2009

INTEGRATION OF AN IT-RISK MANAGEMENT/RISK ASSESSMENT FRAMEWORK WITH OPERATIONAL PROCESSES

Louis Marinos
ENISA

Lutz Kirchner
BOC Information Technologies Consulting

Stefan Junginger
BOC Information Technologies Consulting

INTEGRATION OF AN IT-RISK MANAGEMENT/RISK ASSESSMENT FRAMEWORK WITH OPERATIONAL PROCESSES

Louis Marinos[1], Lutz Kirchner[2], Stefan Junginger[2]

Abstract
This paper discusses the background and results of a research project which was conducted by ENISA (European Network and Information Security Agency) in cooperation with the BOC Information Technologies Consulting GmbH. The project was initiated with respect to the main task of ENISA: ensuring a high and effective level of network and information security within organisations in the European Union. As an important step towards this goal the research project aimed at increasing the level of integration between an enterprise-level IT Risk Management/Risk Assessment on the one hand, and selected operational business processes, on the other hand. The proposed integration is mainly established on the level of document flows between processes and activities respectively. In particular, operational processes which are closely related to IT were selected for integration. The introduced approach promises a better overall quality of IT Risk Management in an enterprise in general, as well as an improved management of risks in operational processes.

1. Motivation

IT Risk Management is frequently implemented as an isolated process which shows little or no interaction with the various operational processes in an organisation (cf. [22]). This concerns value-generating business processes, e.g. procurement and sales, as well as support and management processes, like IT Service Management. As a consequence, risks which have to be dealt with on a daily basis during the execution of those processes are often not taken into account, neither in the course of planning nor of performing IT Risk Management. This causes a potentially negative impact on the overall quality of the operational business processes regarding aspects such as execution time, reliability and cost efficiency. At the bottom line, we assume that an isolated IT Risk Management is generally not as effective as one that is tighter integrated with operational processes and hence does not sufficiently contribute to the achievement of the organisations goals.
Some approaches to IT Risk Management, like the *Probabilistic Risk Analysis*, address this issue by including the frequent gathering of information about operational risks from operational processes (cf. [4]). However, they primarily focus on risk assessment. Thus, their integration with

[1] ENISA, 71001 Heraklion, Greece, http://www.enisa.europa.eu
[2] BOC Information Technologies Consulting GmbH, 10117 Berlin, Germany, http://www.boc-de.com

the operational processes is only limited and mostly constricted to quantitative data analysis. The most high-level approaches, i.e. especially IT Risk Management frameworks, usually do not cover the above addressed issue in sufficient depth (cf. paragraph 2.2). To overcome this desideratum, an adequate integration of IT Risk Management processes[3] with the operational processes of an organisation – at least on the level of information flows - is recommended. Some of the necessary risk-related information may emerge from Risk Management activities, as they may be already implemented as an integral part of operational processes (e.g. in ITIL Service Continuity and Security Management). Additional information entities are generated "all over" the whole operational process.

In consideration of the above discussed issue, the paper at hand aims at identifying interfaces between the IT Risk Management processes described in a Risk Management/Risk Assessment (RM/RA) framework (designed by ENISA, see paragraph 3.1) and selected operational process frameworks (namely ITIL, RUP, PRINCE2™[4] and CMMI, see paragraph 3.2). A pivotal design goal of the interfaces is being as concrete and detailed as it is possible when dealing with reference process frameworks rather than living processes.

The focus of the integration is chiefly on the identification of corresponding information entities, the information flow between the processes, and roles. The information entities, which are to be exchanged between the IT Risk Management processes and the operational processes, are semantically mapped to each other for the specific context in which they are used. Thus, it is assured that the terminology of IT Risk Management and operational processes is compatible at any time.

Main addressees of the research results are these individuals in an organisation which play a central role in the IT Risk Management implementation, integration and execution process (e.g. administrator, change manager, or CIO). 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 outcome.

The results of the research are published in the form of graphical process models created with the tool ADO*it*® 3.0[5]. For easy accessibility and distribution, the ADO*it*®-models are being transformed in navigable HTML-models (cf. [7]). Complementing these models, a generic *integration process model*, which aims at supporting an organisation in the process of integrating IT Risk Management with the supported operational processes, as well as a role mapping table, is included.

