Project Report

Demonstrators of RM/RA in Business Processes

Integration of Risk Management / Risk Assessment into Business Governance

Conducted by the

Technical Department of ENISA
Section Risk Management

and

BOC Information Technology GmbH
Berlin, Germany

March 2008

Executive Summary

This deliverable documents the results of the project *Integration of Risk Management / Risk Assessment into Business Governance* (referred to hereinafter as *the Project*) which was foreseen within the ENISA Work Programme 2007. The Project contributes towards the main task of ENISA to ensure a high and effective level of network and information security within the European Union.

The main goal of this effort is to identify interfaces between the processes described in the ENISA Risk Management/Risk Assessment Framework and selected Corporate Governance Frameworks represented in form of a generic implementation process. This deliverable should provide a valuable support for organisations, which implement or plan to implement Business Governance along with an integrated IT Risk Management.

The achieved results are available in the form of an interactive model (both in HTML and as ADO*it*® process models formats) as well as the present written Report. The process models include the ENISA RM/RA Framework, selected Governance Framework requirements in form of pool models, a generic Governance Framework implementation processes with Internal Control System (ICS) and Enterprise Risk Management (ERM) processes together with the interface among these models. The Report describes briefly all elements of comprehensive Risk Management: Governance Frameworks, ICS, ERM and the ENISA IT RM/RA Framework. For theses elements interdependencies, including interfaces, are explained. Guidance for applying Project results in an organisation is also provided, along with a description of the modelling method and navigation through process models, which contains all details of the models and their interrelationships (interfaces).

The Project results should be of main interest for individuals (e.g. managers, field experts, security experts etc.) who play a significant role in the area of Corporate and IT Governance or Risk Management in general.

The presented material can be used in various scenarios by organisations. Possible benefits from the presented approach are:

- a better guidance for implementation of a comprehensive Enterprise Risk Management focusing on interfaces to IT security and IT RM/RA in particular,
- improved visibility of interrelations between different elements of Risk Management resulting in a better quality of overall system,
- a better alignment with Corporate Governance requirements and a reduced risk of not fulfilling these requirements,

- the generic process of Governance Framework implementation and pool models with requirements for selected frameworks provide a better guidance for implementation of Governance Frameworks, resulting in time and costs savings for a company and

- an overall competitive advantage 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

Table of Figures

Table of Tables

1 Introduction

This Report describes the results of the project *Integration of Risk Management / Risk Assessment into Business Governance* conducted by the European Network and Information Security Agency (see [1]) (ENISA) as foreseen in the ENISA Work Programme 2007. The achieved results go along the lines of the foremost task of ENISA, that of "ensuring a high and effective level of network and information security within the European Union as well as fostering organisational culture in that respect, thus contributing to the smooth functioning of the Internal Market" (see [5]). The following paragraph 1.1 explains the motivation, scope and aim of the Project in detail, paragraph 1.2 describes the Project approach, whereas paragraph 1.3 gives an overview of the Project Report structure.

1.1 Scope and objective of the present effort

The recent financial scandals in conjunction with the increasing complexity and internationality of business relations push regulators to introduce legislations aimed at risk reduction and strengthening the credibility of business. This trend has been most evident in the financial sector, with its high impact on the stability of economic grow and economic security of the majority of population. However, other sectors are also concerned, as within supply chain activities or sector interdependencies the requirements of Corporate Governance are imposed to other areas than the financial sector.

The aforementioned regulations touch different aspects of an organisational culture, e.g. ethics, responsibilities and risk management, to name a few. Some of the regulations have national reach, while others have international validity. In this Report all regulations considered will be referred to as *Business Governance* or *Corporate Governance* (although the scope and definition of Corporate Governance is by far wider than most of the analysed normative acts). Frameworks supporting the above-mentioned regulations will be referred to as Corporate Governance Frameworks (CGF).

As a consequence of existing Corporate Governance regulations, organisations launch different projects in order to achieve compliance. These projects might require major changes in business processes and IT services.

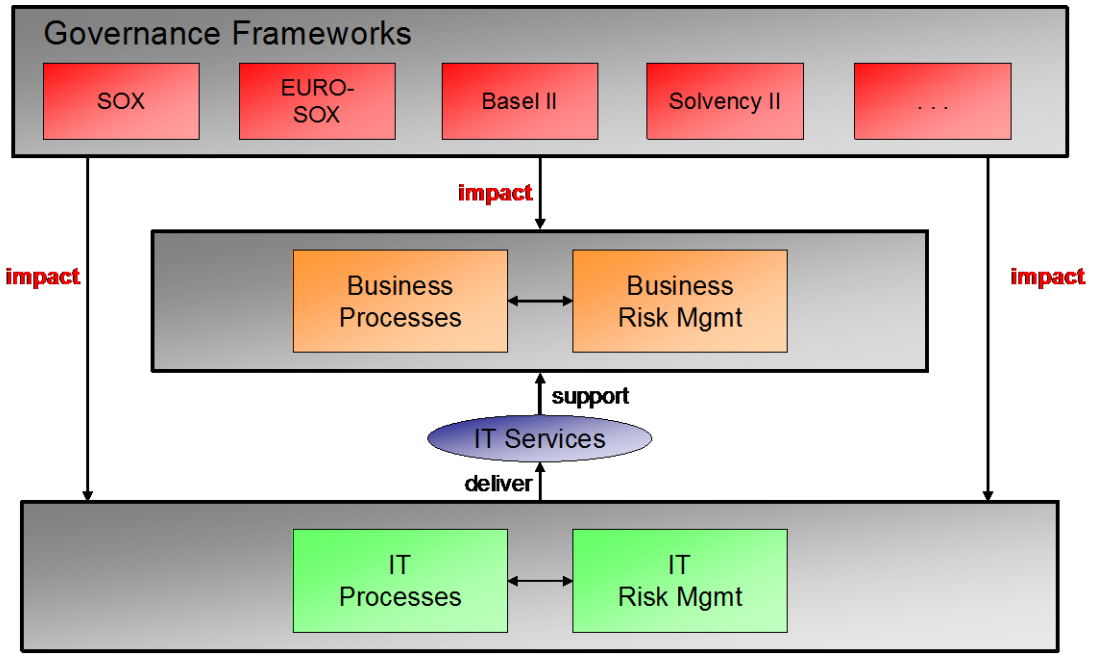

Figure 1: Schematics of Impact of Governance Frameworks on Business

Figure 1 gives a schematic overview of the role of Governance Frameworks towards business processes and IT services. The Frameworks on the top of the figure impact business processes, e.g. by regulating certain procedures and formulating requirements for Risk Management (both business Risk Management and IT Risk Management) in particular. As a matter of fact, Risk Management provides regulatory input to IT Processes, which in turn deal with delivering of IT services aiming is to support business processes.

The present effort focuses on the impact an implementation of a Governance Framework will have on IT Risk Management, as well as on the consequences IT Risk Management might have on the implementation of such frameworks.

Since Governance Frameworks deal mostly with business processes and Business Risks Management, with no direct link between IT processes and IT Risk Management, these areas are often approached separately. However, such an approach leads to general problems in implementation and execution of Governance Frameworks. The overall quality of Risk Management suffers as various aspects of risks are treated in isolation. The first step to address this problem is to identify references between actual business processes and IT processes by the way of designing a comprehensive Governance Framework implementation and execution strategy. With such a strategy it will be

possible to integrate IT RM/RA with Enterprise Risk Management and incorporate their input into business governance.

The process of integration is achieved through recognition of interfaces between IT Risk Management processes described in the ENISA RM/RA Framework and chosen Business Governance processes. The focus of the integration is mainly on the identification of corresponding data, roles and information flows between the various risk management processes. The results are available in the form of graphical process models accompanying the Report. An overview of the elaborated content is given in this Report. With the delivered information, an organisation will be able to plan the implementation of requirements placed by Governance Frameworks as well as the integration with the existing IT Risk Management approach.

This Report follows the interface concept that was developed in the ENISA project *Demonstrators of RM/RA in business processes* (see [2]).

It has to be noted that due to the limited resources the provided set of interfaces is not exhaustive. The aim of the Report is to provide a generic framework/methodology of interface definitions between Risk Management and Corporate Governance practices. Hence, in the course of the application of the Project results to a particular organisation, an adaptation phase and an extension of the delivered content has to be performed.

The delivered results provide valuable information for all managers, experts and involved personnel in areas of Business or IT Governance (e.g. Senior Management, CIO, CSO etc.), Risk Management in general (e.g. corporate Risk Manager) and project managers responsible for implementing Governance Framework regulations.

1.2 Project approach

The approach taken within this effort is summarised in the following points:

- Firstly, various Governance Frameworks were analysed. The focus was put on requirements an organisation has to fulfil in order to become compliant with the given framework. The requirements pool models for each analysed framework has been modelled.

- Secondly, the different integration approaches were analysed in respect with the Project goals and the best suitable integration with Governance Framework design and implementation process was selected.

- Consequently, the generic Governance Framework implementation process was developed.

Figure 2 presents the schematic overview of all main elements related to the Corporate Governance Framework implementation. This process can be considered at two levels: design and execution. The design level focuses at creating and updating business processes an IT services according to frameworks requirements. The execution level relates to the daily usage of the frameworks defined at the design level.

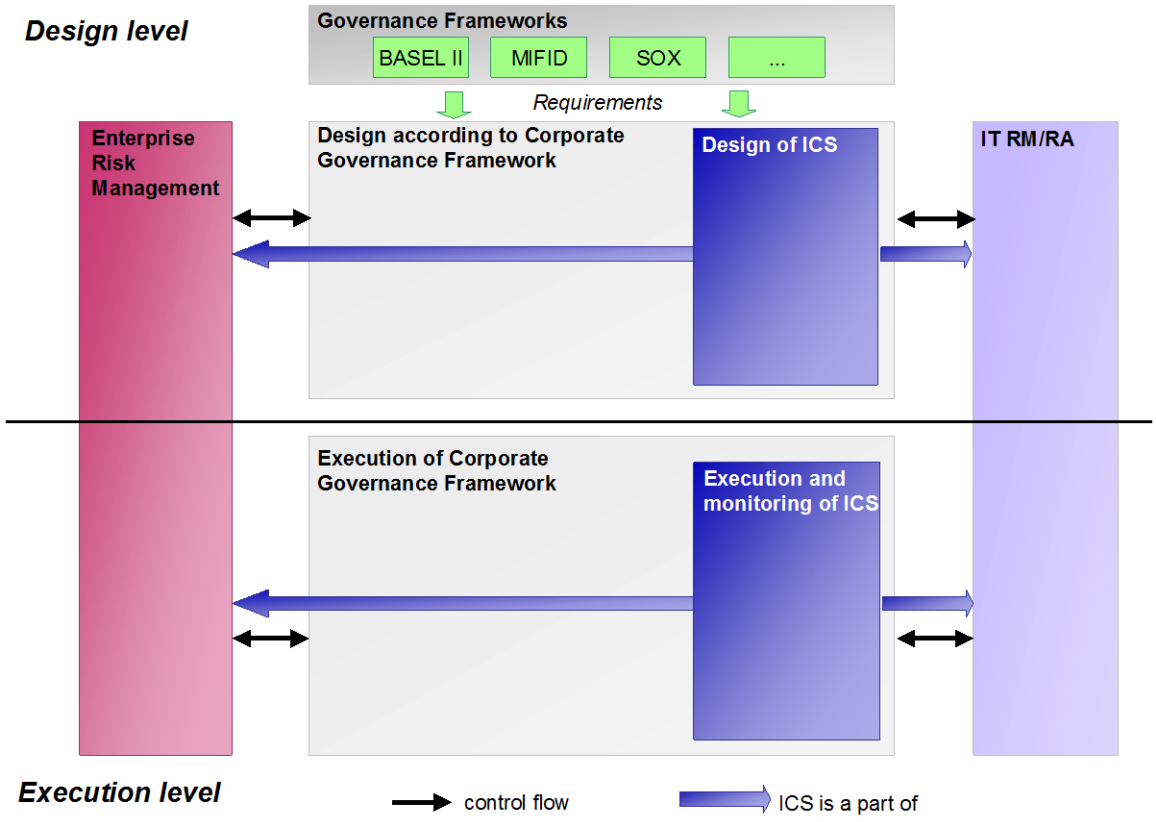

Figure 2: The main elements related to the business governance

The main components depicted in the above Figure are as follows:

- The *Internal Control System (ICS)* was identified as an important part of the generic Governance Framework implementation process. An ICS design and execution process was developed based on the COSO framework and available literature. This process was extended to include a detailed insight into the IT aspects. This approach allowed closing the gap between Business Risk Management (represented as Enterprise Risk Management, ERM) and IT Risk Management (represented as IT RM/RA).

- The Enterprise (or Business) Risk Management (ERM) part is covered by processes that were developed based on the COSO II Framework.

- The ENISA IT RM/RA Framework process structure is based on information as developed by ENISA (available for download from the ENISA web site at [3]).

- After identification of all the elements related to the design and execution of Governance Frameworks, it was possible to create interfaces between these elements and the IT RM/RA Framework. This approach is reflected in the structure of the delivered model and the Project Report as described in the next chapter.

1.3 Structure of the Report

The Project Report is structured as follows:

- Section 2 gives a short introduction of the ENISA RM/RA Framework.

- Section 3 describes different Governance Frameworks that were selected for the integration, namely Basel II, MIFID and SOX.

- Section 4 provides a description of the Internal Control System (ICS) that is associated to both Business Risk Management and IT Risk Management. This section further describes relations between ICS, ERM and IT RM/RA.

- Section 5 provides a description for different integration dimensions. A generic Governance Framework implementation process reflecting the selected approach is presented at the conceptual and process flow level.

- Section 6 describes the method used to perform the integration between the various models considered.

- The various integrated models are discussed in section 7, focusing on navigation and interpretation of the generated models.

- There are different ways Project deliverables can be of use for companies dealing with Governance Frameworks. Section 8 discusses the most significant ones.

- Appendix 1 summarises the modelling notation used in the Project deliverables.

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 on the subject of Risk Management. The following section gives a short overview of the framework, as it is essential for in-depth understanding of the Project results. Refer to [12] for further details.

Figure 3 shows a schematic overview of the framework. The covered processes may be either isolated or performed as a whole. In the latter case, the orange thick arrows accurately represent the control flow in the cycle of Risk Management processes. The most appropriate starting point for this control flow is considered to be the process *Definition of Scope and Framework*. It aims at the establishment of global parameters for Risk Management performance within an organisation. For this purpose it takes into account both internal and external aspects of the organisation.

