A 'Standards Based' approach to Operational Risk Management under Basel II

Patrick Mc Connell

Introduction

In June 2004, the Basel Committee finally released the 'Revised Framework for the International Convergence of Capital Measurement and Capital Standards' - in effect, the definitive Basel II proposals on Operational Risk. During the three years prior to final publication, consultation with the industry had resulted in a pronounced switch in emphasis, away from a mainly quantitative, towards a more qualitative, approach to the management of Operational Risk.

Under proposals for allowing "internationally active" banks to calculate capital using their own internal models – so called AMA (Advanced Measurement Approaches) - the Basel Committee backed away from dictating any explicit methodologies for calculating operational risk capital charges[1], stressing instead the importance of qualitative standards for management of operational risks (Basel 2004). Other than urging that an Operational Risk Management (ORM) system must be "conceptually sound and implemented with integrity", Basel II, however, gave few clues as to what such a 'system' might look like. As banks (and their regulators) are about to begin investing large sums of money and effort in developing the ORM systems necessary for Basel II, it is timely to consider whether there are models outside of Finance that could usefully be employed in this context.

This paper argues that:

- The wording of Basel II is sufficiently vague that banks are in danger of developing internal ORM systems that run the risk of not complying with interpretations of Basel II by local supervisors.
- However, there are mature frameworks[2] from other industries upon which the *processes* of Operational Risk Management could be based.
- In particular, there are two risk management standards - AS/NZS 4360/2004 and COSO/ERM – that, alone or in combination, could satisfy the requirements of Basel II for systems that are 'conceptually sound'; and
- The adoption of operational risk management processes that are based on proven, practical and usable standards, should reduce the overall costs to the industry of complying with Basel II.

In January 2004, the National Australia Bank (NAB) reported losses in excess of $350 million, due to 'irregular' options trading. The regulatory report into these losses contains some very pertinent lessons for management and supervisors, not least the need to develop a robust risk management 'culture' across an organisation. It is disconcerting to note that almost identical problems were revealed in the regulatory reports into earlier losses at Barings and Allied Irish Bank. Nevertheless, despite the publicity given to these events, almost identical failures of internal controls and operational risk management occurred at NAB. This paper illustrates how standards based framework[3], such as AS/NZS 4360: 2004, could be used to address some of the serious problems highlighted by regulators in these cases.

Operational Risk Management under Basel II

The 2004 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". Furthermore, the Basel II Committee states that the framework developed and implemented by a bank must be "credible and appropriate", "well reasoned, well documented" and "transparent and accessible". To comply with regulations, the framework must also be capable of being "validated" and reviewed regularly by internal and/or external auditors and be seen to "have and maintain rigorous procedures".

While Basel II uses words such as, 'credible', 'well reasoned', and 'transparent', these are, unfortunately, subjective and open to some interpretation by banks and their regulators. How can banks ensure that the ORM systems, in which they are have invested considerable sums of money, are able to meet such subjective criteria when tested by their local banking supervisors? In a warning to banks, the Basel Committee 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". This lack of clarity creates a level of uncertainty (and operational risk) that the industry must address, sooner rather than later.

One of the key differences between the management of operational risks and credit/market risks that has been overlooked during the Basel II debate is the size and sophistication of the respective 'risk taking' communities. The relatively small group of people who make credit and market risk-taking decisions in banks consist of dedicated professionals who tend to be experienced and well educated and are supported by professional analysts and subject matter experts. The independent risk managers, who monitor their credit and market risk-taking colleagues, tend also to be well educated and are increasingly professional, belonging to industry-wide certification bodies, such as GARP.

On the other hand, operational risks are 'taken' by all levels of staff in banks on a daily basis. For example, a decision to employ a new member of staff; to accept confirmation of a trade; or to change a working process or computer system, all involve taking some level of operational risk, albeit small. Should it be argued that such risk-taking examples are trivial, these activities are just some of the examples of "lax decision making" that were strongly criticised by the report of the Australian Prudential Regulatory Authority (APRA) into the recent trading losses at the National Australia Bank (APRA 2004). Risk taking is not in the job description of the typical operational supervisor, but under Basel II an understanding of operational risk will have to become an integral part of their day-to-day work. At the very least, this implies that banks must, under Basel II, undertake a significant risk training and education programme for their managers and front line staff. Given the high level of mobility within, and between, banks, particularly of operational staff, this need for education and training will rapidly become an industry-wide, rather than an individual firm, problem.

In recognising the need to ensure credibility, Basel II requires that ORM systems developed by banks must be "subject to validation and regular independent review" and must use "risk management experts to derive reasoned assessments of plausible severe losses". In addition to an increased role for internal and external auditors, the Basel II proposals imply a new and heightened level of scrutiny of operational decision-making across banks. At the very least, Basel II implies a need for operational managers to document their decisions *and assumptions* clearly. In practice, this also implies some standardisation of 'risk management processes' so

that external auditors and experts can quickly come to grips with the rationale for the risk-taking decisions being reviewed.

The need to raise the level of understanding of how operational risks are created and how they should best be managed, argues strongly for developing industry-wide standards that not only allow staff and skills to be transferable between institutions but also permit independent validation and review, improving transparency for all concerned.

