 1.2 gives an overview of the structure of the project report.

1.1 Scope and Objective of Project

Corporate IT Risk Management is frequently implemented as an isolated process which shows little or no interaction with the various operational processes in an organisation (see [5]). As a consequence, risks which have to be dealt with on a daily basis are usually not taken into account on the level of planning and performing IT Risk Management. This causes a potentially negative impact on the overall quality of the business processes regarding aspects such as execution time, reliability and cost efficiency, among others. At the bottom line, isolated IT Risk Management is generally still not as effective as it could be.

For this reason ENISA strives towards good practices for establishing an *Integrated Risk Management*. This objective spans the limits of this project and includes forthcoming activities in the area of Corporate Governance, e-resilience, Business Continuity etc. Many of these activities started in 2007 and are going to be continued in 2008 and 2009.

To address this problem, an adequate integration of IT Risk Management processes with operational processes of an organisation is recommended. This allows for a better planning of IT Risk Management in general by including operational risks³ as an input during the process of the definition of the superordinated corporate Risk Management concepts. Furthermore, the dedicated and documented interfaces of IT Risk Management to the operational processes - including the description of role responsibilities - provide the executive personnel with guidelines for dealing with operational risks according to the organisation-wide risk strategy. Due to the well-defined information flows between operational processes on the one hand, and monitoring and review processes on the other

² <http://www.enisa.europa.eu>

³ E.g. risks from IT operations, project risks, risks faced during application development, to mention a few.

hand, a continuous review, adaptation and optimisation of IT Risk Management can also be performed.

In consideration of the above statement this effort aimed at identifying interfaces between the IT Risk Management processes described in the ENISA RM/RA Framework and selected operational processes. The focus of the integration was chiefly on the identification of corresponding data, roles and information flows between the processes. The results are available in the form of graphical process models, as well as this text document. With the included information, an organisation should be able to plan the implementation of an integrated IT Risk Management and hence improve the overall quality and effectiveness of its business processes.

It should be noted, that the set of interfaces is not exhaustive since it is aimed at providing a generic framework of interface definitions (i.e. good practice). Hence, in the course of the application of the generated results to a concrete organisation, an adaptation and extension phase has to be performed.

The target group of these results can be staff members, who play a significant role in the area of Corporate or IT Governance (e.g. Senior Management, CIO), Risk Management in general (e.g. corporate Risk Manager), and persons accountable for certain operational processes including the handling of operational risks (e.g. IT Service Manager, Software Architects).

Other persons may also be interested since IT Risk Management affects nearly every business unit. However, the responsibility for the implementation of IT Risk Management and its integration with operational processes should be assigned to a small group of staff members dedicated to this task. Consequently, the latter are the main target group.

1.2 Structure of the report

The project report is structured as follows:

- Section 2 gives a short introduction of the ENISA RM/RA Framework.
- In section 3 the operational processes that were selected for integration, are presented. This includes processes dealing with IT service management, application development, project management and process maturity.
- In section 4 the modelling concepts, which are used to represent the project results as well as the modelling tool *ADOit*[®], which was used to create the models, will be briefly presented.

- Section 5 describes the method, which was used to integrate the processes.
- The project deliverables are discussed in section 6.
- Section 7 proposes a generic integration process model which may be used as an initial guideline for the application of the project results.
- The report closes with a conclusion in section 8 including a discussion of benefits a user may expect when adopting the models.

2 The ENISA RM/RA Framework

The ENISA Risk Management/Risk Assessment (RM/RA) Framework is basically an overview of relevant content found in corresponding literature about Risk Management. In this section we give a short overview of the framework, since it is essential for understanding the project results. You may refer to [5] for further details.

Figure 1 shows a schematic overview of the framework as it has been published by ENISA in the past (see http://www.enisa.europa.eu/rmra/rm_process.html). The various (sub-) processes of the Risk Management Framework may be performed in isolation or as a whole. In case that all of the processes are performed, the orange, thick arrows represent a cycle which depicts a control flow through the Risk Management processes. The process *Definition of Scope and Framework* is considered to be the ideal starting point for this control flow. The process aims at the establishment of global parameters for the performance of Risk Management within an organization. For this purpose it takes internal and external aspects into account. Subsequently, a process describing activities which deal with the identification, analysis and evaluation of risks is executed (*Risk Assessment*). This process is succeeded by *Risk Treatment*, which selects and implements measures to modify risk. *Risk Acceptance* aims at deciding which risks are accepted by the responsible management of the organisation. *Monitor and Review* describes a continuously ongoing process for monitoring the success of the Risk Management implementation and delivering valuable input to any recursion of the (re)definition of the corporate Risk Management. Also included in the framework is a *Risk Communication* process, which aims at exchanging information about risk to and from all stakeholders. In addition to the above processes the interfaces to operational processes are indicated but not elaborated. This is subject to the project whose results are summarised by this report.

Complementing the framework a number of data elements were identified by ENISA which describe the exchange of information between the various Risk Management processes.

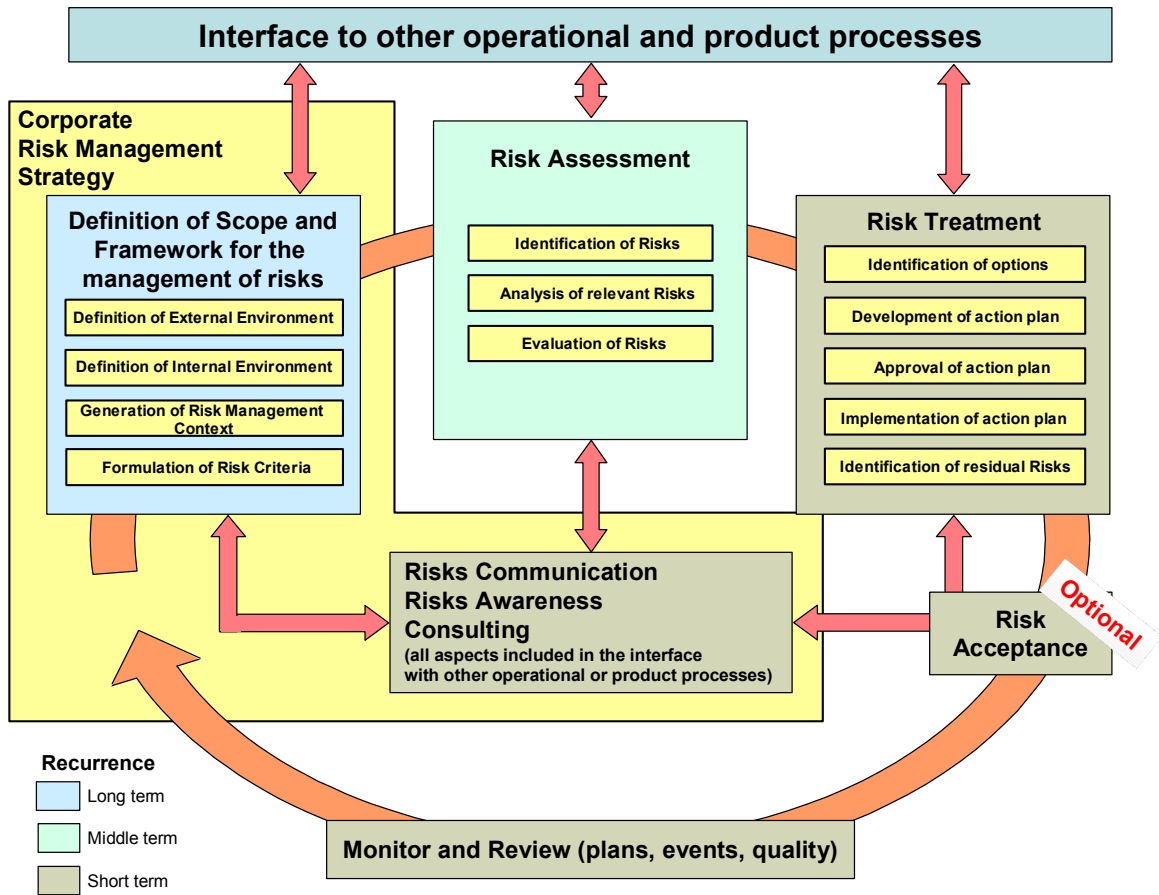


Figure 1: The Risk Management Process (from [5], Fig. 4, p. 13)

3 Operational IT Processes

This section gives a short overview of the operational processes which were selected for the integration with the Risk Management framework. At the end of each of the following paragraphs a short statement regarding the relevance of each process framework to IT Risk Management is included. For further information about the frameworks you may refer to the respective literature given in the paragraphs below.

Due to limited resources, the number of operational process frameworks, which could be considered for integration, was restricted. Hence, the decision was made to include ITIL, an application development process based on RUP, PRINCE2TM and CMMI in the project. The main reason for this choice is that these processes represent commonly used procedures and solutions for dealing with challenges which most companies have to meet, regardless of the business sector they are operating in. They are all to a certain extent accepted as de-facto standards. Furthermore, they are generally well documented and offer enough detail for integration with the ENISA RM/RA Framework, especially regarding the documentation of activities, roles and data elements. Additional frameworks, like CobiT⁴, MOF⁵ among others, were also considered for integration, but could not be included mainly due to the above mentioned lack of resources. However, due to the significance of the selected process frameworks in practice, the project results are expected to be highly beneficial for the stakeholders of corporate IT Risk Management.

