

Measuring Operational Risk Management Systems under Basel II

Patrick Mc Connell

Abstract

In mid 2004, after a lengthy period of industry consultation, the Basel Committee finally released its definitive proposals on capital charges for Operational Risk under Basel II. In its proposals for allowing ‘internationally active’ banks to calculate regulatory capital using their own internal models, the Basel Committee backed away from its original quantitative emphasis, concentrating instead on ‘qualitative standards’ for Operational Risk Management (ORM) systems. In doing so, however, the Basel Committee gave few concrete clues as to what such ‘systems’ should look like. The lack of clear direction raises serious questions for banks in developing their approaches to managing operational risk and for supervisors in creating a level playing field between banks with differing approaches.

This paper proposes an approach to evaluating the ‘quality of compliance’ of ORM systems within, and between, firms and is based on concepts proven in other industries, specifically the concept of ‘Maturity Models’.

Keywords

Basel II Regulation,
Operational Risk,
Advanced Measurement Approach,
COSO Enterprise Risk Management,
Maturity Model

Introduction

In June 2004, the Basel Committee released the ‘Revised Framework for the International Convergence of Capital Measurement and Capital Standards’, which contained the definitive proposals on capital charges for Operational Risk under Basel II (Basel 2004). Under proposals for allowing “internationally active” banks to calculate regulatory capital using their own internal models – so called AMA (Advanced Measurement Approaches) - the Basel Committee backed away from dictating explicit methodologies for calculating operational risk capital charges¹ towards a more qualitative approach to the management of Operational Risk.

In their final proposals, the Basel Committee stressed the importance of ‘qualitative standards’ for banks that wish to use an AMA for management of their operational risks². However, other than urge that an Operational Risk Management (ORM) system must be “conceptually sound and implemented with integrity”, the Basel Committee gave few clues as to what such a ‘system’ might look like. Furthermore, Basel II states that any system developed and implemented by a bank must be “credible and appropriate”, “well reasoned”, “well documented” and “transparent and accessible”. Unfortunately, phrases such as ‘credible’, ‘well reasoned’, and ‘transparent’ are subjective and are open to interpretation by banks and their regulators.

The lack of clarity in the Basel II definitions of Operational Risk raises some very important practical questions for banks, in particular:

- What would a ‘conceptually sound’ ORM system look like?
- How can regulators compare one bank’s ORM system with another and, by implication, how can Operational Risk capital charges be compared – i.e. what constitutes a regulatory level playing field?
- Internally, what criteria can a bank use to allocate economic capital across its business units to satisfy the Basel qualitative standards for being “integrated into the day-to-day risk management processes of the bank”?

These questions are far from trivial. Banks are beginning to invest considerable sums of money and effort in developing the ORM systems necessary for Basel II, and they are doing so somewhat in the dark as to what will be acceptable. The Basel Committee can also change the ground rules and have reserved the right, prior to implementation, to “review evolving industry practices, ... review accumulated data, and the level of capital requirements estimated by the AMA, and may refine its proposals if appropriate” (Basel 2004). This ambiguity creates a level of uncertainty (and operational risk) that the industry should address - sooner rather than later.

As part of the on-going research called for by Basel Committee, this paper considers the important questions raised by the ambiguity in the Basel II proposals and suggests mechanisms, proven in other industries, for evaluating ORM systems both within, and between, banks. After summarising the Basel II proposals on Operational Risk, the paper provides an overview of the COSO framework and its “Key Principles”. The paper then describes the concept of a ‘Maturity Models’ before proposing the concept of an ‘Operational Risk Management Maturity Model’

¹ The Basel committee specified only that AMA models must be based on a 99.9th percentile confidence interval of a distribution constructed from internal and external loss data.

² Note that many of the same qualifying criteria also apply to the use of the Standardised Approach (SA) in calculating operational risk capital for Basel II.

(ORMMM). Finally, the paper describes how such a model could be used to measure the quality of ORM compliance across the industry.

Operational Risk Management under Basel II

The final Basel II proposals stipulate that an Operational Risk Management ‘system’ must be implemented by an independent operational risk management function responsible for developing and implementing “strategies, methodologies and risk reporting systems ... to identify, measure, monitor and control/mitigate operational risk” (Basel 2004). To comply with these qualitative standards, any ORM system must also be capable of being “validated” or reviewed regularly by internal and/or external auditors and be seen to “have and maintain rigorous procedures”. Such reviews “must include both the activities of the business units *and of the operational risk management function* [author’s emphasis].”

