Policy Statement

Financial Services Authority

# Building a framework for operational risk management: the FSA's observations

Feedback on industry practice as we prepare to implement CP142

July 2003

FSA®

# Contents



Annex 3 provides references to additional material that may be of interest to firms. Where appropriate, we refer to this material in the report using the mark [R#].

This Policy Statement reports on the progress and issues encountered by the industry with the implementation of risk management systems for Operational Risk consistent with the proposed policy in PRU 6.1 of Consultation Paper 142 Operational Risk Systems and Controls.

Enquiries can be addressed to:
Fagun Shah
Prudential Standards Division
The Financial Services Authority
25 The North Colonnade
Canary Wharf
London E14 5HS

Telephone: 020 7066 0452
Fax: 020 7066 0453
E-mail: cp142@fsa.gov.uk

# 1 Executive summary

1.1 In July 2002, we published Consultation Paper 142: Operational risk systems and controls (CP142). It contained draft guidance on operational risk (OR) systems and controls for both **SYSC** (one of our high level sourcebooks, entitled *Senior management arrangements, Systems and Controls*) and **PRU** (our forthcoming *Integrated Prudential Sourcebook*). Following consultation, we issued a Policy Statement in March 2003. In that paper, we stated that we did not propose to make any significant amendments to the draft text and were planning to publish our near-final Handbook text later this year. This is likely to take effect in September 2004, as part of the first phase of the implementation of the Integrated Prudential Sourcebook.

1.2 Over the last year, we have reviewed how the management of OR is evolving in firms, to enhance our knowledge of industry practice. As part of this review, we held discussions with 22 firms actively developing risk management systems for OR, on how they were developing both the governance structures and the tools used to identify, assess and monitor OR. We call these the OR Framework.

1.3 The purpose of this second Policy Statement, therefore, is to outline the main findings of this review, which confirmed our view that our proposed **PRU 6.1** policy on risk management systems for OR meets our statutory objectives. We also report on the progress and issues encountered by the industry in developing and implementing risk management systems for OR. This paper, and the OR Framework it describes, is not aimed at proposals for regulatory capital requirements for OR. It is for information only and is not ‘guidance’ within the meaning of section 157 of the Financial Services and Markets Act 2000.

## Who should read this paper?

1.4 This paper will be of particular interest to managers responsible for developing and implementing OR systems and controls in firms.

## Main findings of our review

1.5 As a discipline, OR remains at an early stage of development compared with other areas of risk management. Whilst there are many areas that still require attention, firms have made significant progress in developing practices to manage OR. In part, this is driven by an increased emphasis on senior management accountability and regulatory focus. We observed increasing convergence between the OR methods and tools used by firms, with emerging practices consistent with our draft **PRU 6.1** guidance.

1.6 Firms we visited said that the evolving OR Frameworks were helping them better control and mitigate underlying risks. However, they acknowledged that, in most cases, it was too early to assess the full benefit to their business. Although firms were setting about planning and developing their frameworks in different ways, we noted some common messages from the more advanced firms on the challenges they have had to deal with:

- **Senior management commitment to OR management**. Senior management had been involved in considering what OR meant to their firm and had incorporated OR into their overall governance and risk management effort. Their role in setting internal expectations, allocating resources, and monitoring progress against objectives was essential to setting up a successful OR Framework.
- **OR management integrated into business activities**. More progress had been made where firms had considered at the outset their requirements (for example, through a detailed and systematic assessment of the management information required by the organisation). Firms making most progress had considered how a particular approach would enhance their business and risk management objectives rather than solely how it would meet FSA policy requirements.
- **OR Framework development based on experience**. Most firms were taking an evolutionary approach to developing a framework, using their own and industry experience as well as regulatory statements to inform their direction. Firms had started by adapting existing control and risk management frameworks, going on to add new tools and processes specific to OR. Although consultants could advise on good practice and assist in implementation work, internal effort and management time was considered crucial if the framework was to be effective.

- **Nominated resource for OR management**. A centralised and independent OR function helped to provide challenge and coordination of effort, enhancing the quality of information given to senior management. This was not always appropriate for some smaller firms, where coordination was provided through another function such as Internal Audit. Considering the full range of resources (people in various functions, existing processes and systems) available to them allowed firms to make better use of limited resources.

1.7 Some firms have taken a 'wait and see' approach because of a lack of knowledge over what good practice might constitute, as well as the uncertainties over regulatory requirements. We observed that implementing a sound effective approach that delivers business benefit took considerable time and effort. Chapter 3 and Annex 1 detail some of the activities firms are undertaking and the areas that still need to be resolved before CP142 is implemented in September 2004.

**CONSUMERS**

This Policy Statement will be of some interest to retail consumers, because our guidance on operational risk systems and controls is designed to promote our consumer protection objective.

# 2 Introduction

2.1 Inadequate management of OR could present a significant threat to three of our statutory objectives: securing the appropriate degree of protection for consumers; maintaining market confidence; and reducing financial crime.

2.2 CP142 published in July 2002 proposed new draft policy that covered:

- **SYSC 3A** *Operational Risk: Systems and Controls* – guidance on some of the main areas that a firm should consider when managing OR. In so doing, it covered a range of topics, including people risk, IT systems and information security, business continuity management, and outsourcing; and
- **PRU 6.1** *Operational Risk: Prudential Systems and Controls* – guidance on the risk management systems that firms should put in place to identify, assess, monitor and control their OR in a prudential context.

2.3 In March 2003, we issued a Policy Statement summarising the responses that we received to CP142. In that paper, we stated that we did not propose to make any significant amendments to the draft policy and were planning to publish our near-final Handbook text later this year. This material is likely to take effect in September 2004, as part of the first phase of the implementation of the Integrated Prudential Sourcebook.

2.4 In April 2002, we initiated a project to enhance our understanding of the risk management systems firms are setting up for OR. The objectives of the project were to:

- obtain a better understanding of actual and developing OR management practices;
- develop a better awareness within the FSA and in the industry on good practice;
- develop a method and centre of expertise for the future review of OR management practices at firms;

- inform our position on issues being discussed internationally; and
- verify the appropriateness of the draft **PRU 6.1** policy.

2.5 The main activity of the project was a programme of short discovery visits to firms that were actively developing risk management systems for OR. Two-thirds of the 22 firms we visited were banks or other deposit takers, although the majority of the bank-led groups contained investment and/or insurance businesses. Our review focused on how they were developing both the governance structures and the tools used to identify, assess and monitor OR. We call these the OR Framework.

2.6 There is an overview of our approach to the review of industry practice in Annex 2.

## Purpose of this Policy Statement

2.7 This second Policy Statement summarises our observations on developing industry practice and how it compares with our proposed guidance in **PRU 6.1** of CP142. It also reports on the progress and issues encountered by the industry with the implementation of risk management systems for OR. This paper aims to enhance industry awareness and is not 'guidance' within the meaning of section 157 of the Financial Services and Markets Act (FSMA) 2000.

2.8 Our review was restricted to analysis of submitted documentation and discussion with relevant management and staff identified by the firm. It did not include any detailed sampling or testing. In presenting our findings, we have made assumptions on the maturity and quality of the risk management systems for OR of individual firms based on documents sent to us. All the firms we visited were still developing and adapting their frameworks and approaches to OR management. We identify good or innovative practice and, where relevant, distinguish between practices at major financial groups and smaller, less complex firms. Poor practice is also highlighted.

2.9 In certain cases our review concentrated on a subsidiary, branch or division of a larger firm. Our review also included firms where the responsibility for lead supervision was with a fellow regulator. In these instances, our findings have related primarily to the business area that we reviewed rather than the wider organisational structure.

