OPERATIONAL RISK MANAGEMENT IN FINANCIAL INSTITUTIONS: PROCESS ASSESSMENT IN CONCORDANCE WITH BASEL II

B. Di Renzo, M. Hillairet, M. Picard, A. Rifaut

Centre de Recherche Public Henri Tudor (Luxembourg)
{bernard.direnzo, magali.hillairet, michel.picard, andre.rifaut}@tudor.lu

C. Bernard, D. Hagen, P.Maar, D. Reinard

Commission de Surveillance du Secteur Financier (Luxembourg)
direction@cssf.lu

Abstract

The improvement of banks' operational risk management frameworks concerns new requirements addressed in the Basel II Framework, a new capital adequacy regulation proposed by the Basel Committee on Banking Supervision (BCBS). Basel II will apply to internationally active banks and to all banks and investment firms in the EU via transposition of a new Directive into national regulations.

By doing so, the national financial supervisory authority (CSSF)in Luxembourg, and a public research center (CRPHT) have engaged in a joint research project that investigates solutions conformant to ISO/IEC 15504 for assessing operational risk management frameworks implemented in banks.

The ISO/IEC 15504 requirements can meet the CSSF's expectation on consistent, transparent and sound risk assessments, as well as the expectation on promoting enhancements in institutions' risk management practices without dictating the form or operational detail of their policies and practices.

Moreover, although the domain is largely outside the scope of software and systems engineering, the ISO/IEC 15504 process assessment standard provides for an adequate solution to the so-called supervisory review process. This adequacy is validated through the structure of Basel II and financial domain requirements. Last but not least, we will show that ISO/IEC 15504 provides an adequate approach to assessing institutions in two sub-domains, namely the domain of credit operational risk management and the domain of IT risk management (including IT security risks management).

1. Introduction

The reviewed focus of ISO/IEC 15504 on process assessment in domains other than software and system engineering provides for interesting innovation perspectives for both research and markets within a large spectrum of business areas. Our research lies within this extended scope of process assessment including non-IT domains in an epistemological approach by investigating the

application of IT-related methods and techniques inside financial institutions. It provides for a generic building block approach for financial sector supervisors[1] to assess the appropriateness of institutions operational risk management and measurement systems as an integral part of the so-called supervisory review process.

Indeed the international banking sector and supervisors alike now face new challenges with the requirements spelled out in the Revised Framework for International Convergence of Capital Measurement and Capital Standards (often referred to as the "Basel II Framework") proposed by the Basel Committee on Banking Supervision[2] [2]. Besides financial risks such as credit and market risks, Basel II highlights the link between risk exposures and operational risk capital charges and proposes in particular three approaches for calculating the operational risk minimum capital charges in a continuum of increasing sophistication and risk sensitivity. Banks are encouraged to move along the spectrum of available approaches. In this context, an emerging question for the financial institutions is: how to move along the spectrum of available techniques by developing more sophisticated operational risk measurement systems and practices? And for supervisors: how to assess and review banks' operational risk management practices and systems as well as their compliance with the qualifying criteria of one of the three approaches for calculating minimum capital requirements?

To investigate both these questions and to provide for new methods allowing banks and financial supervisors to address these challenging tasks are the purpose of the joint research project between the Commission de Surveillance du Secteur Financier[3] (CSSF) and the CRP Henri Tudor.[4]

After an initial modeling of IT risk management, our research has lead us to broaden our scope by investigating the use of ISO/IEC 15504 [9] as a federative approach to assess and improve operational risk management in the financial institutions and thereby warranting a coherent risk control method to be implemented by those institutions.

This paper draws our first answers to how an operational risk management process reference model (PRM) and associated process assessment model (PAM) built on the new regulatory requirements or expectations can be of tremendous usefulness for the financial institutions and supervisors. The Basel II Framework is presented in the next section with a focus on operational risks. The proposed solution, mainly a PRM and PAM, is described in section 3, and its validation is explained in section 4. Future work, presented in section 5, concerns further validation and also integration with two complementary approaches. Conclusions are found in section 6.