To qualify to use the AMA approach to calculate operational risk capital under Basel II, a bank must meet stringent “qualitative standards”, in summary (Basle 2004, section 666):

- An independent operational risk management function.
- An operational risk measurement system that is closely integrated into the day-to-day risk management processes of the bank.
- Regular reporting of operational risk exposures to business units, senior management, and the Board, with procedures for appropriate action.
- The operational risk management system must be well documented.
- Regular reviews of the operational risk management processes/systems by internal and/or external auditors.
- Validation of the operational risk measurement system by external auditors and/or supervisory authorities, in particular, making sure that data flows and processes are transparent and accessible³.

How can banks ensure that the ORM systems, in which they are about to invest considerable sums of money, will be able to comply with such subjective criteria when tested by their local banking supervisors?

To qualify to use the AMA approach, Basel (2004 section 665) states that a “bank’s measurement system must also be capable of supporting an allocation of economic capital for operational risk across business lines in a manner that creates incentives to improve business line operational risk management.”

This implies a commitment to ‘continuous improvement’ of operational risk management, and associated operational risk management processes, across the organization.

While specifying that calculation of regulatory capital must be based on a detailed analysis of ‘internal loss data’, the Basel committee recognises, however, that ‘subjective adjustments’ may have to be made and notes that (Basel 2004 section 671):

“internal loss data is most relevant when it is clearly linked to a bank's current business activities, technological processes and *risk management procedures* Therefore, a bank

³ In raising the bar on how ORM systems must be documented, Basel (2004 section 666) states, “it is necessary that auditors and supervisory authorities are in a position to have *easy access* [author’s emphasis], whenever they judge it necessary and under appropriate procedures, to the [ORM] system’s specifications and parameters.”

must have documented procedures for assessing the on-going relevance of historical loss data, including those situations in which *judgement overrides, scaling, or other adjustments may be used*, to what extent they may be used and who is authorised to make such decisions” [author’s emphases].

The Basel committee also recognises, that internal loss data can provide only part of the picture and notes that (Basel 2004 section 676):

“in addition to using loss data, whether actual or scenario-based, a bank’s firm-wide risk assessment methodology must capture *key business environment and internal control factors that can change its operational risk profile*. These factors will make a bank’s risk assessments more forward-looking, more directly reflect the quality of the bank’s control and operating environments, help align capital assessments with risk management objectives, and *recognise both improvements and deterioration in operational risk profiles in a more immediate fashion* [author’s emphases].”

These directives imply that any ORM system aiming to qualify for AMA status, must be aware of, and be closely aligned with, the business strategies of the firm and the external factors that could impact its risk profile.

How can banks create the necessary ORM systems when the Basel terminology is (deliberately?) vague? What, for example, constitutes ‘actively involved’, ‘conceptually sound’, ‘implemented with integrity’, ‘well documented’, ‘transparent’ or ‘accessible’? Furthermore, how does one evaluate if ‘sufficient resources’ have been allocated to an ORM system?

On an industry basis, how can the soundness and integrity of ORM systems be compared across banks of different sizes, operating in different markets – the regulatory problem of ‘capital adequacy’? Within an individual firm, how can ORM systems be compared across business units – the business problem of ‘economic capital allocation’? These are serious questions that must be addressed with some urgency, given the impending deadlines of Basel II implementation in 2007.

To help answer these questions, we can pose two, more general, questions:

1. Is there a set of (reasonably) objective criteria that could be used to evaluate the ‘quality of compliance’ of a particular ORM system?
[*Quality* here would encompass all of the ‘qualitative standards’ identified in Basel II.]
2. If such a set of criteria exists, is there a mechanism whereby the ‘quality of compliance’ of a particular ORM system’s implementation can be compared against other implementations within a bank and with similar situations in other banks?

This paper argues that there are proven models/frameworks that can be used to provide a ‘conceptually sound’ basis for answering these questions and to help create a ‘level playing’ field for evaluating ORM systems under Basel II. Specifically:

1. The recently published COSO standard for Enterprise Risk Management (COSO 2004) describes a set of “Key Principles” for creating an effective ‘risk management process’ in an organization. While these Key Principles are generic they are comprehensive (120 in all) covering the full spectrum of activities in a generic risk management process. To be applicable to Operational Risk Management under Basel II, the *specific* criteria for satisfying these principles for Operational Risk would have to be identified.