Risk Management Processes

Much of the theory underlying the **process** of risk management is based on the work of Nobel Prize winner Herbert A. Simon, who identified three basic 'phases' of 'decision-making under risk and uncertainty': intelligence, or risk identification; design, or risk analysis/ assessment; and choice/implementation, or risk mitigation/treatment. Most formalised approaches to risk management, such as project risk management[4], are based on these three key activities, usually augmented by an activity of monitoring/controlling risks.

Many formal approaches to risk management address important public concerns such as Health and Safety (H&S) or the Environment, for example in the design of nuclear power plants. In light of large-scale public crises, such as the BSE and SARS crises, governments around the world are becoming increasingly interested in risk management at the policy level[5].

There are a number of national 'standards' for risk management. The first was developed by Standards Australia/New Zealand in 1995 (AS/NZS 4360), 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, or at least standard terminologies, for risk management. In 2001, COSO (the Committee of Sponsoring Organisations of the Treadway Commission), which comprises US accounting and auditing standards bodies, initiated a project to define a so-called 'enterprise risk management framework' within the context of corporate governance[6]. After a lengthy period of consultation, the final COSO document was delivered in late 2004 as the 'Enterprise Risk Management – Integrated Framework'.

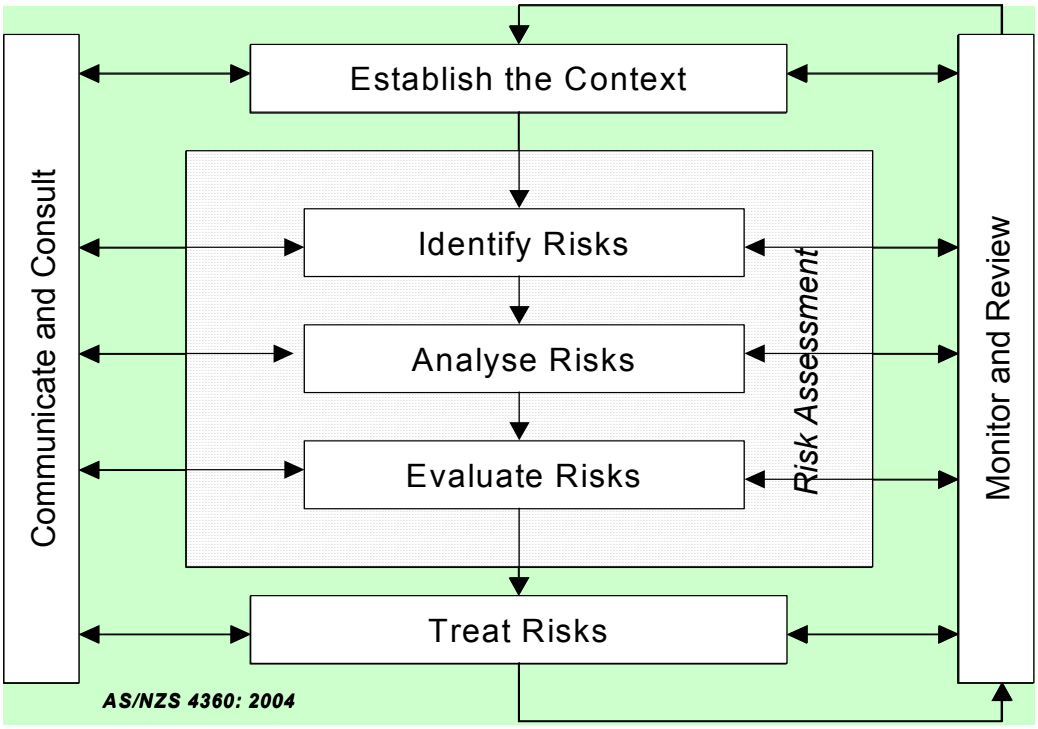
The AS/NZS 4360: 2004 Framework

Of the existing international standards, AS/NZS 4360 is the oldest, and arguably the most popular, being the basis for several industry/issue specific implementations (such as HB 240:2000 for managing outsourcing risk - an issue recently highlighted in Basel II). This standard has been revised over time, first in 1999 before being recently upgraded and re-published in 2004, in particular to place a greater emphasis on "embedding [systematic] risk management practices in an organisation's culture and processes" (SAI 2004).

In the standard, AS/NZS 4360: 2004 is described as a "generic guide" for managing risk that may be applied to a wide range of public or private activities or operations. While its broad scope and lack of industry-specific features require that additional work would be needed for the standard to be applicable to Operational Risk Management under Basel II, the AS/NZS 4360: 2004 standard provides a practical framework for developing a 'culture' that aligns risks (including both potential losses and gains) with the business strategies of a company[7].

The AS/NZS 4360:2004 standard defines a 'Risk Management Process' as the "systematic application of management policies, procedures and practices to the tasks of communicating, establishing the context, identifying, analysing, evaluating, treating, monitoring and reviewing risk".