3.1 ITIL

ITIL (*Information Technology Infrastructure Library*) was developed by the OGC (*Office of Government Commerce*) starting back in 1987. It aims at defining guidelines for the appropriate and efficient provision of IT services in organisations. The standard comprises a number of publications describing the best practices which are included in ITIL. The subsets of ITIL which are of interest for this report are Service Delivery, Service Support and Security Management (see [6], [7] and [8]). These processes are part of version 2 of ITIL and were selected for integration with Risk Management since they likely represent the most commonly used parts of ITIL at this point in time. Service Delivery mainly deals with planning and controlling aspects of IT service management. Service Support contains processes chiefly describing the support of customers in case of occurring incidents and problems. Security Management treats aspects like data security, risks and protection measures and therefore provides some parallels to Risk Management

⁴ *Control Objectives for Information and Related Technology*, see <http://www.isaca.org/cobit>

⁵ *Microsoft Operations Framework*, see <http://www.microsoft.com/mof>

processes. ITIL V3 is available since early 2007 but not widely-used yet, so it was not considered for inclusion in this project.

ITIL represents a framework for the design of service management processes. The data that is gathered during the execution of such service processes is highly valuable for assessing IT risks and helps to improve the corporate IT risk strategy. This applies especially for processes such as Incident Management and Problem Management, which deal with the consequences of IT risks. Moreover, an integration of IT Risk Management and ITIL allows for including Risk Treatment measures in the service process definitions – e.g. in IT Service Continuity processes - and thus improving these processes.

3.2 Application Development Process

The application development process used in the project for integration purposes is a generic heavy weight process, which is loosely based on the RUP (*Rational Unified Process*, see [3]). RUP is developed and published by Rational, which was acquired by IBM in 2003. The application development process should be used as a framework which can be tailored according to the requirements of the user. It comprises a number of process steps including analysis, design, implementation, testing and deployment. These most commonly used process steps are typical for almost every heavy weight software development process and hence were selected as a basis for creating the process models.

The integration of an application development process with IT Risk Management ensures that on the one hand Risk Management receives valuable input from software development projects, thus contributing to the overall definition of IT Risk Management strategies. On the other hand, considering well defined Risk Treatment activity plans as an input to software development projects helps steering such projects and minimising the risk of failure.

3.3 PRINCE2™

PRINCE2™ (*Project Management in Controlled Environments 2*), which like ITIL is developed by the OGC, is designed as a standard method for project management (see [4]). The documented processes describe the typical activities which are performed in the different project phases, like initiation, planning, directing, controlling and closing of a project. The aim of PRINCE2™ is to provide a repeatable, teachable method for project management which builds on the experience of a large number of organisations (best practice).

Project management frameworks, such as PRINCE2™, can be used to apply IT Risk Management to IT projects on a higher level of abstraction than by integration of an application development process, as has been described in the previous paragraph. The generic specification of how to plan, manage and control a project allows for covering a

larger area of activities and therefore a larger scope of integration with IT Risk Management. Thus, the project management framework can be used to plan and perform the implementation of measures arising from Risk Treatment.

3.4 CMMI

CMMI (*Capability Maturity Model Integration*) is a process improvement maturity model for the development of products and services (see [1]). It is developed and published by the Software Engineering Institute of the Carnegie Mellon University, Pittsburgh (USA). The documented CMMI processes, which were selected for integration with Risk Management processes, cover activities which guide through the implementation of highly mature development and service processes (CMMI for Development V. 1.2). The CMMI processes themselves are generic and may be applied to various concrete business processes.

Similar to PRINCE2TM, CMMI has a very large scope and can thus be used to integrate IT Risk Management with the (re-)design phase of any kind of IT process, i.e. IT Risk Management can be included in the IT process improvement efforts. CMMI is not focussed on projects, like an application development process or a project management framework, but on regular business processes which are executed on a daily basis. During the maturity improvement process execution, valuable information about expected operational risks can be gathered and passed to IT Risk Management. In turn Risk Treatment measures coming from IT Risk Management can be included in the process design.

4 Modelling Tool and Modelling Language

This section introduces the modelling tool that was used for creating all models in the course of this project, as well as the modelling concepts which were used for the creation of the models.

4.1 The Modelling Tool ADOit 3.0[®]

ADOit[®] 3.0 is a modelling tool which aims at supporting service management and architecture management by providing the means to illustrate, analyse and optimise service processes and IT infrastructures (see [2]). Additionally, predefined reference models according to ITIL and CobiT can be acquired for the tool, which may be used to support the adaptation and implementation of the best practice approaches. ADOit[®] is available in several languages (e.g. English and German). Figure 2 shows a screenshot which displays the graphical user interface of ADOit[®].

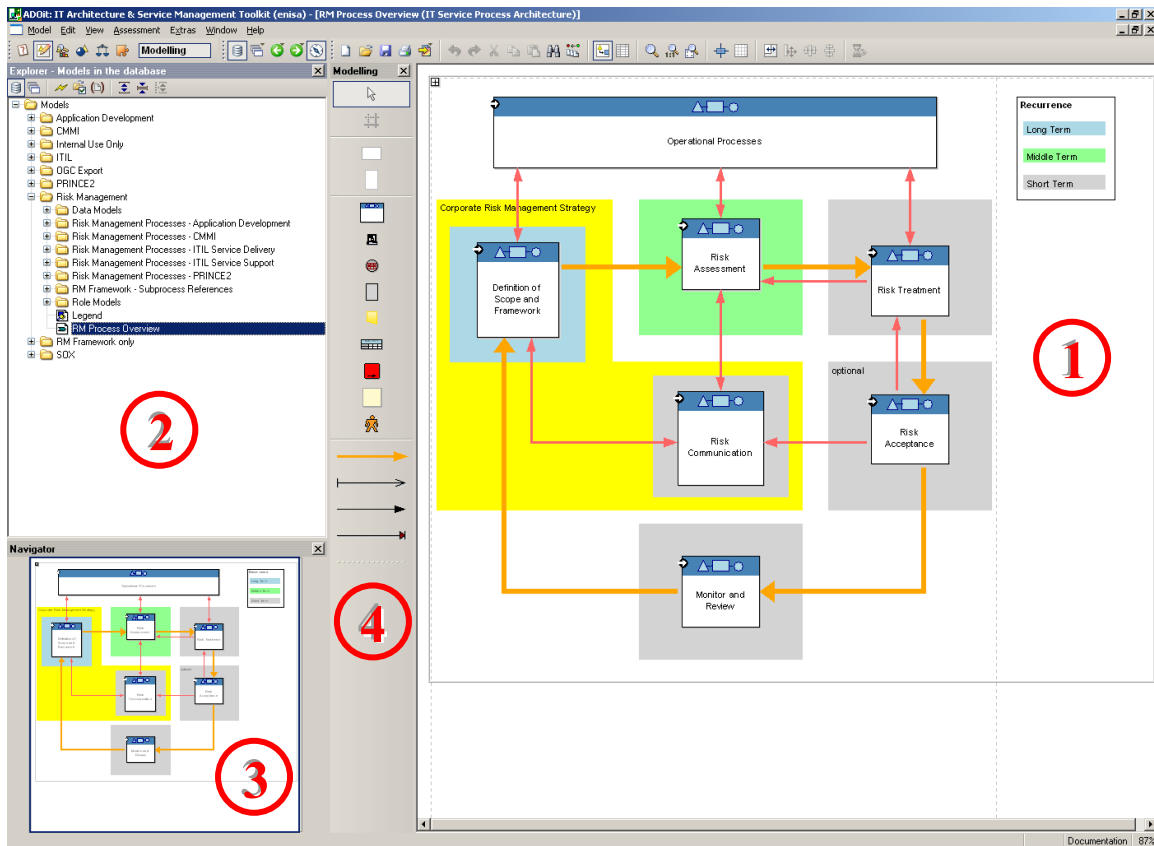


Figure 2: Screenshot of ADOit[®] 3.0

On the right hand side the *modelling area* (marked by the red **1** in the above figure) is located. To its left is placed the *model explorer* (**2**). The explorer shows the model groups, which are used to organize the models. To the lower left the *navigator* (**3**), which shows an overview of the currently displayed model, is located. In the middle of the screen the vertical *modelling toolbar* with the available model elements is placed (**4**). Any of these tool bars and panels can be moved, resized and hidden according to the user's preferences. Besides the modelling functionality, a number of analyses on models, process simulation, the generation of HTML and Word documents as well as various import/export options are implemented in the tool. Additionally, the meta-modelling approach allows for an easy customisation of the modelling concepts including analyses on the models etc. with respect to the user's requirements.

4.2 The Modelling Language

Since ADOit[®] follows a meta-model based approach a variety of modelling concepts can be used within the tool. The specific modelling language used in the project is briefly described below. It is based on the set of standard modelling languages of ADOit[®] as a part of the BOC Architecture Management Framework (see [2]) and was modified according to the specific requirements of the project.