2. The concept of a ‘Maturity Model’ has been developed in the IT industry as a means of evaluating, on a reasonably objective basis, where a particular organization stands relative to its peers in the quality of its ‘software development processes’. The concept has been extended from the original CMM (Capability Maturity Model) to measure the maturity of other management practices, such as development of staff (People Maturity Model – PMM) and Project Risk Management (PRMM).

The paper argues that together these two models, or ‘frameworks’⁴, provide a solid platform for objectively evaluating the ‘quality of compliance’ of ORM systems under Basel II. After giving a brief introduction to these two frameworks, the paper describes how, in combination, they may be used to develop evaluation processes and how they may be used by banks and regulators to improve the management of Operational Risk across the industry.

The COSO ERM Framework

In the early 1990s, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) published the ‘Internal Control – Integrated Framework’ to help “businesses and other entities assess and enhance their internal control systems” (COSO 2004). Promoted by global auditing and accounting bodies, this framework has been widely used in thousands of firms to improve their controls. During the 1990s, the need for improved risk management was identified as a major concern across industries and governments and COSO, reacting to this need, initiated a project in 2001 to develop a framework that would help management to improve their organizations’ ‘enterprise risk management’⁵. The resulting ‘Enterprise Risk Management – Integrated Framework’ expanded on the Internal Control framework, aiming to provide “a more robust and extensive focus on the broader subject of enterprise risk management”.

The COSO ‘Enterprise Risk Management (ERM) – Integrated Framework’ defines ERM as a **process** (COSO 2004)

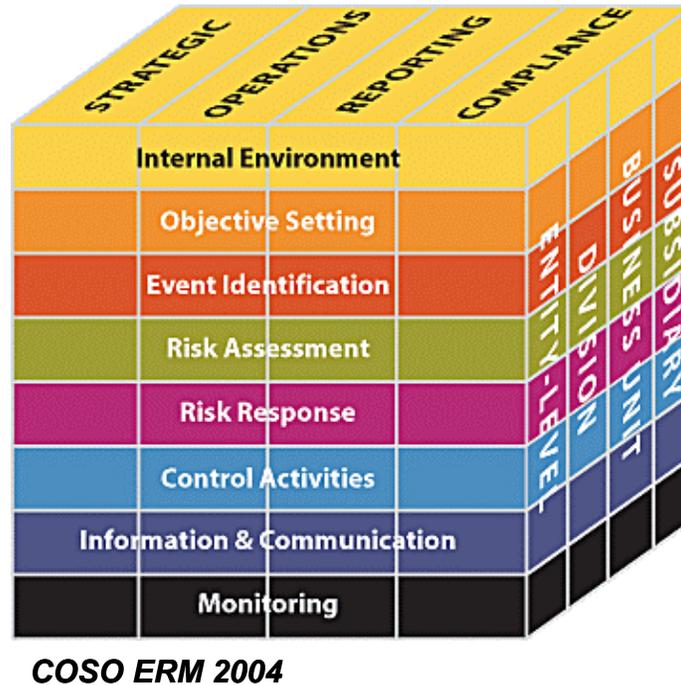
“effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives”.

The COSO ERM Framework shown in Figure 1 below consists of eight ‘components’ organized by four ‘objectives’: Strategic; Operations; Reporting; and Compliance. The third dimension of this ERM matrix/cube is organizational: Subsidiary; Business Unit; Division, and Entity. COSO (2004) notes that the ERM Framework is “purposefully broad”, capturing “key concepts fundamental to how companies and other organizations manage risk, and may be applied across “organizations, industries, and sectors.”

⁴ In this paper, the term “framework” is used rather than “system” because of the confusion that can arise between IT and management systems. While IT systems are essential components of the management of Operational Risk under Basel II, they are only one part of a much more wide-ranging framework, involving people, processes and organisations.

⁵ It should be noted that there are a number of national ‘risk management standards’ upon which COSO drew in developing the ERM. The first was developed by Standards Australia/New Zealand in 1995 (AS/NZS 4360:1995), followed by Canada (CAN/CSA-Q850) in 1997 and the United Kingdom (BS-6079-3) in 2000. The International Standards Organisation (ISO) and the European Union (EU) are also working on standards for risk management terminology. The AS/NZS standard has recently been updated as AS/NZS 4360:2004, which is almost identical to COSO.