Figure 1 – AS/NZS 4360: 2004 - Risk Management Process



The AS/NZS 4360: 2004 Risk Management Process is shown in Figure 1 above and consists of seven main 'elements':

- **Establish the Context**: for strategic, organisational and risk management and the criteria against which business risks will be evaluated.
- **Identify Risks**: that could "prevent, degrade, delay or enhance" the achievement of an organisation's business and strategic objectives.
- **Analyse Risks**: consider the range of potential consequences and the likelihood that those consequences could occur.
- **Evaluate Risks**: compare risks against the firm's pre-established criteria and consider the balance between potential benefits and adverse outcomes.
- **Treat Risks**: develop and implement plans for increasing potential benefits and reducing potential costs of those risks identified as requiring to be 'treated'[8].
- **Monitor and Review**: the performance and cost effectiveness of the entire risk management system and the progress of risk treatment plans with a view to continuous improvement through learning from performance failures and deficiencies.
- **Communicate and Consult**: with internal and external 'stakeholders' at each stage of the risk management process.
  Note that Identify, Analyse and Evaluate Risks are collectively grouped as 'Risk Assessment'.

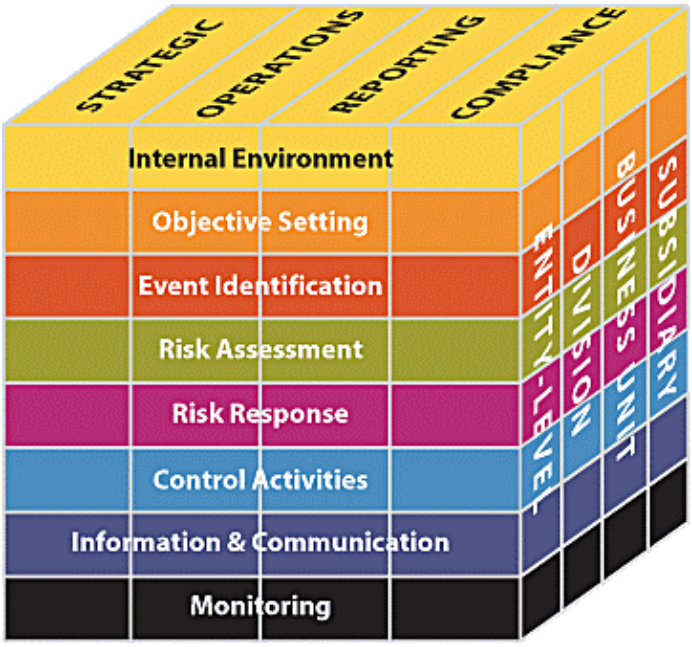
The COSO ERM Framework

In the early 1990s, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued the 'Internal Control – Integrated Framework' to help "businesses and other entities assess and enhance their internal control systems." Promoted by global auditing and accounting bodies, this framework has been widely used in thousands of firms to improve their internal controls. During the 1990s, the need for improved risk management was identified by the accounting and auditing profession as a major concern for its clients across industries and government. Reacting to this need, COSO initiated a project in 2001 to develop a framework that would be help management to improve their organizations' 'enterprise risk management'. 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, "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 is shown in Figure 2 below and consists of eight 'components' organized by four 'objectives': Strategic; Operations; Reporting; and Compliance. As befits an 'enterprise' or 'portfolio' approach to risk management, the third dimension of this ERM matrix/cube is organizational: Subsidiary; Business Unit; Division, and Entity.

Figure 2 – COSO Enterprise Risk Management – Integrated Framework



COSO ERM 2004

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 that could impact the achievement of a firm's objectives (both positively and negatively).
- **Risk Assessment**: analysing risks "considering likelihood and impact, as a basis for determining how they should be managed."
- **Risk Response**: selecting 'risk responses' 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 itself, modifying it as necessary.

COSO 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."

Comparing the two Risk Management Frameworks

The objectives of the AS/NZS 4360:2004 and the COSO ERM frameworks are **almost identical** aimed at helping organizations to achieve their business objectives through the effective management of internal and external risks. Both approaches recognize the importance of embedding a 'risk culture' in the organization and the need for change to be driven from the very top of the firm, its Board of Directors. Both approaches are *deliberately* broad in focus, recognising that there is no single template for risk management that can be applied to all business, in all industries.

In addition, both frameworks recognize that Risk Management is a **process** (though a very complex, multidimensional and iterative one) that requires multidisciplinary skills to implement and manage properly. In defining this process, both approaches emphasise the importance of clearly articulating the firm's business objectives and its 'risk appetite' in striving to achieve those objectives[9]. But merely setting risk policies and procedures at the top of the organization will not create an effective 'risk culture', the commitment to the highest standards of risk management must be communicated clearly to *all levels* of the organization. Both frameworks also agree that in order to be effective, the operation of the risk management process must be carefully 'monitored' and decisions at all levels must be 'reviewed'.

However, the emphasis of each framework is slightly different. As an international standard, AS/NZS 4360:2004 is aimed at consistency and attempts to define clearly *and sparingly* a 'common language' that can be applied widely by many different sizes of organization. While COSO has a broadly similar objective, it reflects its origins in the auditing and accounting

professions by emphasizing organizational structures and internal controls. The level of detail also reflects the different origins of the two frameworks. Whereas COSO tends to provide a mini case study to illustrate a particular aspect of the risk management process, the more technical origins of AS/NZS 4360:2004 are betrayed in example forms and lists of data elements. These differences, however, are not major and are manifested in the overall style rather than the content of the explanatory text[10].

From a practical perspective, the most obvious difference between the two frameworks is the slight, but nonetheless annoying, use of different terminology. For example, whereas AS/NZS 4360 uses 'Risk Treatment', COSO employs 'Risk Response' for the same basic process that Basel II in turn refers to as Risk Mitigation. Nor do the seven 'elements' of AS/NZS 4360:2004 align exactly with the eight 'components' of the COSO process although the 'end to end' process is identical[11].