Subsequently, a process describing activities dealing with identification, analysis and evaluation of risks is executed (*Risk Assessment*). This process is succeeded by *Risk Treatment*, which selects and implements risk-modifying measures. The goal of *Risk Acceptance* is to decide which risks are acceptable by the management responsible within the organisation. *Monitor and Review* describes a continuously ongoing process of monitoring the success in the Risk Management implementation that delivers valuable input to any future (re)definition of the corporate Risk Management. Another process included in the framework is a *Risk Communication* process, which aims at exchanging information about risk to and from all the stakeholders. In addition to the abovementioned processes interfaces to operational processes are also indicated, however with no in-depth description. This was covered by a dedicated ENISA project "*Demonstrators of RM/RA in Business Processes*" (see [2]).

A number of data elements complementing the framework as identified by ENISA, describe the exchange of information between the various Risk Management processes and their activities. The structure of the ENISA IT RM/RA Framework is depicted in Figure 3 below.

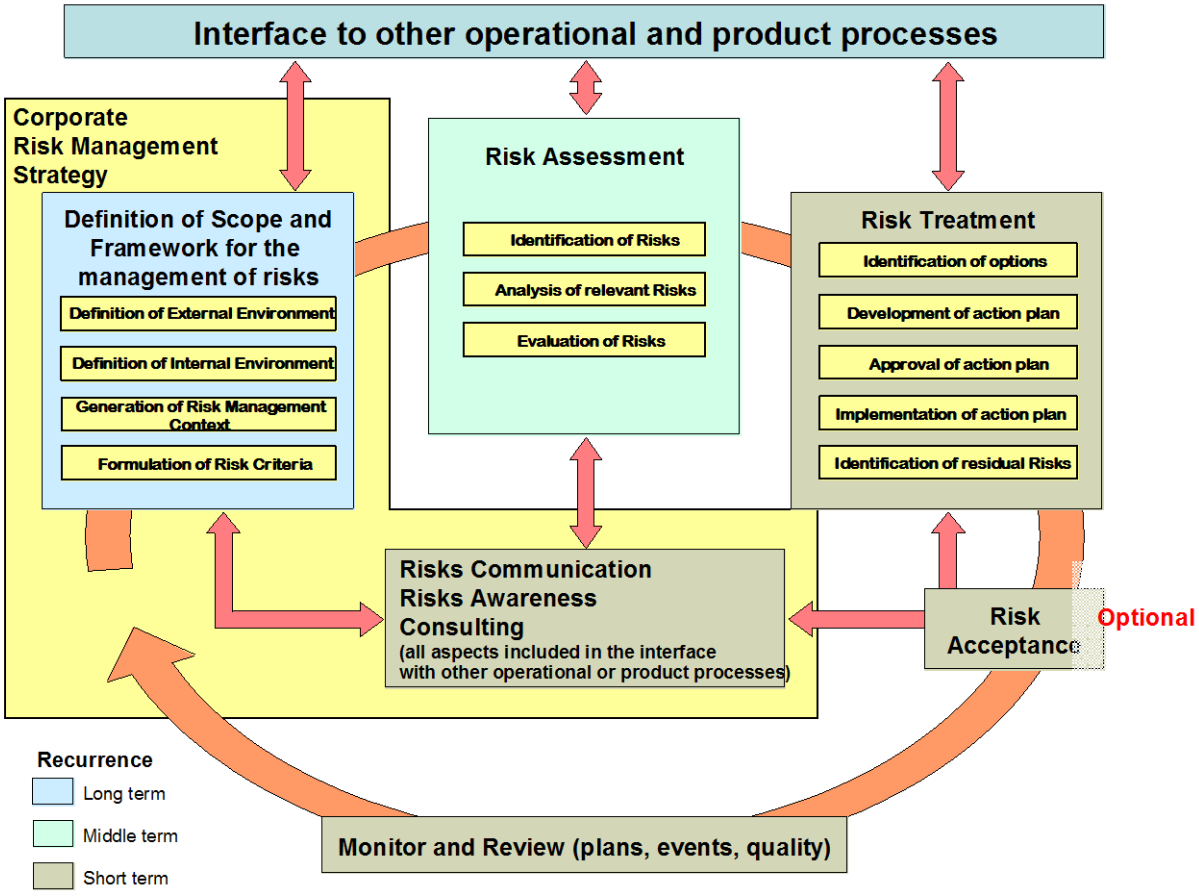

Figure 3. The Risk Management Process (from [12])

3 Governance Frameworks

This section gives a short overview of important Governance Frameworks. Firstly, various Frameworks are listed from which three were selected for further analysis. The analysed Frameworks are described in the following sections. Governance Frameworks worldwide

The demand for a more transparent way of directing corporations resulted in increased popularity of Corporate Governance also known as Business Governance.

Corporate Governance is concerned with holding the balance between economic and social goals and between individual and communal goals. The Corporate Governance Framework is there to encourage the efficient use of resources and equally to require accountability for the stewardship of those resources. The aim is to align as nearly as possible the interests of individuals, corporations and society (see [6]).

A large number of Business Governance Frameworks exist in a national and international context. They affect various geographical regions and apply to different industry sectors. There are guidelines for business governance in every country – however, not all are formulated as regulations of the governing law, some are only generally accepted norms of conduct. Furthermore, the OECD has developed its own set of principles for corporate governance. The table below contains a selection of well-known frameworks and regulations. It should be noted that some regulations, while being formally only national, have actually a much wider scope.

Name	**Description**	**Region**	**Sector**
Basel II	Introduces modifications to the way banks define risk-weighted assets. Basel II alters the basic risk equation, defined in the original Basel Accord, to include operational risk in addition to credit risk and market risk when computing requirements for reserve capital. This allows banks to reduce their overall reserve cash position set aside for credit risk by adopting a set of internal controls to reduce operational risks.	Worldwide	Bank
SOX	Standard for all publicly traded companies in the U.S. Contains 11 sections, ranging from additional Corporate Board responsibilities to criminal penalties. Covers issues such as auditor independence, corporate governance, internal control assessment, and enhanced financial disclosure. Has raised the profile and general awareness of the COBIT® framework, in particular through its application for identifying IT controls relevant to the SOX section 404.	USA	All sectors

Solvency II	Updated set of regulatory requirements for insurance firms. Based on economic principles for the measurement of assets and liabilities. Includes a risk-based system where risks are measured on consistent principles and are connected to capital requirements. Known as the insurance version of Basel II, it will come into effect in 2012.	Europe	Insurance
COSO	A U.S. private-sector initiative, which major objective is to identify the factors that cause fraudulent financial reporting and to make recommendations to reduce its incidence. Has established a common definition of internal controls, standards, and criteria against which companies and organisations can assess their control systems.	USA	All sectors
CobiT	The Control Objectives for Information and related Technology (CobiT) is a set of best practices for IT Management created by ISACA and ITGI. COBIT provides managers, auditors, and IT users with a set of generally accepted measures, indicators, processes and best practices to assist them in maximizing the benefits derived through the use of information technology and developing appropriate IT governance and control in a company. It is largely based on the control concepts of COSO.	Worldwide	All sectors
MiFID	The Markets in Financial Instruments Directive (MiFID) is a European Union law, which provides a harmonised regulatory regime for investment services across the 30 member states of the European Economic Area. The main objectives of the directive are to increase competition and consumer protection in investment services.	Europe	Financial services
European Data Protection Directive	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 formulates regulations on the protection of individuals with regard to the processing of personal data and on the free movement of such data.	Europe	All sectors
ISO/IEC 27002	ISO/IEC 27002 is an information security standard published by the ISO and the IEC as ISO/IEC 17799:2005 and subsequently renumbered ISO/IEC 27002:2005 in July 2007. It provides best practice recommendations on information security management for use by those who are responsible for initiating, implementing or maintaining Information Security Management Systems.	Worldwide	All sectors
KonTraG	The KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich - German Act on Control and Transparency in Business), aims at improving corporate governance in German companies.	Germany	All sectors

SESTA	The Federal Act on Stock Exchanges and Securities Trading is a directive intended to encourage issuers to make certain key information relating to corporate governance available to investors in an appropriate form. Applies to all issuers whose securities are listed on the SWX.	Switzerland	All sectors
TransPuG	Transparency and publicity law (TransPuG) for the reform of the share and balance legislation, which entered into force on 26 July 2002, is representing a further step in the direction of a modern European compatible enterprise legislation.	Germany	All sectors

Table 1. Evaluated Governance Frameworks

Due to the limited resources it was decided that only three most relevant Governance Frameworks will be considered within this effort, namely Basel II, MIFID and SOX. Criteria for the selection of these Frameworks were the global reach and the maturity level of their contents. Descriptions of the selected Frameworks can be found in the following three sub-sections.

Basel II is an international regulation. While SOX and MiFID were created for specific markets (respectively USA and EEA) they heavily influence companies operating outside of the said markets. All discussed frameworks have either been present and active for a reasonable time period (Basel II, SOX) or are based on previously existing regulations (MiFID) and have already multiple implementations worldwide.

It should be noted that all analysed Frameworks are business oriented. However, they also influence IT – either directly or indirectly. This aspect is of a special interest to this effort, as most interfaces to ENISA IT RM/RA Framework will exist in the area of IT.

3.1 Basel II

Basel II or *International Convergence of Capital Measurement and Capital Standards* is a set of recommendations issued by the Basel Committee on Banking Supervision (see [7]). Latest version of this standard is a comprehensive version from June 2006. It is a compilation of the June 2004 Basel II Framework, the elements of the 1988 Accord that were not revised during the Basel II process, the 1996 Amendment to the Capital Accord to Incorporate Market Risks, and the November 2005 paper on Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework.

The purpose of Basel II is to create an international standard that banking regulators can use when creating regulations about how much capital banks need to put aside to guard against the types of financial and operational risks banks face.

The goals of Basel II are:

- Ensuring that capital allocation reflects level of risk
- Separating operational risk from credit risk, and quantifying both
- Attempting to align economic and regulatory capital more closely to reduce the scope for regulatory arbitrage

Figure 4 depicts the scope of application of this framework. It shows that Basel II can be applied both at a level of banking group (1) and at lower levels (2, 3, 4).

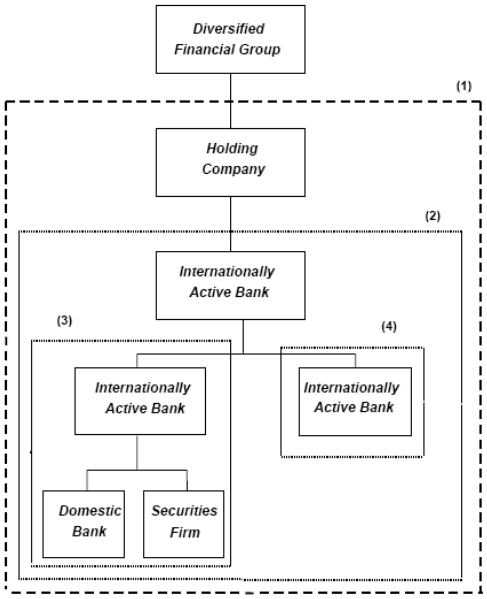

Figure 4: Scope of application of Basel II framework (source: www.bis.org)

Basel II approach is based on three so-called *pillars*:

1. Minimum Capital Requirements
2. Supervisory Review Process
3. Market Discipline

The first pillar relates to calculating capital necessary for a given level of risks. Considered types of risks are: credit risk, operational risk and market risk. The first pillar

provides several approaches for risk calculation, so that a bank can choose which technique shall be used.

The second pillar defines how the supervisory review should be organised in order to guarantee that internal processes and controls are properly implemented. It also covers risk types not present in the first pillar.

The third pillar refers to disclosures that are required from banks in order to provide the general public with information concerning the implementation of this framework.

The influence of implementing Basel II on IT mainly relates to the security of operations. Focus areas are:

- Preventing improper disclosure of information
- Preventing execution of unauthorised transactions as well as providing means of transmission that will not allow neither modifications nor access to confidential data
- Preventing system outage and unauthorised changes in the system that would compromise existing security measures

It should be noted that banks implement country specific regulations based on Basel II rather than Basel II itself.

Practice has shown that financial institutions use Basel II requirements/methods when rating their customers. Hence, although Basel II originally concerns financial institutions, it has high relevance for all kinds of sectors either for rating credit risks or by means of supply chains.

3.2 MiFID

MiFID or *Markets in Financial Instruments Directive* is a European Union law, which provides a regulatory regime for investment services. It came into effect on November 2007 thus replacing the Investment Services Directive (see [8]).

The goals of MiFID are:

- Increasing transparency
- Providing protection for retail consumers
- Increasing competition in investment services

This framework is mostly relevant for companies offering investment services that operate within the European Economic Area (EEA).

MiFID focuses on following areas:

- Avoiding conflict of interest
- Providing customers with necessary information in a timely manner
- Best execution of the customer orders
- Ensuring compliance

Avoiding conflict of interest refers to creating rules aimed at preventing conflicts of interest that could adversely affect customers.

Providing customer with necessary information in a timely manner embraces transparency of information about costs, risk warnings and customer categorisation (retail, professional, eligible counterparties). For each category suitable procedures should be implemented.

Best execution of the customer orders aims to guarantee that each customer is offered the best possible product, according to the client category and other relevant factors. Important part of *best execution* is providing client with the best attainable price.

Ensuring compliance focuses on creating a system that guarantees conformance with MiFID obligations including internal audit, Enterprise Risk Management and compliance functions. It also covers outsourcing in order to guarantee that important processes will not be handled outside the EEA without agreement of authority.

The influence of MiFID implementations on IT mainly relates to performance, extended analytics and storage. Focus areas are:

- Processing of client and market data in a timely manner
- Analytics that ensure *best execution* of orders
- Analysis of risks and conflicts of interest
- Recording trading data and storing them
- Providing additional types of reports

MiFID needs to be implemented on a country level but it should be noted that "Maximum harmonisation" does not allow states to change regulations in a way that would harm competition. This practice - also known as "gold-plating" - refers to exceeding requirements of the European Community directives while incorporating them into local law in a way that may limit competitiveness of a certain groups of companies.

3.3 SOX

The Sarbanes-Oxley Act of 2002 (SOX) or *Public Company Accounting Reform and Investor Protection Act of 2002* is a United States federal law for boards and management of US public companies as well as accounting companies enacted on July 30, 2002 (see [9]).

The purpose of SOX is to prevent corporate scandals and rebuild the trust of the general public towards the stock markets.

Goals of SOX are:

- Ensuring independence of auditors and preventing conflict of interest
- Increasing transparency by providing additional financial disclosures
- Creating an environment which supports corporate responsibility

This framework influences US public companies and their auditors. Its reach is however wider since US-listed companies that are subject to SOX often control companies outside of the US. In addition some countries created their own versions of SOX (e.g. Japan).

SOX consists of 11 titles divided into more detailed sections as indicated below:

1. Public Company Accounting Oversight Board
2. Auditor Independence
3. Corporate Responsibility
4. Enhanced Financial Disclosures
5. Analyst Conflicts Of Interest
6. Commission Resources And Authority

7. Studies And Reports
8. Corporate And Criminal Fraud Accountability
9. White-Collar Crime Penalty Enhancements
10. Corporate Tax Returns
11. Corporate Fraud And Accountability

Most often referred to sections are 302 and 404.