## Structure of this Policy Statement

- **Chapter 3** identifies some of the issues firms are considering as they develop and implement OR Frameworks.
- **Chapter 4** is a summary of the main conclusions from our review and the next steps in developing our regulatory approach and capital adequacy framework for OR.
- **Annex 1** outlines the range of practice we observed during our review with sections on the development, governance arrangements, and tools of an OR Framework.
- **Annex 2** provides an overview to the approach and method of our review.
- **Annex 3** provides references to additional material that may be of interest to firms. Where appropriate, we refer to this material in the report using the mark [R#].

# 3 Issues firms consider in establishing Operational Risk Frameworks

## Rationale for an Operational Risk Management Framework

3.1 Our review investigated how OR management had evolved and the motivation for firms in developing an OR Framework. For instance, was OR adopted by firms because of increased market expectations, internal drivers or regulatory pressures? In line with our *principles of good regulation*, our aim is for firms to implement an approach because it enhances their business operations and helps them control or mitigate their risks, rather than solely to meet a regulatory requirement.

3.2 In considering and applying the policy in **PRU 6.1** of CP142 on the establishment of a risk management system for OR, firms will need to evaluate the adequacy of current systems and controls. Firms may have to address a number of initial objections internally in obtaining support for implementing new, or significantly adapting existing, systems and controls. We identify below some of the most frequently expressed concerns and our observations on these.

### Why change, if the firm has always adequately managed Operational Risk?

3.3 The concept of OR is not new. Historically, it has sometimes been defined as all risks other than market, credit, insurance and liquidity. For example, it includes risks arising from failures in corporate governance, IT, outsourcing, and business continuity[1].

3.4 The traditional approach tolerates OR as being a cost of doing business, and relies on line management to establish and maintain appropriate systems and controls to reduce the frequency and impact of operational exposures within

1 More recently, the Basel Committee on Banking Supervision in the context of regulatory capital has defined it as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. The definition includes legal risk but excludes strategic and reputational risk" (see *CP3: The New Basel Capital Accord* paragraph 607).

their remit. Under this approach, senior management monitors these activities in an ad-hoc manner through management information from operational and financial control functions, and from centralised support areas such as Human Resources, Finance and Information Technology. Internal Audit performs an essential role by providing independent assurance on these activities. However, OR tends not to be formally articulated or quantified.

3.5 Recent high-profile control failures have resulted in a growing appreciation of the impact a single incident can have on an increasingly complex business operation. As a result there has been a focus on senior management accountability and a requirement for transparency about the extent and nature of operational exposures. This has increased debate on the concepts around OR, relating to the management of people, process, and technology risks.

3.6 Expectations on senior management accountability are, of course, not new. Within the UK, the *Combined Code*[R3] that applies to all listed companies incorporated in the United Kingdom (and has also been adopted by other organisations as good practice) has for some time established this expectation[2], as has our approach to regulation[3].

3.7 Firms recognise there is a need for a more proactive approach to managing OR. Whilst still challenging, firms are aiming to define what is an acceptable or unacceptable risk exposure (i.e. their risk appetite) and monitor their actual exposure. For example, quantitative measures, such as risk indicators, are being developed and monitored by newly established independent centralised risk management functions.

## Is Operational Risk only relevant for large internationally active banks?

3.8 A view sometimes expressed is that OR management is more relevant for banking firms that are large and complex. Therefore, focus on OR management is less of a concern for smaller firms or non-banking firms.

3.9 Whilst, we found that large internationally active banking groups had a more evolved and sophisticated approach to managing OR (as they have been working on their frameworks for longer), progress has been made in other sectors, particularly investment firms and smaller deposit taking firms. We observed that insurance firms and market infrastructure providers had the least developed approach. However, we noted exceptions in all of these sectors. Also, a number of the banking groups visited had significant

2 *Combined Code* principle A1 states that every listed company should be headed by an effective board which should lead and control the company.

3 Our *principles of good regulation* require us to hold senior management responsible for risk management and controls within firms, and this is reflected in our Handbook policy, for example, in our high level sourcebooks **PRIN** *Principles for Businesses* and **SYSC** *Senior management arrangements, Systems and Controls*.

investment and/or insurance businesses that were also included in the groups' OR Frameworks.

3.10 Although progress was being led by the internationally active major financial groups, we also saw smaller firms using some of the more advanced techniques outlined in Annex 1. Particular observations on the approach in smaller organisations included:

- a more informal governance and management framework reflecting the less complex organisational structure, including more qualitative and subjective reporting on OR; and
- a smaller range of OR tools being implemented and more reliance on manual processes rather than complex systems.

3.11 Following our review, we believe that the same core principles apply to all firms. The differences we observed related more to the resource and time applied to developing OR Frameworks by firms. Whilst a more informal and less automated approach to OR is consistent with the scale and complexity of smaller organisations, firms generally have the same broad categories of people, process and systems risks irrespective of their specific business lines. To obtain appropriate management information on OR, firms will need similar means to collect data, albeit to a different degree of sophistication.

### Can disciplines established for managing credit, market and insurance exposures be applied to operational risks?

3.12 Firms disagree on whether OR can be quantitatively defined and assessed, and whether risk management principles developed for financial risks such as credit, market and insurance risk can therefore be applied to OR.

3.13 Recognising their accountability, senior management at many firms have for some time carried out a subjective assessment of their risks. However, they recognise that they must ensure their assessment is accurate, and clearly communicate their expectations of management. So they accept that they must articulate their risk appetite and set objective criteria for the identification of issues that need to be brought to the attention of senior management.

3.14 A number of firms have processes for obtaining qualitative information (for example, controls risk assessment), and business line management raise issues that they believe are important (i.e. subjectively). However, firms are finding it difficult to state their risk appetite in a quantitative manner, as well as establish quantitative measures of risk exposure.

3.15 Encouragingly, a significant number of firms in our sample have started work on developing risk indicators, although we observed fewer firms developing an explicit statement of risk appetite. Yet, at a few firms, their work on risk indicators was also assisting their thinking on risk appetite.

3.16 We acknowledge that assessing and monitoring risk exposures quantitatively continues to be challenging for firms, but see further consideration of OR reporting as helping progress in this area. However, it was not apparent to us that firms had actively discussed the frequency and type of information that should be produced for the Board, management and relevant committees. This will inevitably impact on their processes to collate and ensure the accuracy and completeness of this information.

## Establishing the Operational Risk Framework

3.17 Where a decision to establish a new, or significantly adapt an existing, risk management system for OR has been made, a firm may have to resolve a number of issues in developing and implementing its OR Framework. We identify below some of these issues and our observations on these.

### What is the OR Framework trying to deliver?

3.18 Firms who appeared to have made the most progress were those who had:

- fully considered what OR meant to them individually (rather than relying on a generic definition); and
- had incorporated OR into their overall governance and risk management effort.

3.19 Firms were better able to identify the systems and controls that need to be established or adapted by more detailed and systematic consideration of the management information required by the organisation, including:

- the type and source of data required;
- how this data is collated and validated;
- by whom this data is analysed and how it is communicated and escalated; and
- the completeness of coverage across business areas and OR categories.

3.20 The coverage and level of detail of documentation on the developing framework was variable. This was perhaps due to the ‘trial and error’ nature of the development process. Where it existed, a clear statement of the firm’s strategy and policy for managing OR, together with corresponding plans for implementing this strategy had clarified and focused effort, and made communication with internal and external stakeholders possible. Documentation was also important in mitigating firms’ business continuity risks.