However, differences in terminology and structure are relatively minor in the context of the very large problem that these two frameworks are attempting to address. While there will inevitably be proponents of each framework and differing views on terminology, it should not be difficult, as illustrated below, to meld the (best of the) two framework, together with the Basel II requirements, into a single coherent approach to create an Operational Risk Management system that satisfies the requirements of both banks and their regulators[12].

Basel II and the standard frameworks

Basel II identifies the responsibilities of the independent Operational Risk Management function as "developing strategies to identify, assess, monitor and control/ mitigate operational risk". These responsibilities map directly onto the AS/NZS 4360 and COSO frameworks as shown in the table below.

AS/NZS 4360: 2004 Framework	COSO ERM - Integrated Framework	Operational Risk under Basel II
Establish the Context	Internal Environment plus Objective Setting	*Implied by Basel II*
Identify Risks	Event Identification	Identify
Analyse Risks	Risk Assessment	Assess
Evaluate Risks	Risk Assessment	Assess
Treat Risks	Risk Response & Control Activities	Control/Mitigate
Monitor and Review	Monitoring	Monitor
Consult and Communicate	Information & Communication	*Implied by Basel II*

In should be noted that the Basel Committee did not **explicitly** address important elements/ components that have been clearly identified as important in these two frameworks. For example, Basel II states, "the Board of directors and senior management, as appropriate, [must be] actively involved in the oversight of the operational risk management framework". Such 'oversight' implies that, at a minimum, a Board must be involved in 'establishing the risk context' and must 'communicate' its appetite for risk throughout the organization. The two frameworks make explicit the important elements, of setting the organizational context and objectives and clear communication throughout the organization.

While this paper argues that a generic, rather than specific, approach is most relevant to managing the risks in the wide range of activities undertaken by a modern bank, it is recognised that there are strengths and weaknesses in all such models. Although the paper attempts to illustrate how a generic framework could be used to satisfy the requirements of Basel II, it is important to note that **any *good* standard is better than no standard** and that the industry would be best served by adopting one model (albeit with deficiencies) rather than endlessly debate the minutiae of one standard versus another.

The paper argues that, since the two frameworks are almost identical, a superset of both, which is here based on the *terminology* of AS/NZS 4360:2004, would form a sound basis for implementing an ORM framework that satisfies Basel II requirements.

The Importance of *Context*

Basel II clearly identifies the responsibility of the Board to create a risk management 'culture' throughout their organisation and to oversee its implementation. This is not a trivial undertaking and, if not done properly, can impact a company deeply, as was illustrated at NAB (APRA 2004). The regulatory inquiries into the events at Barings, AIB and NAB all found one important factor in the losses – the traders involved were found to be following high-risk trading strategies *in direct contravention of* the directions desired by their Boards and senior management[13]. How and why could this happen?

Without a clear statement of a firm's 'risk appetite', it is difficult for operational managers and independent control functions to determine the acceptable limits of risk taking. For example, some proprietary trading is essential for supporting a successful client-related business, but when does prudent position management turn into unacceptable risk taking? In order to do their job effectively, independent ORM functions need clear direction on the limits of risk taking within each business. It is the responsibility of the Board therefore to clearly identify the 'context' in which risks should be taken and to ensure that limits are not exceeded[14]. The AS/NZS 4360: 2004 standard states "the organisation's board or executive should define and document its policy for managing risk, including the objectives for, and its commitment to, risk management; … the objectives and rationale for managing risk; and the links between the policy and the organisation's strategic plans" (SAI 2004).

In terms of a practical framework, a risk management 'context' would not only define a firm's 'risk appetite' (i.e. the markets, products and client base within which the firm desires to operate) but also its 'risk regime' (i.e. the policies, procedures, responsibilities and organisations that will be deployed to implement an ORM system for Basel II). In addition to risk appetite and regime, supporting policies, such as the firm's approach to ethical issues, such as 'whistle blowing' (Coleman 2001), must also be defined and mandated from the top. In order to be effective, prudent risk management would dictate that, although difficult to articulate, the definition of the firm's risk appetite should be as specific and precise as possible (e.g. 'proprietary trading should comprise no more that 20% of the total risk positions of a [particular] business').

The Importance of *Communication*

Basel II clearly identifies the responsibility of a Board to ensure that appropriate management processes are implemented throughout their organisation and to make sure that proper resources are allocated to these processes. The investigation into the losses at NAB (APRA 2004) pointed

out that, although the Board (appeared to have) stated its risk policies clearly, the importance that they attached to them was not communicated sufficiently to the 'front line'.

An important component of any risk management process therefore is a 'communication plan' for all 'stakeholders', which addresses issues pertinent to the risks that the firm is prepared to take and the processes that are needed to manage those risks. The AS/NZS 4360: 2004 standard states that there must be a clear identification of "those accountable for the management of particular risks or categories of risk, for implementing treatment strategies and for the maintenance of risk controls". Obviously those designated as accountable should be clearly informed of, and be educated in, their responsibilities.