The paper is structured as follows: Section 2 gives a short introduction to IT Risk Management and presents a selection of IT Risk Management approaches. Section 3 describes the approach used for integration, additionally presenting the ENISA RM/RA Framework as well as two of the integrated operational process frameworks. Also the models, which document the integration results, are being presented in form of an exemplary excerpt. The paper closes with a conclusion in section 4 including a discussion of benefits a user may expect when adopting the models.

2. IT Risk Management

This section gives a short overview of the terms *risk* and (*IT*) *Risk Management* (paragraph 2.1). It also introduces and briefly evaluates existing IT Risk Management frameworks (paragraphs 2.2 and 2.3).

---

[3] In the context of Risk Management the associated processes, like e.g. risk assessment and risk control, are often denominated *phases*.

[4] PRINCE2™ is a Trade Mark of the Office of Government Commerce.

[5] ADO*it*® is a modelling tool for supporting Enterprise Architecture Management and IT Service Management. For further information see http://www.boc-group.com/ADOit.

2.1. Terminology

A *risk* in general may be regarded as "the potential for realisation of unwanted, negative consequences of an event" (see [11]). Viewed from a decision oriented perspective a risk is the possibility of reaching a wrong decision and having to deal with the resulting negative consequences. Supplementing these definitions, a risk can also be interpreted as the possibility of failing to achieve a certain goal. In this context a positive derivation from a predefined goal specification may be seen as a chance (cf. [19], p. 22; [9], p. 1751).
In general, *Risk Management* aims at making sure, that the existence of an organisation is ensured in the long run ([8], p. 12,). Risk Management is a recurrent process that deals with the analysis, planning, implementation, control and monitoring of implemented measurements. In contrast, *Risk Assessment*, that usually is seen as a part of Risk Management, is executed at discrete points of time (e.g. once a year, on demand) and provides a temporary view of assessed risks, while giving input to the Risk Management process (cf. [22], p. 6).
IT Risk Management is a specialisation of Risk Management and focuses on the implementation of IT with respect to the overall organisational goals (cf. [3], p. 4). Risk Management principles and activities are applied to information technology specific processes.
In this paper we assume that there usually exists a corporate-wide IT Risk Management in contrast to an IT Risk Management specifically applied to selected operational processes[6]. The possible integration of these two perspectives is also covered by this research in form of the definition of specific interfaces.

2.2. Introduction of Existing Approaches

There exist numerous standards and good practices that provide guidance for IT Risk Management/Risk Assessment (cf. [22]). Standards like CobiT and ITIL chiefly aim at guiding activities in the area of IT Governance and IT Service Management, also hinting at the management of operational risks. In contrast, Risk Management frameworks focus on the definition of Risk Management processes and controls on a strategic or operational level respectively, but usually lack explicit relations to operational processes (see below). Complementing these approaches, there exists a plethora of sector- and enterprise-specific frameworks developed to fulfil special requirements of certain sectors and companies. This paper does not aim at providing a complete or ultimately well-defined categorisation and evaluation of IT Risk Management approaches. Instead, we pick out a small number of - in our opinion - representative approaches to highlight their general desiderata in terms of integration, according to the discussion in section 1.
The approaches, which we briefly introduce in the subsequent paragraphs, provide some rather distinct perspectives on IT Risk Management. They were selected du to the fact, that they are well recognized, widely applied in practice, developed by representative organisations and institutes, and well documented in numerous publications or free-of-charge documentation.

IT-Grundschutz of the German *Bundesamtes für Sicherheit in der Informationstechnik* provides a method for an organisation to establish an Information Security Management System (see [12] and [22], pp. 34 and pp. 93). It comprises both generic IT security recommendations for establishing an applicable IT security process and detailed technical recommendations to achieve the necessary IT security level for a specific domain. The key goal of IT-Grundschutz is to provide a framework for IT security management, offering information structured by typical *building blocks* (Bausteine), like e.g. infrastructure, IT-systems, and applications. In [13] potential synergies between a number

[6] The gap between these two Risk Management approaches is also mentioned in [10], where a newly developed framework is announced for the end of the year, which claims to address this issue.

of ITIL processes and IT-Grundschutz are being discussed, but without offering concrete hints on how such an integration can be implemented.