Figure 3 shows a legend which is included as an additional diagram within the set of models which forms the main deliverable of the project (see section 6). On the top of the diagram an exemplary process model is displayed, including a process start (triangular shape *Process Start*), followed by a parallel branch (triangular shape pointing to the left) of the control flow (black arrows). After the branch two activities (*Activity 1* and *Activity 2*) are executed concurrently. Communication to actors, i.e. in our case usually external roles, is expressed by data flows (lines with solid arrowhead). In the example a data flow to the actor symbol above *Activity 1* is shown.

The diamond shaped symbol after *Activity 2* represents an alternative branch, i.e. depending on the condition at the branch (e.g. a question, which can be answered with *yes* or *nor*) only one of the following paths will be followed. On the right hand side the parallel control flows are merged again with the triangular shape pointing to the right. The circular *Process End* symbol marks the end of the process execution. Roles involved in a process execution are annotated to the right of the respective activity. In the modelling of the particular processes in the project we distinguish between *responsible* (role that executes the process), *accountable* (role that is accountable for the outcome), *consulted* (role that gives advice) and *informed* (role that has to be briefed about the

results of an activity). To the right of *Activity 1* some exemplary roles are attached. The letters R, A, C and I indicate the type of the role attached (*RACI* notation⁶).

The blue sub-process symbol which is connected to the alternative branch and *Activity 3* represents another process model (here *Risk Assessment*) which is invoked at the position of the sub-process symbol. By using this model element the graphical complexity of a diagram can be reduced. To the left of Figure 3 a red interface object is shown. The text below the symbol shows the name of the process which contains the related interface (in this case *Process Name*). Every interface of this type is connected to exactly one interface of the same type in another process. These interfaces are used for showing the information flow between the Risk Management processes on the one hand and the operational processes on the other hand. The exchanged data elements are represented by yellow document-like symbols (*Data Element*). Every incoming data element is mapped to one or more data elements inside the *Data Port* (for an example see paragraph 5.3).

The whole exemplary process is arranged inside a *level* or *swimlane*, which is used to display a role or organisational unit responsible for the included part of the process. Every activity is assigned to zero or one swimlanes.

On the bottom of Figure 3 two additional model objects are displayed. To the left a special interface in front of a red box can be seen, which shows the parallel execution of Risk Management activities in the connected processes. Whenever this interface is used, data is exchanged between an activity of the Risk Management framework and an activity in an operational process, which also deals with Risk Management, i.e. usually in terms of operational risks.

The model object to the right of the above described interface is the process symbol. This object stands for a process in a process map and therefore is linked to a diagram containing a process model (with activities and control flows) or another process map (with processes). Finally, the light yellow boxes connected to the other model elements by a dotted line contain commentaries which contribute by providing additional semantics to the models.

For information about how to navigate through the models refer to section 6.

⁶ This way of describing role relations is e.g. used in the CobiT documentation.

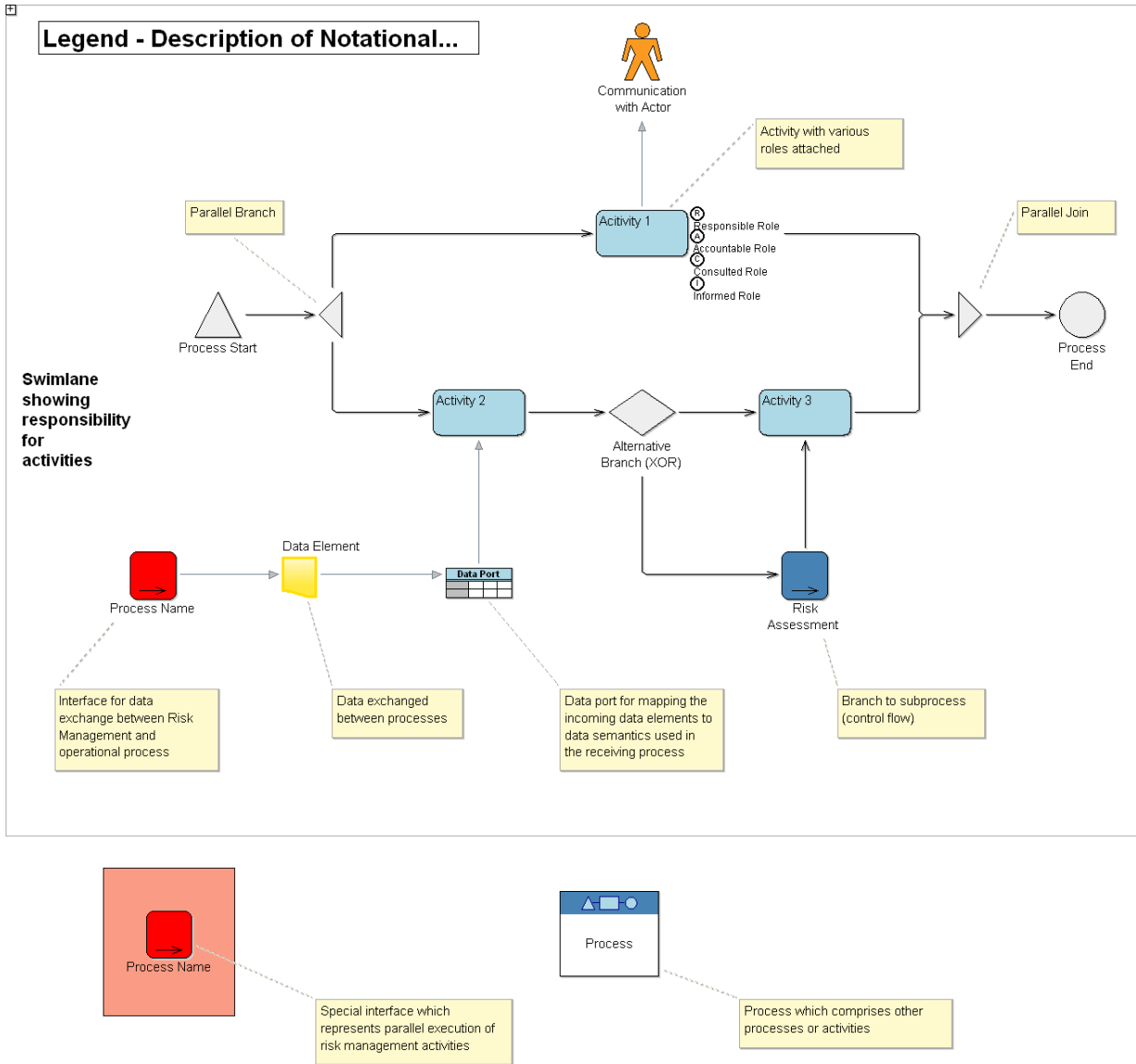


Figure 3: Legend of Basic Model Elements

5 The Integration Method

The method which was developed for the integration of the various processes is introduced in this section. The method's process model consists of the following fundamental working steps, which were executed consecutively in the course of the project:

1. Modelling of the ENISA RM/RA Framework
2. Modelling of the Operational Processes
3. Modelling of the Interfaces between the Processes

The above working steps are discussed in detail in the following paragraphs.

5.1 Modelling of the ENISA RM/RA Framework including Roles

The ENISA RM/RA Framework was depicted in the form of a graphical process model in ADOit[®]. The data elements which were identified by ENISA were included in the model as dedicated input and output of the processes. These elements can be viewed by displaying the properties of an activity. Additionally, a number of roles were identified, which are typically involved the execution of the Risk Management processes. These roles are the following:

- Senior Management/Board of Directors
 - This role is accountable for inventing Risk Management in the organisation, defining the basic participating roles, creating and communicating risk awareness, as well as deciding on the degree of risk tolerance of the organisation. The Senior Management will not be directly responsible for any of the Risk Management processes (since it does not execute them) and hence does not appear as a role in any of the swimlanes in the model.
- Risk Manager
 - The Risk Manager is chiefly responsible for the definition, structuring, implementation, and coordination of Risk Management in the organisation. The Risk Manager can be an individual or a group, which may be hierarchically organised (local, global Risk Manager).
- Risk Owner
 - The Risk Owner is usually an officer in a business unit/functional unit. The Risk Owner is responsible for dealing with risks in his business unit. The main

task of this role is to implement Risk Management processes according to the guidelines defined by the Senior Management and the Risk Manager. Often the role is assigned to the same person as the role Domain Expert (especially in smaller organisations), due to a flat organisational hierarchy.

- Internal Audit
 - Internal Audit is responsible for monitoring the Risk Management processes. Events are being tracked and the processes are being evaluated towards the background of the previously created Risk Management plans.
- Domain Expert
 - The role Domain Expert is responsible for assisting the management of risks by delivering input from a specific domain perspective (consulting role). His special knowledge about a particular domain in the organisation serves as a basis for identifying and treating the specific risks in that area. Additionally, the role participates in the process of monitoring the risks. The Domain Expert may be an internal or external (consultant) person. Due to his role specification he will not be responsible for any of the Risk Management processes and hence not appear as a role in any of the swimlanes in the model. Often the Domain Expert role is assigned to the same person as the Risk Owner role (especially in smaller organisations), due to a flat organisational hierarchy.