Basel II calls for an interactive dialogue between banks and their regulators and it is important that the results of such a dialogue are also communicated to appropriate staff. The NAB case (APRA 2004) illustrates the problems that can occur when information concerning risks does not flow properly up and down the organisation and with regulators[15]. The AS/NZS 4360 and COSO frameworks argue that, to be effective, risk management must become an integral part of a firm's culture and "should be embedded into the organisation's philosophy, practices and business processes rather than be viewed or practiced as a separate activity". In particular, keeping good records of the "assumptions, methods, data sources, analyses, results and reasons for [risk] decisions" are an important aspect of good corporate governance (COSO 2004). As required by Basel II, all such documentation should be available for review and consultation by outside auditors and experts (Basel 2004).

As the events at Barings, AIB and NAB proved, however, merely drawing an organisation chart and articulating policies does not ensure that those involved will necessarily live up to their responsibilities. An over-arching framework does, however, permit the 'quality' of processes to be tested against best practice in a specific area and consequently for risk management to be continually improved across a firm. For example, a clear management statement of 'risk appetite' that is well documented, transparent and, most importantly, 'accessible' would provide the basis upon which potential whistle-blowers could justifiably raise concerns and complaints when they encounter problems (Coleman 2001). In the case of NAB, for instance, vital information did not flow up, *or down*, the organization (APRA 2004). A clear and public statement of the desired focus on client related, as opposed to proprietary, trading by senior management in NAB would undoubtedly have raised warning flags for more junior staff well before the significant losses occurred – the whistle was eventually blown, but blown too late!

Implementing Basel II using the AS/NZS 4360 Framework

The final Basel II proposals (Basel 2004) require that in order to qualify for either the AMA or the less strict Standardised Approach (SA), a bank must satisfy its supervisor that,
"at a minimum:

- Its board of directors and senior management are actively involved in the oversight of the operational risk management framework;
- It has an operational risk management system that is conceptually sound and is implemented with integrity; and
- It has sufficient resources in the use of the approach in the major business lines as well as the control and audit areas."

In addition, to qualify to use the AMA approach to calculate 'operational risk capital', a bank must meet stringent 'qualitative standards' in summary (Basle 2004, section 666)[16]:

(a) An independent operational risk management function.
(b) An operational risk measurement 'system' that is closely integrated into the day-to-day risk management processes of the bank.
(c) Regular reporting of operational risk exposures to business units, senior management, and the Board, with procedures for appropriate action.
(d) The operational risk management system must be well documented.
(e) Regular reviews of the operational risk management processes/systems by internal and/or external auditors.
(f) 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 accessible.

While there are many different ways that such criteria could be met, this paper shows that they can be accommodated within the framework of AS/NZS 4360: 2004 (augmented by COSO/ERM) as in Table 1 below[17]. This Table shows: each element of the Risk Management Framework; the functions with Primary Responsibility for ensuring the integrity of each element; and the 'components and tools' that could be used to deliver a working ORM. Such a classification would allow management and auditors to 'see the wood for the trees', clarifying responsibilities and ensuring that auditors and regulators can identify those accountable for any breakdowns in the risk management process.

Table 1 – Combining Basel II with the AS/NZS 4360: 2004

Elements of the 4360 Framework	Primary Responsibilities	ORM Components and Tools
Establish the Context *(Covers COSO – Internal Environment plus Objective Setting)*	Board and Senior Management (supported by Strategic Analysts)	- Risk Appetite: Products, Markets and Limits/Tolerances - Risk Regime: Philosophy, Responsibilities, Policies and Procedures - Risk Organization: Oversight, Segregation and Accountabilities - Policies on Ethics, Risk/Reward Incentives and Whistle Blowing - Business and Operational Strategies and Objectives - SWOT Analysis - Communications Plan - Budget Allocations for risk-related Resources and Training
Identify Risks *(Covers COSO – Event Identification)*	Business Units, (supported by ORM and outside experts)	- Questionnaires, Interviews and Structured Workshops - Control Risk Self Assessment (CRSA) - Brainstorming/Delphi Techniques/Affinity Maps - Process Maps/Flow Charts - Risk Register organised by People, Processes, Systems and External - Expert Judgement - Scenario Analysis
Analyse Risks *(Covers COSO – Risk Assessment- part)*	Business Units, ORM and outside experts	- Risk Classification (Likelihood and Impact) - Risk Heat Maps - Loss Events Database - Risk Drivers - Pareto Charts - Failure Mode and Effect Analysis (FMEA) - Cause and Effect (Fishbone) Charts - Sensitivity Analysis - Critical Incidents Analysis - Industry and Organisational Benchmarking
Evaluate Risks *(Covers COSO – Risk Assessment- part)*	Business Units, ORM and outside experts	- Risk Assessment, Quantification and Prioritisation - Loss Distribution Analysis such as Extreme Value Theory (EVT) - Monte Carlo Simulation - Sensitivity Analysis - Bayesian Belief Networks - Causal Modelling - Calculation and Allocation of Capital Charges - Identification of Key Risk Indicators (KRIs) - Stress Testing
Treat Risks *(Covers COSO – Risk Response)*	Business Units, ORM and outside experts	- Risk Treatment Options (Avoid, Reduce, Share, or Retain/Accept[18]) - Cost/Benefit Analysis of Risk Treatments - Risk Treatment Planning, Resourcing and Cost/Benefit Tracking - Risk Treatment Communications Plan - Business Continuity Planning