ISO/IEC IS 17799:2005 is an international ISO standard that provides information technology security techniques (see [17] and [22] p. 34 and pp. 86). It focuses on risk identification and risk treatment techniques, largely neglecting analysis and evaluation activities. It is mostly appropriate for initial threat identification. The documentation enlists various points that have to be taken into account to manage IT suitably. Interfaces to the organisational processes Human Resources Management, Change Management and Business Continuity Planning are also discussed.

Octave v2.0 (and Octave-S v1.0 for Small and Medium Businesses) is a standard originating from Carnegie Mellon University (see [1] and [2] respectively, also [22] p. 36 and pp. 105). It provides a RM/RA method covering risk identification, analysis and evaluation, but only by provision of relevant criteria without further techniques. It includes however a complete framework to deal with the communication of risks. OCTAVE® (Operationally Critical Threat, Asset, and Vulnerability Evaluation℠) is a self-directed approach meaning that people from an organisation assume responsibility for setting the organization's security strategy. OCTAVE-S is a variation of the approach tailored to the limited means and unique constraints typically found in small organisations (cf. [2], p. 3).

2.3. Summary

The above as well as the plethora of other existing approaches all offer some mostly generic and therefore generally applicable guidance to IT Risk Management with a varying focus on specific Risk Management activities, and hence different specific strengths and weaknesses. In [21] the current situation is summarised as follows: "Each one of the standards has aspects that could benefit particular deployments; some include more detailed recommendations, while others prefer to use a more general approach". Additionally, we may safely state, that the existing approaches do not deal with the challenge of the integration of an enterprise-wide IT Risk Management/Risk Assessment with operational processes in a satisfying manner. However, to truly leverage the synergies that may be created by combining IT Risk Management activities on different organisational levels, such an integration seems imperative. Based on this assumption, we make a proposal for an approach, which addresses this integration matter, in the subsequent paragraphs of this paper.

3. The Integration Approach

The major working steps, which were executed consecutively in the course of this work, are discussed in detail in the following paragraphs.

3.1. Modelling of the ENISA RM/RA Framework

The ENISA RM/RA Framework was depicted in the form of a graphical process model in ADO*it*®. The framework is basically a comprehensive summary of relevant concepts found in corresponding methods and literature about IT Risk Management. Due to this fact, it forms a highly adequate basis for the design and conceptualisation of an integration approach, such as it is described in this paper. In the following we give a short overview of the framework. Please refer to [22] for further details.
Figure 1 shows a schematic of the framework. The covered processes (or phases) may be performed isolated or collectively. In case that all of the processes are performed, the thick arrows form a cycle which depicts a control flow through the Risk Management processes. The process

Definition of Scope and Framework is considered to be the starting point for this control flow. The process aims at the establishment of global parameters for the performance of Risk Management within an organisation. 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 an ongoing process for monitoring the success of the Risk Management implementation and delivering valuable input to any recursion of the (re)definition of the IT Risk Management. A supplementing *Risk Communication* process aims at exchanging information about risk to and from all stakeholders. In addition to the above processes, possible interfaces to operational processes are indicated, but not elaborated at this point.
Complementing the framework, a set of information entities is identified by ENISA and incorporated in the model. These entities describe the exchange of information between the various Risk Management processes. Additionally, some roles are identified, which are typically involved in the execution of the Risk Management processes. These are *Senior Management/Board of Directors*, *Risk Manager*, *Risk Owner*, *Internal Audit* and *Domain Expert* (cf. [7]).