Figure 1 – COSO Enterprise Risk Management – Integrated Framework



The eight ‘components’ of the ERM process are (COSO 2004):

- **Internal Environment:** establishing the ‘tone’ of an organization, including “risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate”.
- **Objective Setting:** ensuring that “management has in place a process to set objectives and that the chosen objectives support and align with the entity’s mission and are consistent with its risk appetite”.
- **Event Identification:** identifying internal and external events (i.e. risks and opportunities) that effect the achievement of a firm’s objectives.
- **Risk Assessment:** analysing risks “considering likelihood and impact, as a basis for determining how they should be managed.”
- **Risk Response:** selecting ‘responses’ to identified risks and developing “a set of actions to align risks with the entity’s risk tolerances and risk appetite”.
- **Control Activities:** establishing and implementing policies and procedures “to help ensure the risk responses are effectively carried out.”
- **Information and Communication:** identifying, capturing and communicating information that is relevant “in a form and timeframe that enable people to carry out their responsibilities.”
- **Monitoring:** Monitor the risk management process and modifying the process as necessary.

COSO (2004) points out that Enterprise Risk Management is “not static, but rather a continuous or iterative interplay of actions that permeate an entity. These actions are pervasive and inherent in the way management runs the business.”

Basel II identifies the responsibilities of the independent Operational Risk Management function as “developing strategies to identify, assess, monitor and control/ mitigate operational risk”. It can be seen that the Basel responsibilities are, not surprisingly, aligned very closely with the COSO ERM Framework, with the addition of two components – Internal Environment and Objective Setting – which are identified in Basel as responsibilities of the Board and Management. COSO’s remit is comprehensive, covering all levels of an organization in line with Basel II qualitative standards.

Given the breadth and depth of effort that has been put into developing it, and earlier frameworks, the COSO ERM Framework should satisfy Basel II qualitative standards for being ‘conceptually sound’, ‘credible and appropriate’ and ‘well reasoned, well documented’. However, other Basel II qualitative criteria, such as ‘implemented with integrity’, ‘active involvement’, ‘sufficient resources’, ‘transparent’ and ‘accessible’ are functions not of the ERM Framework itself but how well it has been implemented in a particular situation. Before considering how those ‘implementation criteria’ may be evaluated, the ‘Key Principles’ of the COSO ERM Framework are discussed.

COSO ERM Framework – Key Principles

Appendix B of the COSO ERM Framework (COSO 2004) identifies 120 ‘Key Principles’ that are “inherent in the eight enterprise risk management components”. It should be noted that COSO gives a caveat that “Appendix B ... purports neither to precisely or fully describe the principles set forth in the Framework, nor to represent a complete list of principles”. Nonetheless, it is probable that this initial list is rich enough to cover the needs of the emerging discipline of Operational Risk Management and it would only be after considerable experience in the field that the Key Principles might require significant amendment.

It is not the purpose of this paper to list the full set of principles, which are available in COSO (2004), but to illustrate by example. Table 1 below shows a subset of the Key Principles in the ‘Risk Response’ component of the COSO/ERM.

Table 1 –COSO/ERM – Selected Key Principles

COSO Component	Element	Key Principles
Risk Response		In responding to risk, management considers among risk avoidance, reduction, sharing, and acceptance
	Evaluating Possible Responses	
		Responses are evaluated with the intent of achieving residual risk aligned with the entity’s risk tolerances
		In evaluating risk responses, management considers their effects on likelihood and impact
		Management considers their costs versus benefits, as well as new opportunities
	Selected Responses	
		Responses chosen by management are designed to bring anticipated risk likelihood and impact within risk tolerances
		Etc.

As the selected subset shows, each Key Principle addresses one aspect of one specific ‘element’ within a single component of the ERM (here Risk Response). Each principle is articulated as high-level statements of ‘competence’ in a particular aspect. Taken as a whole, these principles are a rich recipe for developing and implementing a comprehensive ORM system.

It should be noted that this paper does not argue that COSO/ERM is the only risk management model upon which a ‘conceptually sound’ system could be built. For example, the AS/NZS 4360: 2004 Risk Management Framework is almost identical to COSO/ERM and has some advantages in that it is based on experience gained with a successful earlier version (i.e. AS/NZS 4360:1999). However, COSO/ERM has already done some of the difficult work of developing a comprehensive set of Key Principles to support its processes; of course, this could also be done for AS/NZS 4360:2004 if that framework was preferred by a particular bank/jurisdiction.