2. Operational risk management in financial institutions

During the past decade financial institutions have been modifying both their products and internal processes at a rapid pace leading to an increased exposure to operational risk. Consequently supervisors of financial institutions have expressed increased concerns on institutions' potential

[1] Bank supervisors are some national entities having the power to control compliance to national banking laws and to terminate unsafe and unsound banking practices in their country.
[2] The Basel Committee consists of senior representatives of bank supervisory authorities and central banks from Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, the Netherlands, Spain, Sweden, Switzerland, the United Kingdom, and the United States.
[3] CSSF is the national supervisory authority of the financial sector in Luxembourg and represents Luxembourg at the Basel Committee.
[4] CRP Henri Tudor is a public research centre based in Luxembourg.

exposures to operational risk and institutions will be required to enhance their risk management capabilities with respect to their operational processes. Although well-defined tools and techniques are used for the assessment and modeling of financial risks inherent in financial products, comparable approaches are still in a developing stage on the operational risk side. Up to now, no international agreement has been reached on how to actually implement or assess compliance with those requirements. This research aims at showing that a solution for the assessment of operational risk management compliant with ISO/IEC 15504 standards may form a sound basis to meeting those future regulatory requirements.

2.1. The Basel II framework

One of the aims of the new capital framework is to strengthen the stability of the international banking system. This stability objective is expected to be achieved by improving the soundness of the international banks, in particular through a closer alignment of capital to actual risks ("risk-sensitive capital requirements") and the improvement of risk management practices currently in use in those institutions.

The framework is decomposed into three *pillars*. The first pillar sets out the calculation of minimum capital requirements. The second pillar addresses the supervisory review processes aiming at ensuring the appropriateness of the capital level chosen by each bank as well as encouraging better risk management practices. The third pillar addresses market discipline through disclosure requirements on banks' risk exposures and measurement systems.

New requirements addressing the improvement of operational risk management inside the banks are found in each of these three pillars.

Moreover, within the first pillar, the framework proposes three different approaches for the calculation of minimum capital requirements with regard to operational risk in an increasing order of risk-sensitivity and sophistication: the *Basic Indicator Approach*, the *Standardized Approach* and the *Advanced Measurement Approach*. The Basic Indicator Approach uses a single risk indicator as a proxy for a bank's overall exposure to operational risk, whereas the Advanced Measurement Approach relies on comprehensive analysis of internal and external loss data, scenario analysis and aspects of the business and internal controls. This latter approach requires the definition of operational risk categories and the mapping of historical loss data into the risk categories. Thus this approach calls for a more detailed operational risk model.

2.2. Operational risk management

It has become more than a recognized fact over the last decade that large observed bank losses originated from vulnerabilities in the operational processes and appearances of threats which together cause operational loss events. One striking example is the collapse of Barings Bank in 1996 where misuses of accounts ("assets") by a rogue trader ("threat"), lack of accounting control and audit as well as inappropriate segregation of duties ("vulnerabilities") were at the source of fraudulent transactions.

As can be seen in this example, although IT risk has to be considered and constitutes one of the four operational risk causes, the main concern is about non-IT operational risks, such as for instance risks related to inappropriate processes and procedures of a bank's trading activities.

As a result of this, the definition of operational risk used in this work is the one stated in the Basel II framework, which is based on the four identified causes of operational risk at financial institutions: *Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk* [2, §644].

3. Operational risk management assessment conformant to ISO/IEC 15504

The Basel II framework does not constraint banks on how to implement the framework, but just sets the goals that must be fulfilled by each bank. This can be considered as a strong requirement: the assessment method cannot impose any constraint on the actual implementation of the framework. Moreover, because the operational risk management has a high level of consistency (i.e. *″[It] is conceptually sound and is implemented with integrity.″*[5] [2]), this imposes a high expected level of consitency (repeatability, reliability, …) on the assessment process. The ISO/IEC 15504 standard is compatible with both constraints.

The focus on business operational level leads to an innovating use of the standard for non-IT processes with the expectation to preserve the intrinsic characteristics.

Moreover the standard does not only offer the flexibility of encompassing current good or best industry practices, but also the emergence of new bank practices within an innovation perspective.

This section describes a solution based on ISO/IEC 15504 and designed to assess processes not belonging to the IT domain. Although the proposed solution is compliant with ISO/IEC 15504 requirements, the focus of this paper is about the compliance with financial domain requirements. The term “requirement” will refer to financial domain requirements except when ISO/IEC 15504 requirements are explicitly stated.

In this section, an adequate structuring of requirements about the Basel II Framework is presented, before explaining how this is used during the design of the solution.