Section 302 (*Corporate responsibility for financial reports*) describes a set of procedures that guarantee the quality of financial disclosures.

Section 404 (*Management assessment of internal controls*) requires the evaluation of internal controls and risks by management board.

The influences of implementing SOX on IT mainly relates to data integrity and support for audits. Focus areas are:

- Confidentiality of information
- Ensuring integrity of data and its availability to entitled entities
- Audits and logging of events
- Change management

There are several frameworks supporting SOX implementation. The most popular Internal Control System framework is COSO – described more in-depth in Section 4.

4 Description of the Internal Control System

The previous chapter contained descriptions of the most relevant Governance Frameworks for this Project. All of them demand – more or less explicit – the existence of additional controls that allow monitoring whether goals of an organisation are being met or not. More detailed information concerning those requirements can be found in section 4.3.

In order to guarantee that all controls will be deployed and maintained properly, organisation needs to move from ad-hoc activities to a planned implementation and monitoring system. This system is known as Internal Control System – ICS.

The Internal Control Systems is a tool that supports attaining objectives of an organisation An Internal Control System is defined by COSO (Committee of Sponsoring Organisations of the Treadway Commission) (see [10]) as *a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:*

- *Effectiveness and efficiency of operations.*
- *Reliability of financial reporting.*
- *Compliance with applicable laws and regulations.*

It should be noted that most Governance Frameworks utilises an ICS because of the need to measure and control selected aspects of organisation processes. An implementation of a Governance Framework requires a (re)design of the ICS since new controls need to be added. After implementation the established ICS controls are used at the execution level for monitoring of running business processes.

As with Governance Frameworks, several models for Internal Control System exist. One of the most complete and extensive model that is widely used is COSO's Internal Control Integrated Framework (see [10]). It consists of five components:

- Control Environment
- Risk Assessment
- Control Activities
- Information and Communication and

- Monitoring

Elements of COSO ICS are often depicted in the form of a cube – shown at Figure 5.

Figure 5: COSO ICS (see [10])

This Project focuses on integration at the level of a Governance Framework implementation. Since that implementation is described as a set of processes it was necessary to present ICS also in the form of process models. In order to provide suitable coverage and avoid a business-IT gap, it was decided that the business oriented COSO ICS has to be extended to include IT aspects and selected elements of COSO ERM (described below).

4.1 The Internal Control System and ERM

The COSO Internal Control System has been extended by a publication from September 2004 that expanded the existing model with an Enterprise Risk Management method (see [10]). COSO ERM consists of the following components

- Internal Environment
- Objective Setting
- Event Identification
- Risk Assessment
- Risk Response
- Control Activities

- Information and Communication
- Monitoring

As with COSO ICS, the elements of COSO ERM are also often described in the form of a cube – shown at Figure 6. The ERM cube is more complex than the ICS cube, but some common elements can be found.

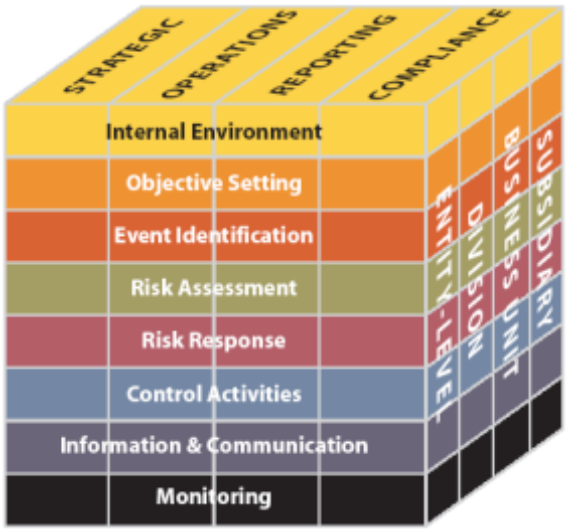

Figure 6: Elements of COSO ERM

As the ERM represents business risk management, a mission critical aspect for every organisation, it was included in the models describing processes of Governance Framework implementation. For this purpose COSO ERM was selected.

Figure 7 shows elements of the COSO ERM process model. They are present both at the design level and execution level (where the monitoring takes place). It should be noted that information and communication is present at both levels: at the design level it deals with the development of a communication system, while at the execution level it provides additional information (like for example providing employees with actionable information).

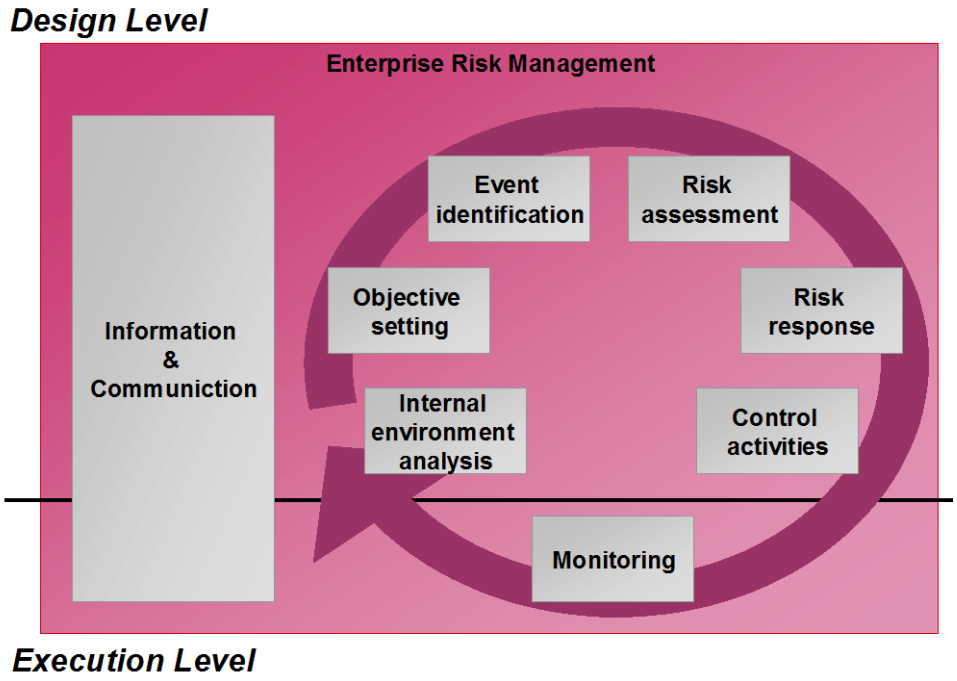

Figure 7: Overview of the ERM process

4.2 Internal Control System in Business Governance life cycle

The implementation of Business Governance is not a one-time event but a continuous activity aiming at the systematic improvement of alignment/compliance with Corporate Governance requirements. The continuous improvement activity of Business Governance embraces all components of Governance Frameworks including ICS, ERM and IT RM/RA at both the design and execution levels. Figure 8 presents a schematic overview of the Business Governance life cycle.

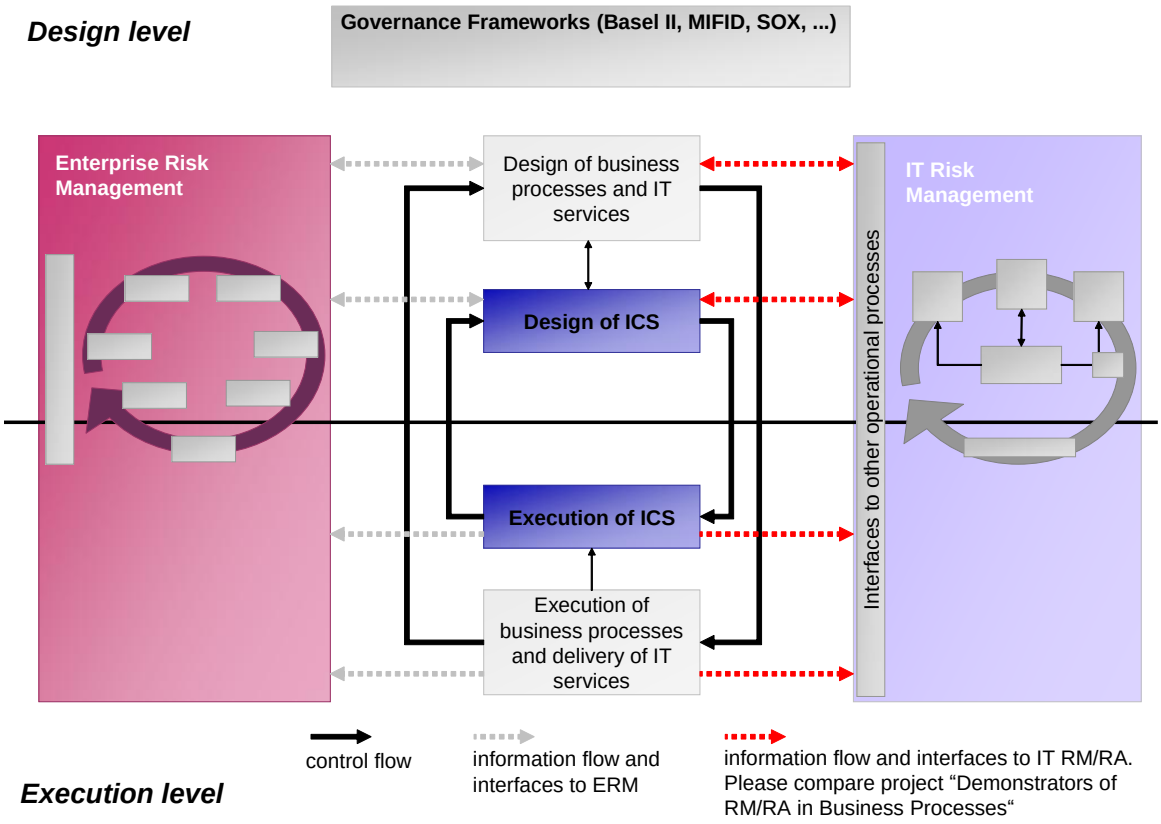

Figure 8: Business Governance life cycle

Following the main elements of a Business Governance life cycle have been identified:

- Cycle of business process and IT services (light-gray objects). Triggered by Governance Frameworks requirements, different business processes and IT services are modified and implemented. These processes are executed and IT services are delivered in the execution phase. As a result of requirements modifications (e.g. new law) or changes in the company (new products, new markets, etc), an adaptation of processes and IT services might be necessary again.

- The ICS (blue objects) has its own cycle. It is designed to control alignment with Governance Framework regulations but it also controls other aspects (e.g. conformity with national law, etc). Therefore it is expected that in the design phase the ICS will rather be adapted and extended to meet Business Governance requirements instead of creating a new ICS. In the execution phase, different

aspects of the company are monitored. As a result, ICS could be adapted (e.g. to improve measurement system).

- Figure 9 presents a detailed life cycle of the ICS. It should be noted that the *Information and communication* component is present at both levels and enables the communication between design and execution

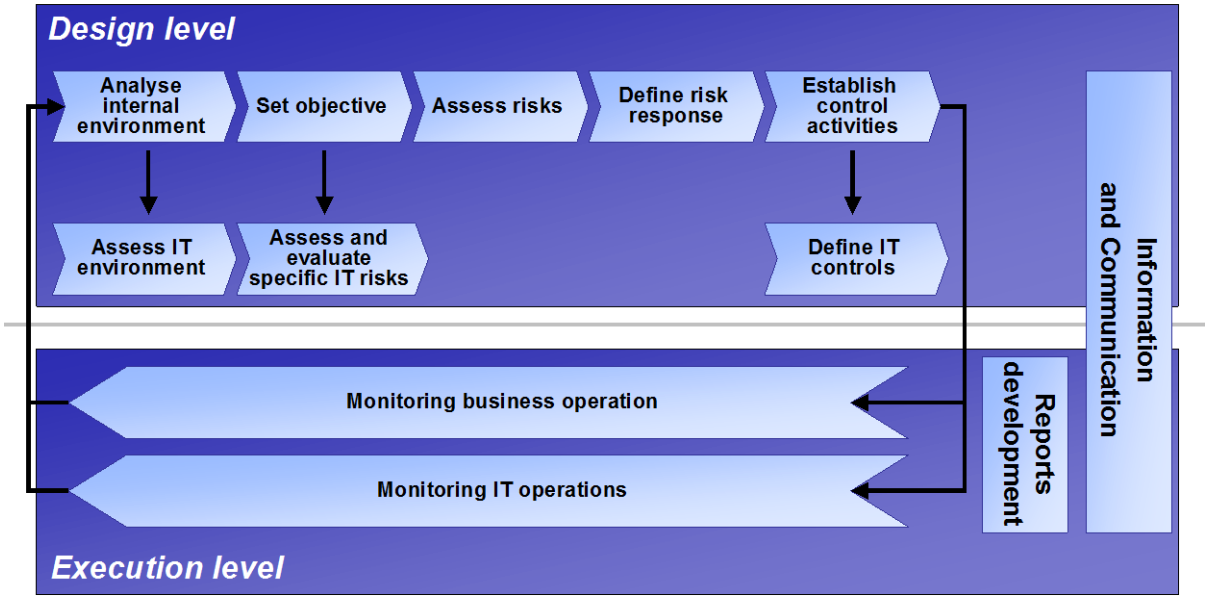

Figure 9: Internal Control System life cycle

- Enterprise Risk Management also follows the cycle described in detail in section 4.1. There is an information flow between ERM and design and execution of business process, IT services and ICS (represented by grey arrows). These interfaces are out of scope in the Project. However, some ERM processes are identical with ICS processes, which are represented in process documentation using the references between these processes.

- The IT RM/RA Framework cycle is described in section 2. The red arrows show the information flow between Governance Framework processes and IT RM/RA Framework. These are the interfaces representing integration of these two elements. The interfaces are built based on the same concept as in the other ENISA project *Demonstrators of RM/RA in business processes* (see [2]).

4.3 The ICS in the considered Governance Frameworks

4.3.1 SOX

The establishment and maintenance of the Internal Control System is covered in section 404 of SOX.

Section 404: Management Assessment of Internal controls

- *the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting*
- *an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting*

In 2003 the COSO framework was defined as an accepted standard by the SEC. Usage of COSO in SOX is depicted in Figure 10. Due to the popularity of COSO it was selected as a candidate for further works within the Project.