### What resources are required and available to implement the OR Framework?

3.21 Responsibility for the development and implementation of the OR Framework varied between firms, although often this was carried out in addition to other business-as-usual responsibilities. We noted that centralised and independent resource, where it existed, performed an important role in coordinating effort and providing challenge. Similarly, the use of formal project management disciplines enabled more effective identification of requirements and allocation of resource, and helped assess progress against objectives.

3.22 Whilst there were some 'quick wins' (for example, where firms were able to adapt and make use of existing risk management activities), establishing the framework properly was taking longer than originally expected. This was partly due to the time and effort taken to plan, develop, and implement processes and systems, as well as educate the business.

3.23 The process was more efficient and effective where firms had identified their requirements and, considered at the outset, the full range of resources (people as well as existing processes and systems) available to them. From a human resource perspective, we saw that firms had a wide, but often not fully utilised, breadth of expertise and perspective available, that included:

- senior management;
- decision-making committees;
- business line management;
- centralised and business line OR functions; and
- other central functions (such as finance, compliance, and internal audit).

3.24 The clear apportionment of roles and responsibilities of the different organisational categories above was important. Some firms had needed to resolve internal conflicts where there were potentially overlapping responsibilities.

3.25 Firms made more effective use of pre-existing processes and activities by reviewing how they could be adapted and adopted to the OR Framework. For example, firms were adapting existing management information on processes and controls to reflect other categories of risk exposure, and rolling out tools used in one business line across the organisation.

3.26 Whilst a number of firms had used consultants to advise them on good practice and assist in implementation work, most firms recognised that it was essential to spend a significant amount of internal effort and management time on implementing the framework if it was to be effective. In general, the approach was to start with a manual process, and then to automate once they further understood their requirements as the framework evolved.

# 4 Conclusions and next steps

### The industry is still in an early stage of developing OR Frameworks

4.1 The industry has made considerable progress over the last two years in investing in processes and systems for managing OR. For, example, firms are increasingly setting up independent central OR management functions. Although a few large firms appear to be in a 'near complete' stage where they are using, but still enhancing, their framework, most are still either planning or developing their framework. An important impetus has been regulatory pressure. This has been in the form of increased focus on corporate governance, the development in Basel and the EU of frameworks for risk-based minimum capital requirements (see paragraph 4.12), as well as consultation and discussion papers issued by us and other regulators. The increasing discussion of OR in recent conferences and risk seminars has also contributed to a wider awareness.

4.2 Whilst there are differences in approach, we perceived a convergence in the types of tools used in the OR Framework. For example, internal loss databases, control risk assessments and risk indicators were regularly identified by firms as part of their means to identify, assess, and monitor risks and mitigating controls. However, few firms had sufficient data to be able to test whether their tools were appropriate. We discuss these tools in more detail in Annex 1 section C.

4.3 However, OR is still a developing field, and we recognise that firms will need time to plan, develop and implement an approach appropriate to the scale, nature and complexity of their business operations. We are encouraged by the fact that firms have recognised and started to establish such risk management systems.

4.4 Due to a lack of knowledge of what good practice might constitute, as well as the uncertainties over regulatory requirements, some firms have taken a 'wait and see' approach. We observed that implementing an effective approach that delivers business benefit took considerable time and effort.

### There appear to be net benefits from the regulatory focus on operational risk

4.5 A majority of firms stated that their primary motivation for developing the OR Framework was increased regulatory focus, with regulation a more significant driver in smaller firms than in major financial groups. A number of firms stated that the forthcoming regulatory developments had focused management attention on this area and had been a catalyst for initiating or accelerating development, rather than imposing superfluous practices for internal OR management.

4.6 Firms highlighted that the evolving framework was starting to help them better control and mitigate underlying exposures, although they acknowledged that in most cases it was too early to assess the extent of business benefit.

### Our draft Handbook policy sets standards consistent with industry practice

4.7 Our review indicated that the processes and systems that firms are developing to identify, assess, monitor and control OR can be broadly mapped into our draft PRU 6.1 guidance. Significantly, this is just as true of firms who had started developing their framework before the publication of CP142.

4.8 With regard to the revised Accord/RBCD[4], firms are developing the types of internal systems and controls that they hope will meet the proposed qualitative entry criteria for the Standardised Approach (TSA) and Advanced Measurement Approaches (AMA). However, whilst a number of major financial groups are considering how to model OR in support of both economic and regulatory capital, this is generally still at a conceptual stage.

## Next Steps

### Regulatory approach and risk assessment framework

4.9 The management of OR features significantly within our ARROW firm risk assessment framework[R2]. Whilst ARROW *Risk Element 6 Operational Risk* is the main heading under which a firm's OR Framework is assessed, underlying operational exposures also feature in most of the other Risk Elements.

4.10 The method developed and information gathered in this review will inform our approach to firm risk assessment and risk mitigation programmes. In

4 Revised Basel Accord and Risk Based Capital Directive (see paragraph 4.12)

assessing the effectiveness of a firm's approach to the development and implementation of an OR Framework, we will consider for example:

- *analysis of risk profile* – the extent of understanding in the organisation of the types of operational risks faced by the firm and its exposure to them;
- *ownership at business and corporate/group level* – the level of senior management sponsorship, and clarity in the apportionment of roles and responsibilities for OR management throughout the organisation;
- *clarity of strategy and policies* – the firm's strategy for developing and implementing an OR Framework, the comprehensiveness of their policy documentation, and its communication within the organisation;
- *independent review* – the firm's ability to validate the effectiveness of the OR Framework at meeting the risk management objectives of the firm; and
- *management information* – the type and quality of management information on OR produced at all levels of the firm.

### Policy developments

4.11 As outlined in our first Policy Statement on CP142, we expect to publish our near-final Handbook text for operational risk systems and controls, along with all of our other new policy on systems and controls, later this year. This material is likely to take effect in September 2004, as part of the first phase of the implementation of the Integrated Prudential Sourcebook.

4.12 The revised Basel Accord[R9] and Risk Based Capital Directive (RBCD)[R10], which take effect on 31 December 2006, will establish new capital standards, including for OR, that will affect all deposit takers and certain types of investment firms. As noted in Consultation Paper 189[R12], we recognise that further information from us will help firms decide their approach to OR. This information will be used to inform our approach to implementing the revised Accord/RBCD. We plan to consult on the Prudential Sourcebook (PSB) text that will implement the revised Accord/RBCD in mid-2004.

4.13 For the insurance sector, the EU Solvency II project[R11] may identify specific risk management and internal control standards with related prudential capital requirements. We are currently conducting a broader review of risk management practices in the insurance industry and plan to provide feedback to the industry on our findings later this year. Both the OR review findings and this insurance risk management project work will inform our supervisory approach and policy discussions.

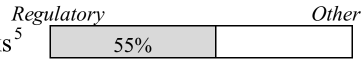
**Annex 1**

# Detailed findings

## A Development of an Operational Risk Framework

A1 Our review investigated how OR management had evolved and the motivation for firms in developing an OR Framework – whether increased market expectations, internal drivers or regulatory pressures. In line with our *principles of good regulation*, our aim is for firms to implement an approach because they believe that it enhances their business operations and assists them to control or mitigate their risks, rather than solely to meet a regulatory requirement.

Why firms are developing OR frameworks[5]




A2 Of the 22 firms in our review, those that we perceived as having more mature or sophisticated models had an internal business motivation for developing the OR Framework. For example, as a result of significant organisational change following corporate activity or restructuring, a large operational loss, reputational concerns, or senior management sponsorship.