Maturity Models

The concept of maturity (or capability) models can be traced back to the pioneering work of Philip Crosby on ‘Quality’. In reflecting on successful implementations of quality management systems, Crosby (1979) noted that management do not immediately accept complex concepts, such as quality, but evolve their understanding of, and competence in, such concepts over a (potentially long) period of time. In his QMMG (Quality Management Maturity Grid), Crosby identified five ‘phases’ of acceptance of a new ‘quality system’ within an organization: “Uncertainty, Awakening, Enlightenment, Wisdom, and Certainty”. Crosby’s ideas of ‘process evolution’ through five stages have been adopted in other situations, in particular to manage the processes of developing complex software in the IT industry.

Building on work by IBM in the 1980s, the Software Engineering Institute (SEI) developed the influential “Capability Maturity Model”, known as the CMM or lately as CMMI⁶. SEI (2002) identifies the purpose of the CMMI as:

“To provide guidance for improving [an] organization’s processes and [the] ability to manage the development, acquisition, and maintenance of products or services. CMM Integration places proven approaches into a structure that helps [an] organization appraise its organizational maturity or process area capability, establish priorities for improvement, and implement these improvements.”

This purpose could equally well apply to the implementation of a new Operational Risk Management process as to a software development one.

The five stages of process evolution within CMMI are identified as (SEI 2002)⁷:

1. **Initial** - processes are usually “ad hoc and chaotic”.
2. **Managed** - processes are “planned, performed, measured, and controlled”.
3. **Defined** - processes are “well characterized and understood, and are described in standards, procedures, tools, and methods”.

⁶ In 2002, SEI upgraded and generalized the representation of its CMM for Software to take into account many years of practical experience using CMM upgrading the model and renaming it CMMI or CMM Integration.

⁷ Confusingly, the terminology of CMMI differs slightly from the earlier CMM, where the 5 phases were identified as: Initial, *Repeatable*, Defined, *Managed* and Optimising.

4. **Quantitatively Managed** – processes are “predictable” in that “quality and process performance are understood in statistical terms and are managed throughout the life of the processes”.
5. **Optimising** – processes are ‘continually improved’ based on “a quantitative understanding of the common causes of variation inherent in processes”.

In the CMMI model, organizations move from a situation where there is little common understanding of a particular process/problem through increased awareness and measurement until the process becomes an integral part of ‘doing business’. This progression from qualitative, ‘seat of the pants’ management to continuous improvement based on well-understood quantitative measures is clearly in line with the objectives of Operational Risk Management under Basel II. It is also aligned with other process improvement approaches, such as Six Sigma (George 2003).

Lainhart (2001) identifies some of the benefits of taking a ‘Maturity Model’ approach to process implementation and improvement in IT, which can be generalised to other complex management processes. He notes that a maturity model, such as CMMI:

- Provides a ‘scale’ that lends itself to ‘pragmatic comparison’ between implementations of the same process in different situations.
- Provides a scale where differences can be easily measured.
- Is recognisable as a “profile” of the enterprise in relation to a particular process.
- Assists in determining “As-Is” and “To-Be” positions relative to a process and its maturity.
- Lends itself to doing “Gap Analysis” to determine what needs to be done to achieve a chosen maturity level for a particular process; and
- Is not industry specific or generally applicable since “the nature of the business will determine what is an appropriate level”.

If, therefore, a ‘Maturity Model’ approach were to be applied to the process of Operational Risk Management, it would help to answer the second question posed above, “is there a mechanism whereby the ‘quality of compliance’ of a particular ORM system’s implementation can be compared against other implementations within a bank and with similar situations in other banks?” In order to answer this question fully, however, it is necessary to identify the criteria that would constitute each maturity level in an Operational Risk Management Maturity Model (ORMMM).

Operational Risk Management Maturity Model

The Table below is proposed as a starting point for developing an Operational Risk Management Maturity Model (ORMMM)⁸. The relevance of COSO ERM concepts is also identified at each level.

