Financial Services Authority

Operational risk management practices

Feedback from a thematic review

February 2005

Contents

The Financial Services Authority is publishing this paper primarily for information.
We are not consulting on the contents of this paper, but if you have any comments please address them to:

Fagun Shah
The Financial Services Authority
25 The North Colonnade
Canary Wharf
London E14 5HS

Telephone: 020 7066 0452
Email: fagun.shah@fsa.gov.uk

1 Overview

1.1 The FSA's Principles for Businesses include a requirement for adequate risk management systems. These include systems for managing operational risk (OR). This report sets out the findings from our recent review of OR management practices in eight firms. We carried out this review in support of our implementation project for the Capital Requirements Directive (CRD).

1.2 The purpose of this paper is to enhance industry awareness. It is not 'guidance' as defined in section 157 of the Financial Services and Markets Act 2000 (FSMA). Instead, it aims to help firms' senior management and staff involved in OR management compare their practices with those of their peers.

Main findings

1.3 We were encouraged by the commitment institutions have made to enhancing OR management effort and the continuing progress they are making. The firms we looked at were formalising OR management processes and improving OR data collection and management reporting.

1.4 However, considerable progress is still required – particularly for those firms wishing to adopt the AMA. In particular, we noted that many firms needed a clearer understanding of what they wanted to achieve from the OR framework and communicate this within their organisation. Correspondingly, firms would benefit from more internal challenge to the effectiveness of processes being developed.

1.5 We also saw a need for more comprehensive consideration of the relationship between data collection, its interpretation and resultant risk mitigation. Management needed to consider how they expected OR management reports to influence business decision-making at all levels of the organisation. This will be an area of continued focus for us.

1.6 Development of the OR framework was still 'work in progress' at the firms we visited. At times, documentation was behind the pace of management thinking, or reflected high-level principles rather than detailed activities.

Provisions of the Capital Requirements Directive

1.7 Under the requirements of the CRD (14 July draft), CRD firms will be required to meet specified general risk management standards which include 'robust governance arrangements' that are 'comprehensive and proportionate to the nature, scale and complexity' of the firms' activities.

1.8 CRD firms looking to use the standardised approach (TSA) to calculate their OR capital charge will need to comply with additional qualifying requirements. Our current view, as noted in CP05/3: Strengthening Capital Standards published in January 2005, is that the TSA requirements will represent good practice for all CRD firms. However, we acknowledge the importance of proportionality, and would consider it appropriate that larger, more complex firms who use the TSA approach to calculate their OR capital requirements should have risk management systems that are more sophisticated and advanced than those of the simpler firms (such as investment firms who do not trade on their own account). We consider it is the role of senior management, in line with their senior management responsibilities, to determine what is appropriate for each particular firm, subject to our subsequent review.

1.9 CRD firms wishing to use the advanced measurement approaches (AMA) to calculate their OR capital charge will need to apply for a waiver from the requirement to use the Basic Indicator Approach (BIA) and/or TSA to calculate the OR charge. They will need to demonstrate that they meet all the relevant qualifying criteria. We have outlined our current thinking on some these criteria in Chapter 11 of CP05/3.

2 Introduction

2.1 The FSA's Principles for Businesses include a requirement for adequate risk management systems[1]. These include systems for managing operational risk (OR). In July 2003, we published PS142_2, which outlined the findings of a review carried out in 2002-2003 on the progress and issues the industry had encountered in establishing and maintaining risk management systems for OR[2]. In that paper, we focused on the processes firms were developing proactively to identify, assess and monitor operational exposures. We also identified some specific areas that our supervisory work was likely to consider in assessing the effectiveness of a firm's approach to OR.

2.2 Since publishing that report, we have continued assessing firms' approaches to OR management through discussions with the industry and supervisory work. As part of our implementation effort for the Capital Requirements Directive (CRD)[3] and Basel 2 Accord[4], we have recently completed a thematic visit programme to eight firms.

2.3 One purpose of this review was to follow up on the implementation challenges faced by a firm subject to that Directive (CRD firms) in building a comprehensive OR management framework. This paper provides feedback on our observations from this review. While we only visited CRD firms, our findings may also be of interest to other financial services firms that are implementing an OR framework.

1 Principle 3: A firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems (PRIN2.1.1R).

2 PS142_2: Building a framework for operational risk management: the FSA's observations (www.fsa.gov.uk/pubs/policy/ps142_2/).

3 Capital requirements for credit institutions and investment firms (http://europa.eu.int/comm/internal_market/regcapital/index_en.htm#capitalrequire).

4 Basel II: International Convergence of Capital Measurement and Capital Standards: a Revised Framework (www.bis.org/publ/bcbs107.htm).

2.4 The purpose of this paper is to enhance industry awareness and is not 'guidance' as defined in section 157 of the Financial Services and Markets Act 2000 (FSMA). It aims to help firms' senior management and staff involved in OR management compare their practices with those of their peers.