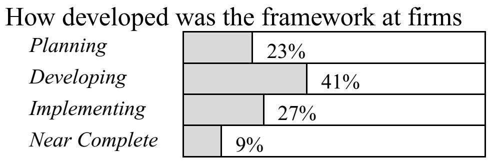
A3 However, a majority of firms stated that their primary reason for developing an OR Framework was increased regulatory focus (for example, in anticipation of the revised Accord/RBCD), with regulation a more significant driver in smaller firms than in major financial groups. A number of firms stated that forthcoming regulatory developments were focusing management attention on this area and were a catalyst for initiating or accelerating development – rather than imposing superfluous practices for internal OR management.

A4 No firm stated that it was currently being compelled to develop an OR Framework by rating agencies[6], nor did any mention customer / counterparty expectations as being a driver. However a number of firms believe that there

5 Unless noted otherwise, results are based on the 22 firms included in our review.

6 Although we note that at least one rating agency has recently published proposals on how they could incorporate OR into their overall analysis of financial institutions.

are competitive reputational advantages from being perceived by the market as having leading-edge OR practices. This last finding indicates that the Pillar Three disclosure aspects of the revised Accord/RBCD proposals will have a positive effect.




A5 From our assessment of firms' progress against plans, we found that whilst firms have begun planning, developing and implementing their OR Frameworks, no firm has fully completed this task. Nevertheless, we observed that a few large firms were at a 'near complete' stage where they were using, but still enhancing, their framework. Smaller firms tended to be planning or developing their approach to OR management.

A6 This progress is in relation to the management rather than the measurement of OR. Of the firms who stated to us that they were considering applying for the AMA, all were still either planning or developing an OR model.

A7 Those firms that had made some progress highlighted that implementation of the full framework was taking longer than they had initially estimated. This was due not only to the 'trial and error' nature of the development process, but also to the amount of time and effort taken to plan, develop, and implement processes and systems as well as educate the business. Uncertainties over regulatory requirements and lack of knowledge of best practice had also delayed progress.

A8 In a number of cases, pre-existing processes and activities were adapted and adopted into the OR Framework. However, some tools, such as a database of internal OR losses or events, usually required development from scratch (although some data existed in other forms). In general, a firm's approach was to start with a manual process, and then to automate once they further understood their requirements as the framework evolved. Automation was through a mixture of in-house development, collaborative development with software vendors, and the acquisition of off-the-shelf applications.

A9 Whilst a number of firms had used consultants to advise them on good practice and assist in implementation work, most firms recognised that it was essential to spend a significant amount of internal effort and management time on implementing the framework if it was to be effective. Our findings support the assertion that there is no easy or quick off-the-shelf solution to the development and implementation of an OR Framework.

A10 Based on this review, we consider that firms intending to apply for the TSA or AMA approaches of the revised Accord/RBCD will need to allow for a realistic period of time in which to implement a framework that will comply with the entry criteria for those approaches.

## B Governance and Operational Risk Management

B1 As a new OR Framework is developed and implemented (or an existing framework adapted), this may have an impact on other aspects of corporate governance within the firm. Our review investigated the extent to which OR management fits into the overall corporate governance structure of the firm. We consider that a good fit is important to deliver an appropriate level of oversight and delegation of authority.

### Policy and strategy

B2 In our request for pre-visit information, we asked firms to send us documents on their OR Framework, including policy and strategy statements. Strategy, in this context, referred to both the firm's overall approach to OR management, and how they intended to develop and implement an OR Famework. We expected these documents to help us assess the sophistication and maturity of the firm's famework, and to increase our knowledge of developments in OR practice.

| | Yes | |
|---|---|---|
| Firms with documented Policy / Strategy | 77% | |
| Where documented, this included an explicit statement of:[7] | | |
| • Strategy for framework development | 47% | *see paragraphs A1-10* |
| • Project plan for framework development | 35% | *see paragraphs A1-10* |
| • scope of the OR framework | 76% | *see paragraphs B9-17* |
| • risk appetite / tolerance | 0% | *see paragraphs B18-21* |
| • management framework | 82% | *see paragraphs B22-57* |
| • identification & assessment requirements | 76% | *see paragraphs B58-65* |
| • monitoring & reporting requirements | 76% | *see paragraphs B58-65* |
| • incident management & escalation requirements | 56% | *see paragraphs B58-65* |
| • description of OR tools | 47% | *see paragraphs C1-55* |

B3 Most firms had some form of documentation on their OR Framework, although the coverage and level of detail was patchy. In general firms were more likely to have a policy document than a statement of strategy. Management were often able to describe to us their approach to OR, the interactions between different

7 Results for firms with documented policy/strategy statements.

business areas and their strategy for developing the framework. However, we found few examples of comprehensively documented policy or strategy statements. Where these existed, we gained significant comfort that efforts were being made to communicate the approach and some indication as to the thoroughness and completeness of the firms' OR Frameworks.

B4 The absence of detail on firms' strategies for developing their OR Frameworks was indicative of the 'trial and error' nature of development, lack of knowledge over what good practice might constitute, and uncertainties over regulatory requirements. Even so, a number of firms had completed a detailed gap analysis between their current and desired frameworks (using, for example, consultancy guidance on best practice, CP142 and Basel documentation). However, fewer firms were at the next stage of developing roadmaps and/or project plans.

B5 We recognise that the variable quality of policy and guidance may have been due to the relatively undeveloped and evolving nature of the OR Framework within institutions. Although again, a few institutions had managed to clearly outline their policies and procedures even though their frameworks were evolving.

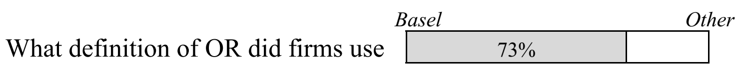
B6 **PRU** 6.1.10-6.1.14 of CP142 includes specific guidance on the contents of a firm's OR policy statement.

B7 Where there was no clear statement of expectation and practice on OR management, firms could not demonstrate how they had communicated to the business the OR Framework and its importance to the overall corporate governance framework. As outlined in CP142, the OR policy statement should communicate the firm's strategy (such as risk appetite and long term objectives) and processes for OR management. In an evolving framework, there should also be an outline of the firm's strategy, plans and roadmap for developing the OR Framework.

B8 Whilst a comprehensive documented statement of policy and strategy will facilitate communication within the institution, we recognise that it does not necessarily mean that the firm has implemented the OR Framework well.

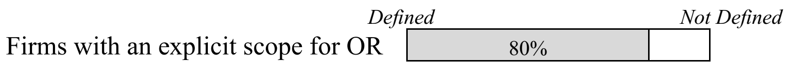
## Definition and scope

B9 Historically, whilst the concept of OR has been recognised, its definition has varied and the categorisation of risk exposures (for example, internal and external fraud, damage to physical assets, and transaction processing failures) covered by the scope of the OR Framework has been unclear. So, we were interested in how firms defined OR and applied this definition within their organisation.



B10 We observed that there was strong convergence within the industry to the Basel definition of OR. Where firms had their own previous definition, almost all had since substituted it for the Basel definition.

B11 The Basel definition has been developed in the context of regulatory capital. So, a number of firms had amended their interpretation of it. For example, a number of firms explicitly stated that their definition included regulatory risks (this is only implicit in the Basel definition) or reputational impacts (excluded from the Basel definition due to the difficulties of quantifying the 'risk of loss').