Table 2 – Proposed Operational Risk Management Maturity Model

Maturity Level	Criteria	Relevance of COSO - ERM
1 Initial	Management recognise that Operational Risk Management needs to be addressed but there are no standardised processes in place and Operational Risk issues (such as major losses) are only addressed reactively.	There is no awareness of the COSO ERM framework or other comprehensive risk management model.
2 Managed	Management are aware of Operational Risk Management issues, and selected processes have been identified and implemented, but standardised measurement has not been implemented across the organization.	Selected 'components' of the CSO ERM have been implemented across selected businesses (e.g. consistent Risk Assessment). Operational Risk Management organizational structures have been identified but not fully staffed. Management react to 'crises'.
3 Defined	Standardised Operational Risk Management processes are in place across the organization, performance is being monitored but root cause analysis of problems is only occasionally being applied.	The CSO ERM has been implemented across those businesses with most Operational Risk. ORM staffing is complete. No consistent quantitative measurements of performance are in place and management actions are initiated only to address critical issues.
4 Quantitatively Managed	Standardised processes are in place and responsibilities and process ownerships are clearly defined. Operational Risk Management processes are aligned with business strategy. Quantitative measurements, such as Key Risk Indicators (KRI), are in place for all processes and economic capital is being allocated against these measures. However, there are no continuous improvement programs in place to align Operational Risk with the organization's 'risk appetite'.	All 'components' of the CSO ERM have been implemented across most businesses. Consistent monitoring is in place and information flows to all levels of management. External experts are employed to assess the operation of all processes. Management actions are initiated to reduce areas of significant Operational Risk.
5 Optimised	'Best practice' Operational Risk Management processes are in place and are closely aligned with business strategies. Costs and benefits of Operational Risk Management are defined, are balanced against risks and are communicated and applied across the whole organization.	The full COSO ERM framework is in place across the organization and being <i>applied</i> by all levels of management. Management have funded plans to improve the level of Operational Risk Management Maturity of all businesses.

A model, such as that proposed above, could be used to evaluate the quality of ORM systems in different ways:

1. A firm could identify a standardised ORM process – not necessarily COSO/ERM – and evaluate each of their businesses against such a maturity model, allocating economic capital to each business unit based on the level of competence achieved.
2. A firm could identify target maturity levels for each of their businesses (depending on economic capital employed) and reward businesses for attaining their targets.

⁸ These descriptions are loosely based on models of best practice IT Governance as proposed by the IT Governance Institute (ITGI) www.itgi.org

3. A regulator could identify target levels, and associated criteria, for various levels of compliance with Basel II regulations⁹.
4. As with the IT industry, maturity levels of banks, and their constituent businesses, in Operational Risk Management could be assessed by independent experts and openly reported to the marketplace, in support of Basel’s ‘Third Pillar’ of ‘Market Discipline’ (Basel 2004).

Integrating COSO with the ORMMM

It order to integrate the concept of COSO/ERM with the Operational Risk Management Maturity Model (ORMMM), some work remains to be done; the major task being, to expand the Key Principles of the COSO/ERM so that they can be used as criteria’ for evaluating ‘maturity level’. To achieve this, each COSO/ERM Key Principle would have to be re-phrased in such a way that (instead of a simple Yes/No answer) compliance with a particular principle could be evaluated on a 5-point scale.

For example: a Key Principle associated with the ‘Monitoring’ component of COSO is:
 “Monitoring activities are built into the entity’s normal, recurring operations, performed in the ordinary course of running the business”.

In order to align with the proposed Maturity Model, such a question would have to be re-phrased to produce a numeric score, in the range 1-5, for example as shown in the table below.

Table 2 – Example of ORMMM ratings for a Selected Key Principle
 “Select the most appropriate rating for Monitoring of ORM activities (as defined by COSO/ERM) for the business/organization being evaluated:

Rating	Level of Maturity
1	- While there is some monitoring, there are NO standards for ORM Monitoring processes within units of the business/ organization being evaluated.
2	- There is some standardisation of Monitoring ORM processes within units of the business/ organization being evaluated, but no consistent measurement or reporting between the various units. - Periodic reports to management are produced by staff outside of the business line.
3	- Monitoring of ORM processes has been standardised in units identified as having the highest Operational Risk of the business/organization being evaluated. - There are consistent qualitative measures and reporting across those units. - Regular reports to management are produced, in a standardised format, by designated staff within the operational units of the business/organization being evaluated.
4	- Monitoring of ORM processes has been standardised in all units of the business/ organization being evaluated (excepting those units formally exempted as having negligible risk). - There are consistent quantitative measures of performance and reporting across all units. - Reports are produced on a regular (at least weekly basis) by staff within the business line, and deficiencies, progress against treatment plans, and trends are reported to management on a regular basis. - All supervisory staff within the business line have been trained in the production of these reports and the results are discussed formally at staff meetings.

⁹ It is probable, for example, that firms complying with the criteria for levels 1 or 2 in the proposed model would not qualify for using AMA approaches under Basel II, whereas levels 4 & 5 would qualify. Businesses at maturity level 3 could, for example, be gauged as compliant, or otherwise, depending on the firm’s plans/commitments to improve beyond that level, at least for those businesses with the greatest operational risk.