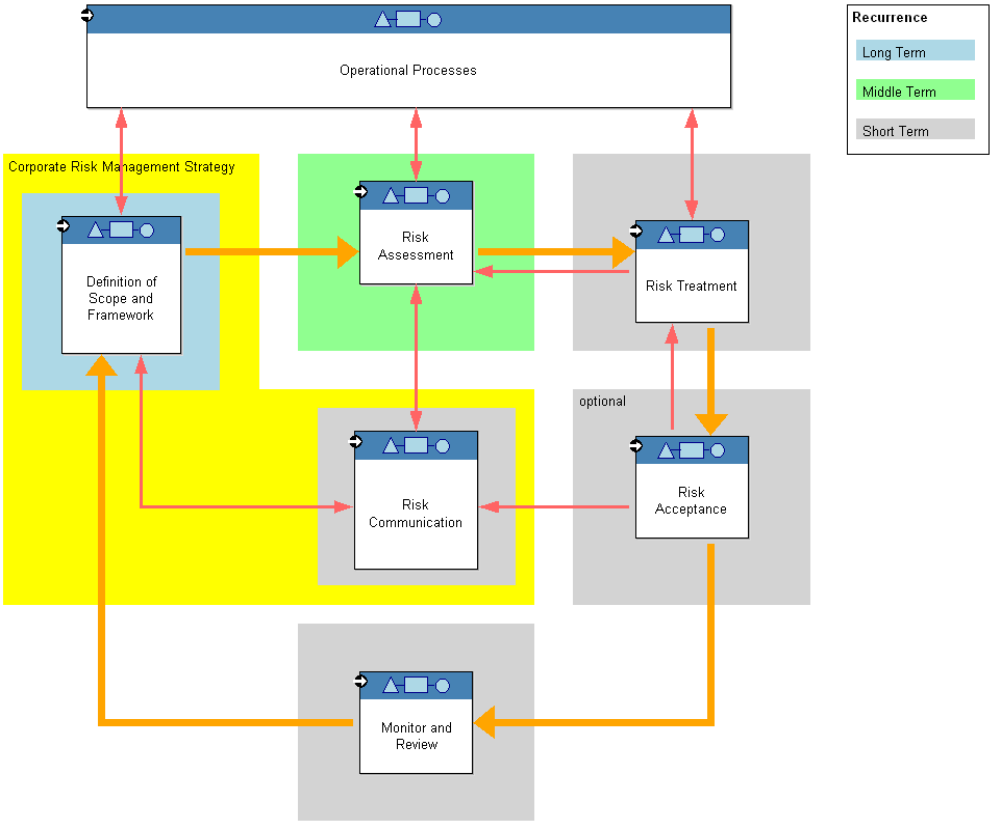

Figure 1: The Risk Management Process in ADO*it*®

3.2. Modelling of the Operational Processes

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 (see below), an application development process based on RUP (also see below), PRINCE2™ (*Project Management in Controlled Environments 2*, see [20]) and CMMI (*Capability Maturity Model Integration*, see [5]). The main reason for this choice is that these processes represent commonly used procedures and solutions for dealing with challenges in the field of IT Management, which

most companies have to meet, regardless of the business sector they are operating in. Moreover, they are to a certain extend 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 information entities.
The following paragraphs give an overview of two of the operational process frameworks selected for integration.

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 subsets of ITIL which are of interest for this report are Service Delivery, Service Support and Security Management (see [14], [16] and [15]). 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 processes.[7]
The data that is gathered during the execution of ITIL 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.

Application Development Process: The application development process used for integration purposes is a generic heavy weight process, which is loosely based on the RUP (*Rational Unified Process*, see [18]). 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.

The selected operational processes are modelled in the same way as the RM/RA framework, thus beginning with control flows, followed by information entities, information flows and finally roles.

3.3. 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, are identified. Secondly, the information flow between the integrated activities or processes respectively is depicted. A third step is necessary when a data element is used as an incoming information flow to an activity. In this case a semantic data

[7] ITIL V3 is available since early 2007 but has to ultimately supersede ITIL V2 yet, so it was not considered for inclusion.