B12 In stating the scope of OR, a number of firms (particularly those considering applying for the AMA approach) had adopted the 'Basel matrix'[8] or industry equivalent as a generic scope. Others had developed their own classification of OR categories, which were often mapped to the Basel matrix. In some cases, firms' own classifications were very high-level and generic. We noted that even where defined, no firm had mapped the scope to their internal organisational structure.

B13 We observed that there was at times a discrepancy between the defined scope of the OR Framework and what was actually covered. For example, risk management systems focused primarily on *operations* risk (i.e. processing risk), or support and control areas (such as HR and finance) were excluded.

B14 Conversely, for a number of institutions (especially smaller firms), whilst OR was separately defined, in practice the distinction between operational, strategic, business and reputational risk was not made, and the risk management framework covered all risks (other than market and credit). One reason for this approach was that firms had already implemented processes to meet the good practice principles on the review of internal controls in the *Combined Code*[9].

B15 As stated in paragraph 3.5 of CP142, firms need to decide for themselves what OR means to them, and consider a more specific definition that is appropriate to the range and nature of their business activities and their operating environment.

B16 We observed that the framework was more effective where there was:

- a clear scope of the category of risks that the firm was trying to manage;
- consistent use and definition of terminology on risk exposures across the organisation; and

8 See *CP3: The New Basel Capital Accord* Annex 7 Detailed loss event type classification

9 *Combined Code* code of best practice D2.1 states that a review of the effectiveness of the firm's system of internal controls that covers all controls, including financial, operational and compliance controls and risk management should be carried out at least annually (commonly referred to as 'Turnbull Reporting').

- clear guidance on how boundary risks with other risk management systems (for example, a credit loss due to an operational failing) were treated.

B17 A number of firms highlighted that they had mapped their internal scope to the risk elements in our ARROW firm risk assessment framework. This was presumably to verify and demonstrate the completeness of their risk management systems as part of their processes to manage regulatory risk exposures.

### Risk appetite/tolerance

B18 The use of the terms 'risk appetite' and 'risk tolerance' in the context of OR have been controversial. In particular, some firms have argued that these terms cannot be used in the same quantitative way as for market and credit risk, primarily due to a lack of common terminology or metric. Our findings indicated that this was an area where institutions continued to have difficulty.

B19 Most firms implicitly consider such a risk appetite / tolerance in their day-to-day management activities. For example, firms have new product approval processes that require a formal risk analysis. Also, most decisions on whether to implement or change a process or system to enhance the control environment include some assessment of cost and benefit. Similarly, line management commonly define thresholds for routine (i.e. expected) operational failures (such as system downtime or processing errors), and it is only when an unusual (i.e. unexpected) number of failures or events occur that the issue is escalated and additional action considered.

B20 Although no firm we visited had incorporated an explicit statement of risk appetite/tolerance into their OR Framework, some of them were actively thinking about how best to do so.

B21 For example, one firm was already expressing operational exposure in terms of financial impact across 23 categories of risk by estimating at different confidence levels the financial impact according to the potential likelihood of the event occurring. The firm was considering whether this approach could also be used to articulate risk tolerance (i.e. the financial losses that would be acceptable against the different risk categories in both a normal year and one year out of five). It was also considering if risk appetite could be articulated by identifying, for example:

- activities that would generally be regarded as unacceptable OR;
- exposure to levels of financial loss or reputational damage that should be regarded as unacceptable;
- control standards that should be applied across the business; and
- specific matters that should be escalated to management.

## Management and oversight

B22 The management framework for OR includes not only the day-to-day management structure for controlling and mitigating underlying operational exposures (i.e. people, process, systems, and external events), but also responsibilities for the identification, assessment, and monitoring of risks and mitigating controls. Our primary interest was in the apportionment of responsibilities for the identification, assessment, and monitoring of OR.

B23 We observed, as might be expected, that the management framework varied considerably between firms – reflecting not only the size and complexity of the organisation but also internal political considerations. In a significant number of the organisations we visited, the OR Framework was still in early development – and therefore the management framework was also fluid.

B24 In major financial groups, the complexity of the organisation resulted in multiple layers of hierarchy and matrix reporting. For example, business line OR coordinators reported into divisional OR functions that in turn reported to both divisional management as well as the group OR function. Smaller organisations had less formal management structures, with management committees or ad-hoc discussions used to communicate and address OR issues.

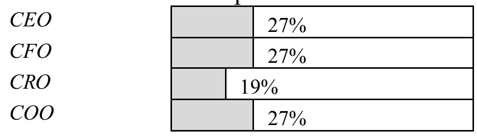
B25 Our review indicated that irrespective of size, there were six generic organisational categories within the management framework:

- senior management;
- decision-making committees;
- business line management;
- a central OR function,
- business line OR functions; and
- other central functions.

*Senior management responsibilities*

B26 The limited scope and time of our review meant that we were unable to fully assess the level of understanding within firms of the need for OR management. However, all of the firms that we visited stated that senior management sponsorship was essential to the implementation of the OR Framework.

Which Executive is responsible for OR[10]




B27 Responsibility for the control of OR was recognised to rest with the Board as a whole, although most firms had allocated responsibility for their OR Framework to a specific executive. This varied between the Chief Executive Officer (CEO), Chief Financial Officer (CFO), Chief Operating Officer (COO) and Chief Risk Officer (CRO) roles.

B28 Where a firm had chosen to appoint a *CF14 Risk Assessment Function* as part of the Approved Persons regime[11] this person was often a CRO responsible for all risk types (i.e. market, credit and operational). However, the CRO was less often a member of the Board. We noted that firms were still grappling with the implications of the Approved Persons regime, and in particular the extent to which responsibility should and could be delegated.

B29 In general, Non-Executive Directors (NEDs) did not request or receive additional information on OR other than that received as part of Board or audit committee papers. However, this is an area that may evolve in future, particularly in the light of the Higgs Report: *Review of the role and effectiveness of non-executive directors*[R4].

### *Committee structures*

B30 The number of committees (Board delegated or otherwise), their terms of reference and membership, and their frequency and formality, depended on the size and complexity of the organisation. The purpose of the committees also varied – in some firms committees were primarily a mechanism for communication, whilst in others all key decisions were made by committee.

B31 In smaller firms, as well as at institutions where the OR Framework was less mature, OR continued to be discussed in operations and/or control committees. A potential issue here was that the focus was on *operations/controls* risk rather than the broader scope of *operational* risk (including, for example, people risks).

B32 In larger institutions with more mature risk management systems, OR tended to be discussed at (or additionally at) an OR committee or overall risk committee – both in the business lines as well as at group level.

10 Results based on title or equivalent of individual identified by the institution as being responsible for OR

11 Rules and guidance on the Approved Persons regime are outlined in **SUP 10**. In particular, **SUP** 10.8.3-10.8.5 outlines our policy on the *CF14 Risk Assessment Function*.

B33 Where there was an audit committee, generally it obtained regular updates on the overall OR Framework – particularly in the context of its review of compliance with the *Combined Code* requirements. This is another area that may evolve in the light of the Smith Report: *Audit Committees – Combined Code Guidance*[R5].

B34 At one institution, a non-executive led risk committee, with an equivalent status to that of the audit committee, had been set up with membership consisting of a NED Chair, the NED Chair of the audit committee, and the executive CRO.

### *Business line management*

B35 Without exception, it was principally the role of business line management to control and mitigate operational exposures. Line management were also an important source of OR management information, such as risk indicators and internal OR incidents.

### *Central operational risk function*

B36 In a similar vein to that for market and credit risk, firms are increasingly establishing independent centralised OR functions; and firms believe that the role of such a function is of a similar standing to other risk, compliance and internal audit functions.