3.1. Basel II requirements analysis

A good requirements analysis, as a key input into the project, leads to build a knowledge base structuring all the requirements the solution must satisfy. This was important in this work due to the use of very different kinds of sources of information.

The main sources are the publications of the Basel Committee: mainly, the description of the Basel II Framework [2], and the ″Sound Practices for the Management and Supervision of Operational Risk″ [3]. Another important source were the workshops organized by the CSSF where supervisors described their expectations on banks’ operational risk management framework and the assessments’ organizational constraints. Then, descriptions of risk management methods and good practices were used (e.g. EBIOS [6]). Finally, information gathered from banks and finance experts via personal communications, conference proceedings and technical reports was exploited.

Although the requirements acquisition resulted in a significant number of statements (more than 400), their analysis allowed building a structure based on taxonomies. Some examples are given

[5] In the rest of the paper, the requirements extracted from [1] can be found on pages 137 to 149.

hereafter for the specific Basel II domain, the risk management domain and the responsibilities aspects.

3.1.1. Requirements structure based on the three Basel II approaches.

As mentioned in section 2.1, three approaches are proposed in the Basel II Framework for the calculation of minimum capital requirements for operational risk. So, the requirements were structured along those three approaches. For instance, the requirement that *"As part of the bank's internal risk assessment system, the bank must systematically track relevant operational risk data including material losses by business lines"* [2] is essential to the *Standardized Approach*.

Moreover, these approaches are ranked in increasing order of sophistication. Generally the more advanced approach encompasses the requirements of the less sophisticated approaches. This structure has been adopted for the definition of the categories of requirements. For instance, if a bank adopts an *Advanced Measurement Approach*, it will have to meet the following requirement: *"Any internal risk measurement system must be consistent with [...] the loss event types [...]"* [2] in addition to the requirement given above for the *Standardized Approach*.

3.1.2. Requirements structure based on risk management activities.

The structure of the risk management activities can also be gathered from the requirements. For instance, the requirement *"The operational risk management function is responsible for developing strategies to 1. identify 2. assess 3. monitor 4. control/mitigate operational risk."* [2] indicates activities composing the management of risks. In this example the following activities are identified: "Risk identification", "Risk assessment", "Risk monitoring" and "Risk mitigation/control".

3.1.3. Requirements structure based on responsibilities.

Some requirements refer to a clear assignment of responsibilities and authorities, such as the requirement that *"the bank must have techniques for creating incentives to improve the management of operational risk throughout the firm."* [2]. This example shows that financial and managerial incentives must be used in order to ensure that each bank employee contributes to the improvement of the operational risk management framework.

Another example is contained in the requirement: *"The operational risk management function is responsible for developing strategies to 1. identify 2. assess 3. monitor 4. control/mitigate operational risk."* [2].

The categories based on the approaches were taken into account as follows: for each activity, each responsibility, the requirements corresponding to an approach were gathered. This resulted in an easy access to the requirements that a financial institution must satisfy: they can easily be found in the requirements collection in line with the selected approach and any other indicators.

To conclude, the requirements have been given a rich structure that helps to find the right solution to implement them, as can be seen in the next section.

3.2. Operational risk management PRM and PAM

The structure of requirements has been used to develop an ISO/IEC 15504 compliant PRM and PAM for operational risk management assessment. First, the activities have been reflected into the structure of the PRM. Yet, the PRM is further structured in two main categories, namely: "Primary" and "Support" (see *Figure 1*).

In the Primary category, two subgroups form the core of operational risk management: the first one addresses operational risk analysis including identification and assessment of operational risks; and the second one addresses the operational side of operational risks management including operational risk control and monitoring (see process exemplar in *Table 1*).

