



Quadrant

The Power to
Measure, Manage and Understand

Emerging Best Practices in Operational Risk Management and Operational Risk Capital

Quadrant Risk Management (International) Limited

Executive Summary

During the initial phase of Basel II implementation, the regulatory spotlight was primarily focused on those firms applying for AMA approval for operational risk ("OR") regulatory capital. It is, however, becoming apparent¹ that in the wake of the recent high-profile operational risk losses incurred by institutions around the world, the FSA and other financial regulators are considering rolling out the "regulatory use test" to a wider audience of firms.

As a result, irrespective of whether a firm has opted for the simplest Basel II OR approach (i.e. the Basic Indicator Approach/BIA), one of the intermediate approaches (i.e. The Standardised Approach/TSA or Alternative Standardised Approach/ASA), or the most advanced approach (Advanced Measurement Approach/AMA), regulators are likely to place the OR culture and practices of the firm under considerable scrutiny, effectively "raising the bar" on regulatory compliance in this area. If it becomes apparent that that firm's OR framework is not satisfactory in the eyes of the regulator, the firm may be subject to an increased regulatory capital requirement at least until such time as the underlying issues have been addressed to the satisfaction of the regulator.

Increasing emphasis is being placed by regulators on firms' pro-active management of operational risk exposure. As a result, firms' adherence to the key qualitative standards of the use test will be as important as their compliance with the "quantitative" use test standards² and is likely to be increasingly applied by the regulators in their assessment of the soundness of any firm's operational risk framework, regardless of the approach used for regulatory OR capital calculation.

- **Qualitative criteria:** The key measures of whether or not a firm has adopted sound practices in relation to operational risk management, from the regulatory perspective, will be in terms of:
 - Governance in respect of operational risk, including the development of a strong OR culture throughout the organisation
 - OR management/risk control infrastructure
 - Independent validation and regular review of the complete OR framework
 - OR policy and documentation
 - OR processes
- **Quantitative criteria:** The quantitative standards which currently apply to AMA institutions, but which are likely to be used as benchmarks for regulators' assessment of firms' internal capital adequacy assessment process/ICAAP under Pillar 2³, particularly in terms of:
 - Requirements relating to the setting and documentation of risk appetite for operational risk, and its integration into day-to-day risk management/measurement
 - Models and the use of scenarios for OR measurement (including the difficult question of data quality/integrity in relation to operational risk)
 - Risk mitigation (insurance and risk transfer mechanisms)

¹ Following comments made by the FSA during its Operational Risk Seminar (4 Nov 2008)

² Relevant both for firms applying for the Advanced Measurement Approach for regulatory capital and for those wishing to develop OR measurement methodologies for Pillar 2/internal capital management purposes

³ The second part of the "International Convergence of Capital Measurement and Capital Standards - A Revised Framework" (Basel II), which concentrates on the supervisory review process and the ICAAP requirement (alongside other issues not covered in the Pillar 1 regulatory capital requirements)

Qualitative Standards for Operational Risk Management

In view of the increased regulatory focus on continual, pro-active management of operational risk⁴, firms are strongly encouraged to benchmark their ORM framework against the principles set out in the Basel Committee for Banking Supervision's "Sound Practices for the Management and Supervision of Operational Risk", published in February 2003, which remains a key reference tool for financial institutions in terms of qualitative standards for the management of operational risk.

The following issues were specifically emphasised during the recent FSA Operational Risk Seminar⁵:

□ Governance

Key to the management of operational risk is a sound governance structure and policies specifying clearly defined responsibilities for the Board and senior management. In particular, the Board and senior management are expected to:

- develop and nurture a culture of operational risk awareness throughout the organisation, underpinned, where appropriate, by risk-sensitive remuneration structures and/or disciplinary processes
- possess (and maintain) sufficient knowledge of their firm's operational risk framework to ensure effective challenge to and informed sign-off of OR initiatives and issues in their organisation
- have adequate understanding/knowledge of the assumptions underlying the OR capital models and methodology used in their organisation to enable them to take fully informed decisions based on the outputs of the models⁶
- ensure a clear articulation of operational risk appetite, such that the organisation's risks are managed in accordance with it⁷
- ensure that sufficient attention and time is allowed for the discussion of OR issues at all levels of the organisation

□ Organisation and independence of operational risk management/control functions

Firms are expected to ensure the existence – and ongoing functional ability – of a strong, independent OR control infrastructure, consisting of an OR Management ("ORM") function, Compliance, Internal Audit and, where appropriate, the external auditors of the organisation, all of which should have clearly defined, separate but "interactive" areas of responsibility.