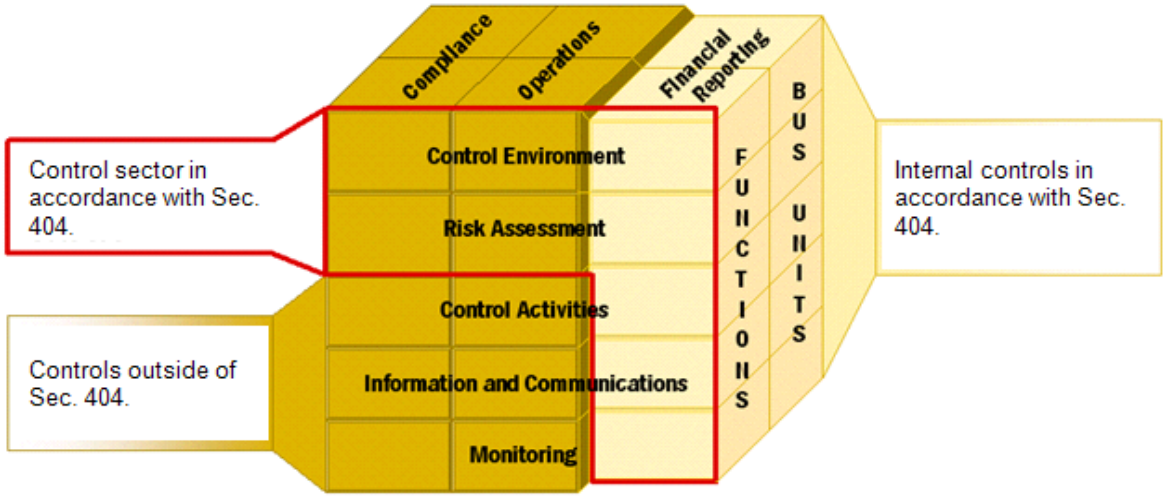

Figure 10: COSO ICS used in SOX

4.3.2 Basel II

Basel II contains principles for the assessment of internal control systems. Those 13 principles are classified into six categories:

- Management oversight and the control culture
- Risk Recognition and Assessment
- Control Activities and Segregation of Duties
- Information and communication
- Monitoring Activities and Correcting Deficiencies
- Evaluation of Internal Control Systems by Supervisory Authorities

According to Basel II the Internal Control System consists of five interrelated elements, which can be easily mapped to the COSO framework. This mapping is shown at Figure 11.

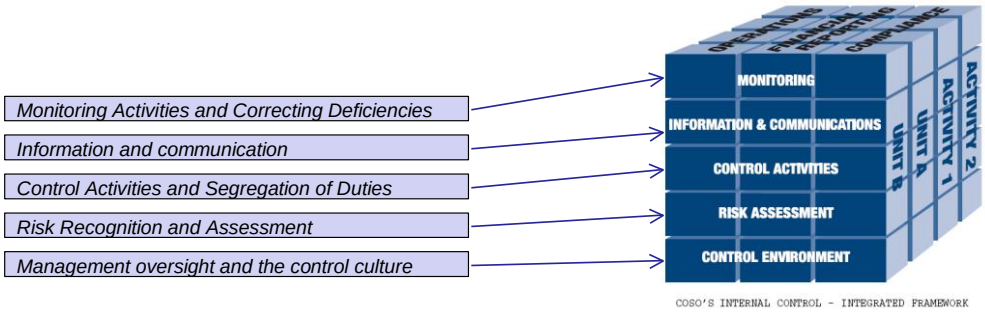

Figure 11: Mapping of Basel II controls to COSO

4.3.3 MIFID

MiFID does not explicitly describe how an ICS should look like. However it is clearly stated that an ICS is necessary.

TITLE II AUTHORISATION AND OPERATING CONDITIONS FOR INVESTMENT FIRMS; CHAPTER I CONDITIONS AND PROCEDURES FOR AUTHORISATION

Article 13, Paragraph 5

An investment firm shall have sound administrative and accounting procedures, internal control mechanisms, effective procedures for risk assessment, and effective control and safeguard arrangements for information processing systems.

5 Integration overview

5.1 Integration dimension

For the selected Governance Frameworks and the ENISA IT Risk Management, various possible dimensions of integration exist. These incorporate e.g.:

1. Integration of operational IT processes, which are regulated by the Governance Frameworks with IT Risk Management
2. Integration of Governance Frameworks requirements with IT Risk Management
3. Integration of Governance Frameworks implementation process and IT Risk Management

The above integration options may not be fully exhaustive, but represent the distinct choices. Figure 12 presents a scheme, which summarises these integration approaches.

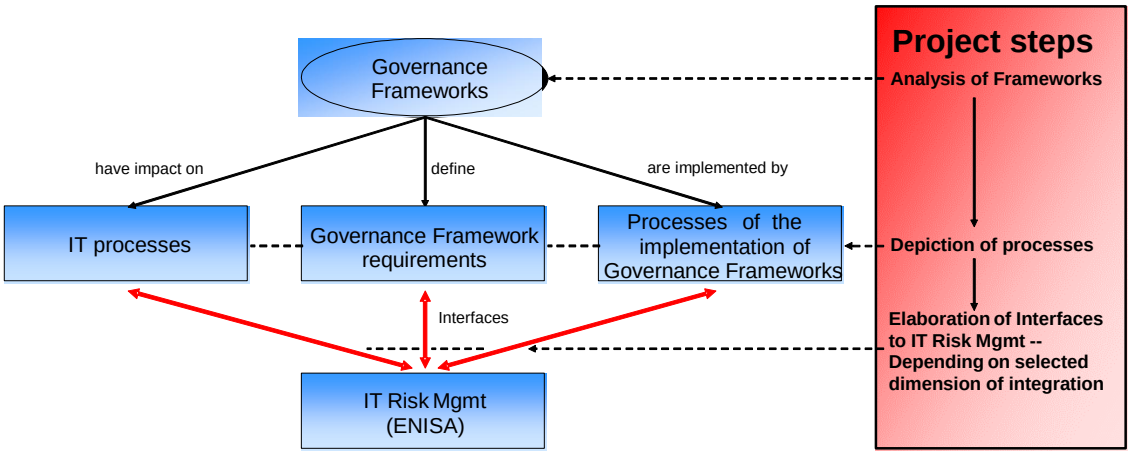

Figure 12: Possible integration approaches in the Project

The first option describes a situation when an operational IT process is being completely redesigned during the course of implementation of a Governance Framework. As a result, the final IT process is significantly different from the organisation's usual IT processes. This dimension remains out of scope of this Project, because:

- A number of wide-spread best practice IT frameworks exist (e.g. ITIL, CobiT). These frameworks regulate IT processes - mostly with respect to compliance to Governance Frameworks. In addition, Business Governance rarely defines direct requirements for IT processes (some examples can be found in MIFID).

Therefore, there is no need to modify or use other IT processes as these described in the best practice IT frameworks.

- The integration of IT operational processes and IT Risk Management was already presented in the other ENISA project "*Demonstrators of RM/RA in business processes"* (see [2]).

The second option suggests a direct integration of Governance Framework requirements with the IT Risk Management. This approach is also out of scope because of following reasons:

- Each Governance Framework has its specifics reflected by numerous requirements. These requirements can be implemented in a variety of ways, depending on country, branch, etc. In addition, some Governance Frameworks requirements must be adapted to the country's specific law, which again multiplies the number of possible integration variants. Therefore, this kind of integration would provide very little added value for a specific company.

- Fulfilling Governance Framework requirements means not only introducing them, but also e.g. monitoring. Therefore, more comprehensive process is required, which will include design and execution of organisation's processes and IT with regard to Governance Framework requirements.

The third option is the integration of IT Risk Management with the processes defined for the implementation of Governance Frameworks in an enterprise. The main advantages of this integration approach are:

- The implementation process could by split into design and execution phase. In that way IT Risk Management is included in the early phase.

- The implementation process is provided in a generic form, therefore can be useful for enterprises representing different branches, operating in different countries, and environments.

- The specific Governance Framework requirements (in this case Basel II, MIFID and SOX) can be included in Project results by creating links from the activities in the implementation process to these requirements

Taking the abovementioned factors into consideration, it was decided that the third option, i.e. integration of IT Risk Management with the Governance Framework implementation process, fits the best to meet the overall Project goals.

5.2 Governance Framework implementation process

For the selected integration approach, a generic Governance Framework implementation process was developed. However, it should be noted that before using Project results in specific implementation, this process should be refined for the selected organisation or implementation scenario (please refer to Section 8). This includes especially all aspects related to project management, like e.g. assigning a project manager, building a project team, etc. These aspects were not included in the generic Governance Framework implementation process as they depend from the selected project methodology (e.g. PRINCE2).

This section describes the main elements of the Governance Framework implementation process as well as the interfaces with the ERM and IT RM/RA. The Governance Framework implementation process is split into design and execution phase. For each phase both conceptual overview as well as process flow view is described. This structure is reflected in the next four sections (from 5.2.1 to 5.2.4). The detailed process can be found in the HTML process documentation.

5.2.1 Implementation of Business Governance - design level (conceptual)

The main elements of the Governance Framework implementation process were already presented in

Figure 2.

Figure 13 presents a more detailed version of the Design level:

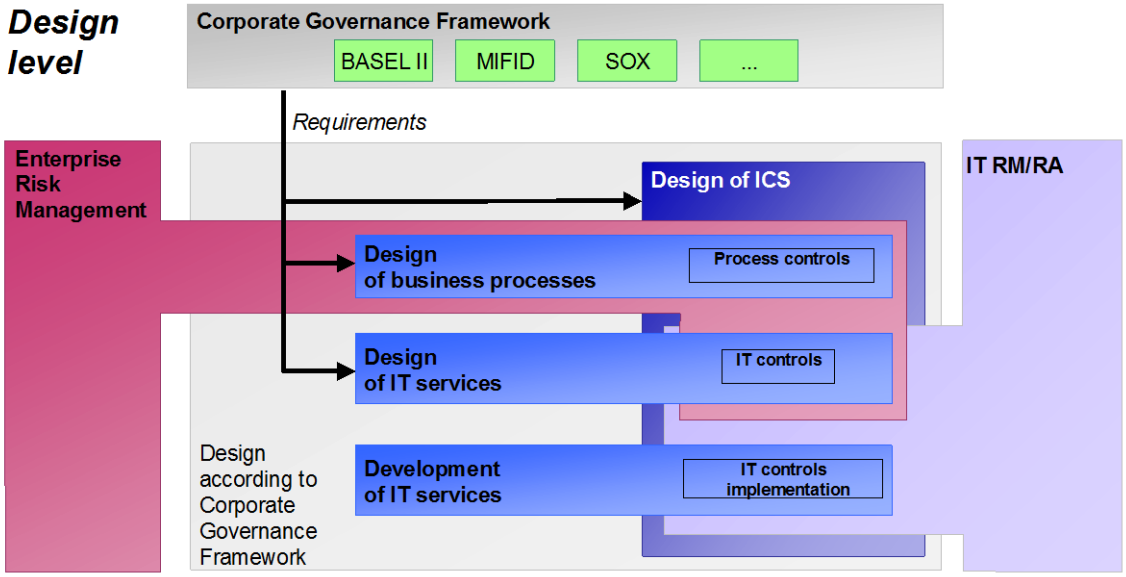

Figure 13: Implementation of a CGF - design level (conceptual)

At the Design level, various Governance Frameworks regulations influence the following aspects, also depicted in the above figure:

- *Design of business process*. Requirements of Governance Framework translate into necessary changes in business processes, e.g. financial processes, HR processes, etc.

- *Design of IT services*. IT services have to be designed according to Governance Frameworks requirements. As a matter of fact, the definition of an IT service covers different elements of an IT environment, including applications, and IT infrastructure. Figure 14 gives an overview of the elements of IT services. This structure will be used in this Report when referring to IT services.

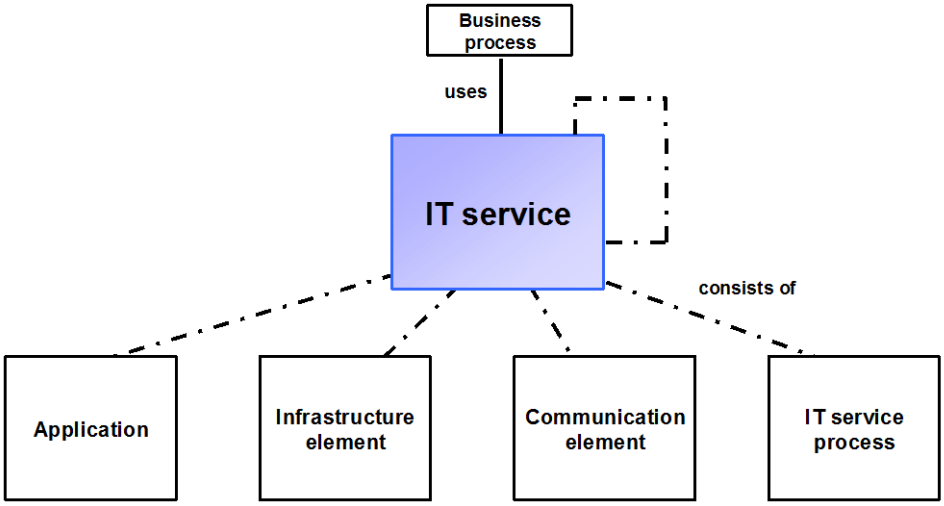

Figure 14: Elements of an IT service (see [11])

In most cases Governance Framework requirements affect directly business processes, which, as a consequence, formulate requirements on IT services (e.g. reporting, more analytics, better storage etc.). However, in some Governance Frameworks, direct requirements regarding IT services can be found, for instance, in MIFID[1]. The black arrow on

Figure 13 represents the direct impact of Governance Framework requirements on business processes and IT services.

- Eventually, requirements regarding IT services have to be implemented. This process is represented as a *Development of IT services*.
- *Design of the ICS* (as already described in section 4)

The structure of the ICS is also presented in more details:

[1] For example Article 3, point 2, in the document 2006/73/EC defines direct requirements regarding accessibility of a web page if such a web page provides information for customers.

- *(Business) process controls* are designed in order to guarantee correctness and compliance of business processes with Governance Frameworks. A request for process controls can arise:
    - Directly from Governance Frameworks requirements
    - From the ICS
    - From ERM
- *IT controls* are automated controls where design could be triggered by:
    - Changes in IT services (as a result of direct or indirect requirements from Governance Frameworks),
    - Extension of the ICS (e.g. to support business process controls or to directly monitor IT services)
    - Requirements from IT RM/RA
- Eventually, *IT controls are implemented* by the means of configuring or developing an IT service

Enterprise Risk Management deals primarily with business process controls and to some extend with IT controls (area on the left side of the graphics). IT RM/RA focuses on risks related with the design and implementation of IT services (area on the right side of the graphics). The integration of Business Governance and IT RM/RA is provided for these processes (area on the right side of the graphics).

5.2.2 Implementation of Business Governance - design level (process flow)

Figure 15 presents in an abstract form the components of the delivered process models for the generic Governance Framework implementation at the Design level. The structure of the figure follows that of Figure 13 and the contents are available in form of a model that is part of this deliverable.