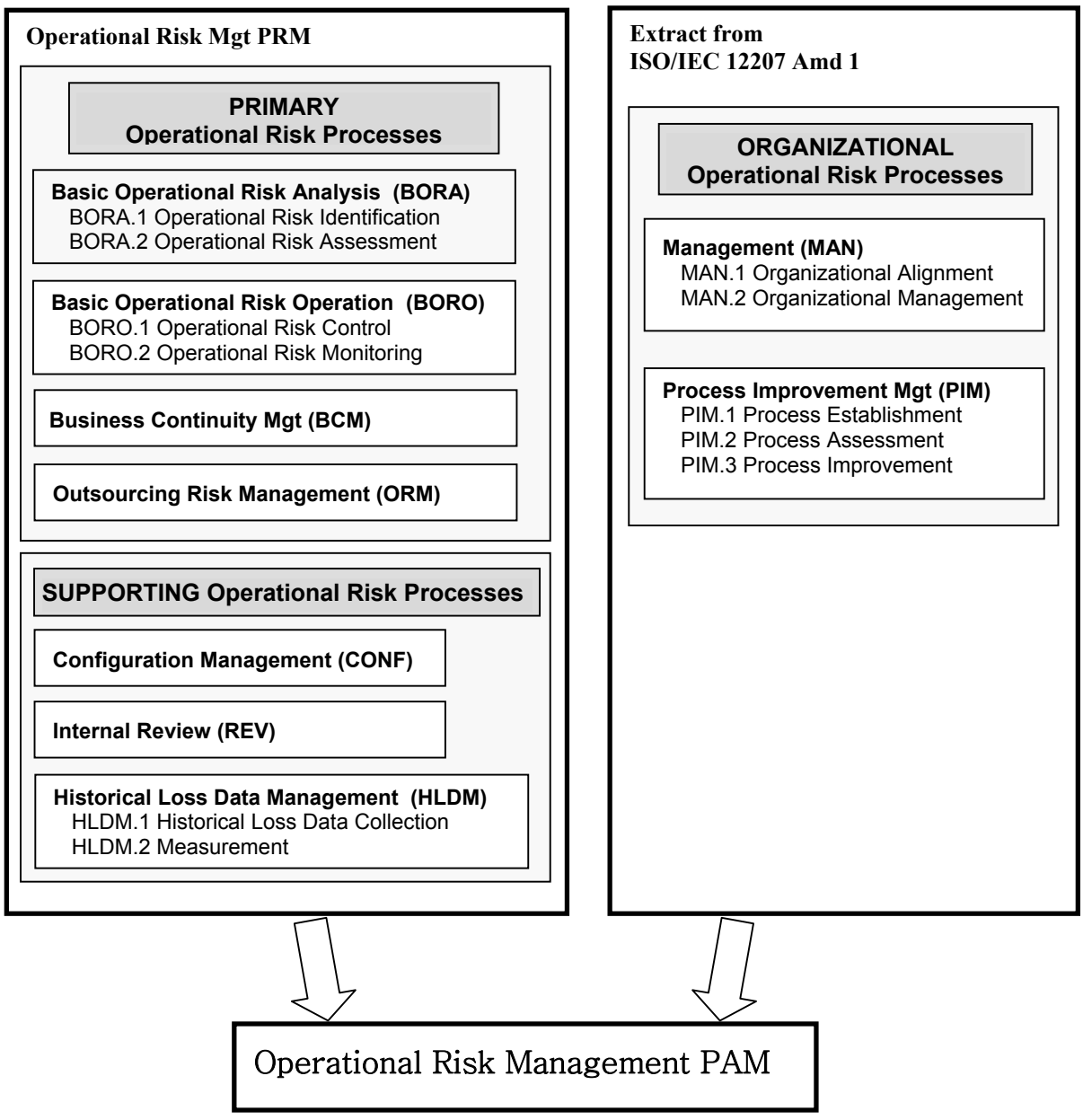

Figure 1. List of PRM processes

Two additional processes are added to this category, business continuity and outsourcing risk management, because the nature of risks is very specific and asks for separate activities to be translated into distinguished base practices.

Table 1. Operational Risk Control Description

Name	Operational Risk Control (BORO.1)
Purpose	The purpose of the Operat ional Risk Control process is to mitigate the analyzed risks and control risk that is under way.
Outcome	An operational risk mitigation and control strategy is developed and periodically reviewed;
Outcome	A security policy is developed, reviewed and communicated to all people involved in bank's operational activities;
Outcome	Changes in bank's organization and activities to mitigate risks are identified and implemented in accordance with bank's risk profile; and
Outcome	Appropriate action is ta ken to correct or avoid the impact of risks, and this action is tracked until risks are mitigated.

In the Support category, we have a significant process group concerning the management of data about uncontrolled risk realization and related losses. These last two processes differentiate the *Standardized Approach* and the *Advanced Measurement Approach*. Broadly, in the first approach internal data is only collected, and in the second one, additional data must be collected to develop a relevant measurement system and to establish scenarios for estimating expected and unexpected losses.