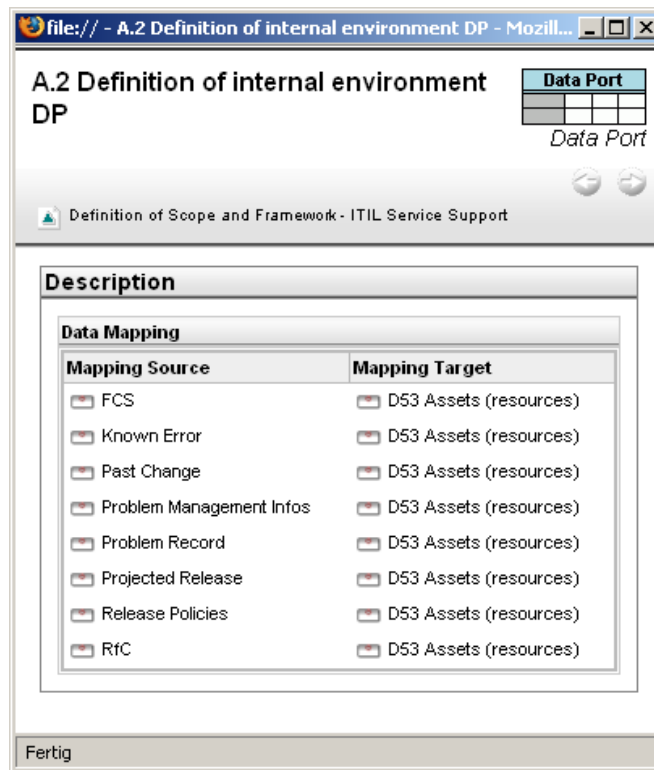
The roles are displayed to the right of the activity to which they are attached.

5.2 Modelling of the Operational Processes

The selected operational processes were modelled in the same way as the framework. First, the processes itself including the control flows were depicted. Second, the data elements, which are of fundamental importance for later conducting the modelling of the information flows between the processes, were identified and included in the model. Finally, the role definitions were supplemented. Note that this does not apply to all operational processes, since e.g. the PRINCE2TM and CMMI documentation does not provide a detailed description of a role model. Moreover, the roles in the operational processes are not depicted in the same way as in the Risk Management process (RACI notation), since usually only the responsible role is annotated, which can also be identified by looking at the name of the swimlane. An example of this notation can be seen in Figure 3 on the left hand side (*Swimlane showing responsibility for activities*).

5.3 Modelling of the Interfaces between the Processes

As a first step of integration, the activities of the operational processes, which provide interfaces to the Risk Management processes, were identified. Secondly, the information flow between the integrated activities or processes respectively was depicted. A third step was necessary when a data element was used as an incoming information flow to an activity. In this case a data mapping was conducted, which related the incoming data element to the corresponding data elements of the receiving process. Figure 3 shows an example of an interface to another process or activity (the red symbol), an exchanged data element (the yellow document-like symbol with the exemplary *data element* item above) and the *data port* symbol. The latter contains a table which maps the incoming data elements to the data definitions of the receiving process. Figure 4 shows an example of a data mapping. The left column shows the incoming data elements whereas the right column contains the mapping target, i.e. the data element which is used in the receiving activity to store the incoming information.



| Mapping Source | Mapping Target |
|---|---|
| <input type="checkbox"/> FCS | <input type="checkbox"/> D53 Assets (resources) |
| <input type="checkbox"/> Known Error | <input type="checkbox"/> D53 Assets (resources) |
| <input type="checkbox"/> Past Change | <input type="checkbox"/> D53 Assets (resources) |
| <input type="checkbox"/> Problem Management Infos | <input type="checkbox"/> D53 Assets (resources) |
| <input type="checkbox"/> Problem Record | <input type="checkbox"/> D53 Assets (resources) |
| <input type="checkbox"/> Projected Release | <input type="checkbox"/> D53 Assets (resources) |
| <input type="checkbox"/> Release Policies | <input type="checkbox"/> D53 Assets (resources) |
| <input type="checkbox"/> RfC | <input type="checkbox"/> D53 Assets (resources) |

Figure 4: Mapping of Data Elements

As a final step, the mapping of roles was conducted for these processes which were provided with adequate role definitions.

At this point, the integration process was completed. The results of this procedure are presented in section 6.

6 The Project Results: ADOit® Models

The results of this project are documented in the form of this project report as well as the ADOit®-models showing the integration of the processes. The ADOit®-models can be exported to HTML and viewed using an internet browser, like the Internet Explorer, Firefox or Opera. This kind of publication has the advantage that the viewer of the models does not have to have a version of ADOit® installed on his computer. However, the main limitation of that kind of representation is the lack of editing options, since the output is read-only. For a modification of the models a version of ADOit® is necessary.

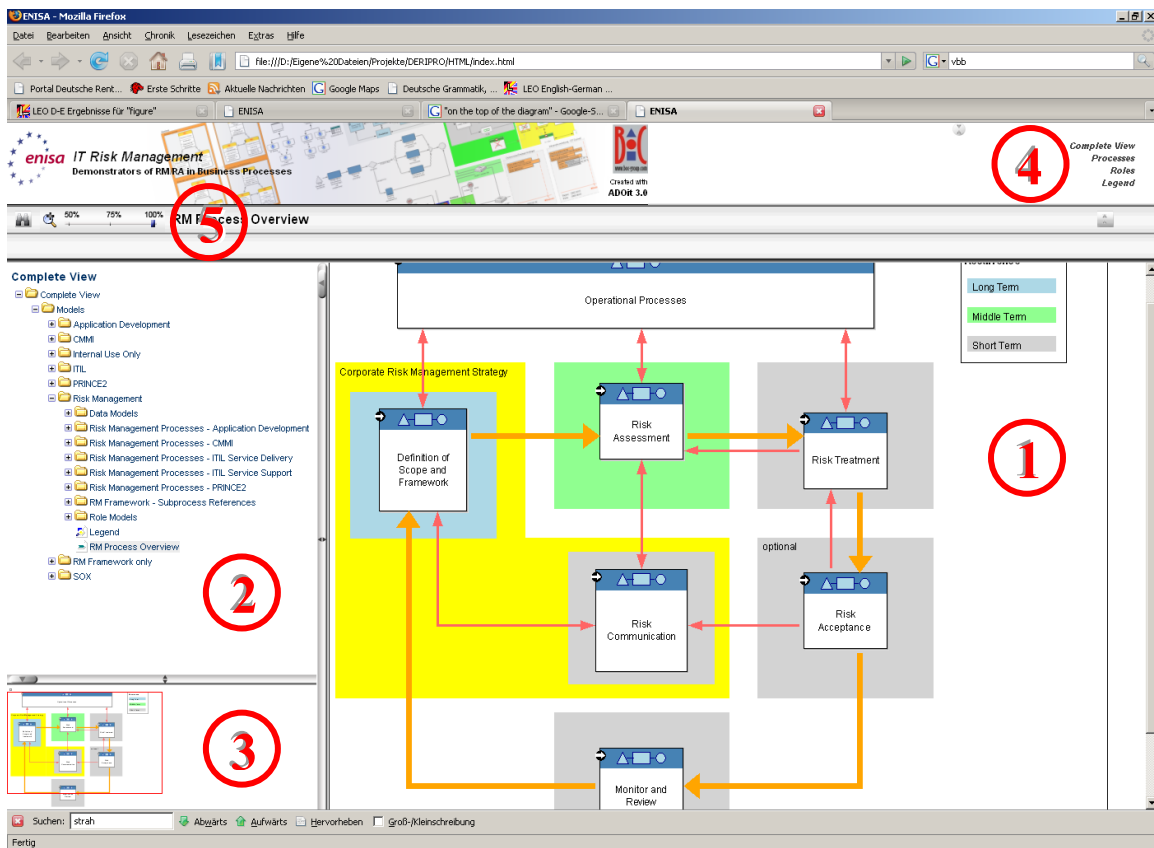


Figure 5: Browser Window with Model

Figure 5 shows an initial model opened in a browser. On the right hand side the model itself is displayed (marked by a red 1 in the figure). To its left the model explorer showing the model groups (2), as well as the navigational pane (3) can be seen. On top of these areas the header is located, which contains a menu for the selection of the available model views on its right hand side (4, *Complete View, Processes, Roles, Legend*). By selecting a view the model types which will be available for viewing can be restricted. It

can be chosen between all, process or role models as well as the legend diagram only. On the left hand side above the model groups *Search* and *Zoom* functionalities can be operated (5). There are three possible zoom modes, which determine the size of the models. The search function allows for scanning for certain model elements.

The following paragraph 6.1 shows how the models can be navigated. Paragraph 6.2 complements this section by showing a proposal for a role mapping between the operational processes and the IT Risk Management processes.

6.1 Navigation through the Models

Navigation through the models is designed to be straight forward. After clicking on a model element, its details (properties) will be displayed. Alternatively, in case a reference to another model or model element is part of the element's properties, it can be chosen between displaying the model element's properties or navigating to the referenced model or model element (see Figure 6, *Details* for the properties, *Risk Acceptance* for navigating to the respective process).