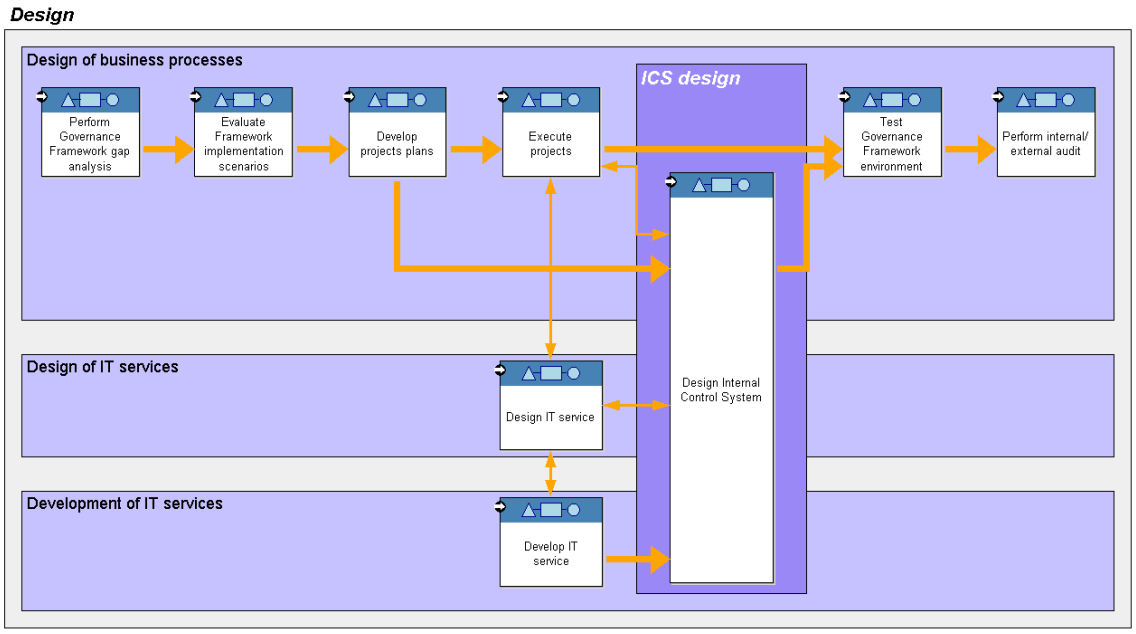

Figure 15: Governance framework process at the design level - abstract from HTML process documentation (process flow)

The following processes were identified:

- *Perform Governance Framework gap analysis* – in this process gaps between processes, IT services and organisational structure and Governance Frameworks requirements are determined.

- *Evaluate (Governance) Framework implementation scenarios* – various scenarios can result both from different variants in Governance Framework requirements (e.g. BASEL II requirements regarding the measurement of operational risks) as well as different implementation approaches the particular company could select for the same requirement. These scenarios are evaluated in this process.

- *Develop project plans* – Governance Framework requirements affect different areas of company and may run within smaller, dedicated implementation efforts (e.g. small projects). Plans for these projects (including analysis of dependencies) are developed in this step.

- *Execute projects* – projects described in the previous step are executed here. If the change in IT service is required, the process moves to the *Design IT service* and consequently to the process *Develop IT service*.

- *Design Internal Control System* - in parallel to *Develop project plans*, the Internal Control System is designed. For the detailed description of the ICS design and execution process, please refer to section 4.

- *Test Governance Framework environment* – after implementation of Governance Framework requirements, the modified processes and IT services should be tested.

- *Perform internal/external audit* – the audit checks the alignment of a company with Framework requirements. Depending on Governance Framework, the audit can be performed by an external institution or using the company's internal resources.

For process details please refer to HTML documentation (navigation details can be found in the section 7)

5.2.3 Implementation of Business Governance - Execution level (conceptual)

Figure 16 presents a detailed version of the Execution level:

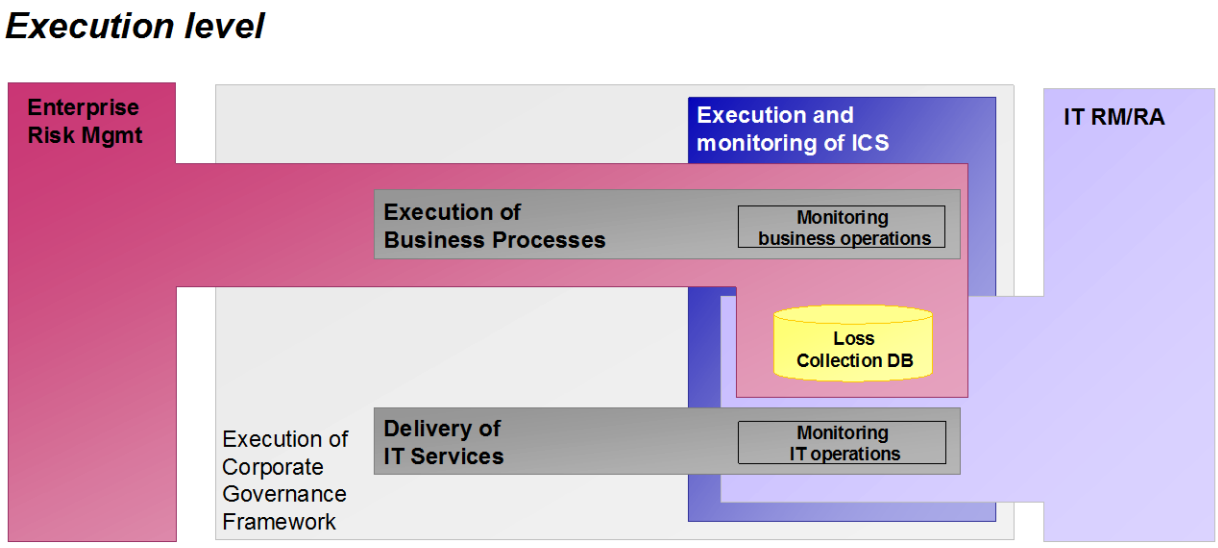

Figure 16: Implementation of a CGF - execution level

At the Execution level, the following elements were identified:

- *Execution of business processes*. The processes considered here are, for instance, Monitoring of changes in Governance Framework regulations or Managing Changes (entering new markets, introducing new products, etc.).

- *Delivery of IT services*. Processes in this area are not provided as it was assumed that these processes are regulated by other frameworks (e.g. ITIL, CobiT).

The contents of the ICS execution are as follows:

- *Monitoring business operations*. This process deals with monitoring, collection of data and reporting of business risks.

- *The Loss Collection DB* is a common element of both ERM and IT RM/RA. It is used to collect event details regarding Risk Management. Although many frameworks do not explicitly require Loss Collection, it is assumed that companies should still gather information on potential events (using data base, spreadsheets, text notes, etc.) for proper risk management.

- *Monitoring of IT operations*. This is the *Monitoring* process from the IT RM/RA framework.

Enterprise Risk Management covers the area of business process monitoring whereas IT RM/RA focuses on monitoring of IT operations. The integration of Business Governance and IT RM/RA is provided for these processes (see area marked violet).

5.2.4 Implementation of Business Governance - Execution level (process flow)

Figure 17 presents in an abstract from the components of the delivered process models for the generic Governance Framework implementation at the execution level. The structure of the figure follows that of Figure 16 and the contents are available in form of a model that is part of this deliverable.

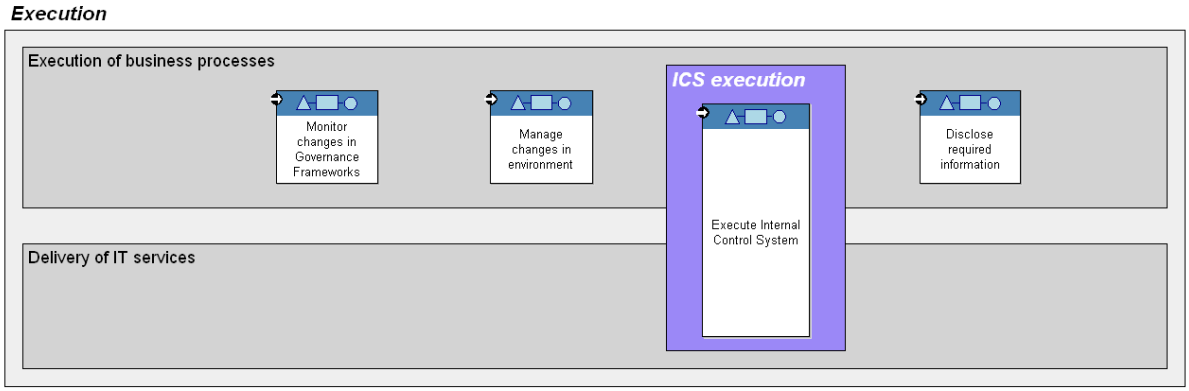

Figure 17: Governance framework process at the execution level - abstract from HTML process documentation (process flow)

The following processes were identified:

- *Monitor changes in Governance Frameworks* –this process it is checks if Governance Frameworks regulations changed or new best practice information are available. If yes, it triggers the design phase.

- *Manage changes* – major changes within the internal or external environment (e.g. entering new markets, introducing new products, etc.) might also trigger the design phase. These changes are monitored here.

- *Execute Internal Control System* - For the detailed description of ICS design and execution process, please refer to section 4.

For process details please refer to HTML documentation (navigation details can be found in the section 7)

6 The Integration Method

The method that 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 generic Governance Framework process, including ICS and ERM process
3. Modelling of the interfaces between the Processes

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

6.1 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 ADO*it*®. 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 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 against 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.

6.2 Modelling of the Corporate Governance Framework implementation process

The Governance Framework implementation process was modelled in the same way as the ENISA IT RM/RA Framework. Firstly, the processes themselves, including the control flows, were determined. Secondly, 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. Governance Frameworks provide very little information on roles. For purpose of the generic Governance Framework implementation process the roles were depicted basing on the available literature and BOC experience (RACI notation). Therefore it is advisable to adapt roles to the specific customer's implementation scenario. Looking at the name of the swimlane can also identify responsible roles.

6.3 Modelling of the interfaces between the processes

In the first step of integration, the activities of the Governance Framework implementation process, 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 34 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 18 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 that is used in the receiving activity to store the incoming information.

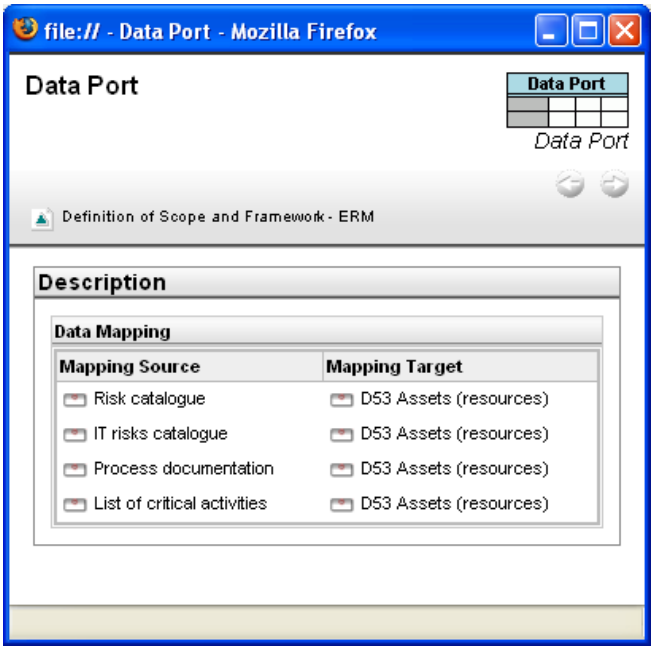

Figure 18: Mapping of Data Elements

At this point, the integration process was completed. The results of this procedure are presented in section 7.

7 The Project Results: ADO*it*® Models

The results of this Project are documented in the form of this Project Report as well as the ADO*it*® models showing the integration of the processes. The ADO*it*® 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 ADO*it*® 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 ADO*it*® is necessary.

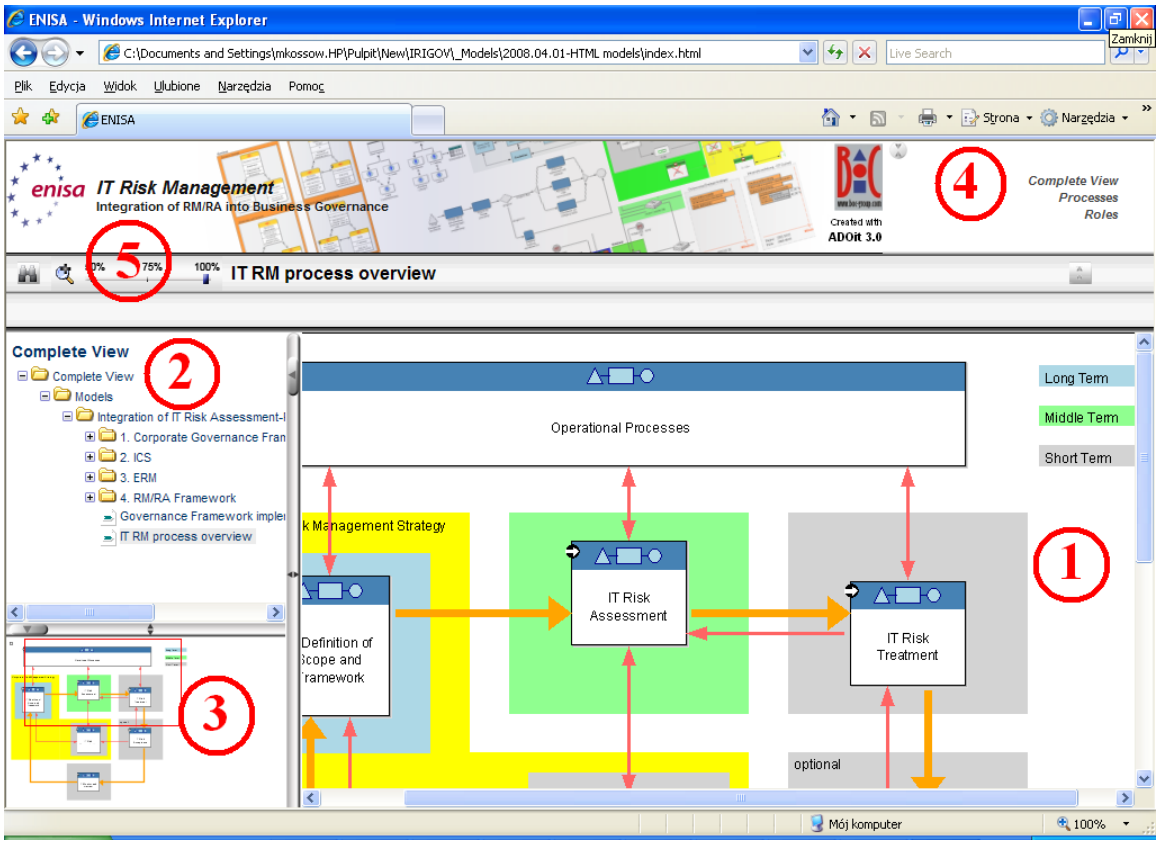

Figure 19: Browser window with a model

Figure 19 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*). 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. 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 scanning for certain model elements.