The last two processes of this category relate to the role of the internal review process and function of configuration management. The latter processes ensure the accuracy of all the information needed to obtain an effective and efficient operational risk management. For instance, detailed document job descriptions is mandatory, in particular, on the respective responsibilities assigned, on the accompanying incentives, as well as on all the controls put in place to detect deviations from the assigned responsibilities and tasks.

That represents an original part of our work, and crosses current risk management and service management methods (e.g. EBIOS [6], ITIL [1] [4]…) with the Basel II requirements.

Next to this new PRM, there is another subset of requirements directly modeled by existing processes belonging to ISO/IEC 12207 Amd 1 [8] that are grouped in an organizational category.

To cover all requirements some of them are implemented in base practices of the Operational Risk Management PAM, others are better implemented by integrating them in indicators of capability level attributes. This is illustrated below, in *Figure 3*, illustrating requirements traceability.

The PRM and PAM embrace the three approaches defined in the Basel II Framework for calculating minimum capital requirements about operational risk. Furthermore a subset of processes and a target capability profile are defined for each approach according to the Basel II Framework. *Figure 2* illustrates this *approach-driven* process selection. In the most advanced approach, all processes are selected and associated with the highest capability target compared to the other two

approaches. Hence, if a bank has opted for a given approach, assessors will be aware of processes to assess as well as the capability profile that should reach to meet all requirements of this approach.