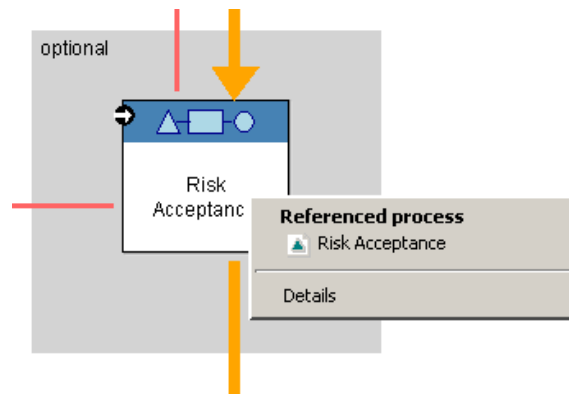


Figure 6. Example for Context Sensitive Menu

The models themselves are organised in a tree-like structure. There are two possible ways to navigate from the starting diagram – the RM/RA Framework Overview – to the operational processes. These navigation options are explained by providing appropriate examples in the following two paragraphs 6.1.1 and 6.1.2. This kind of navigation can be applied to all models which were created in the course of the project.

6.1.1 Exemplary Navigation through a Risk Management Process

The first possible path is depicted in Figure 7. This example shows a way through the model hierarchy to the ITIL process *Release Management*.

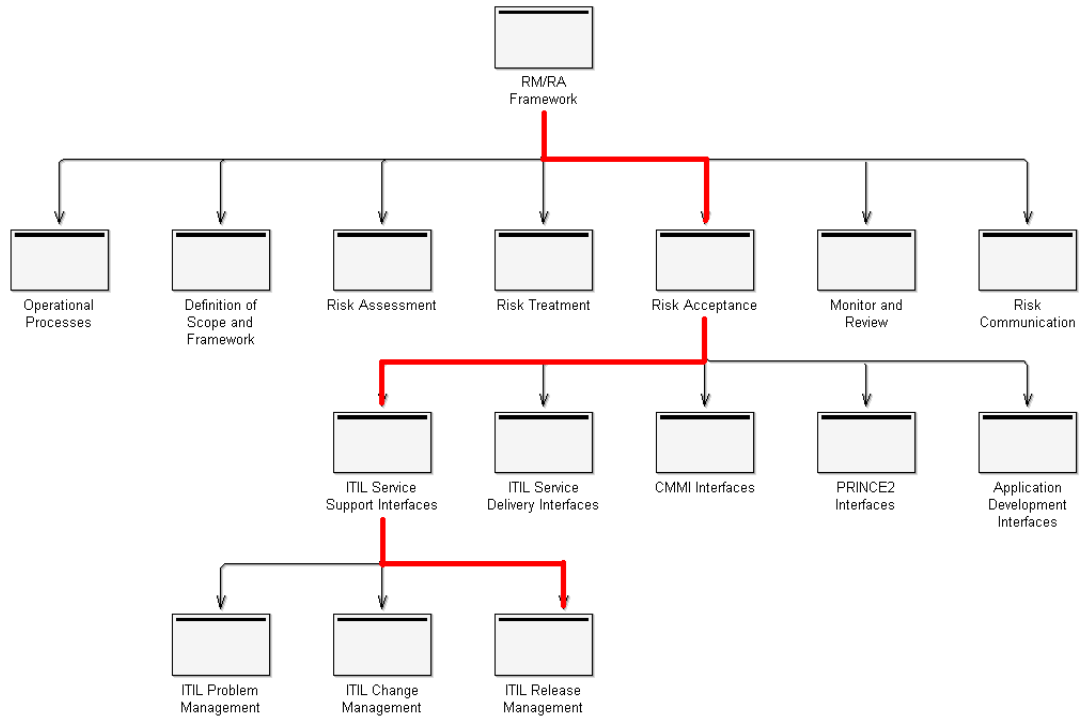


Figure 7: Navigational Path through Models – Example 1

On the framework level a Risk Management process can be selected. In our example this is *Risk Acceptance* (see Figure 8).

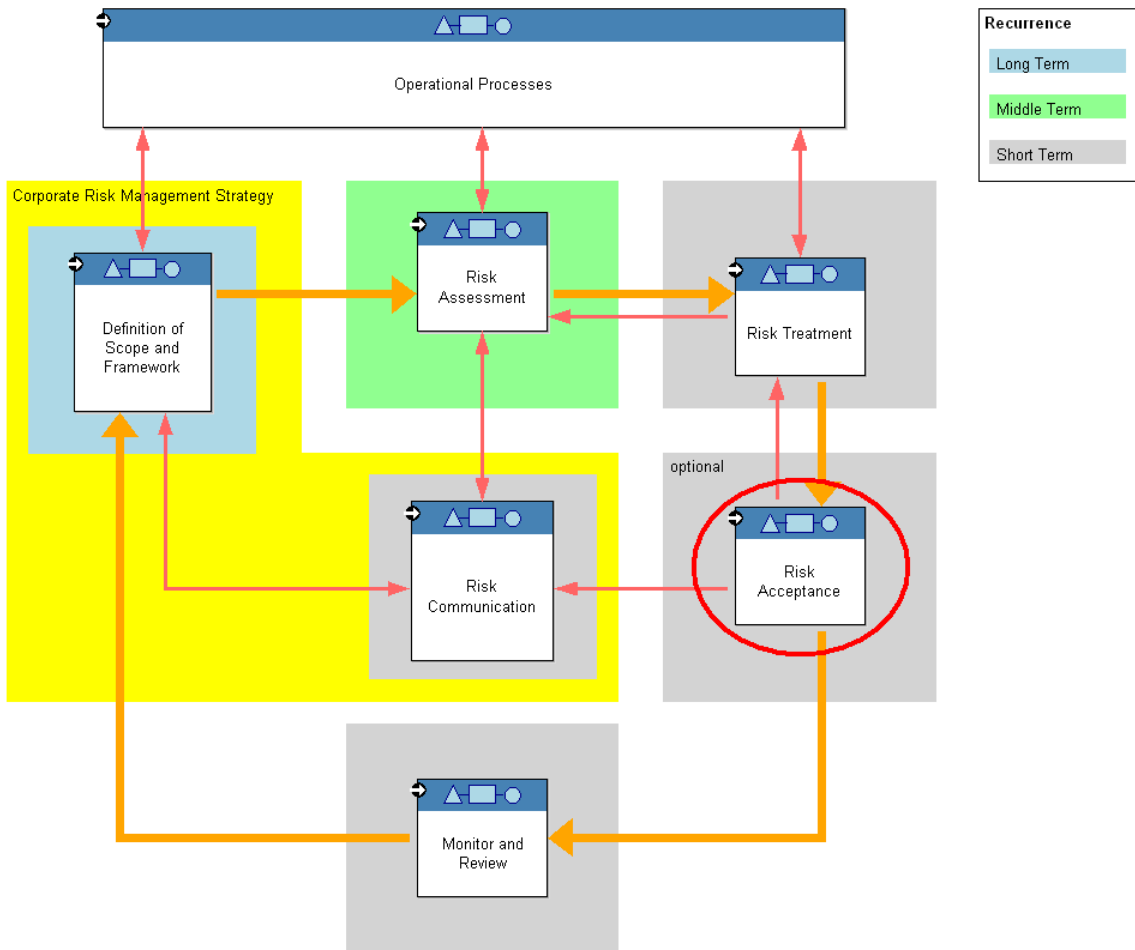


Figure 8: RM/RA Framework Overview – Example 1

In this diagram on the lower side the operational processes are listed which provide interfaces to Risk Acceptance (see Figure 9). In our example, the process ITIL Service Support is selected.

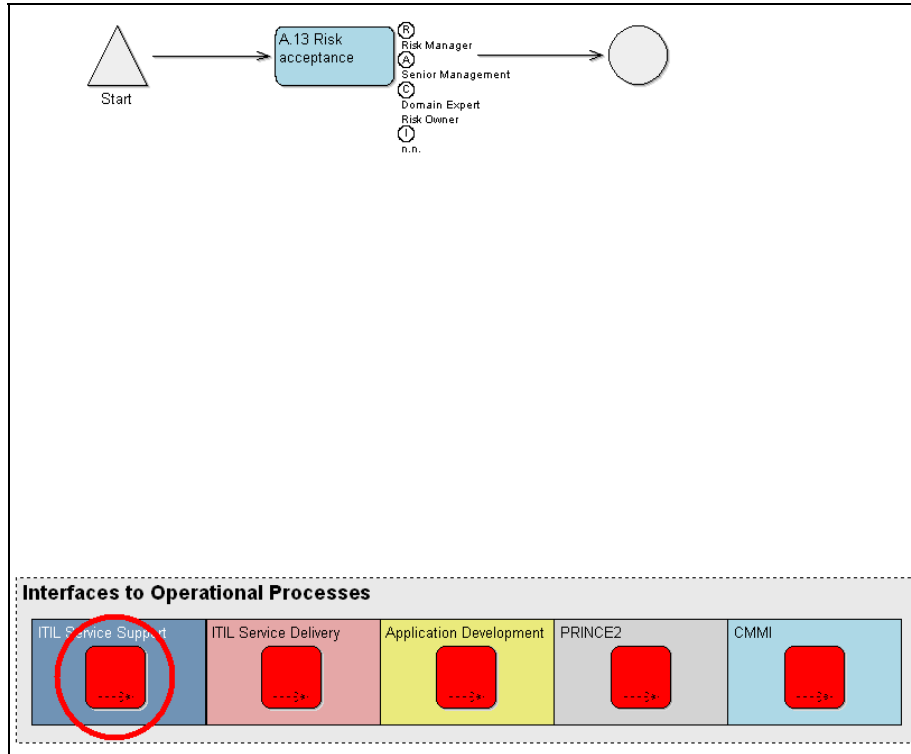


Figure 9: Risk Acceptance Process

As a result the Risk Acceptance process is displayed with the various interfaces to ITIL Service Support (see Figure 10).