B37 Where a central OR function existed, it was generally performed by an independent risk function (i.e. by group risk or reporting into group risk). However, in smaller (and also in less mature) firms, the role was sometimes performed by, or reported into, the internal audit, compliance or operations function – recognising the overlap in skill sets and activities.

B38 Significantly, in a number of firms, whilst the OR Framework had initially been developed by internal audit, the firm had subsequently decided to establish a separate OR function. This resolved the potential compromise to internal audit's independence as the OR Framework developed from periodic risk assessment into routine management activity[12].

B39 An important consideration for some firms in deciding the reporting line was the role and resourcing of this central OR function in their governance structure (in particular to establish appropriate segregation of duties between control activities). For example, a number of firms had adopted a 'three lines of defence' approach, where business line management provided the first line, risk functions

12 The Institute of Internal Auditors position statement on *The Role of Internal Audit in Risk Management*[R6] issued in June 2002 states: "The primary responsibility for risk management lies with line management. Internal audit's involvement should stop short of responsibility and accountability for risk management across the organisation and of managing risks on management's behalf. However, in order to add value, it is often beneficial for internal audit to give proactive advice or to coach management on embedding risk management processes into business activities."

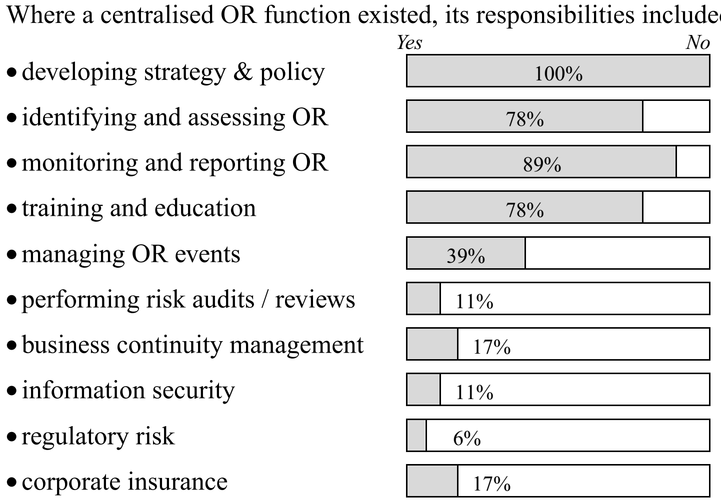
the second line, and internal audit a third line (each of which reported into different executive management).

B40 Conversely, in some major financial groups, 'integrated risk management' was considered essential to the effective operation of the firm, and therefore the risk, compliance and internal audit functions all effectively reported into one executive (in a few institutions this included financial and/or operational control functions as well). In one firm, the OR function acted as a check on the reconciliations and other controls performed by the finance function.

B41 Resourcing of central OR functions varied considerably – reflecting not only the size and complexity of organisation, but also the expected role and origin of the function (for example, from a pre-existing operations control function). However, most institutions were seeking an appropriate mix of audit and business operations knowledge. Where required, quantitative expertise was borrowed from the market risk area.

B42 The responsibilities of the OR function (whether formally stated or informally assumed) varied. Activities such as developing the OR Framework, drafting policies and procedures, and increasing awareness were considered core to the function by nearly all firms. Other firms included tasks such as managing OR incidents, performing risk audits, or coordinating business continuity management.

Where a centralised OR function existed, its responsibilities included:[13]




B43 Most firms believed that the central OR function had a role to play in the identification, assessment, monitoring and reporting of OR – although this was in practice more the facilitation, coordination and validation of activities performed by the business. Similarly, whilst business line management always had primary

13 Results for firms with such a function based on documented terms of reference or on subjective assessment where not documented.

responsibility for managing OR incidents, the central OR function sometimes had an explicit role in monitoring actions taken to minimise the impact of the incident, and ensuring that lessons were learnt to reduce future exposure to that type of event.

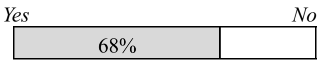
B44 A significant amount of time was spent by the central OR function in training and education activities for both business line management and the business line OR function. Even so, there was a more general jurisdictional issue that firms had to consider and address. For example, at one firm the central OR function noted their lack of authority to require business line management to follow best practice.

B45 For a number of firms, the central OR function was responsible for carrying out periodic business line risk assessment audits or reviews to produce a map of operational exposures. Most considered and addressed the potential for duplication with similar internal audit or compliance activities. For example, one firm acknowledged the duplication explicitly, and scheduled reviews to be carried out by the different functions at separate times of the year to obtain multiple assurance on the effectiveness of controls. Another firm was considering joint reviews by the OR function, internal audit and compliance each focusing on different aspects. Another more common approach was for Internal Audit to rely on the work performed by the OR function, and to carry out sample testing to validate findings.

B46 In a few firms, the central OR function was given responsibility for coordinating the control/mitigation of corporate-wide operational exposures. Some also had functional areas such as business continuity management, information security, regulatory risk, and corporate insurance reporting to the Head of OR. Whilst there are benefits for bringing the oversight of these important exposures into one area, this could cause potential segregation of duty issues, for example where the OR function is also responsible for performing risk assessments.

*Business line operational risk functions*

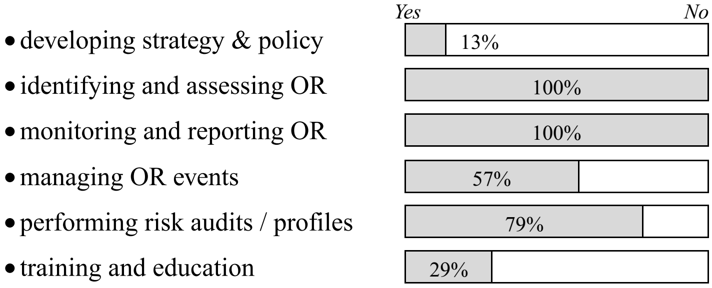
Is there a business line OR function




B47 The concept of a business line OR function varied considerably – from dedicated OR functions, to operations staff with liaison responsibility, to OR champions in the business area. Generally, major financial groups with more mature OR Frameworks had dedicated OR resource in each business area, whilst in smaller firms the function was either considered unnecessary or was performed by an individual with other responsibilities. Only one firm we visited had established business line OR functions without also creating a central OR function. However, another firm had disbanded their central OR function before our visit as they believed that the function had achieved its objective – that of establishing the framework.

B48 Generally, the purpose of the business line OR function was to act as a bridge and facilitator between the central OR function and the business area. So, in most cases the function had matrix reporting to the central OR function and business line management.

Where business line OR functions existed, their responsibilities included:[13]




B49 In a number of the major financial groups we noted that there were significant differences in method between divisional business line OR functions – for example, in scoping OR, in the tools used to monitor and assess risks, and in the frequency and type of reporting they performed. This appeared to be due more to the way in which these functions had developed (for example, from legacy operational control areas) rather than differences in needs between business lines. We observed that these differences made it harder for firms to assess and monitor their risks and mitigating controls on an aggregate basis.

B50 Only a small proportion of firms had assigned training and education responsibilities to the business line OR function (in contrast to the responsibilities of the central OR function). This may be because of the developmental nature of the OR Framework, so may change as the framework is fully established within the organisation.

### *Other central functions*

B51 It was generally recognised that other central functions played an essential role in the OR Framework. For example, Support functions such as finance, HR, legal, and IT were centres of expertise that played a unique role in coordinating activities to mitigate OR. Risk and Control functions such as credit and market risk, compliance, and internal audit were fundamental to the identification, assessment and monitoring of operational exposures.