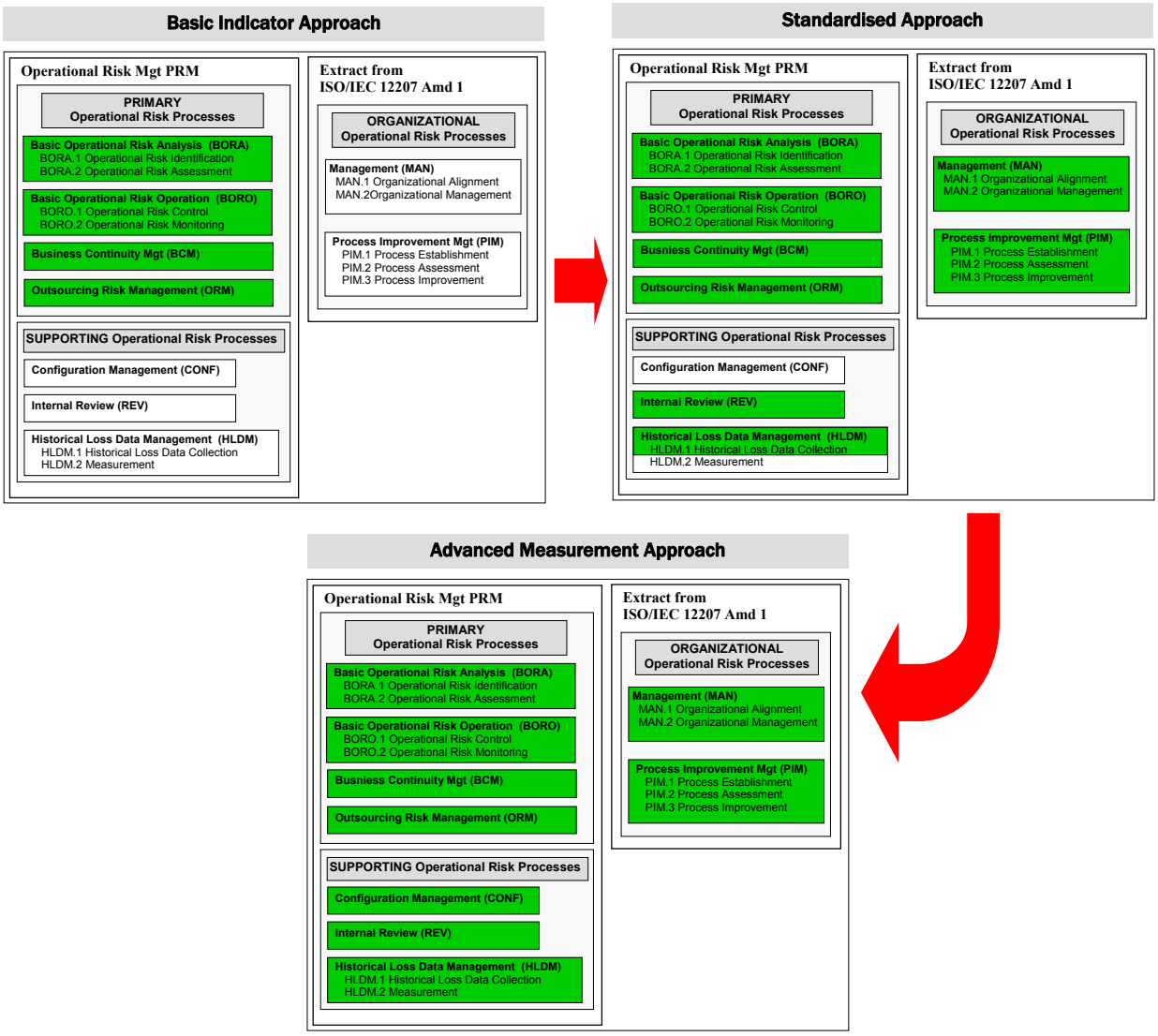

Figure 2. PAM compliance with Basel Approaches

For example, in a bank having chosen the *basic indicator approach*, assessors will assess only the primary category processes against a target capability profile set at level 1 for all these processes, without care about the support and organizational categories processes.

4. Validation of the solution

Due to the complex nature of this work, different validations are performed to illustrate the appropriateness of the proposed solutions.[6] A first validation, based on the requirements, ensures the match between the requirements and the PAM.

[6] A future validation is explained in section 5.

Then, the operational risk management model is checked against two examples of risk management of operational aspects found in financial institutions: the operational aspects of credit management and the aspects of IT management.

4.1. Fulfillment of the requirements

A systematic design can greatly help to fulfill the requirements. The requirements are decomposed in the following taxonomy: activities (*"risk control"*), goals (*"[...] creating incentives to improve the management of operational risk throughout the firm [...]"* [2]), responsibilities (*"[...] the operational risk management function [...]"* [2]). All taxonomy elements are mapped to ISO/IEC 15504 concepts: activities are described using base practices, goals are mapped onto purposes, responsibilities corresponds to generic practices among the attributes of the capability levels, etc. This mapping is at the basis of our design rationales. Completeness is essential to be sure that the whole requirements are comprehensively introduced into the PRM and the PAM. Traceability allows finding the requirements that motivate each element occurring in the implementation of the requirements. For each requirement, its origin and its uses are specified. First, each requirement is linked to the source of information it pertains. Then, a traceability link is recorded between the requirement and its implementation in the PRM or the PAM (see *Figure 3*). In order to determine quickly if a requirement is implemented in the PRM or in the PAM, the requirements are tagged with the name of the process together with the attribute or the level of capability used to implement the requirement. For example, the following requirement *"[...] developing strategies to control operational risk [...]"* [2] is linked to the objective of the Risk Control Process: the purpose of the Operational Risk Control process is to mitigate the analyzed risks and control risk that is under way".