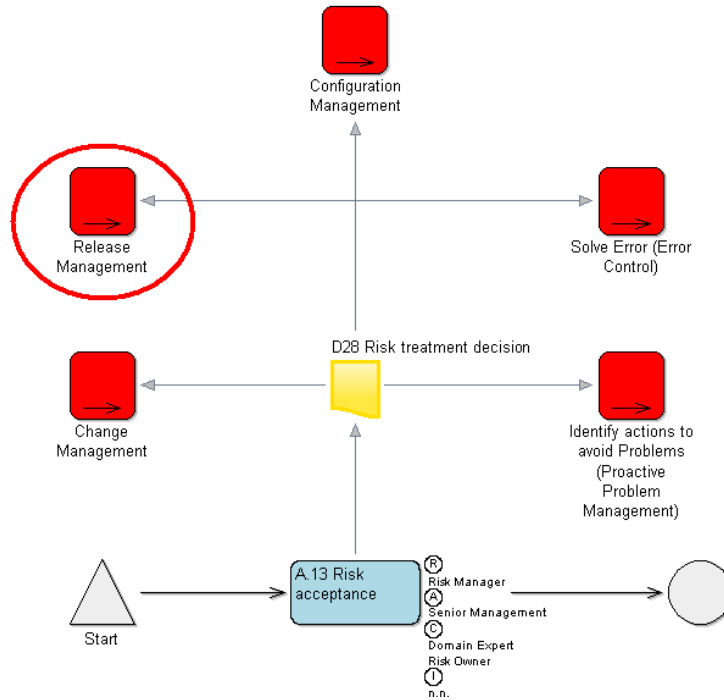


Figure 10: Risk Acceptance Process with Interfaces to ITIL Service Support

After choosing the respective interface (upper left side), the model seen in Figure 11 is displayed, which represents the ITIL *Release Management* including the interfaces to Risk Management.

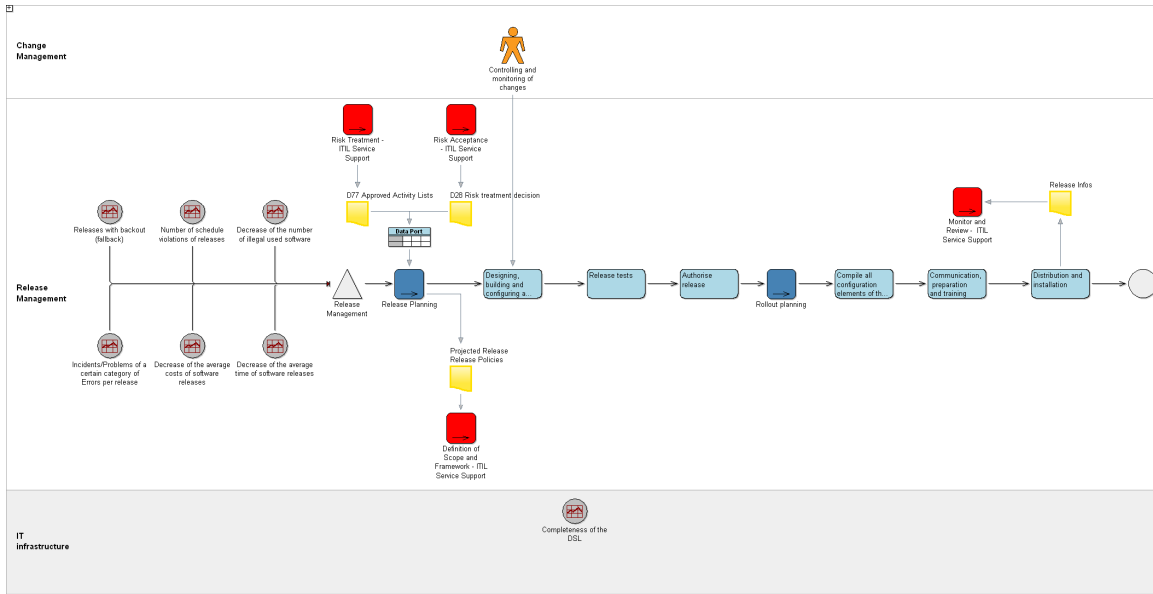


Figure 11: ITIL Release Management

6.1.2 Exemplary Navigation through an Operational Process

An alternative way to navigate through the models also starts at the framework level, but continues by selecting the process *Operational Processes*. The path is displayed in Figure 12.

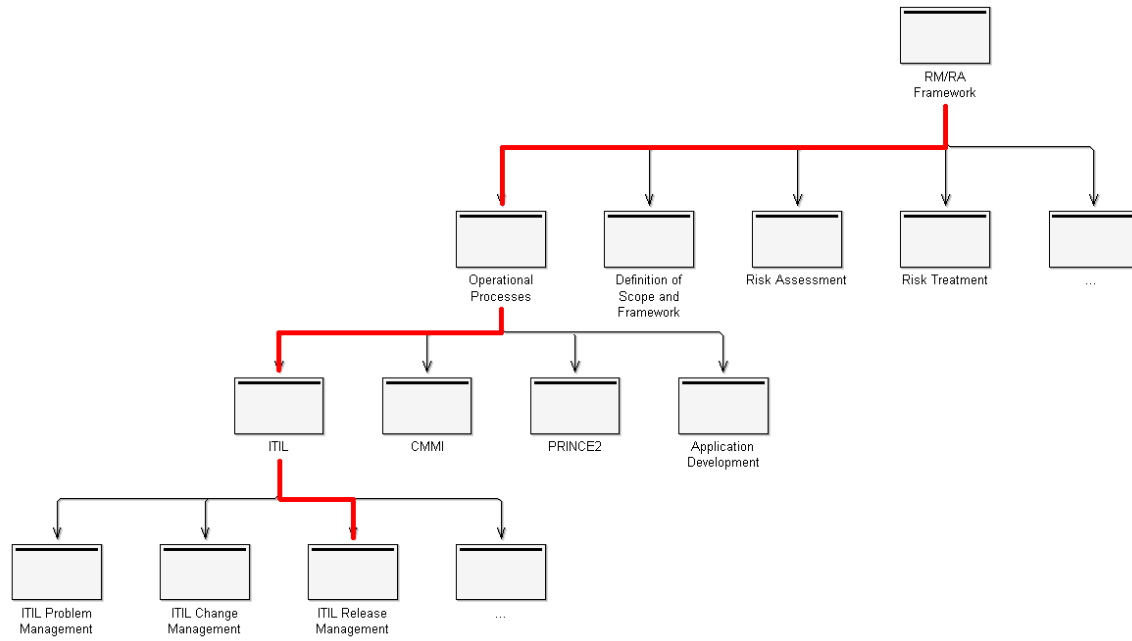


Figure 12: Navigational Path through Models - Example 2

On the framework level the process object *Operational Processes* is selected (see Figure 13).