Our review

2.5 Our sample of firms included some we had visited before and some that were intending to apply to use the advanced measurement approaches (AMA) to calculate minimum regulatory capital. The majority were trying to take account of emerging industry practice in their implementation effort, rather than being at the forefront of development. All the firms had active implementation projects and so our review was of work in progress. Our review took into account any planned enhancements – for example, we did not expect documentation to be fully developed.

2.6 We considered it important that management were able to articulate their risk management approach; justify its appropriateness given the organisation's scale, nature and complexity; and demonstrate that it was being implemented effectively. We reviewed how firms addressed issues such as:

- scope of OR – *was the framework sufficiently clear, comprehensive and consistent throughout the organisation?*
- governance – *was senior management directing risk management strategy and reviewing its effectiveness at meeting business objectives?*
- communication and documentation of strategy and policies – *was the framework clearly communicated so that it was understood by business line management?*
- collection of data – *how did the organisation address issues relating to the integrity, relevance and sufficiency of data?*
- use of management information – *how did the framework impact business decision making?*
- independent review – *how was the effectiveness and adequacy of the framework assessed?*

3 Scope of operational risk

3.1 All of the firms in our sample have adopted the broad 'Basel' definition of operational risk or a close variant: 'Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events'.

3.2 The breadth of the definition, however, has meant that firms' interpretations of it vary widely. For example, while some firms have interpreted 'loss' to mean direct financial impact, others also include impacts that are indirect (e.g. opportunity costs) and/or non-financial (e.g. reputational). The boundary between operational and other risk types (e.g. market, credit and insurance) is subjective – often an operational failure can result in a credit or market loss – and this also results in different views on demarcation lines.

3.3 Most of the firms in our sample had addressed at least some of these definitional issues in their documentation. In general, they had covered the inclusion/exclusion of indirect and non-financial impacts. But, generally, they had not covered the boundary with other risk types. Only one of the firms we visited had taken their high-level definition and further classified it into categories and sub-categories of risk exposure. At some other firms, we saw examples of categorisation, but it either applied only to one activity (e.g. internal loss reporting) or was not consistent across activities.

3.4 We recognise that defining and categorising risks can be subject to widely differing interpretations. Our interest in defining and scoping of risk is not to standardise such categorisations, but to ensure that all potential risks have been adequately considered and managed. Categorisation and sub-categorisation of risks also help in ensuring consistency when comparing data.

4 Governance

4.1 In PS142_2, we noted that one of the challenges faced by firms implementing an OR framework was gaining senior management buy-in. In this review, we saw clear buy-in and support for the development of an OR framework by senior management, as reflected in the budget and resource allocated to this work. There was progress at formalising the OR governance arrangements. We saw oversight committees (with formal responsibility for considering OR) were being established, as well as central risk management functions to provide leadership and guidance on risk management processes and reporting.

4.2 However, this activity was sometimes inhibited by the lack of clear direction on risk strategy from the Board of Directors (or other governing body). In many cases, the Board would instruct the central risk management function to implement an OR framework without indicating clear objectives or risk appetite.

4.3 We noted that policy and procedural documentation did not always provide clarity on risk management requirements. These were either generic or focused on a small subset of the risk management effort (such as those tasks initiated by the central risk management function).

4.4 At a few firms, the OR policy stated that responsibility for managing operational risk lay with business line management. However, there was no further clarification on how actual individual responsibilities, risk management activities, or reporting processes differed between different areas. Without explicitly recognising the diverse range of activities (and their interaction) on which the OR framework relies, firms cannot be confident that responsibilities for these OR systems and controls are rightly apportioned. As a result, risk management efforts may continue to be implicit and subjective.

5 Communication and documentation

5.1 At some firms, the central and/or divisional risk management functions were implementing a training and education programme to ensure that business areas could carry out the risk assessment and reporting tasks for which they were responsible. Often this was through one-off workshops and presentations. This was as well as providing routine business operations training.

5.2 However, we observed that policy and procedural documentation was often of limited use in communicating the approach to the organisation as a whole. We saw examples of the policy statement only applying to the central risk management function or, if disseminated to the business, being very general.

5.3 A significant omission at most firms was a lack of guidance to line management on how to weigh potential operational risks against expected profits when making significant business decisions. In those few firms that had adopted risk appetite statements, it was difficult to see how these could be practically used since they were not stated in terms that were relevant to how business areas made decisions. They were neither sufficiently detailed (e.g. by referring to the firm's OR categorisation and organisational structure) nor sufficiently objective (e.g. by referring to likelihood and monetary or reputational impacts).

6 Data collection and management information

Data collection

6.1 We saw considerable progress on OR data collection, which has allowed firms to implement new management reports. In general, firms found the data useful in running their business. Besides, all of the data types firms identified to us could fit into one of the four categories the CRD requires for AMA (internal loss data, external loss data, scenario analysis and factors reflecting the business environment and internal control system).

6.2 We believe firms need to consider how the data can be meaningfully used to increase the organisation's understanding of its OR profile. This requires consideration of issues such as the relevance and sufficiency of the data.