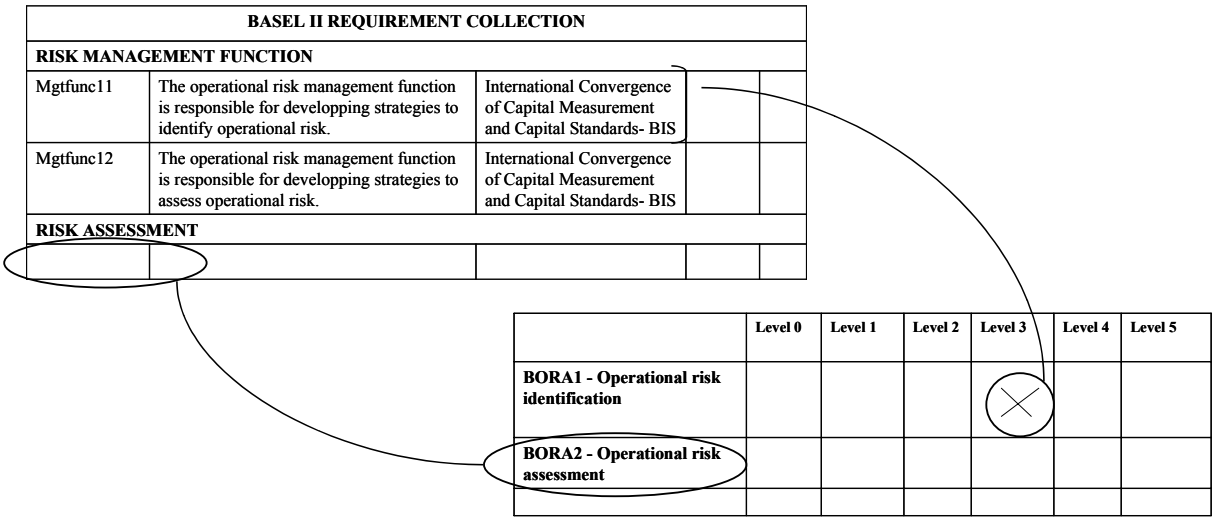

Figure 3: Completeness of the requirements: example

Moreover, traceability links can be used to review our design against the design rationales. For instance, in *Figure 3*, one can verify that all requirements concerning responsibilities are mapped into capability level 3 indicators. Deviations from this design rationale should carefully be analyzed. The opposite direction of traceability links (retro-engineering) can also be used: in the case of *Figure 3*, if an empty cell is found at the crossing between a responsibility requirement row and the

"level 3" column, then the requirement set should be analyzed carefully to motivate the missing responsibility requirement.

4.2. Validation on credit operational risk management and IT risk management

The main difficulty of our work is to successfully develop a PRM and a PAM, in accordance with ISO/IEC 15504, to a domain where core activities are related to financial products (and not IT artifacts). Therefore, it is essential to validate our PRM and PAM, to clarify the meaning of each component of the PRM and PAM in different banks operational contexts. In this case, two examples are meaningful: one within the context of banks IT management and another outside this context. This latter will be the credit operational risk management.

Table 2 shows the PRM covering the credit operational as well as the IT risks management processes. For each identified outcome of the PRM, an example is given in the credit operational risk management domain and the IT risk management domain. This example has been extended to other process elements and indicators of capability level attributes.

Table 2. Application of operational risk control process to IT and credit

		IT	CREDIT
Name	Operational Risk Control (BORO.1)		
Purpose	The purpose of the Operational Risk Control process is to mitigate the analyzed risks and control risk that is under way.		
Outcome 1	An operational risk mitigation and control strategy is developed and periodically reviewed;	The strategy aims to target vulnerabilities in IT infrastructure of a bank like extranet, hardware and software access control, …	The strategy aims to target vulnerabilities in credit operational procedures like credit granting and settlement watching.
Outcome 2	A security policy is developed, reviewed and communicated to all people involved in bank's operational activities;	A security policy is developed for people involved in IT operation of a bank. For example, each employee has to renew its password each other month. (Other examples can be found in [10])	A security policy is developed for people involved in credit operation. For example, employee are asked to carefully verify and authenticate the input data given to credit analysis procedures.
Outcome 3	Changes in bank's organization and activities to mitigate risks are identified and implemented in accordance with bank's risk profile;	Firewall deployment plans reducing intrusion risks are defined and executed, and login monitoring are planned and implemented.	Add a quality system for new credit request to ensure traceability and truthfulness of all information used to grant a credit.
Outcome 4	Appropriate action is taken to correct or avoid the impact of risks, and this action is tracked until risks are mitigated.	When monitoring system detect a intrusion in the firm network, all significant information is cut off from this network and intruder is isolate or sent off.	When a lack of settlement is identified, a reminder is sent to customer, his others credits are closely watched and no more credit will be granted to him before straightening out of his existing credits.

5. Discussion

Recent surveys give insights about how banks and financial institutions will implement the Basel II Framework.[7] This section will focus on the financial institution view of the Basel II Framework.

[7] For instance, Ernst & Young has announced the results of their worldwide survey [7]: nearly 80% of respondents were almost confident in the implementation of the framework, and 50% of institutions consider that they will increase their competitive advantage. Moreover, this study indicates that for over 30% of the respondents Basel II implementation will be the main driver of investments envisaging the enhancement of the risk management systems in place.

5.1. Competitive opportunities

The implementation of the Basel II framework has numerous advantages for bank shareholders, such as a capital alleviating effect when using more advanced approaches, the lowering of costs associated with losses, a better reputation for mastering risks... Moreover, the Basel II framework provides an opportunity for banks to improve their risk management capabilities, because the efforts spent for improvements are financially motivated in the Basel II framework. Note that Basel II will apply to a large share of the global banking system and it will be implemented in the member countries as well as in the EU.