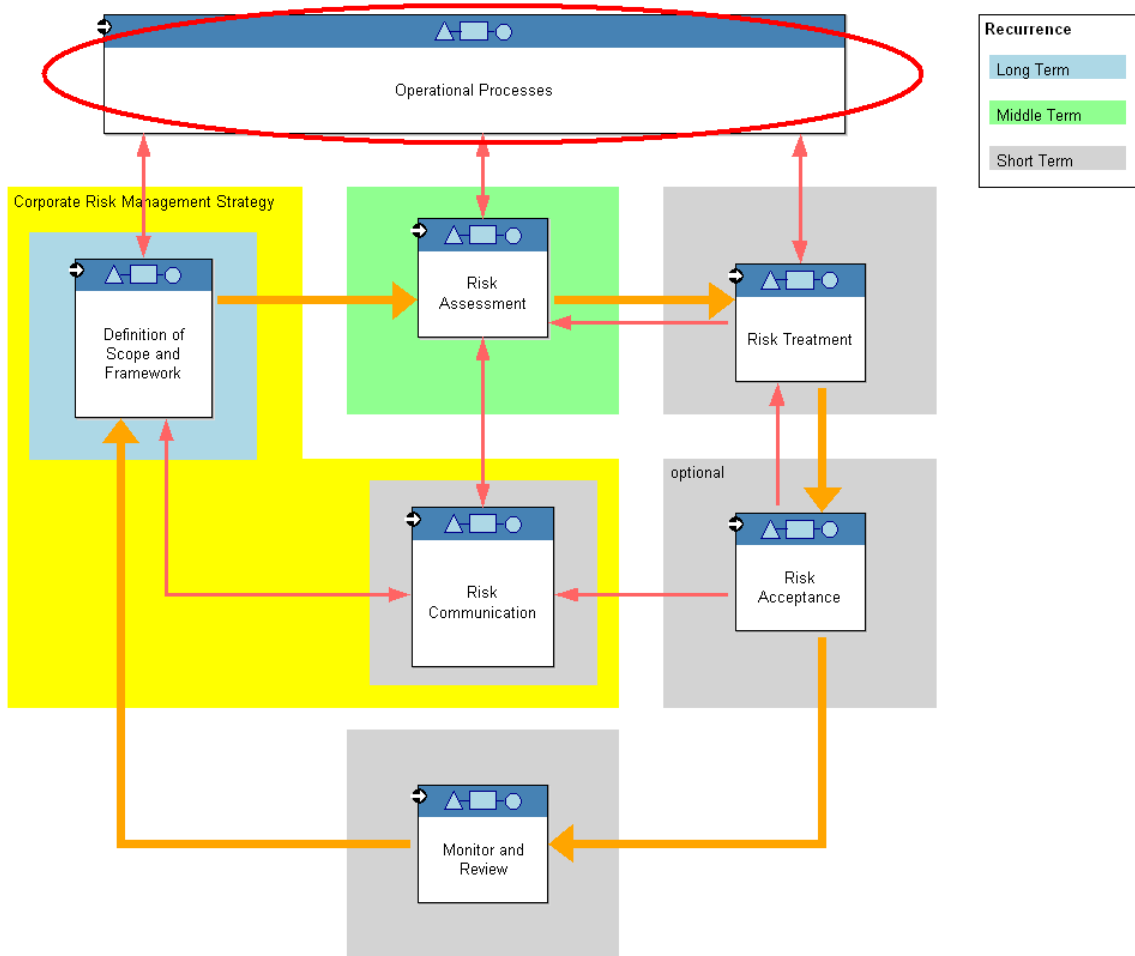


Figure 13: RM/RA Framework Overview - Example 2

After this the desired operational process can be chosen (in our example ITIL, see Figure 14).

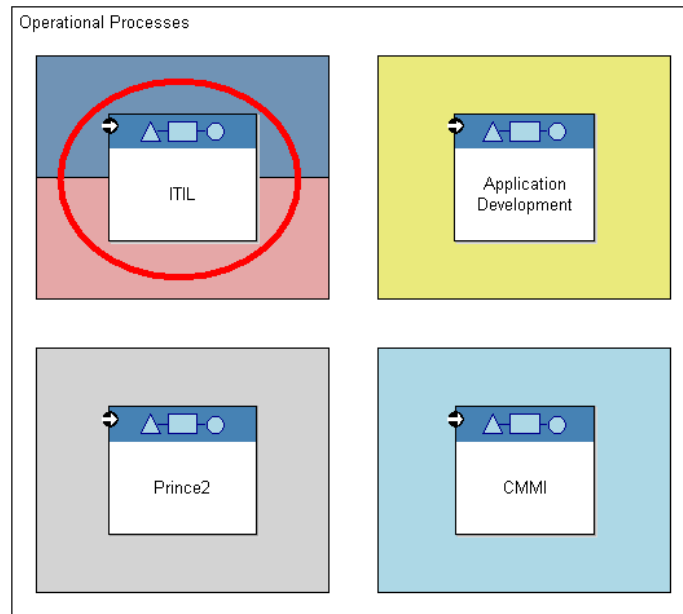


Figure 14: Selection of Operational IT Processes

The model showing the ITIL overview in Figure 15 can be used to switch to the various sub-processes. The example assumes that *Release Management* is selected which results in displaying the same model as in the example of the first navigational path (see Figure 11).

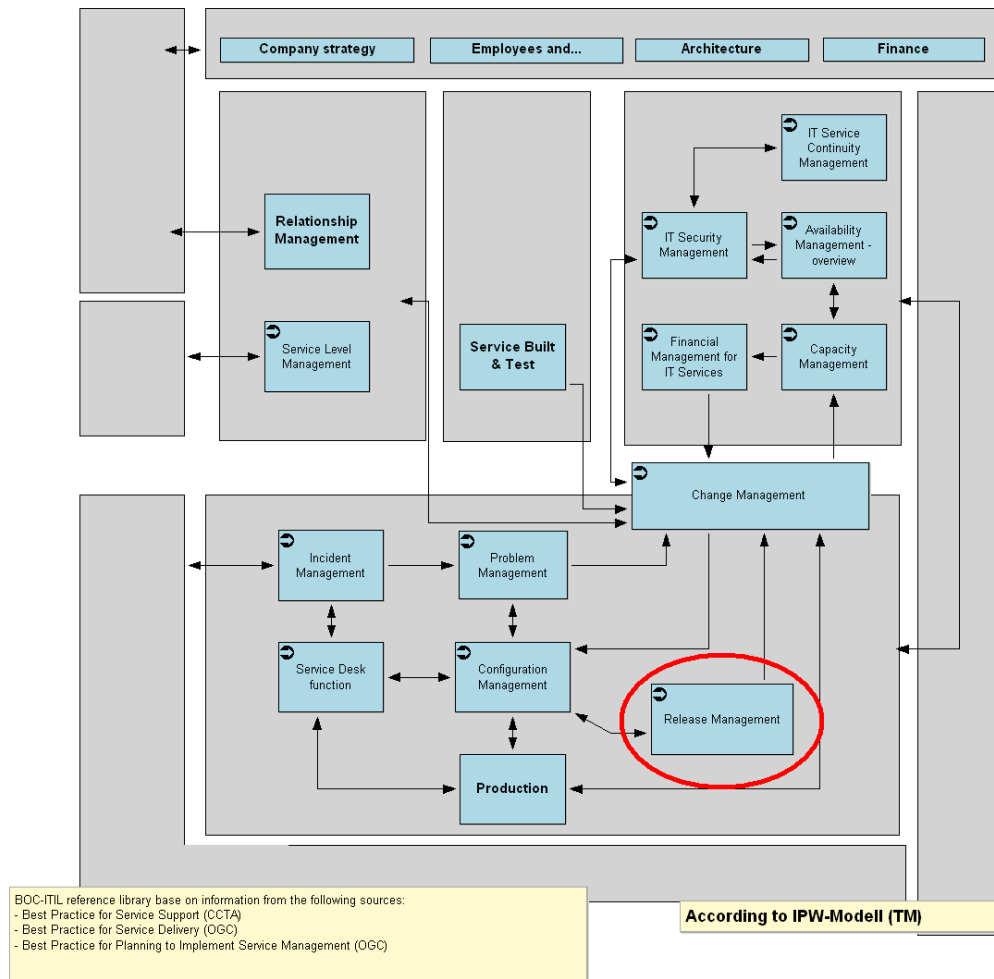


Figure 15: ITIL Overview

6.2 Role Mapping

A proposal for the mapping of the roles of the operational processes to those of the Risk Management processes was made for these processes which were provided with adequate role definitions, i.e. ITIL and application development. The CMMI and PRINCE2TM documentations do not cover role definitions in detail, hence they were not considered for mapping. The result of this working step is documented in Table 1. The roles in the operational processes (columns) are assigned to those of the IT Risk Management framework (rows). The Change Manager in ITIL Change Management for instance acts as a local Risk Manager as well as the Risk Owner. In our case the term “local” refers to the local management of operational risks, whereas “global” would refer to global Risk Management.

| | Senior Management | Risk Manager | Risk Owner | Internal Audit |
|---|-------------------|--------------|------------|-------------------------|
| ITIL Service Support | | | | |
| Change Management | | | | |
| Change Manager | | X (local) | X | |
| Senior Management | X | | | |
| Incident Management | | | | |
| Management | X | | | |
| Incident Manager | | X (local) | X | X (incident monitoring) |
| Configuration Management | | | | |
| Configuration Manager | | X (local) | X | |
| Problem Management | | | | |
| Problem Manager | | X (local) | X | |
| Release Management | | | | |
| Release Manager (may be Configuration and/or Change Manager) | | X (local) | X | |
| ITIL Service Delivery | | | | |
| Availability Management | | | | |
| Availability Manager | | X (local) | X | |

| | | | | |
|---|---|------------|---|-------------------------|
| Capacity Management | | | | |
| Capacity Manager | | X (local) | X | X (asset monitoring) |
| Financial Management | | | | |
| Financial Manager | | X (local) | X | X (controlling) |
| IT Service Continuity Management | | | | |
| ITSCM Manager | | X (global) | | |
| Service Level Management | | | | |
| Senior Management | X | | | |
| SLA Manager | | X (global) | | X (SLA monitoring) |
| IT Security Management (not part of Service Delivery but closely integrated) | | | | |
| Senior Management | X | | | |
| Security Manager | | X (global) | | |
| Application Development | | | | |
| Architect | | X (local) | X | X (project controlling) |
| Designer | | X (local) | X | |
| Database Designer | | | X | |
| Deployment Manager | | | X | |
| System Integrator | | | X | |
| System Analyst | | | X | |
| Test Designer | | | X | |

Table 1: Role Mapping

7 Application of Results

In order to successfully apply the above presented project deliverables in the course of a Risk Management integration process, a methodical approach is recommended. The selection of the activities, which may be executed as a part of the integration process, depends on the initial situation of an organisation prior to the implementation of the integration. Especially depending on the number of operational and Risk Management processes, which are already implemented in an organisation, some of the implementation activities may be omitted. In general, the following processes may be executed to establish an integration process:

1. Risk Management Implementation
2. Operational IT Process Implementation
3. Integration Planning and Initiation
4. Quality Assurance
5. Execution of Processes

The first two processes (not necessarily in the above order) are only relevant if not all processes, which are to be integrated, are already implemented in the organisation. It is beyond scope of this report to present detailed instructions of how to implement operational processes, like e.g. ITIL, or invent a comprehensive corporate IT Risk Management policy. For information regarding these topics please refer to the appropriate literature. It is rather assumed that all the processes are implemented and performed in a way that is for the most part compliant to the reference processes used in the project. If the deviation from these standards is too great, the integration on the basis of the project results may become more difficult. As a result, additional redesign of the processes and interfaces in between them may be necessary.