6.3 On relevance, firms needed to consider:

- the relationship of the data to OR – for example, whether it provides information on potential or actual risk exposures, risk crystallisation, or the effectiveness of mitigating controls;
- single incident thresholds that are relevant to a firm's business and not derived from a perception of what the regulator requires;
- their experience in the collection and use of this data – the less experience firms have, the more difficult it may be to interpret any trends in the data;
- the timeliness of reporting – aged data may not reflect current circumstances;
- the transparency of the collection process – where processes are ambiguous, it is harder to assess the integrity of the data.

6.4 Similarly, for sufficiency, firms could consider factors such as the range of data being captured – for example, whether it:

- comprehensively covers the scope of OR adopted by the firm and all its business activities, including – subject to proper controls – data on events where confidential treatment is required; and
- adequately covers potential risks, actual losses and mitigating controls (whether preventative, detective or remedial).

6.5 Each data type has its strengths and limitations. For example, loss data is backward-looking but objective; scenarios are forward-looking but subjective. We saw corroboration between data types and data sources as one way a firm could accentuate strengths and reduce limitations. For example, by comparing reported internal loss incidents with the results of its control risk self assessments and reported risk indicator data, a firm could be more assured that the data was accurate and complete. Similarly, the results of scenarios performed as part of the OR framework could be compared to business continuity work; or internal loss reporting verified by comparison to the general ledger. The loss experience of other firms (external data) could provide a useful and independent 'completeness check' on the risk scenarios generated internally.

Management information

6.6 We have seen a general increase in the amount of OR management information firms have produced over the last couple of years. Firms suggested these reports were improving the visibility and accountability of risk management decision-making. They said the purpose of these reports was not to provide new unseen information to senior management, but rather to allow them to consider risks in a more informed context. Some firms said that better business decisions were being made because of the enhancements in reporting.

6.7 We were encouraged by this increased focus on management reporting. To enhance this further, firms might ask:

- whether management reporting is comprehensive, yet easy to read;
- whether they were drawing valid conclusions from analysing the data collated – we saw some reporting of losses without supporting analysis, which would have demonstrated a link between pure data collection and remedial action; and
- how this information could be used to inform business decisions throughout the organisation as a whole.

6.8 At many institutions, we noted that while data was being collated centrally and reported upwards to senior management, little feedback and information was dispersed downwards into the business areas that had the day-to-day responsibility for risk management. We will continue focusing on the extent to which OR management information is, in fact, used in risk management and business decisions.

7 Independent review

7.1 In general, firms had not yet established processes to assess the effectiveness and adequacy of their OR frameworks. The focus of the central risk management function was on developing and communicating OR management policies and procedures. The function did not generally play a significant role in assessing the quality of implementation in business areas.

7.2 We also saw little active review and challenge by firms' Internal Audit (IA) at most of the firms we visited. In the main, IA had not yet reviewed firms' OR approach; although the auditors we spoke to indicated that they would carry out a review in future, once the OR framework was more embedded. Documentation was incomplete, which also constrained auditors' ability to comment on observed practices relating to required standards and procedures.

7.3 There should be greater focus on the independent review of operational risk arrangements, as these are embedded in firms.

8 Provisions of the Capital Requirements Directive (CRD)

8.1 The CRD is being implemented by the 'recasting' (i.e. revision) of two existing EU directives: the Banking Consolidation Directive (BCD) and Capital Adequacy Directive (CAD). In general, CAD refers back to text in the BCD.

8.2 Under the requirements of the CRD (14 July draft)[5], CRD firms will be required to meet specified general risk management standards, which include 'robust governance arrangements' that are 'comprehensive and proportionate to the nature, scale and complexity' of the firms' activities.

8.3 CRD firms looking to use the standardised approach (TSA) to calculate their OR capital charge will need to comply with additional qualifying requirements. Our current view, noted in paragraph 10.8 of CP05/3[6], is that the TSA requirements will represent good practice for all CRD firms. However, we acknowledge the importance of proportionality, and would consider it appropriate that larger, more complex firms who use the TSA approach to calculate their OR capital requirements should have risk management systems that are more sophisticated and advanced than those of the simpler firms (such as investment firms who do not trade on their own account). We consider it is the role of senior management, in line with their senior management responsibilities, to determine what is appropriate for each particular firm, subject to our subsequent review.

8.4 CRD firms wishing to use the AMA to calculate their OR capital charge will need to apply for a waiver from the requirement to use the Basic Indicator Approach (BIA) and/or TSA to calculate the OR charge. They will need to demonstrate that they meet all the relevant qualifying criteria. We have outlined our current thinking on some these criteria in Chapter 11 of CP05/3.

5 Capital requirements for credit institutions and investment firms (http://europa.eu.int/comm/internal_market/regcapital/index_en.htm#capitalrequire).

6 CP05/3: Strengthening Capital Standards (http://www.fsa.gov.uk/pubs/cp/cp05_03.pdf)

The Financial Services Authority
25 The North Colonnade Canary Wharf London E14 5HS
Telephone: +44 (0)20 7066 1000 Fax: +44 (0)20 7066 1099
Website: http://www.fsa.gov.uk
Registered as a Limited Company in England and Wales No. 1920623. Registered Office as above.