The following paragraph 7.1 shows how the models can be navigated.

7.1 Navigation through the models

Navigation through the models is designed to be straightforward. 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 20, *Details* for the properties, *Risk Acceptance* for navigating to the respective process).

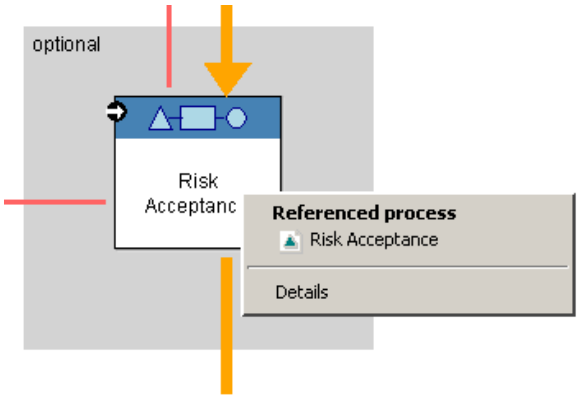

Figure 20: Example for context sensitive menu

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 7.1.5 and 7.1.6. This kind of navigation can be applied to all models, which were created in the course of the Project.

7.1.5 Exemplary Navigation through a Risk Management process

The first possible path is depicted in Figure 21. This example shows a way through the model hierarchy to the ICS process *Define IT controls* and Governance Framework requirements, which relate to this process.

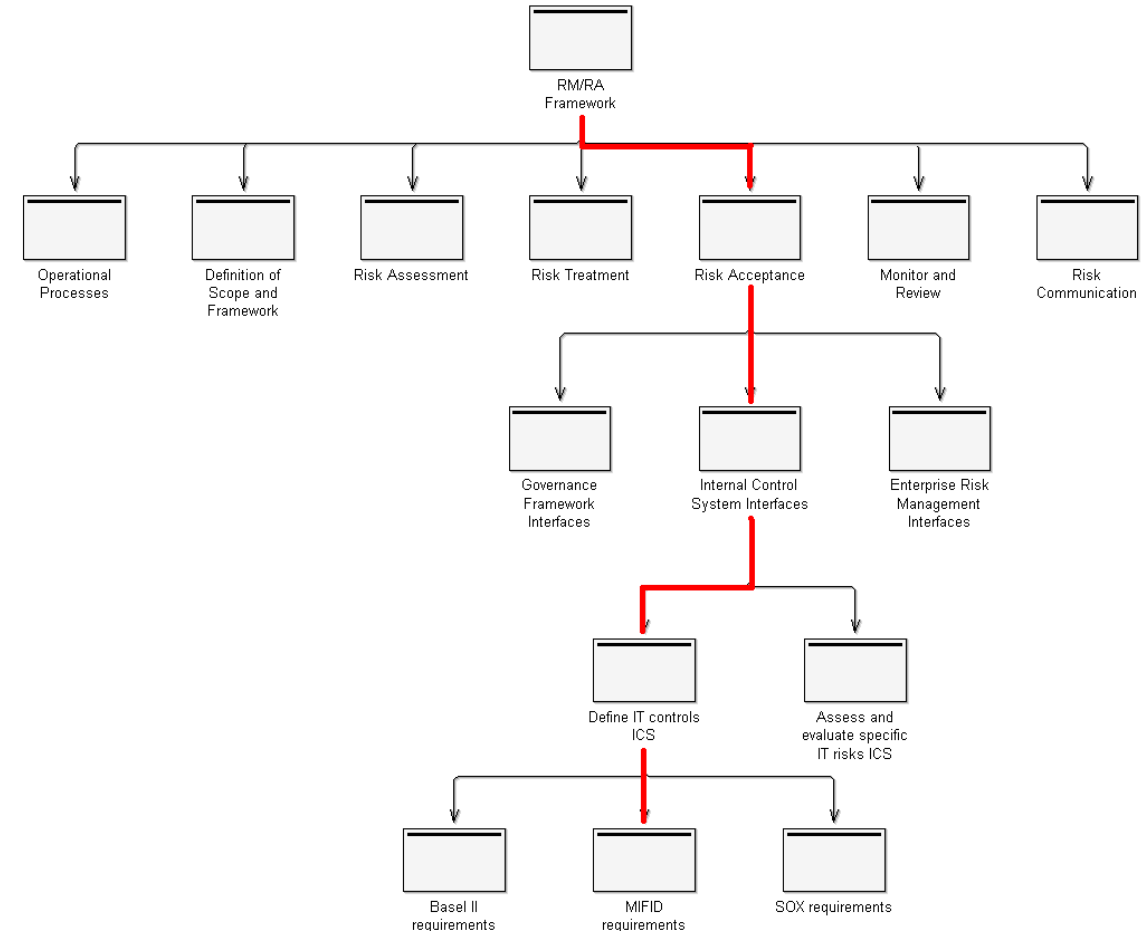

Figure 21: Navigational path through models – Example 1

On the framework level a Risk Management process can be selected at will. In the following example this is *Risk Acceptance* (see Figure 22).

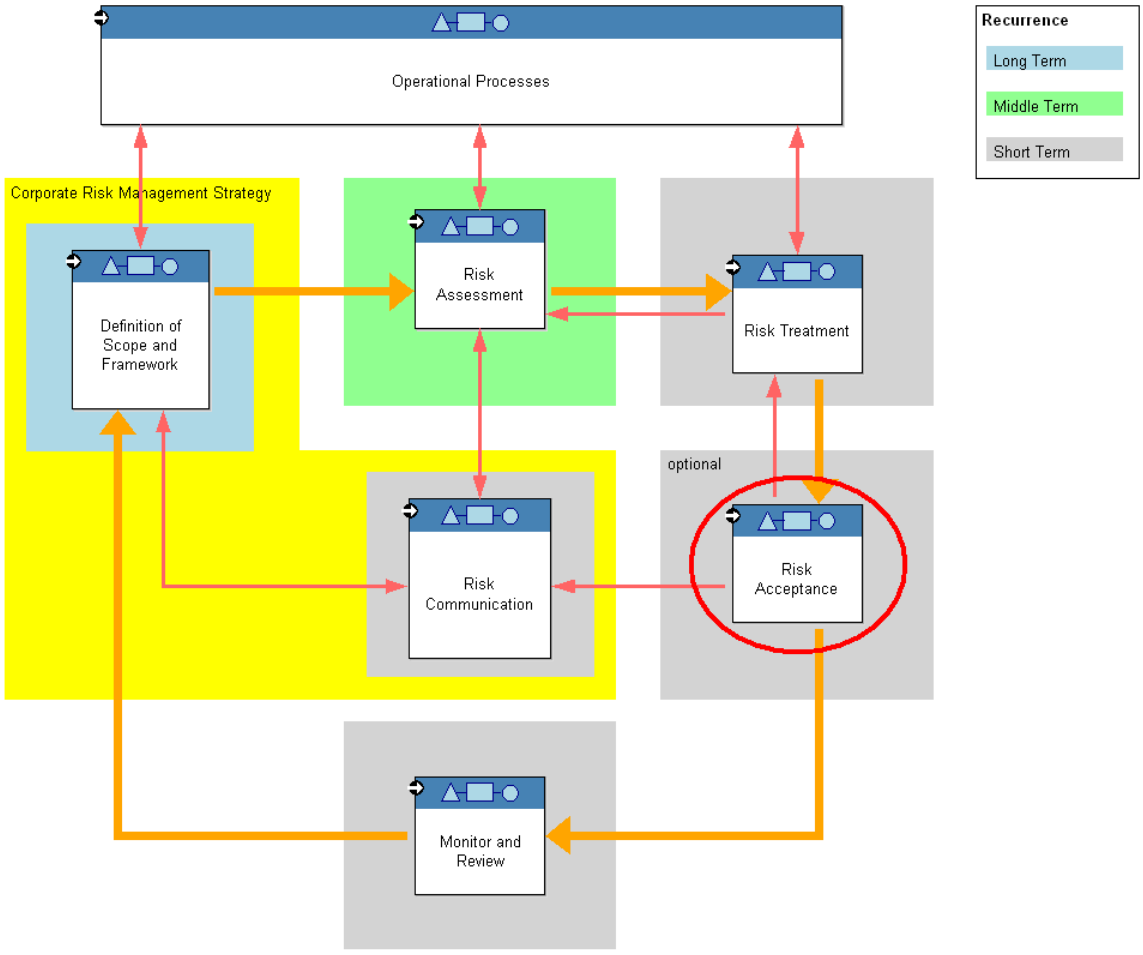

Figure 22: RM/RA Framework Overview – Example 1

In this diagram on the lower side the operational processes are listed which provide interfaces to Risk Acceptance (see Figure 23). In the following example, the process ICS is being selected.

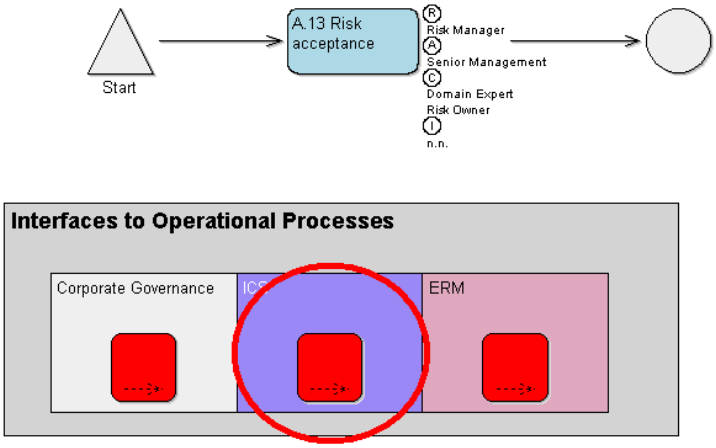

Figure 23: Risk Acceptance process

As a result the Risk Acceptance process is displayed with jointly various interfaces to ICS (see Figure 24).

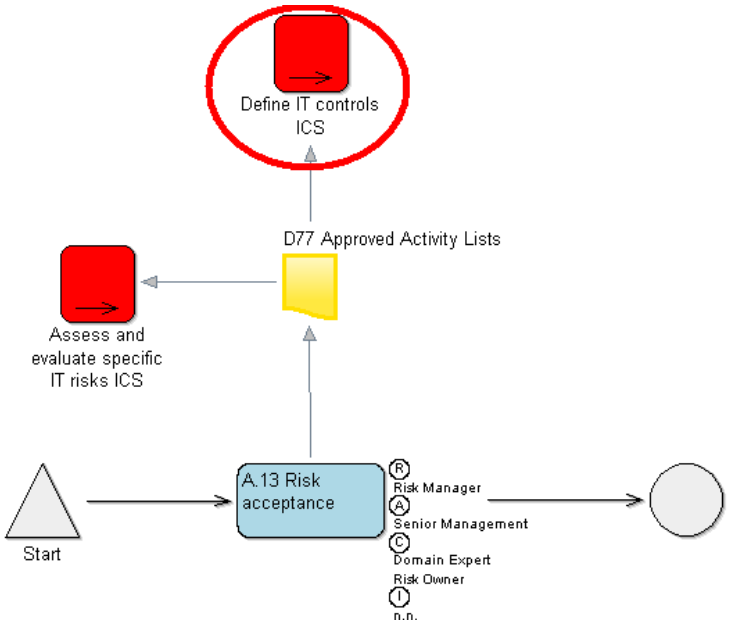

Figure 24: Risk Acceptance process with interfaces to ICS

After choosing the respective interface (upper left side), the model seen in Figure 25 is displayed, which represents the ICS *Define IT controls* including the interfaces to Risk Management.

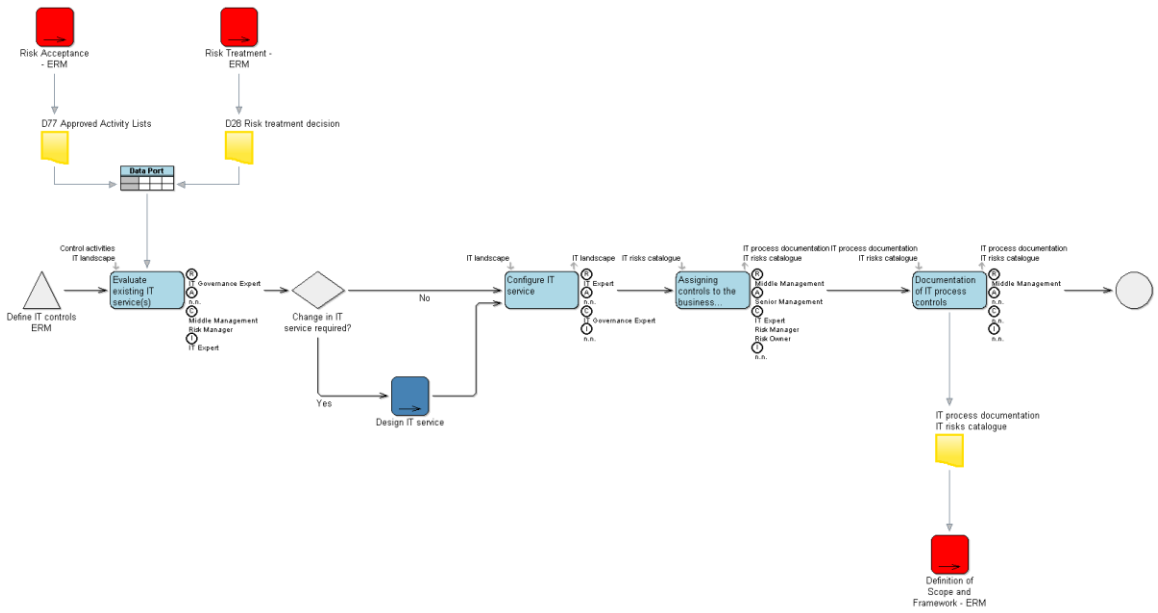

Figure 25: Define IT controls ICS

For the detailed process level it is possible to navigate to Governance Framework requirements. After clicking on an activity, its details (properties) will be displayed. These details contain information on which Governance Framework requirements should be considered in this activity (see Figure 26).