The risk control structure should be proportionate to the nature, scale and complexity of the activities of the organisation.

However the overall risk control framework is structured (e.g. in some organisations, the control functions of ORM and Compliance are combined), firms should work towards co-ordinating and mutually building on the work of the different operational risk management and control functions, particularly in areas of potential overlap. (Note: This is also important to avoid overload of the businesses.)

In order to increase effectiveness of the risk control infrastructure, the FSA, for instance, recommends a "3 lines of defence" approach:

- Business units, as risk owners, are the first line of defence and are primarily responsible for the day-to-day management of operational risk in their processes

⁴ Particularly following the SocGen event earlier this year

⁵ 4 Nov 2008

⁶ see "Standards for Operational risk measurement (AMA and Pillar 2/Internal capital)"

⁷ see "Standards for Operational risk measurement (AMA and Pillar 2/Internal capital)"

- An independent ORM function acts as the second line of defence and is responsible for the design and ongoing effectiveness of the operational risk management framework. The ORM function must be effective at the senior level. It should be pro-actively involved in managing operational risk in the institution, providing challenge to the decisions and actions of business management and, where necessary, to the OR information emanating from the business units, such as RCSA⁸ outputs, operational risk events and KRI trends. It should also ensure that relevant information is escalated in a timely fashion to senior management (see "Management information and OR reporting" below)
 - The audit function provides the third line of defence, delivering objective and independent assurance of the effectiveness of the ORM framework, including independent validation of the design of the overall ORM framework and the structure of and assumptions underlying the op risk measurement/modelling methodologies. Internal Audit should include the ORM processes and infrastructure in its regular audit monitoring and testing plan. (Note: There appear to be regulatory concerns that, in some firms, the IA function may lack the specialist resources/expertise needed to provide effective challenge to models and methodologies used for measurement of operational risk and capital decisions. In such cases, it is important that the firm's external auditors or another external party provide an additional level of review and validation.)
- **Policy and other OR documentation**
- Considerable emphasis should be placed on appropriately documented OR policy, but also on other documentation relating to a firm's operational risk framework.
- Documentation in respect of operational risk is key for regulatory approval of firms' AMA approaches⁹, but will also play an increasingly important role in regular regulatory review of firms (such as the ARROW/risk reviews of FSA-regulated firms). During the recent seminar, the FSA commented negatively on the quality of documentation presented to them by a number of firms.
- The baseline should be for documentation to be comprehensive, providing detailed evidence of all aspects of firms' ORM framework and processes, including OR models and measurement methodologies and other systems, responsibilities, core processes, decisions and actions by the governance bodies, reports, memos, etc., but, at the same time for it to be clear enough for an independent third party¹⁰ to be able to gain a clear understanding of the detail of the firm's approach to operational risk.
- **ORM processes**
- The following factors (in relation to the different OR processes) are considered by regulators to be key for firms' pro-active management of operational risk:
- **Risk assessment/RCSA:** It is critical to ensure that the risk assessment/RCSA exercise is a regular and "living" process, which should be "owned" by the business units themselves, and which should aim pro-actively to identify risk and to take remedial action where the need is identified.
 - **KRIs/KPIs¹¹:** The objective should be to ensure that the selected range of indicators, whether singly or in combination, provide information on the firm's OR exposure as comprehensively as possible. Nonetheless, firms should be cautious of treating KRI's as the key source of management information in respect of operational risk. The monthly provision and consideration of KRI/other operational risk information, although an important means of analysing the development of the firm's OR profile over time, is not necessarily timely enough to enable senior management to respond appropriately where urgent action is required.
 - **New products, processes and systems:** Firms need to ensure that any new business initiative is properly evaluated in terms of the potential operational risks involved, using all the tools available to the firm (i.e. operational risk assessment, scenario analysis, consideration of external loss data, etc.)