Monitor and Review *(Covers COSO – Monitoring)*	ORM, internal/ external auditors, Business Units, Board and Senior Management and Regulators	- Management and Regulatory Reporting - Performance Analysis of the Operational Risk Management System - Formal Reviews of Risk Limits and Breaches - Monitoring and reporting of progress against Risk Treatment plans - Internal/External Auditing of Risk Management Process - Reviews of Escalation and Deficiencies - Peer Reviews and Internal/External Benchmarking - Monitoring of Key Risk Indicators (KRIs) - Management Dashboards - Stress Testing - Back Testing - Whistleblower/Ethics hotline
Consult and Communicate *(Covers COSO – Information & Communication)*	All Stakeholders	- Board and Management Risk Reviews - Corporate Communications and newsletters - CEO/Management town halls and messages - Corporate Intranet and emails - Formal and informal Risk Education and Training - Risk Awareness Workshops - Participation in Industry Forums and Standards Development - Balanced Scorecard

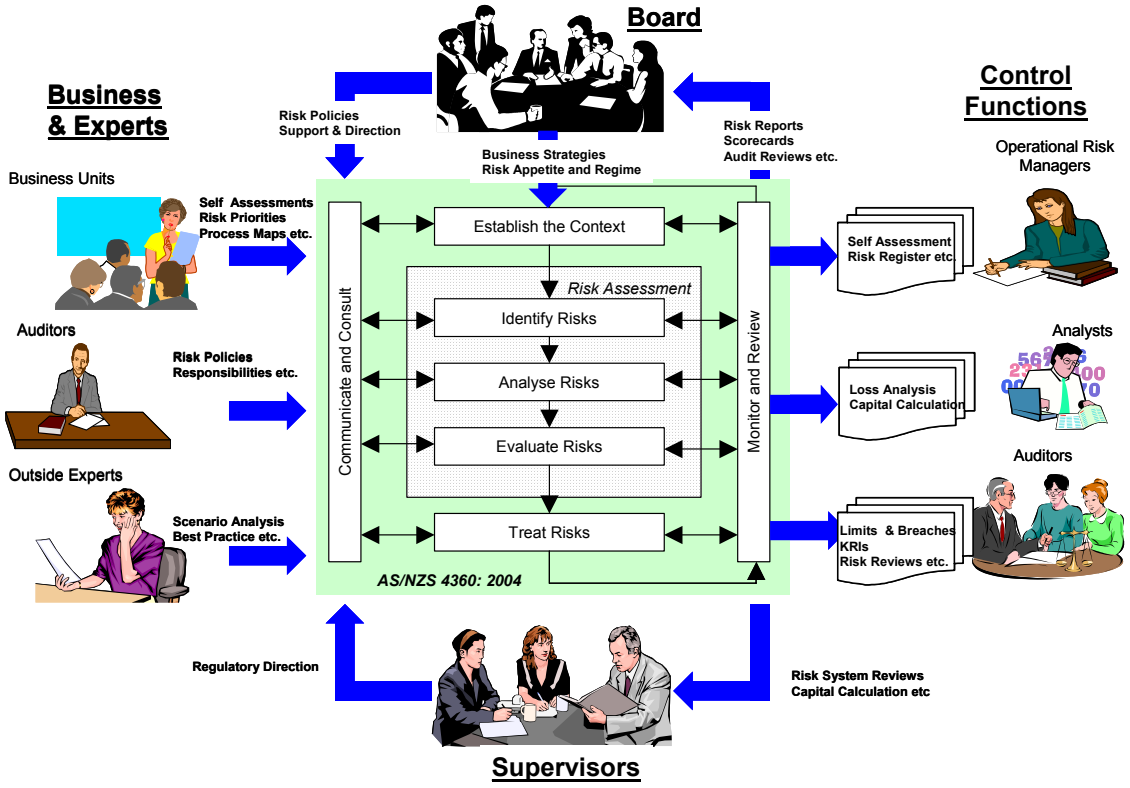
Ideally, each element of a comprehensive Operational Risk Management framework would be somewhat self-contained, taking inputs from previous elements and producing outputs to an agreed standard that would be used by other elements 'down-stream'. However, any risk management process is, of course, iterative since, for example, the impact of a change to business objectives or risk appetite would have to be applied rigorously through each of the down-stream elements. COSO 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" (COSO 2004).

Risk Management Process - Stakeholders

The AS/NZS 4360: 2004 standard points out that stakeholders are likely to make judgments about risk based on their perceptions and that perceptions of risk "can vary due to difference in values, needs, assumptions, concepts and concerns as they relate to the risks or the issues under discussion" and, since stakeholders' views will have a significant impact on the decisions made it is important that their "perceptions of risk be *identified and recorded and integrated into the decision making process* [author's emphasis]" (SAI 2004).

The diagram below shows the major 'stakeholders' in the Risk Management Process as outlined in Basel II and how they might interact with an ORM framework based on of AS/NZS 4360: 2004 framework (augmented by COSO/ERM). It should be noted that the outputs shown here are for illustration purposes and are only some of those that would be produced within any framework that complied with Basel II.