5	<ul style="list-style-type: none"> - Monitoring of ORM processes has been standardised in all units of the business/ organization being evaluated with consistent quantitative measures of performance and reporting across all units. - Production of, and action against, reports are part of the day-to-day activities of all operational units. - Improvements to the Monitoring process have been identified, measurable targets articulated and implementation plans developed and monitored.
---	--

The numeric score for this question, plus the 119 others, could then be averaged (with some weighting of individual categories if necessary) to produce an overall score for Operational Risk Management Maturity of the business/organization being evaluated¹⁰. While an ORMMM score, such as that proposed above, could be used numerically, for example to allocate economic capital for Operational Risk¹¹, its main use would be in allowing management to set and monitor targets for improving ORM processes across an organization.

Application of an ORMMM for Basel II

The objective of the proposed ORMMM is not only to develop a ‘conceptually sound’ model for evaluating ORM systems that need to comply with Basel II but also to provide practical tools for assisting Boards and management in developing and improving their management of Operational Risks.

Attachment A shows a hypothetical example of a ‘heat map’ that summarises the current state of ORM systems across an organization using the classification of ‘Business Lines’ mandated by Basel II against the high-level ‘components’ of COSO/ERM. The colouring of each cell (using ‘traffic lights’) indicates how far a business line is away from its target maturity level, e.g. green means on target. As recommended by COSO (2004) up/down arrows illustrate improvement, or otherwise, since the last report and, combined with the colour, indicate where current processes are deficient and where management action is needed. It should be noted that two additional rows have been added here, for the ORM function and the Board/Management. As these two groups are critical to the success of any ORM system their performance should also be evaluated and open reporting would, hopefully, demonstrate leadership and commitment to implementation of high quality ORM processes.

A ‘heat map’, in the format shown in Attachment A, should permit management to ‘drill down’ to identify areas that need attention and to initiate appropriate corrective action. For example, a similar ‘heat map’ could be created for each unit within the Trading & Sales business line, which is shown as ‘red’ in the example in Attachment A. Likewise a similar heat map could expand on a column, such as Information & Communication, using the Key Principles defined by COSO/ERM to show where effort is required to improve information flows throughout the organization.

¹⁰ As the ratings assigned to individual questions, and certainly any overall weighting applied, are still somewhat subjective, the precision of the overall ORMMM score is an important consideration. It is suggested that the result of the averaging be rounded to the nearest third of a point resulting in a more granular scale that can be interpolated between two levels as for example: 2, 2+, 3-, 3, 3+ etc.

¹¹ Obviously, calculation of economic capital would have to take into account not only an ORMMM score but also any history of Operational Losses. For regulatory capital purposes, Basel (2004) allows banks to make ‘adjustments’ to the capital calculated from analysis of Loss History. ORMMM scores could form the basis for making and justifying capital adjustments, such as demonstrating improvements to scores (and by inference the underlying ORM process/system) over time.

A ‘heat map’ similar to that in Attachment A that showed, in numeric terms, the ‘gap’ between actual and target maturity level for each business could also be used as the basis for allocating economic capital for Operational Risk across business lines, providing incentives to improve in line with the ‘risk appetite’ articulated by management. Such an allocation process would be in line with the requirements of Basel II for “supporting an allocation of economic capital for operational risk across business lines in a manner that creates incentives to improve business line operational risk management” (Basel 2004).

Further Research

As noted by the Basel Committee (Basel 2004), there are extensive opportunities for research into the topic of Operational Risk Management, covering both quantitative and qualitative methodologies. For this particular topic (i.e. compliance of ORM systems) there are several areas of further research, in particular:

- Empirical research into and case studies on the approaches, methods and tools that are being adopted by banks aiming to comply with AMA qualitative standards for Operational Risk Management.
- Research into the theories of Risk Management Processes and how banks might use those theories in complying with Basel II.
- Further consideration of the proposed approach, including:
 - (a) The applicability and deficiencies, if any, of COSO/ERM and various Maturity Models to Operational Risk Management as defined by Basel II.
 - (b) Developing the concepts of the ORMMM using COSO Key Principles, testing for ‘reliability’ etc.
 - (c) Consideration of how such a model may be used for allocation of economic capital.
- Studies into technology aspects of Operational Risk Management systems.