B52 Whilst a large number of firms had outlined the role of Risk and Control functions in the framework, few had explicitly identified the role of the Support functions in it. Instead, their role was implicit within the roles and responsibilities of line management. However, there was informal coordination and communication with these functions in some firms.

B53 There was less coordination between finance and the central OR function than we had expected. Theoretically, finance could have a significant and wide-ranging role in the OR Framework, such as in the production or validation of management information ranging from risk indicators to OR losses, or in the computation and allocation of OR economic capital.

B54 We observed that at a few firms there had previously been ‘political’ conflict between the central OR function and internal audit. Issues identified included concerns over the significant overlap in activities performed by both functions, although for slightly different objectives (for example, risk audits as outlined in paragraph B45).

B55 Principle 3 of the *Principles for Business* states that ‘a firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems’. Additional rules and guidance on governance arrangements are also outlined in **SYSC** *Senior management arrangements, Systems and Controls*. **PRU 1.4** *Prudential Systems and Controls* of our forthcoming *Integrated Prudential Sourcebook* will also include policy on senior management responsibilities and risk management[14].

B56 In our review, we looked at the clarity of apportionment and communication of responsibilities. We observed that few firms had fully considered:

- the skills and experience required and existing in different areas of the organisation;
- the commitment and risk awareness of the people performing the role; and
- the relationship between the areas where risks existed to those with primary responsibility for monitoring and controlling them.

B57 Most firms were keen to emphasise (in the context of the revised Accord/RBCD) that there should be no detailed regulatory requirements on the way they organised and managed OR. Whilst this is consistent with our general approach to corporate governance matters, it appeared that some firms would welcome clarification on our expectations in the light of the recent increased focus on corporate governance within the UK and internationally.

## Reporting and escalation

B58 In our request for pre-visit information, we asked firms to send us examples of the OR management information produced for senior management and the Board. We expected this documentation to help us understand what information senior management found useful, as well as developments in OR management information systems.

14 Draft policy was published as **PRAG 6** in Annex A of Consultation Paper 97: Integrated Prudential Sourcebook

B59 Routine information used by management could be categorised as qualitative or quantitative. Qualitative management information was written commentary on operational exposures (sometimes supported by numerical evidence) with a subjective assessment of risk. Quantitative management information was based on numerical indicators with objective assessment based on threshold and tolerance levels. For both types of data, we observed instances where potential issues had been ranked using a traffic-light (i.e. red-amber-green) mechanism.

B60 Overall, we noted that most firms were producing qualitative information rather than quantitative – generally because of the lack of maturity and sophistication of their framework. However, most firms did recognise that to be able to monitor OR (particularly to aggregate OR across business lines or across risk categories) they would need to develop a more quantitative objective method for assessing OR.

B61 There was also significant variation in the type of management information provided. For example, in some institutions the audit committee would receive detailed quarterly risk analysis, whilst in others it was limited to a high-level annual update.

B62 It is worth noting that a number of major financial groups were developing 'OR Dashboards'. These collated a variety of risk indicator data that could be used to provide a scorecard of risk by business unit or risk category. Mainly, firms produced periodic reports compiled from a mixture of automated and manual processes. However, a couple of firms were developing automated systems (using, for example, internet technology) that could be used as part of day-to-day management to see both an aggregate risk position, and the underlying data such as risk indicators.

B63 We found that exception reporting to senior management usually consisted of qualitative information on significant operational losses or events. Most firms had set thresholds for the reporting of operational losses centrally. In addition, a few firms had established processes for the escalation of other OR management information based on predefined tolerances (for example, threshold limits for risk indicators).

B64 **PRU** 6.1.23 of CP142 includes specific guidance on the monitoring of OR, including on routine and exception-based reporting.

B65 We believe that this is an area that firms need to consider further. It was not apparent to us that firms had actively discussed internally the frequency and type of information on OR that should be produced for the Board, management and relevant committees, or had put in place processes to collate and validate this information.

### Validation and assurance

B66 Positively, we noted that the developing framework was being embedded into business operations, with management information used both in business areas and centrally. Whilst activities to validate the data used for management information were generally inherent in the processes and systems being implemented, this appeared to be more ad hoc rather than as part a deliberated review. For example, by wider consideration of how internal audit, central and business OR functions and business line management could provide assurance on the integrity of the data.

## C Tools used in an Operational Risk Framework

C1 We asked firms about their ability to identify, assess, and monitor operational exposures across their organisation, and the processes and systems they used to collect and aggregate OR information. We were interested in how, and if, the tools firms used covered the entire category of risks scoped by the firm. Also, we wanted to understand whether some tools were more appropriate for specific risk categories (for example, processing risks rather than people risks).

C2 In considering tools for the assessment of OR, we focused on their use for management purposes within the organisation, rather than their use in an AMA regulatory capital model[15].

### Identification, assessment and monitoring operational risk

C3 Overall, we observed that firms were still in the planning, development and/or implementation phase for this part of the OR Framework. There was no clear distinction between identification, assessment and monitoring activities, and we found that tools performed multiple tasks.

C4 As we expected, it was difficult for a single tool to cover the full OR scope. Firms were therefore using, or planning to use, a range of tools to give them full coverage (as well as enabling them to cross-validate data). However, due to the developing nature of the framework, this meant that generally firms did not have full coverage across all identified risk categories at the time of our review. Even so, we noted the considerable progress that firms had made in the last few years, and recognised that this progress was likely to continue due to the impetus given by the revised Accord/RBCD, as well as more open discussion on this topic within the industry.

15 The FSA's Operational Risk Implementation Advisory Group (ORIAG) was established to provide guidance on the UK implementation of the revised Accord / RBCD. In January 2003 it published a working paper[R13] that included a detailed discussion on the use of data collated from these tools in the context of regulatory capital.

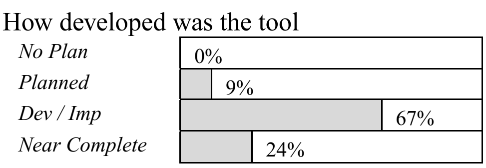
C5 This recognition of progress was tempered by our observation that developments were aimed more at process and system operational exposures rather than people risks. This was due perhaps to the way in which OR had been historically considered and managed.

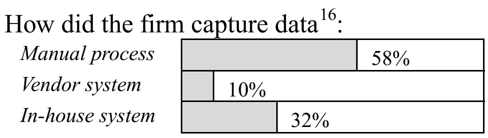
C6 The range of practices (and terminology used) varied considerably between firms, but the tools at the firms used fell into the broad categories described in both CP142 and the revised Accord/RBCD. These are described and discussed further below.

C7 Invariably the tools being developed and implemented by firms were intended to manage ‘expected’ operational exposures (see paragraph B19). However, firms reasoned that by managing their expected OR, they would also reduce the likelihood and impact of ‘unexpected’ operational exposures.

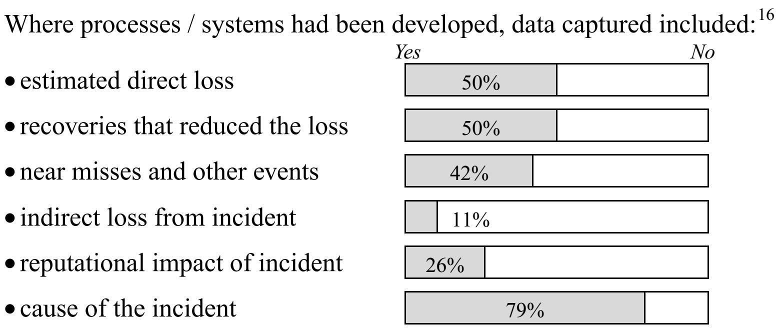
### *Internal loss/event databases*

C8 This category refers to processes and systems that capture data on internal OR incidents. Firms considered that this data could be used in all aspects of OR management. This included the identification (new risk categories), assessment and monitoring (frequency and severity of incidents), and control (lessons learnt) of operational exposures.