5.2. ISO/IEC 15504 advantages

ISO/IEC 15504 standard is appropriate for the assessment of operational aspects. Most of the operational procedures are documented in banks due to the current regulation. This documentation and the assessments will be a good basis for improvement, which can be done at the best pace for each institution, as advocated in the Basel II Framework.

The assessment model is very precise, although it does not impose any constraint on the specific definition of actual processes found in each organization.

These facts increase our expectations in the usefulness and good acceptation of ISO/IEC 15504 for the implementation of the Basel II proposal.

5.3. Validation in banks

In order to see the adequacy of our proposal and its acceptance in supervised institutions, validation of our work through experimental on-site visits at banks in Luxembourg will be needed. In particular, the assessments results should be also useful for supervisors to assess the global improvement of the market place.

5.4. Integration with complementary approaches

To address the Basel II Framework, most of the consultants propose tools and techniques in the field of operational risk measurement bases on quantitative models (see, e.g. [11], [5]).

Another direction concerns IT risk management methods (including IT security risks). Some of them were used to build the set of requirements (see Section 3.1). The models they introduce can be the basis of an operational risk management method compatible with our assessment method.

Our future work will also concern the integration of those two complementary directions with the assessment method.

6. Conclusions

The highlight of operational risk management by Basel II Framework into the banking industry and its supervisors offers promising innovation perspective for process assessment in the financial sector. Indeed banks' need for operational risk management improvement combined with the need of banking supervisors to spell out operational risk management review and assessment

methodologies were at source of a joint research project between the CSSF and the CRP Henri Tudor with a PRM and a PAM as main outputs.

The adaptations of the PRM and the PAM by an expert team of bank supervisory from Luxembourg (CSSF), testify the appropriateness to the review of operational risk management framework in the banking industry. The intrinsic characteristics and the dual purposes (process improvement and capability determination) of ISO/IEC 15504 allow addressing operational risk management for all financial institutions regardless of their sizes. ISO/IEC 15504 appears to be especially well suitable for assessing financial institutions' operational risk management and measurement systems as it addresses the three pillars of the Basel II Framework i.e. banks' needs as well as supervisors ones.

Depending on these outcomes, the CSSF would be willing to broaden the approach and seek cooperation with other national banking supervisors in the spirit of contributing to the international convergence of supervisory practices.

7. References

[1] BARTLETT John, HINLEY David, JOHNSON Brian, et al., *ITIL – Service Delivery*; The stationery Office; London, Great Britain, 2001

[2] Basel Committee on Banking Supervision, *International Convergence of Capital Measurement and Capital Standards*; Bank for International Settlements Press & communication; Basel, Switzerland, June 2004.

[3] Basel Committee on Banking Supervision, *Sound Practices for the Management and Supervision of Operational Risk*; Bank for International Settlements Press & communication; Basel, Switzerland, February 2003.

[4] BERKHOUT Michiel, HARROW Roy, JOHNSON Brian, et al., *ITIL – Service Support*; The Stationery Office; London, Great Britain, 2000

[5] CHOFARAS Dimitris N., Operational Risk Control with Basel II, Elsevier Finance, Oxford, 2004.

[6] Direction centrale de la sécurité des systèmes d'information, *Expression des Besoins et Identification des objectifs de Sécurité (EBIOS*); Paris, France, February 2004.

[7] Ernst & Young, "Ernst & Young global risk survey on current views on Basel II Accord", News Release, (http://www.ey.com/global/download.nsf/EYSEE/Press_Release_-_Global_Risk_Survey_on_Basel_II_-_February_2004_(Eng)/$file/E&Y global risk survey on Basel II (en)@19Feb04.pdf), Feb. 19, 2004.

[8] ISO/IEC 12207:1995/FDAM 1:2002(E), *Information technology – Software life cycle processes;* ISO; Geneva, Switzerland, 2002.

[9] ISO/IEC 15504. *Information Technology – Process Assessment: part1 - Part5*; ISO; Geneva, Switzerland, 2003

[10] ISO/IEC 17799. *Code of Practice for Information Security Management*: *Editor's Draft*. Berlin, Germany, June 2002.

[11] KING Jack L., Operational Risk; Wiley Finance, Series, New York, 2001.