A proposal for a workflow, consisting of activities performed in the processes 3 to 5, is presented in Figure 16. It displays an exemplary integration scenario with activities and control flows and thereby demonstrates how an integration process may look like.

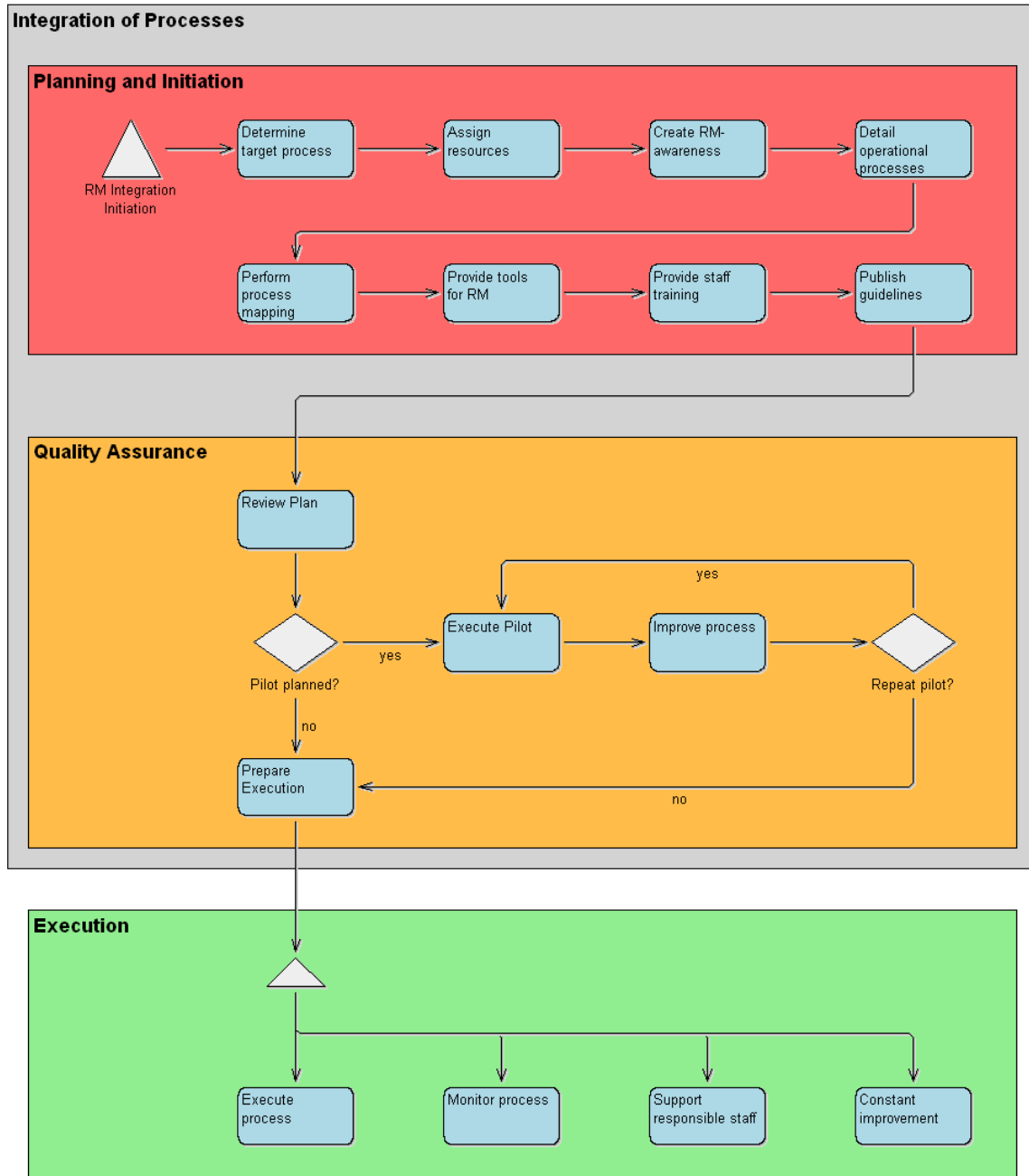


Figure 16: The Integration Process

The following short description explains the semantics of the activities in the integration process model:

Integration of Processes - Planning and Initiation

- Determine target process
 - Determine which process shall be integrated with the RM/RA Framework
- Assign resources
 - Assign resources for implementation (staff, support, technical resources)
- Create Risk Management awareness
 - Create or raise awareness for Risk Management (done by global risk manager, backed up by senior management)
 - Communicate necessity to the respective area of the company
 - Illustrate importance for achieving business objectives
 - Communicate Risk Management as part of any process
 - Apply Risk Management in decision making
- Detail operational processes
 - Detail operational processes which are to be integrated with the Risk Management processes (control flow, roles, information flow)
- Perform process mapping
 - Perform mapping between operational process and Risk Management processes
 - Roles, information, information flow between processes
- Provide tools for Risk Management
 - Implementing, acquiring, testing and deploying of tools for Risk Management

- Provide staff training
 - Training of responsible staff (e.g. by presenting scenario walkthroughs) regarding
 - Activities
 - Responsibilities
 - Tools
- Publish guidelines
 - Publishing and communicating guidelines/rules for Risk Management

Integration of Processes - Quality Assurance

- Review Plan
 - Review the above created documents and assure quality of the integration plan
- Execute pilot
 - Execute a pilot for the integration (optional)
- Improve process
 - Improve process integration and activities on basis of pilot results (also optional)
- Prepare execution
 - Define timetable and plan for execution

Execution

- Execute processes
 - Execute the Risk Management processes as part of the operational processes
- Monitor process

- Monitoring of processes, measuring of success, detection of problems
- Support responsible staff
 - Provide support for staff which executes the processes
- Constant improvement
 - Perform a constant improvement of processes

The activities in the process *Execution* are executed concurrently and usually do not have a determined end.

The above sketched process is to be interpreted as a framework which has to be customised according to the requirements of a concrete organisation. On the one hand, some activities may be omitted, on the other hand additional activities may be required. However, the framework gives a comprehensive overview of the basic activities which may occur in the course of a typical integration process.

8 Expected Benefit

As already mentioned above an isolated corporate Risk Management without an adequate integration with the operational business processes running in an organisation is of little use with respect to the optimisation of the overall effect of these processes. Thus, the benefit of the results of the project for a user can be summarised as following:

- The user receives guidelines for
 - Implementing Risk Management through a provided Risk Management/Risk Assessment Framework
 - Implementing operational IT processes through provided reference models for IT service management, application development, project management and process maturity
 - Implementing an integration between Risk Management and operational processes through provided interfaces, data flow definitions as well as data and role mappings
 - Planning and executing the whole integration process through the exemplary integration process model
- The resulting user benefits are
 - Guidance along the whole implementation and integration process
 - Better quality of IT Risk Management, especially with respect to the handling of operational risks
 - Better protection against disastrous incidents, which may cause severe damage to the organisation and result from operational risks,
 - Improved line-up regarding compliance with frameworks which include regulations on corporate Risk Management (e.g. SOX, Euro-SOX, Basel II, Solvency II)
 - Overall competitive edge compared to business rivals

As already explained in section 1 main addressees of the project results are these individuals in an organisation which play a central role in the IT Risk Management implementation, integration and execution process. The exact responsibilities depend on the kind of processes which run in an organisation. In case of dealing with IT centric

processes, roles like administrator, change manager, and CIO among others, may be addressed by the project results. Generally speaking, every person who is involved in planning and monitoring processes as well as being accountable for their outcome on any level of management may be benefiting from the project documentation.

There exist other possible dimensions of integration between Risk Management and operational business processes, like e.g. integration on the level of control flows, technical interface specification for software tools etc. In specific cases it may be useful to elaborate these aspects too. However, since the aim of the project was the definition of a generic and therefore (almost) universally applicable integration framework, a specification was not considered. This working step might be subject to organisation or application specific follow-up projects.

9 References

- [1] CMMI for Development. Version 1.2, Carnegie Mellon SEI, 2006
- [2] Das BOC Rahmenwerk zum IT Service- und Architekturmanagement und seine Werkzeugunterstützung: IT-Architektur- und Servicemanagement mit ADOit[®], Whitepaper, BOC GmbH, Berlin, 2007
- [3] Kruchten, P.: The Rational Unified Process: An Introduction. Addison Wesley, Reading, 2000
- [4] Managing successful projects with PRINCE2. TSO, London, 2005
- [5] Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools. Technical Department of ENISA, Section Risk Management, www.enisa.europa.eu/rmra, 2006
- [6] Service Delivery. CD-ROM Version, Office of Government Commerce, Norwich, 2003
- [7] Security Management. Office of Government Commerce, Norwich, 1999
- [8] Service Support. CD-ROM Version, Office of Government Commerce, Norwich, 2003
- [9] Tender Specifications *Demonstrators of RM/RA in Business Processes*, ENISA, 2007