mapping is conducted, which relates the incoming data element to the corresponding data elements of the receiving process. This is necessary since the data element terminology of the operational processes is not exactly matching these of the ENISA RM/RA Framework (see below).
Figure 2 shows an excerpt of an IT Risk Management process with two exemplary interfaces to other processes, namely ITIL Service Support processes. The sole activity of the process, "A.14 Risk monitoring and reporting" has several roles attached, which are arranged according to their specific role relation to the activity. The role *Internal Audit* is responsible and accountable for the activity (hence arranged below the R- and A-symbols). The *Domain Expert* and *Risk Owner* are to be consulted (C) and the *Risk Manager* and *Senior Management* informed (I). This kind of role annotation is inspired by the RACI-role definitions, as they are for instance used in CobiT ([6]).
In addition to the activities and roles the exchanged *information entities* (also denoted as *data elements*) and a *data port* are also included in the example. A data port contains a table which maps the incoming data elements to the data definitions of the receiving process. Figure 3 shows an exemplary data mapping. The left column displays the incoming data elements whereas the right column contains the mapping target, i.e. the data elements which are used in the receiving activity to store the incoming information. In this concrete example the incoming data elements are a subset of the documented ITIL-terminology (see [16]) and are mapped to the data elements defined for the ENISA RM/RA Framework. Note, that this is usually not a 1:1 relationship, but rather 1:n.

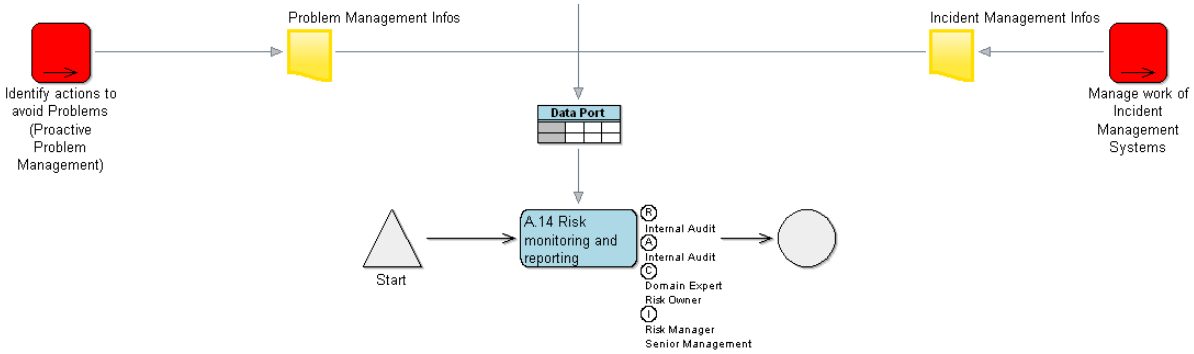

Figure 2: The Monitor and Review Process with Interfaces to ITIL Service Support

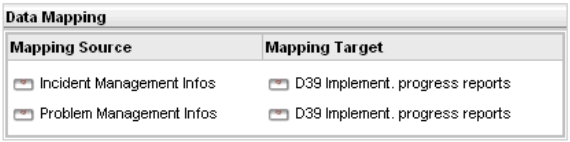

Figure 3: Mapping of Data Elements (excerpt from HTML model version)

Figure 4 schematically illustrates the information flow from the ITIL process *Incident Closure* to the *Monitor and Review* process of the ENISA RM/RA Framework. From the ITIL-activity *Inform User* in the process *Incident Closure* a document *Incident Status* is handed over to the Risk Management activity *A.14 Risk monitoring and review*, where it is used to evaluate the success of the measures defined in IT Risk Management. If an increase of severe incidents in the recent past is discovered, e.g. by measuring these and other values with a set of Risk Management specific KPIs (Key Performance Indicators), Risk Management may be able to react in time and calibrate the concerned processes accordingly.
To track the information flows throughout the complete set of models, model navigation is based on the easy-to-handle navigational features of ADO*it*® and its generated models in HTML-format.