Figure 3 – Major Stakeholders in the Risk Management Process



Advantages of adopting a Standards Based Framework

There are several advantages for individual firms, and the industry as a whole, in adopting a 'standards-based' framework for Operational Risk Management, including:

- **Cost Savings**: by deploying a widely used framework, firms should not only save, potentially significant, set-up costs but should also be able to reduce their on-going costs by having a larger pool of qualified resources, for example, to conduct risk assessments.
- **Risk Reduction**: by using a framework that is well developed and proven, firms will reduce the risks inherent in creating a completely new risk management process, ultimately leading to a more 'conceptually sound' platform upon which to negotiate with regulators for lower capital charges.
- **Training and Education**: by using a standards-based framework that is acceptable across the industry, a full range of standardised training materials can be developed and delivered by professional educators. Based on such training, accreditation standards can be developed, allowing staff to attain skills that are widely recognised and transportable within, and between, firms.
- **Resources**: adopting a standard that is widely used and has independent accreditation, allows resources from inside and outside the industry to be used effectively. Inside a firm, staff can be moved easily between businesses, and temporary (trained) staff can be added as required.
- **Independent Expertise**: With a widely used standard, external experts and auditors can be deployed to better effect, since their learning curve is minimised. Equally important,

external risk management experts can bring insights and alternative approaches from other industries.

- **IT Systems**: With a widely used standard, software suppliers can, with confidence, invest in developing systems that are applicable across the industry and hence more cost-effective to acquire and operate. Common systems would also support moves towards standardised training and flexible resourcing, as knowledge and skills in popular systems would aid staff mobility and resource allocation.
- **Outsourcing**: A widely used and acceptable standard would permit certain ORM functions to be outsourced, such as the statistical analysis of complex Loss Distributions, combining internal and external operational loss data.

There are, of course, many challenges in adopting any standard for Operational Risk Management across the industry. The most obvious problem is that such a standard may inhibit creativity and become a form-filling exercise that can be circumvented by staff smart enough to 'game the system'[19]. It should be noted, however, that implementing any 'enterprise wide' system is fraught with difficulties, not least differences in interpretation between different sections of the firm and the industry. In the case of Basel II, management will have to trade off the costs, benefits *and risks* of developing their own ORM systems against lifting a standard off the shelf and applying it to their unique situation.

Standards are the life-blood of the banking industry. Without standards, such as those promoted by SWIFT and ISDA, international banks simply would not be able to expand into new markets and products. Inevitably, standards will evolve in Operational Risk Management; the only question is whether they will evolve in an ad-hoc, and inefficient, manner or whether the industry can 'boot strap' their efforts with input from other industries that are more experienced in operational risk management.

Conclusion

Given the importance placed on the qualitative aspects of Operational Risk Management systems under Basel II, and the lack of clarity provided by the Basel Committee, there is a need for banks around the world to develop (fairly quickly) ORM processes that are 'conceptually sound' and 'transparent'. This paper argues that mature, comprehensive Risk Management Frameworks already exist in other industries and that they are an excellent starting point for developing compliant ORM systems.

In particular, the AS/NZS 4360: 2004 standard is a proven tool for Risk Management in a variety of operational situations in industries other than Finance. This paper argues that this standard (augmented where necessary by components of the COSO - Enterprise Risk Management Framework) could also be used to help satisfy the requirements of Basel II. Furthermore, by adopting a proven standard, overall costs to the industry of regulatory compliance can be minimised and corporate and regulatory reporting improved.

Notes

[1] The Revised Framework 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. The Basel Committee's initial proposals for quantifying operational risk, through reference to an industry-wide Loss Distribution (the so-called IMA approach), have been replaced by more simplistic measures based on a percentage of Gross Income by firm (the Basic Approach) or by business line (the Standardised Approach). This move away from an overly quantitative approach has been supported by experts, such as Jorion (2003), who warned that "management of operational risk is still beset by conceptual problems", and Embrechts et al (2004) who strongly doubted that a "full operational risk capital charge can be based solely on statistical modeling".

[2] In this paper the term 'framework' is preferred to '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.

[3] The Institute of Internal Auditors (IIA 200) defines a Risk Management Framework as "the totality of the structures, methodology, procedures and definitions that an organisation has chosen to use to implement its risk management processes."

[4] For example, the Project Management Institute (PMI) defines project risk management as "the process associated with identifying, analysing, planning, tracking, and controlling project risks". In their guidelines for decision makers (CSA-850-1997), the Canadian Standards Authority (CSA) identifies similar steps in the risk management process: initiation; preliminary analysis; risk analysis; risk evaluation; risk control and financing; and action. The UK standard for Project Management (BS-6079-3: 2000) identifies the major activities of risk management as: understanding context; identifying risk; analysing risk; evaluating risk; treating risk; and, interestingly, maintaining the knowledge pool, plans and the management process. In their 2002 "Risk Management Standard", the Institute of Risk Management (IRM) recommends the same basic process steps named as Strategic Objectives, Assessment, Decision, Treatment, Reporting and Monitoring. The International Standards Organisation (ISO) has also developed a standard terminology for risk management in "ISO/IEC Guide 73:2002 Risk Management – Vocabulary".

[5] Important Government publications on Risk Management include: "Integrated Risk Management Framework", from the Treasury Board of Canada 2001, and "Improving government's capability to handle risk and uncertainty", from the UK Cabinet Office 2002.