Summary

The final Basel II proposals are far from clear about precisely what banks are required to do to implement Operational Risk Management systems that will comply with the qualitative standards for using AMA approaches in calculating capital charges for Operational Risk. While this lack of clarity is a reflection of the paucity of research in the area, it leaves firms in the invidious position of trying to second-guess the meaning of subjective terms in Basel II, such as ‘conceptually sound’, ‘credible’ and ‘well-documented’.

This paper concludes that, in order to create a level playing field for firms across the industry (and for business lines within a firm), some objective measure of the ‘quality of compliance’ of ORM systems needs to be developed and a mechanism must be devised for evaluating and comparing such systems between and within firms. The paper argues that the ‘Key Principles’ of COSO’s Enterprise Risk Management (ERM) framework provide a reasonably objective measure of the quality of a particular ORM system. Furthermore, the paper argues that the concept of a Maturity Model, used in the IT industry, can be used to evaluate the level of maturity of a particular implementation of an ORM system against ‘best practice’. This paper proposes combining these two proven concepts into an Operational Risk Management Maturity Model (ORMMM).

Though still somewhat subjective, the use of a consistent and comparable measure of the ‘compliance maturity’ of ORM systems would not only allow regulators to compare ORM systems in banks across the industry (and to set criteria for compliance with regulatory requirements) but also would allow firms to allocate economic capital according to the ORM maturity of its business lines. Both regulators and firms can then set measurable targets to improve Operational Risk Management within their respective areas of responsibility.

References

- Basel (2004) “International Convergence of Capital Measurement and Capital Standards - A Revised Framework”, Basel Committee on Banking Supervision. June
- COSO (2004) “Enterprise Risk Management – Integrated Framework” The Committee of Sponsoring Organizations of the Treadway Commission (COSO) <http://www.coso.org>
- Crosby P. B. (1979) “Quality is Free: The Art of Making Quality Certain”, McGraw-Hill
- IIA (2004) “Position Statement - the Role of Internal Audit in Enterprise Wide Risk Management”, The Institute of Internal Auditors UK and Ireland
- George M. L. (2003) Lean Six Sigma For Service Mc Graw Hill
- Lainhart J. W. (2001) “COBIT Management Guidelines IT Governance Forum Trust and Understanding for the Business and the Board”, ITGI Paris
- SAI (2004) “AS/NZS 4360: 2004 – Risk Management and HB 436:2004 - Risk Management Guidelines - Companion to AS/NZS 4360: 2004”, Standards Australia/Standards New Zealand <http://www.standards.com.au>
- SEI (2002) “Capability Maturity Model[®] Integration (CMMISM), Version 1.1”, Software Engineering Institute, Carnegie Mellon University, Pittsburgh

Author

Patrick Mc Connell is a partner in Risk Trading Technology, a consultancy that specializes in methodologies for quantifying and mitigating Operational Risk, in particular Causal Modeling and Simulation. His background is in the field of Information Technology strategy, as applied to the Financial Services Industry, and for many years he has worked with major financial institutions in the USA, Europe and Australia. Dr. Mc Connell holds a Doctorate in Business Administration from Henley UK, and a Masters in Operational Research. He is member of the IEEE, an adjunct of Macquarie Business School, Sydney, and has published many articles on the application of IT to Finance and Risk Management in academic and practitioner journals. If you would like further information please contact by email at pjmconnell@computer.org

Measuring Operational Risk Management Systems under Basel II

Attachment A – Example of an ORMMM Heat Map

	Internal Environment	Objective Setting	Event Identification	Risk Assessment	Risk Response	Control Activities	Information & Communication	Monitoring	OVERALL
Corporate Finance	□	↑	↑	↓	↓	↑	↑	↑	□
Trading & Sales	↓	↑	↑	□	↑	□	↑	↑	↓
Retail Banking	↑	↑	□	↓	↑	↓	↑	↓	↑
Commercial Banking	□	□	↓	↑	□	↑	□	↑	□
Payment & Settlement	↓	↓	↑	↓	↓	↓	↓	↓	↓
Agency Services	↑	↓	↑	↓	↓	↑	□	↑	↓
Asset Management	↑	↑	↑	↑	↑	↑	↓	↑	↑
Retail Brokerage	□	□	↑	□	↑	□	↑	↑	□
ORM Function	↑	↑	↓	↑	↑	↓	↑	↓	□
Board & Management	□	↑	□	↑	↓	□	□	↑	↑
OVERALL	□	↓	↑	□	↓	↑	□	↑	□