⁸ Risk & Controls Self Assessment

⁹ see "Standards for Operational risk measurement (AMA and Pillar 2/Internal capital)"

¹⁰ I.e. including internal parties not involved in the process, such as Board and internal/external auditors

¹¹ It is acknowledged that these are frequently the same indicators

- **OR loss/other events:** Firms should ensure that an extensive review and decision-making process is in place for responding to operational risk losses and events, with emphasis on the "lessons learned" and remedial action steps. During its recent workshop, the FSA highlighted the importance of monitoring for "multiple events", stressing that this is potentially a more timely means of providing management with the necessary information on changes in the firm's OR profile, and thus ensures management's ability to respond more rapidly to alert situations than through the KRI reporting process (see "KRIs/KPIs" above).
 - **Operational risk data:** Importance should be placed on thorough OR data processes. It is recognised that firms are faced with a difficult task, in that they must ensure that the data they use for assessing/measuring their OR exposure is as comprehensive as possible across the entire spectrum of operational risk, while at the same time ensuring that the data is relevant to the firm's operating environment. This latter requirement in particular means that data must go through a careful selection and categorisation process. It is not a requirement to adopt a given minimum threshold for capture of internal loss data (indeed some firms systematically capture all loss data, in order to ensure completeness of their internal data). On the other hand, firms are encouraged to tap all available external sources of operational risk data, such as OR data consortia, case studies and press/media reports. The ultimate aim should be to continually expand the operational risk database, with a view to ensuring that increasingly informed management decisions can be taken. (Note: Data integrity requirements are, logically, particularly stringent where firms rely on real-life data to measure/model their OR exposure¹².)
- **Management information and OR reporting**

The issue of *timeliness*, *quality* and *appropriateness* of management information in respect of operational risk cannot be emphasised enough¹³, as the events leading up to the SocGen losses showed. The following standards, in particular, should be aimed for by firms:

- OR information should be available to senior management as frequently and rapidly as required by the situation. (Note: Ideally firms should aim for OR management information to be available as close to "real-time" as is feasible, see comment below)
- Emphasis should be on quality rather than on quantity of management information, where necessary tailoring the content of reports to the target audience for which it is destined, for maximum effectiveness.
- Firms are also expected by the regulators to ensure that the appropriate reporting "conduits" and escalation processes are in place on a permanent basis to provide for a rapid management/other response, where necessary.

Comment: Quadrant has been working with a number of firms both in the UK and elsewhere in the world with a view to addressing the issue of timeliness and quality of management information, notably through the development of its Continuous Assurance methodology¹⁴.

¹² see "Standards for Operational risk measurement (AMA and Pillar 2/Internal capital)"

¹³ This issue was frequently mentioned by the FSA during its Operational Risk Seminar (4 Nov 2008)

¹⁴ For further details, see the Quadrant Risk Management International website www.qrmi-group.com

Standards for Operational Risk Measurement (AMA and Pillar 2/Internal Capital)

In respect of the soundness standards for OR modelling methodologies, both for AMA firms and for Pillar 2/internal capital purposes, the following issues are of particular importance and were specifically commented on by the FSA during its Operational Risk Seminar¹⁵:

❑ Risk appetite/tolerance

Regulators now require the Boards of financial institutions to explicitly consider and clearly articulate (and document) their appetite for operational risk. However, the benchmark goes further, in that firms will be expected to ensure that their chosen risk appetite is fully integrated into their OR processes, e.g. in the form of "risk tolerance" levels against which their risk exposure and capital requirements can be monitored and reported. As an example, risk tolerance "escalation triggers" may be defined at BU level in terms of RCSA, KRI and loss/event reporting thresholds.

(Note: The FSA is currently carrying out extensive dialogue with UK firms in respect of OR appetite, via the Operational Risk Appetite Expert Group and is in the process of reviewing firms' practices in this area.)

❑ AMA approval requirements and soundness principles

It is acknowledged that Basel II¹⁶ is relatively vague as to the measurement/modelling requirements for the AMA¹⁷ approach to OR regulatory capital, the specific criteria being more around integrity of data and processes. The onus tends to be on the national regulators to set robust AMA approval and/or general soundness requirements (e.g. for internal capital purposes).