[6] The Turnbull report in the UK on improving corporate governance in the UK also placed "emphasis on risk management and the disclosure and reporting of risk management activities" but left the issue of risk management standards for later research and development.

[7] CPA Australia, the national accounting standards body, employs the AS/NZS 4360 standard and describes it as "brief, simple and acknowledges the ability, and necessity, of each organisation adapting these principles to its own situation."

[8] In selecting risks to be 'Treated' (or mitigated), management must, by implication, be prepared to intentionally 'Retain' or 'Accept' certain risks without Treatment. *Acceptance does not mean ignored* but implies that the evaluation of a retained (or 'residual') risk, including known uncertainties, is well documented and well understood and that *lack of action* is formally agreed by the appropriate authorities. It should be noted that retained/residual risks must be as rigorously monitored and reviewed (including stress testing) as other risks where explicit treatment is instigated.

[9] COSO defines 'Risk Appetite' as "the amount of risk, on a broad level, an entity is willing to accept in pursuit of value" and reflects the firm's "risk management philosophy, [which] in turn influences the entity's culture and operating style." (COSO 204)

[10] The style of AS/NZS 4360:2004 reflects its development by a committee of technical experts drawing on the usage of prior versions in industry, whereas COSO ERM reflects its development by a committee of auditors and accountants, coordinated by a team of consultants (PricewaterhouseCoopers – PWC), drawing on a broader perspective of organizational theory.

[11] The differences in structures between the two process definitions are organizational and practical. For example, the 'Risk Treatment' element of AS/NZS 4360:2004 overlaps exactly with the 'Risk Response' and 'Control Activities' components of COSO. The rationale that slightly different organizational responsibilities are involved in the implementation of the two COSO components is valid, but a relatively minor consideration that certainly does not invalidate the AS/NZS 4360 alternative classification.

[12] The author recognizes that Operational Risk is just one dimension (or 'objective' in COSO terminology) of 'enterprise risk management'. However, the author argues that, given the pressing need to implement Basel II, Operational Risk may in fact be the ideal 'Trojan horse' to begin to create a new risk culture in financial services organizations.

[13] While the traders at Barings, AIB and NAB were all involved in large-scale proprietary options trading, their management were under the (mistaken) impression that they were involved in low risk trading businesses. For example, Nick Leeson at Barings was assumed to be undertaking low risk arbitrage trading on the Nikkei while John Rusnak at AIB and the four Traders at NAB were supposed to be engaging mainly in client-related (i.e. non proprietary) trading.

[14] While Value At Risk (VAR) reports may be used to monitor risk taking *in aggregate*, they do not (*nor are they designed to*) ensure compliance with firm-wide policies. It is the role of Operational Risk Managers to ensue that not only are risk limits respected but also that the risks are properly aligned with company policies.

[15] In the APRA report into the losses at NAB, the regulator noted that because of the firm's "highly regimented" culture, "bad news" tended to be suppressed, as management did not welcome it. (APRA 2004)

[16] Note that many of the same qualifying criteria also apply to the use of the Standardised Approach in calculating operational risk capital.

[17] The author also recognises that an almost identical table could be constructed using the COSO ERM Framework, but argues that it is preferable to start with one (here AS/NZS 4360:2004) and then to incorporate additional emphases from the other framework (here COSO).

[18] Treatment (or Mitigation) options are sometimes also known as the 4Ts: Terminate=Avoid; Treat=Reduce (i.e. change the 'likelihood' or 'consequences' of a risk); Transfer=Share (e.g. insure); and Take=Retain (Accept in COSO). Note also that treatment of a particular risk may involve multiple options, for example, part of a risk may be avoided, and another part may be reduced while any 'residual' risk is retained.

[19] The reports into Barings, AIB and NAB all noted that the traders involved were able, relatively easily, to 'game' their firms' control systems. The lesson to be learnt from these cases is that any system can be circumvented, if enough effort is expended; the key is to ensure that, whenever breakdowns occur, prompt action is taken to close any gaps identified.

References

APRA (2004) Report into Irregular Currency Options Trading at the National Australia Bank: Australian Prudential Regulatory Authority. March

Basel (2004) International Convergence of Capital Measurement and Capital Standards - A Revised Framework, Basel Committee on Banking Supervision. June

BBS (1995) Report of the Board of Banking Supervision inquiry into the circumstances of the losses of Barings London: HMSO.

Coleman J. W. (2001) *The Criminal Elite – Understanding White Collar Crime*, 5th Edition, New York: Worth

COSO (2004) *Enterprise Risk Management – Integrated Framework* The Committee of Sponsoring Organizations of the Treadway Commission http://www.coso.org

Embrechts P., Kaufmann R. and Samorodnitsky G. (2004) Ruin Theory Revisited: Stochastic Models for Operational Risk: Working Paper ETH Zurich

IRM (2002) *A Risk Management Standard,* The Institute of Risk Management

IIA (2004) *Position Statement - the Role of Internal Audit in Enterprise Wide Risk Management,* The Institute of Internal Auditors UK and Ireland

Jorion P. (2003) *Financial Risk Manager Handbook*, GARP: Wiley New Jersey

Ludwig E. (2002) Report to the Board of Directors of Allied Irish Banks, p.l.c. … concerning Currency Trading Losses Promontory Financial Group published by AIB plc.

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

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 **pjmcconnell@computer.org**