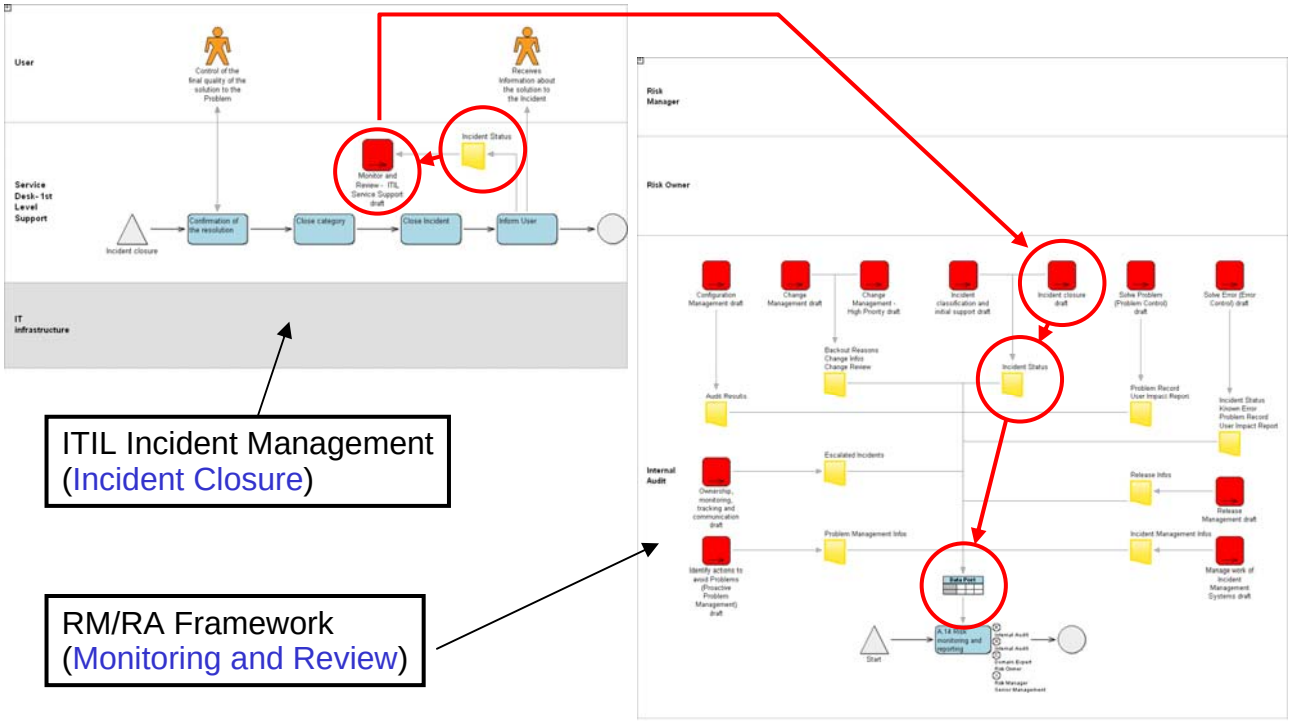

Figure 4: Example of Document Flow between two Processes

Concluding the design step described in this paragraph, the mapping of roles was conducted for these processes which were provided with adequate role definitions. Analogous to the data definitions, the roles used in the context of Risk Management are not identical to those defined in the operational processes. Hence, they were semantically mapped to each other. Thus, in the integrated models the ITIL *Change Manager* e.g. is also acting as a *Risk Owner* and a local *Risk Manager*. A complete list of Risk Management roles and their mapping to roles of the covered operational processes can be found in [7].

3.4. The Process Model for Result Application

In order to successfully apply the above presented project deliverables in the course of a Risk Management integration process, a methodical approach like the one introduced in this paper 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 steps may be executed to establish an integration process:

1. Risk Management Implementation (if not already done in the past)
2. Operational IT Process Implementation (if not already done in the past)
3. Integration Planning and Initiation (resource assignment, process mapping etc.)
4. Quality Assurance (e.g. review and improvement of process)
5. Execution of Processes (support of staff, monitoring and constant improvement of process)

A detailed description of the process steps and related activities can be found in [7].

4. Conclusion

The paper at hand illustrated the need for a thorough integration of an IT Risk Management approach and operational process, and proposed an approach for performing such an integration. The main contribution of the approach is the provision of concrete information flows between activities of IT Risk Management processes and operational process frameworks, which results in a detailed guide for establishing and harmonising both process types in an organisation.