In respect of AMA approval, regulators are expected to want the next wave of applicants to be more sophisticated than the first wave¹⁸, reflecting progress in OR measurement generally. (Note: From comments made by the FSA, there appears to be a general recognition that AMA approaches will remain very diverse, due to the complexity of the subject and differences between firms.) Nonetheless, the "first wave" of AMA firms will clearly be expected to continue to work on their models, evolving their approach to reflect internal changes and market developments.

Firms are encouraged to distinguish between expected and unexpected losses in the breakdown of their capital. There may be potential for an AMA firm to reduce its regulatory capital charge if it is able to provide sufficient evidence that its expected losses are covered through internal business practices, such as pricing and provisioning.

In terms of general soundness requirements for both regulatory and internal capital models, the following should be kept in mind:

- Consistency of approach across business lines (but not necessarily between different types of operational risk, particularly in view of differing data availability on different risk types)
- Scenario-based approaches should avoid using certain prior assumptions (such as use of caps and "super fat tail" distributions). A particular area of regulatory concern involves scenario biases (see "Use of scenarios" below)
- Inputs to the model should include: internal data, external data, scenarios, business environment and internal control factors/indicators, all of which should be regularly refreshed/updated to ensure their ongoing applicability
- Data processes must ensure integrity and (to the degree possible) comprehensiveness of data (e.g. it must be ensured that losses/events are correctly classified/mapped)

¹⁵ 4 Nov 2008

¹⁶ and, for European institutions, the EU Capital Requirements Directive

¹⁷ Advanced Measurement Approach

¹⁸ As at November 2008, only 4 institutions in the UK (out of a total of around 30) have been given approval by the FSA to adopt the AMA (Advanced Measurement) approach to OR regulatory capital

- Comprehensive documentation¹⁹, with the aim of ensuring that uninvolved parties can understand the approach and, if necessary, apply it themselves (e.g. where there is a change in staff)
 - Caution in the use of "off-the-shelf" models and systems which are not sufficiently documented and therefore may not be properly understood by the firm (with the risk that such models may not be appropriate to the firm's circumstances)
 - Informed challenge and sign-off of the modelling approach by the Board/senior management (see also "Governance" above)
 - Where the "actuarial" type of approach²⁰ is adopted (a practice which is prevalent among AMA institutions and which is recognised to be potentially the most appropriate approach for operational risk modelling), firms should exercise caution in respect of potentially distorting factors, such as the inclusion of losses only above a given threshold
 - Firms should be cautious about creating assumptions around correlation and co-dependency between operational risk types and/or business lines (e.g. in relation to linear correlation assumptions or of pre-defined correlation factors)
 - Outputs of the model should be clearly seen to feed into the risk decisions made by the firm's management
 - Changes to the operational risk model must be managed according to a transparent (documented) process
- Use and application of scenarios

Scenarios are agreed to have an important, forward-looking role to play in identifying OR exposure in the context both of OR measurement (for AMA and/or internal capital) and for general OR management. However, they should be based on data obtained through the other OR processes, e.g. building on the RCSA process in terms of sourcing business-specific granular risk and control data.

The scenario process should be "living", with the granular information being refreshed and updated regularly, ensuring that expert input is regularly sought from the businesses and supporting functions in relation to updating and further development. (Note: The FSA commented favourably on the methodology of one AMA firm, which includes business scenario input as part of the RCSA process.)

The quality of scenario documentation should be subject to the same criteria of comprehensiveness and accessibility as for the other aspects of a firm's OR framework (see "Policy and other OR documentation" above).

Another concern expressed by the FSA during the recent Operational Risk seminar relates to the relatively common tendency to take overly long timeframes into account (i.e. the 1 in 1,000 year scenario), since this is beyond the bounds of human experience and thus cannot be evidenced.