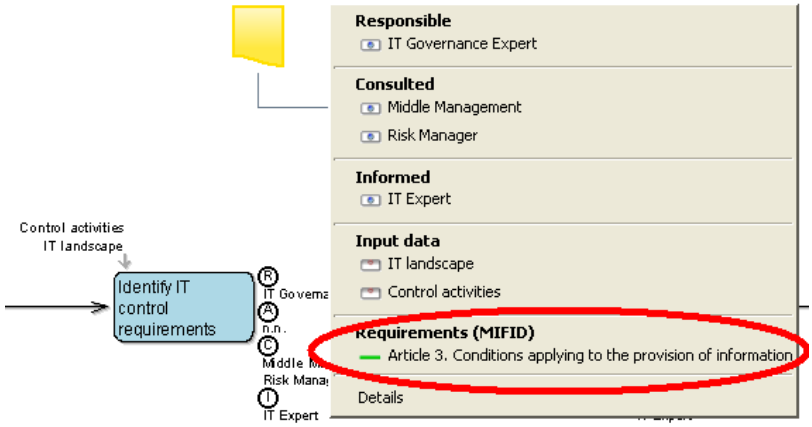

Figure 26: Properties of an activity object

After clicking on the desired requirement, the separate window with the requirement details will open. From that window it is possible to navigate to the pool model with all requirements defined for this Governance Framework.

7.1.6 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 27.

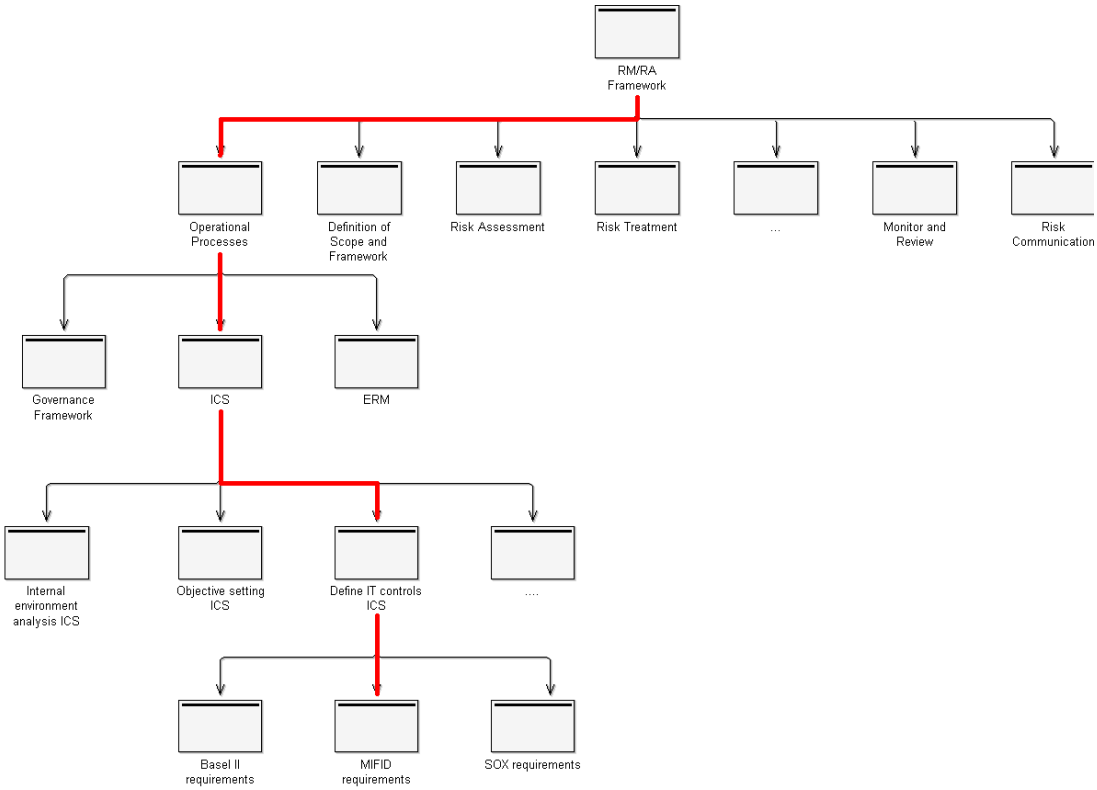

Figure 27: Navigational Path through Models - Example 2

On the framework level the process object *Operational Processes* was selected (see Figure 28).

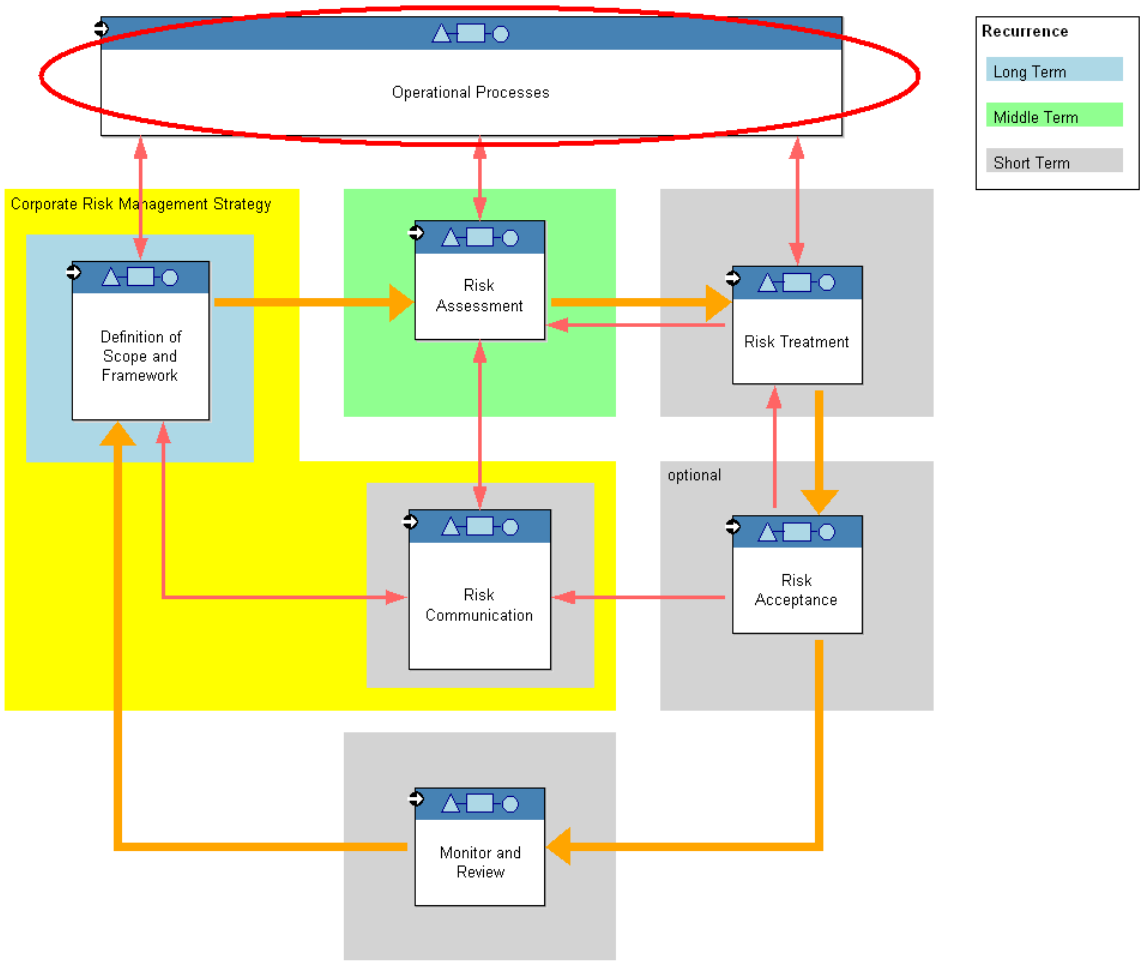

Figure 28: RM/RA Framework Overview - Example 2

After this, the desired operational process can be chosen (in the following example of ICS, see Figure 29).

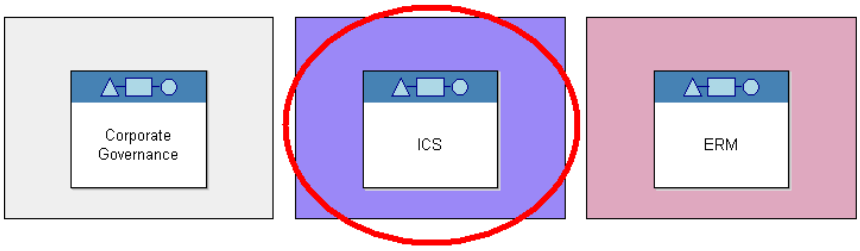

Figure 29: Selection of Operational IT Processes

The model showing the Business Governance overview in Figure 30 can be used to switch to the various sub-processes. The example assumes that *Define IT controls* has been selected which results in displaying the same model as in the example of the first navigational path (see Figure 25).

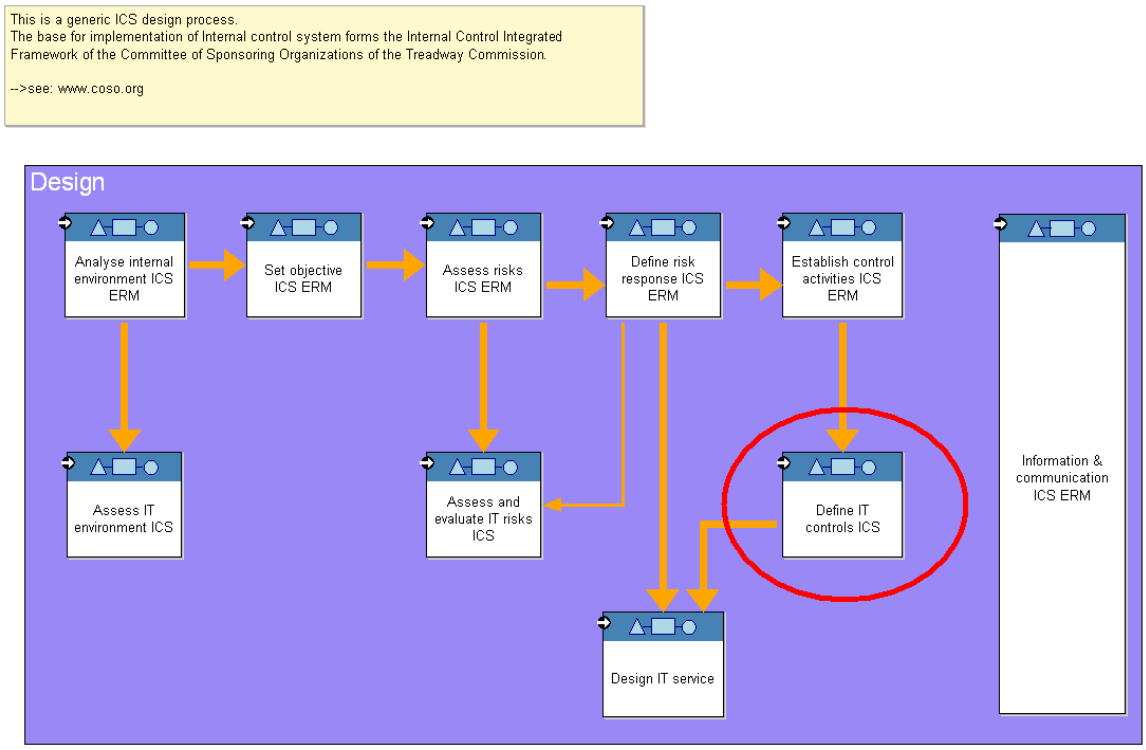

Figure 30: ICS Overview

8 Application of results

Generic approach towards implementing governance framework can be used both by companies implementing their first framework, that need guidance in creating ICS, and by companies adding a new framework to a set of already implemented ones.

The first scenario provides companies with guidance in the area of how to implement Governance Frameworks. Access to reference models and predefined list of requirements allow faster implementations and better errors avoidance.

Proposed approach can be applied in the second scenario, thus providing companies with a tool for quick identification of necessary steps for aligning internal processes and controls with the new framework, as well as with a generic process that can be used for next implementations, thus reducing demand for external experts.

Three important elements can be distinguished within enterprise from the point of view of risk management:

1. Implemented Governance Frameworks and their supportive internal control system

2. Enterprise Risk Management

3. IT Risk Management

Various combinations of the elements mentioned above can exist within organisations. The company can have a Governance Framework (e.g. SOX) implemented together with an ICS but lack IT Risk Management. On the other hand it is also possible for a company to decide to use ERM and IT RM/RA despite the fact that no external regulations (frameworks) force it to manage risks and use internal controls.

Since the focus of this Project is on linking Governance Frameworks and internal control system with IT RM/RA it was decided that describing the implementation of ERM and IT RM/RA is out of scope. In the course of future analysis it will be assumed that the company implemented both ERM and IT RM/RA.

Analysis of interfaces between Governance Frameworks (supported by Internal Control System) and IT RM/RA can be based on two factors: existence of (implemented) Governance Framework and plans concerning implementation of further frameworks. Possible scenarios are shown in Figure 31.

	Planned scenario	
Current situation	Implementation of new framework	Adaptation of existing system
Implemented corporate governance framework	A	B
No corporate governance framework	C	X

Figure 31: Application scenarios

Three scenarios – shown in the figure above as A, B, and C will be described more in-depth in the next paragraphs. Option marked with X is irrelevant as it depicts a situation of a company that does not have Governance Framework implemented and does not plan to implement one.

First scenario (A) describes the situation of a company which already implemented a Governance Framework that plans to further implement new ones. It may be a case of a European bank (compliant with Basel II) that is taken over by US based bank (and thus needing added compliance to SOX standards).

For this scenario the approach developed within the Project greatly facilitates the process of implementation, as the company only needs to compare the requirements of the new framework (pools of requirements for three frameworks are available) with the list of already implemented requirements. The difference serves as an input for further steps of the generic implementation process. The usage of a generic process guarantees, that proper communication with IT RM/RA takes place, thus improving chances of overall success.

The second scenario (B) describes a situation of a company which already implemented a Governance Framework that wants to enhance its existing system. It may be a case of a company adherent to SOX standards that strives for a guarantee that its IT risks will not be overlooked.

For this scenario the proposed approach provides guidelines for design of a Governance Framework and internal control system that can be used in the next planned redesign.

Should the company want to make sure that most critical internal controls do not lack input from IT, a redesign of selected areas can take place ahead of normal schedule in order to provide links to IT RM/RA.

The third scenario (C) describes a situation of a company without an implemented Governance Framework that plans to implement one. It may be the case of a European company from the financial services sector required to achieve compliance with MiFID regulations.

In this case the provided approach allows a faster implementation, thanks to a pre-arranged pool of requirements and generic processes. Those two elements provide guidance and good practice examples, thus reducing demand for external framework experts that would translate legal documents into specific steps required in the particular company.

More detailed information about pools of requirements and generic process is available in the Project documentation in the form of ADO*it*® processes.

Figure 32 illustrates the three scenarios mentioned and shows their entry points to generic process (part: gap analysis).