The overall expected benefit of the research results for a user, who applies the approach, can be summarised as following:

- The user receives guidelines for
  - Implementing Risk Management with a provided RM/RA 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 common 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 Risk Management (e.g. SOX, Euro-SOX, Basel II, Solvency II)

Potential future research could consider other possible dimensions of integration between Risk Management and operational business processes, like e.g. integration on the level of control flows, or technical interface specification for software tools. It has to be evaluated, if these kinds of integration deliver further value to the adopter. Furthermore, the success of the approach depends on the set of operational process frameworks, which are covered by documented integration scenarios. Our approach cannot be applied to an arbitrary operational process without first identifying and documenting the interfaces. To provide these interfaces to a larger number of operational process frameworks is subject to future work.

5. Literature

[1] ALBERTS, C.J.; DOROFEE, A.J.: OCTAVE^{SM} Method Implementation Guide Version 2.0. Software Engineering Institute, Carnegie Mellon University, 2001

[2] ALBERTS, C.J; DOROFEE, A.J.; STEVENS, J.; WOODY, C.: OCTAVE$^{®}$-S Implementation Guide. Version 1.0, Volume 1: Introduction to OCTAVE-S, Software Engineering Institute, Carnegie Mellon University, 2005

[3] BALDUIN, A. v.; JUNGINGER, M.; KRCMAR, H.: Risikomanagement von Informations- und Kommunikationstechnologien mit dem Value at Risk-Ansatz. Arbeitsbericht, Technische Universität München, 2002.

[4] BEDFORD, T.; COOKE, R.: Probabilistic Risk Analysis. Cambridge University Press, Cambridge, 2001

[5] CMMI for Development. Version 1.2, Carnegie Mellon SEI, 2006

[6] CobiT 4.1: Framework, Control Objectives, Management Guidelines, Maturity Models. ITGI, 2007

[7] Demonstrators of RM/RA in Business Processes – Project Report. ENISA and BOC GmbH, 2007

[8] DIEDERICHS, M.: Risikomanagement und Risikocontrolling: Risikocontrolling – ein integrierter Bestandteil einer modernen Risikomanagement-Konzeption. Dissertation, Universität Dortmund, 2004.

[9] FARNY, D.: Risk Management und Planung, In: Szyperski, N., Winand, U. (Hrsg.): Handwörterbuch der Planung, Stuttgart, S. 1749 – 1758, 1989

[10] FISCHER, U.: New Framework for Enterprise Risk Management in IT. In: Information Systems Control Journal, Volume 4, ISACA, 2008

[11] HEEMSTRA, F.J.; KUSTERS, R.J.: Dealing with risk: a practical approach. In: Journal of Information Technology, Volume 4, pp. 333.346, 1996

[12] IT-Grundschutz-Kataloge, 9. Ergänzungslieferung, Stand 2007. Bundesamt für Sicherheit in der Informationstechnik, 2007

[13] ITIL und Informationssicherheit: Möglichkeiten und Chancen des Zusammenwirkens von IT-Sicherheit und IT-Service-Management. Bundesamt für Sicherheit in der Informationstechnik, 2005

[14] ITIL Service Delivery. CD-ROM Version, Office of Government Commerce, Norwich, 2003

[15] ITIL Security Management. Office of Government Commerce, Norwich, 1999

[16] ITIL Service Support. CD-ROM Version, Office of Government Commerce, Norwich, 2003

[17] ISO/IEC 17799:2005: Information Technology - Security Techniques - Code of Practice for Information Security Management. International Standards Organisation, 2005

[18] KRUCHTEN, P.: The Rational Unified Process: An Introduction. Addison Wesley, Reading, 2000

[19] LOCHER, CH.; MEHLAU, J.I.; HACKENBERG, R.G.; WILD, O.: Risikomanagement in Finanzwirtschaft und Industrie – Eine Analyse des Management operationeller Risiken in deutschen Industrie- und Dienstleistungsunternehmen, ibi research an der Universität Regensburg gGmbH, 2004

[20] Managing successful projects with PRINCE2. TSO, London, 2005

[21] RAMIREZ, D.: Risk management standards: The bigger picture. In: Information Systems Control Journal, Volume 4, ISACA, 2008

[22] 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

Acknowledgement

The authors wish to express their gratitude to Aneta Nowobilska and David Heise who offered great support in assessing the literature and gave valuable input.