An area in which a number of regulators appear to be raising the flag relates to scenario biases, such as:

- Distortion through the discrete choices in respect of frequency or severity buckets, where these are based on participants' subjective recollection or experience
- Shortage of relevant recent data
- "Anchoring" of scenarios to specific starting points (yielding potentially over-optimistic outcomes)
- Motivation and potential conflicts of interest of scenario designers (e.g. risk of misrepresentation of expectations because of vested interests)
- Overconfident assumptions

¹⁹ see also "Policy and documentation"

²⁰ i.e. based on separate distributions for frequency and severity and combining them in simulations

❑ Risk mitigation (Insurance and op risk transfer techniques)

Insurance is another area in which there are likely to be increasing regulatory expectations towards both AMA and non-AMA organisations.

The AMA rules for recognition of insurance as a means of reducing operational risk capital are extremely strict, and, to our knowledge, only one bank in the UK has to date achieved a reduction in regulatory capital as a result in this area. The requirements include the following:

- Insurance to be provided by a 3rd party
- Minimum claims paying ability of single A²¹/credit quality step 3²²
- Initial/residual term of no less than 1 year (otherwise stringent haircut rules)
- Minimum 90-day notice period
- Exclusion of cover for fines, penalties, punitive damages
- Insurance coverage to be aligned with mitigation needs (i.e. insurance coverage to be appropriate to OR profile of firm)
- Documentation (i.e. the need to give sufficient details on the assumptions underlying insurance-based risk mitigation, including mapping of insurance to risk profile and how the firm assesses the appropriate level of capital alleviation)
- Taking of uncertainty factors into account (payout timeliness and amount)
- Amount of capital alleviation as a result of insurance (maximum 20% of capital before insurance/mitigation)

In respect of other OR mitigation techniques, comments by the FSA point to a recognition of the (not yet tapped) potential for the market to create means of transferring operational risk, e.g. in the form of "unfunded" instruments such as swaps, options (where the reference/payment trigger event between protection seller and buyer would be based on a specified type of OR event) or "funded" instruments such as bonds or notes linked to OR events.

Firms should continue to prudently explore the available channels for mitigating their OR exposure via insurance and risk transfer mechanisms, whether or not they will be able to benefit from their alleviating effect on regulatory capital requirements.

The Conclusion?

Considerable progress has been made by the financial services industry in terms of their operational risk management practices. Nonetheless, there is still plenty of work to do, in order to satisfy both regulatory expectations and to give comfort to firms' other stakeholders that the risks facing the industry are being fully addressed.

²¹ Basel II

²² EU Capital Requirements Directive

About the Authors

Jennifer Györy, Senior Associate, Operational Risk and Non-banking Services: With seventeen years of experience in investment banking, Treasury and advising investment managers and other clients on collateral management/securities lending and custody-related issues, gained with major European and US institutions, Jennifer has been a consultant with Quadrant for the last eight years, specialising in operational risk, compliance and non-bank financial services.

Simon Baker, Deputy Head of Consulting, joined Quadrant in April 2008 after 26 years in the banking industry. He spent the previous seven years as Group Programme Director of the successful Lloyds TSB Basel II Programme, which bring him unique insights into the complex issues of capital adequacy, regulation and compliance.

Jennifer and Simon would be delighted to hear from readers of this paper, and to assist firms with any of the operational risk issues with which they are faced currently. You can contact them by email as indicated below:

Jennifer Györy (jennifer.gyory@qrmi-group.com)

Simon Baker (simon.baker@qrmi-group.com)

About Quadrant

Quadrant Risk Management (International) was formed in the UK in 1991 as a specialist consultancy by risk management professionals who had previously operated at board level in financial institutions.

For seventeen years Quadrant has helped Banks, Investment Managers and Building Societies in more than 20 countries to create best practice strategy and corporate governance architectures and control processes; Quadrant's client list includes three of the top five UK banking groups and many leading international financial institutions in Europe, Asia, Africa and the Far East.

Contact us

Quadrant Risk Management (International) Ltd.
5 New Street Square
London EC4A 3TW

Tel: +44 (0)1752 264150

Fax: +44 (0)1752 264151

Email: mail@qrmi-group.com

www.qrmi-group.com

Offices in:

Paris, France

Dubai, UAE

Chennai, India

Plymouth, UK

Woking, UK

Toronto, Canada