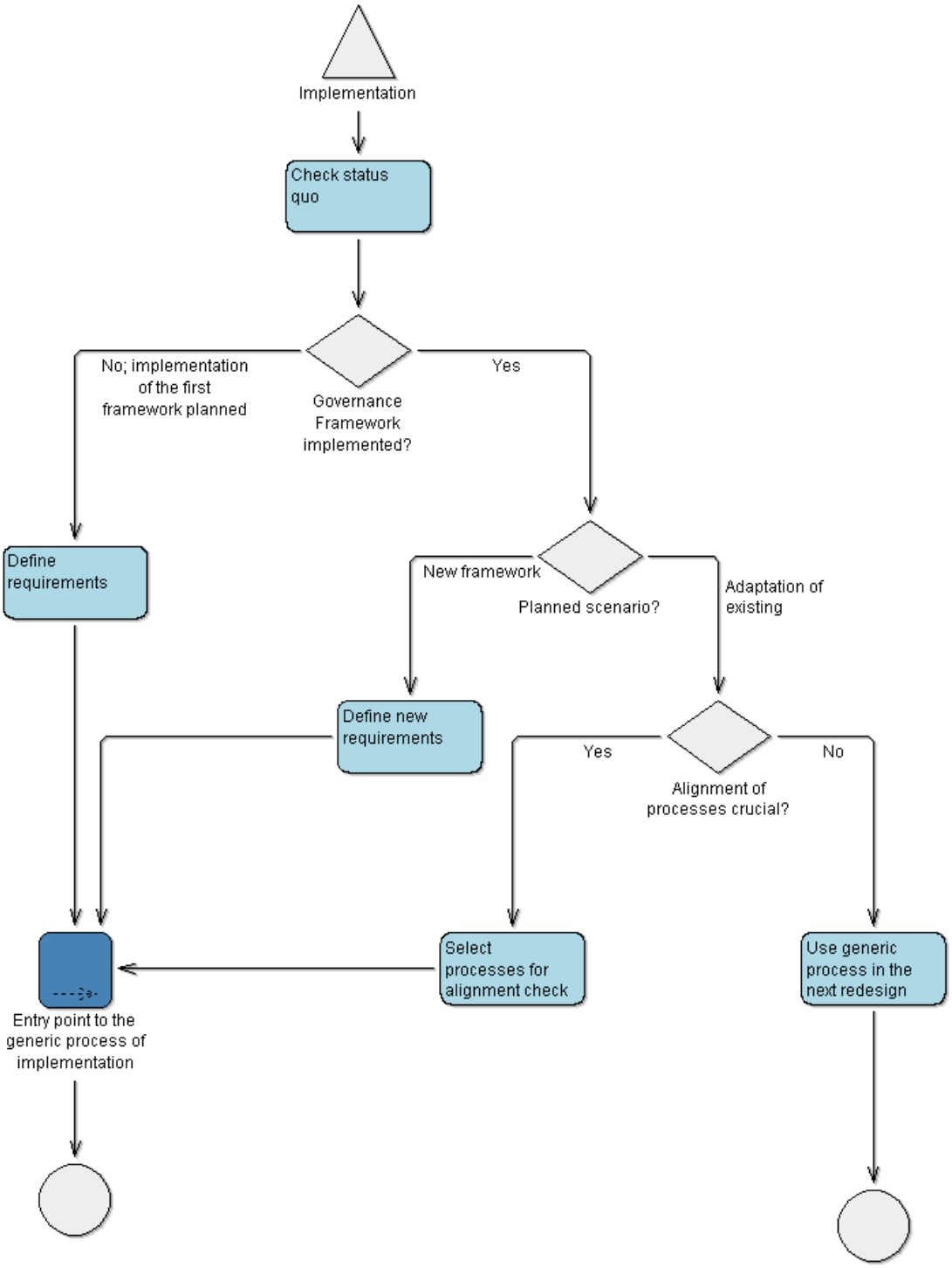

Figure 32: Usage scenarios

9 Expected Benefit

Companies applying Project results for its own purposes can expect a variety of benefits:

- The main Project goal was to identify interfaces between Business Governance and IT RM/RA Framework. These interfaces should allow companies to close the gap between business and IT Risk Management by providing a better guidance for implementation of a comprehensive Risk Management with the focus on the IT RM/RA,

- In addition the Project result can be further used as a base method for identification of such interfaces and data mapping in similar projects, where different elements of a company (business processes, IT services, business and IT risk management) are involved.

- Moreover, the use of this approach greatly improves overall visibility of interrelations between ERM, IT RM/RA and Governance Frameworks, thus simplifying managing risks and translating strategy into action. It also guarantees that designed Internal Control System will be based on inputs from IT RM/RA, thus improving overall quality and reducing possibility that IT-related risks are overlooked. This is of great importance as in some frameworks wrong fulfilment of governance requirements might result in severe penalties.

Apart from these main goals, some additional and very valuable benefits can be expected:

- Availability of the generic process of Governance Framework implementation. Implementing Governance Framework requires time, money and access to experts that can translate legal requirements of Corporate Governance Frameworks into specific steps for a particular company. The generic process can be used as an alternative to this *traditional* approach. It provides company with step-by-step guidance for the implementation of an arbitrary Governance Framework. Reference models contain information about particular phases and steps, used documents and roles therefore providing good practices examples and reducing probability of errors during the implementation process.

- Available list of requirements for most popular Governance Frameworks (Basel II, SOX, MiFID) in form of pool models. The predefined list of requirements allow much faster gap analysis since it is very easy to identify at which level of Governance Framework implementation which requirements are involved. In addition if a company plans to implement more than one framework, the common requirements can be identified easily saving time and money for the same or overlapping projects.

10 References

[1] http://www.enisa.europa.eu

[2] *Demonstrators of RM/RA in business processes*, ENISA, 2007

[3] http://www.enisa.europa.eu/rmra/files/rm_framework.zip

[4] http://www.boc-group.com

[5] Tender Specifications *Integration of IT Risk Assessment/Risk Management into business governance*, ENISA, 2007

[6] Sir Adrian Cadbury in *Global Corporate Governance Forum*, World Bank, 2000

[7] Source: *International Convergence of Capital Measurement and Capital Standards: A Revised Framework - Comprehensive Version*; http://www.bis.org/publ/bcbs128.htm

[8] Sources: http://ec.europa.eu/internal_market/securities/isd/mifid_en.htm; http://www.fsa.gov.uk/Pages/About/What/International/EU/fsap/mifid/index.shtml;

[9] Sources: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ204.107

http://thecaq.aicpa.org/Resources/Sarbanes+Oxley/

[10] Source: http://www.coso.org/publications/executive_summary_integrated_framework.htm

[11] *Das BOC Rahmenwerk zum IT Service - und Architekturmanagement und seine Werkzeugunterstützung: IT-Architektur- und Servicemanagement mit ADOit®*, Whitepaper, BOC GmbH, Berlin, 2007

[12] Risk Management / Risk Assessment, http://www.enisa.europa.eu/rmra, ENISA, 07-February-08

11 Appendix I - 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.

11.1 The Modelling Tool ADOit 3.0®

ADO*it*® 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 [4]). 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. ADO*it*® is available in several languages (e.g. English and German). Figure 33 shows a screenshot, which presents the graphical user interface of ADO*it*®.

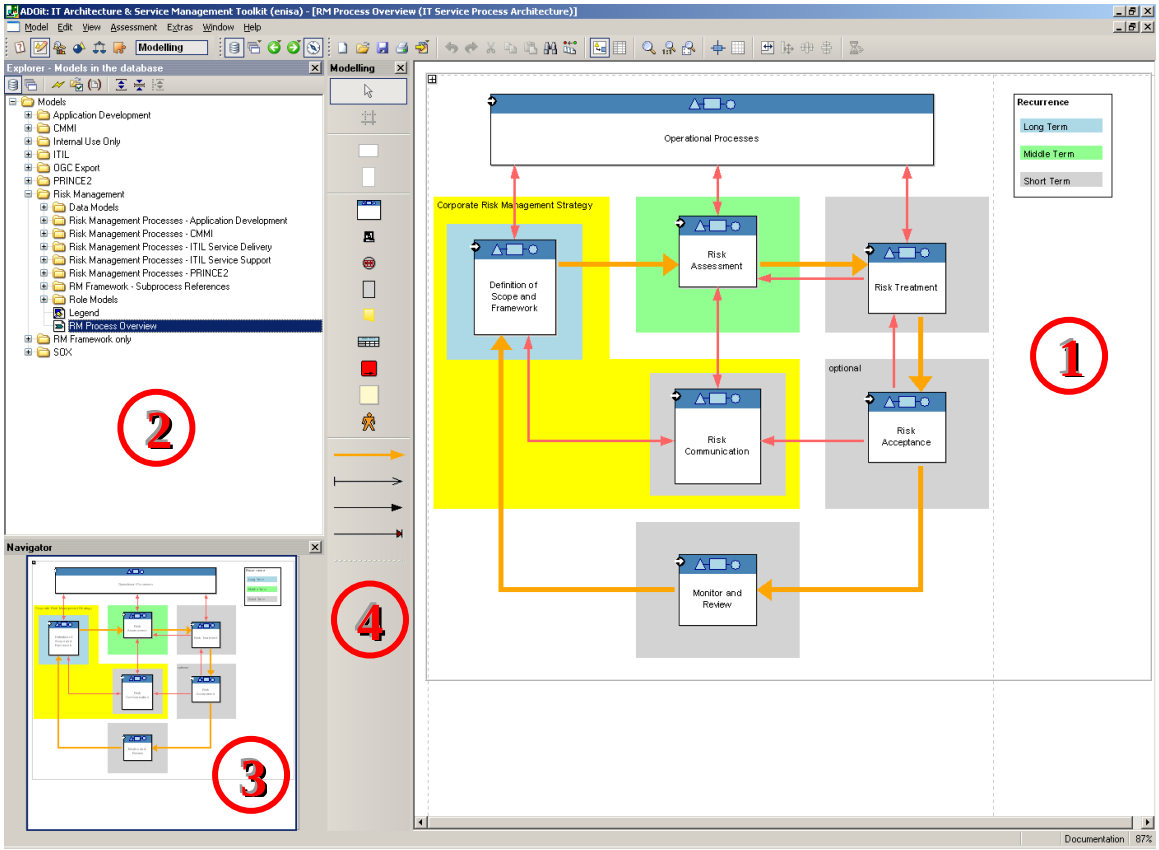

Figure 33: Screenshot of ADO*it*® 3.0

On the right hand side the *modelling area* (marked by the red **1** in the above figure) is located. To its left is the *model explorer* (**2**). The explorer shows the model groups, which are used to organise the models. To the lower left is 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.

11.2 The Modelling Language

Since ADO*it*® 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 ADO*it*® as a part of the BOC Architecture Management Framework (see [4]) and was modified according to the specific requirements of the Project.

Figure 34 shows a legend, which is included as an additional diagram within the set of models that forms the main deliverable of the Project (see section 7). 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 this 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 of 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* notation).

The blue subprocess 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 34 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 **6.3**).

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 34 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 interface described above 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 7.

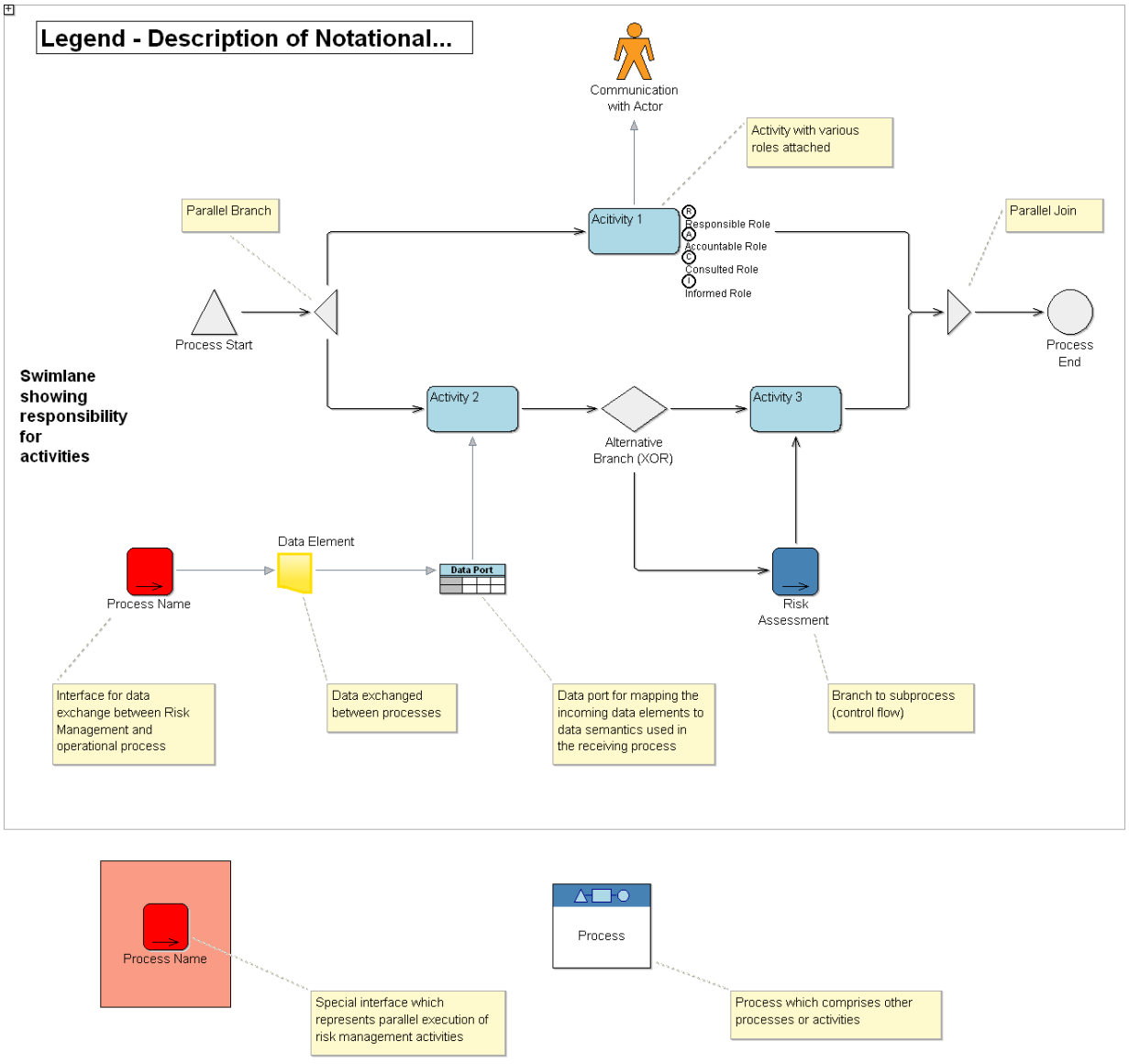

Figure 34: Legend of Basic Model Elements