C9 Most firms were developing (or had developed) either a manual process or an automated system to capture this data – perhaps influenced by the prominence of this category of tool in the revised Accord/RBCD entry criteria.




16 Results for firms who are developing, implementing or have nearly completed the implementation of this tool.

C10 All firms started by reviewing the data they had already captured (for example, in business operations databases or in the general ledger). A number (in particular smaller firms) had not progressed past this stage in practice, as they were only starting in the development of their OR Framework. Other firms had outlined and implemented general processes for the routine reporting of OR incidents (whether restricted to losses or the broader range of events). Where this data was being captured, firms had also included processes to validate the information – either by restricting access to the database to the central or business OR function, or by incorporating line management validation checks as part of the automated process.

C11 We noted that institutions recognised that their incident reporting process was not comprehensive. This also extended to questioning whether the process covered the full category of risks outlined in the scope of the OR Framework.

C12 Only a few firms had considered linking OR reporting with their financial accounting processes. For example, whilst some firms had used the general ledger to identify past OR losses, few had set up specific OR general ledger accounts, built incident reporting into the ledger posting process, or performed periodic reconciliations between the general ledger and the internal loss/event database. Such activities, where performed, could assist in validating the integrity of the data in the internal loss/event database.

C13 For most firms, an area of considerable deliberation was on how and what data to capture. Firms focused on three key areas:

- *Should the database just capture OR incidents that have resulted in a financial loss or other events (i.e. near misses) due to an operational failure?* By restricting the database to the former, it is easier for the firm to capture more comprehensively such incidents (for example, by comparison to the general ledger). If the latter, the organisation needs to define what constitutes a near miss (for example, an operational failure that did not result in a loss or give rise to an inadvertent gain), and also implement processes to identify and assess such incidents.

- *What sort of information should be captured on the OR incident – direct financial loss or other indirect and/or intangible consequences?* There was general consensus that the database should include information such as the actual financial loss suffered, the type of incident that occurred by OR risk category, and the cause of the loss. However, indirect losses suffered (for example, the opportunity cost of business lost) and intangible losses (for example, reputational impact) are important consequences of the event, but are harder to assess accurately.

- *When should the database record details of the OR incident – at the time the incident is identified (but before the severity of its impact can be assessed) or when full details of the loss are known (for example, when* *booked to the general ledger)?* Whilst it is easier to record (and validate) information once all the details are known, if the incident is recorded only once all details are known then it might delay the identification (and therefore correction) of underlying control failures. Alternatively, timely reporting of OR incidents requires an estimate of the likely loss to be recorded (with amendment as expectations change).

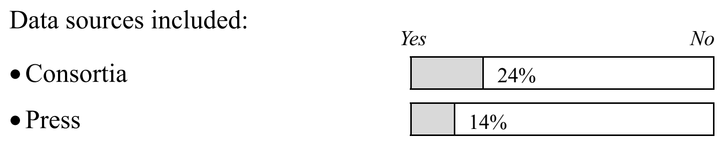
C14 As firms were still establishing processes to collate this data, they were more often considering how it could be used rather than systematically analysing it. Nevertheless, the use planned for this data varied significantly. Most firms stressed the importance they placed on this data in enabling them to identify underlying control failures (i.e. root cause analysis). For other firms this data also supported quantification of risk. Some firms indicated that they were uncertain whether the data would be relevant to the management of both low-impact high-volume (expected) risks and high-impact low-volume (unexpected) operational exposures.

C15 Firms indicated a number of concerns over who had access to the data. For example, they were uncertain if the data would need to be disclosed to a third party as part of a legal action. Firms also stated that to comprehensively collate data, there needed to be a 'no-blame' culture, so that individuals and departments felt that they could report such incidents without being adversely affected.

### *External loss/event databases*

C16 Most firms stated that they reviewed the effectiveness of their internal controls following general publicity in the press of a major incident at another firm. In addition, a few firms were more actively monitoring external events. This category refers to this more routine analysis of OR incidents at other institutions, and primarily supports the identification and control of operational exposures within the organisation.

C17 There were two types of widely available sources of data – consortia where the firm shared (anonymised) data with other members, and press and other agencies that collated information from publicly available sources (such as newspaper articles and company announcements). We noted that one institution was maintaining its own database of publicised external incidents rather than subscribing to an agency.

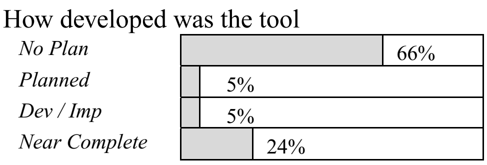


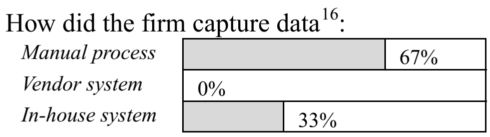
C18 There were very few firms currently subscribing and routinely using this type of data. This is perhaps due to the relatively scarcity of such sources, the quality of the data available, and a general doubt over the relevance of another firm's data.

C19 Where firms were using this data, it was primarily to help them identify high-impact low-volume operational exposures.

*Scenario analysis*

C20 A number of firms considered 'disaster' scenarios as part of their business continuity management activities. In addition, some carried out scenario analysis more broadly covering the whole range of operational exposures. This category refers to the broader consideration of the impact and likelihood of significant risks to the firm, and therefore could support the identification, assessment and control of operational exposures.



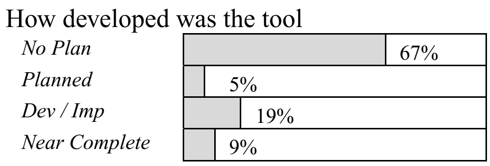

C21 We noted that few firms routinely carried out scenario analysis. Of those that did, generally management performed this periodically (usually annually, but sometimes six-monthly or quarterly) as part of a high-level controls risk assessment (see paragraph C28). Often, they did this to develop a 'top-down' risk profile of the firm in support of the 'Turnbull Reporting' process (see paragraph B14).

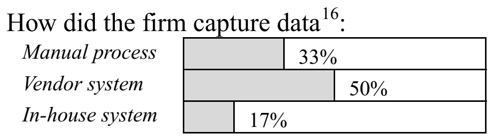
C22 A few firms were performing (usually annually) more detailed 'bottom-up' risk assessments. For example, at one firm, business line management were asked to consider, for each OR element in their category of risks, both the most likely frequency and severity of a loss, as well as a worst-case frequency and severity. These were then aggregated up to provide an overall risk profile of the firm's operational exposures. The firms who performed this type of scenario analysis highlighted the difficulties in aggregating the results.

C23 As highlighted in paragraph B21, one firm developed a risk profile by estimating at different confidence levels the financial impact according to the potential likelihood of the event occurring. This was a subjective 'expert' opinion based on internal and external data (for example, the firm considered what was the likelihood of such an incident occurring to either itself or to four of its competitors over a five year period).

*Process mapping*

C24 This category refers to the analysis of the processes and systems used in the end-to-end operating cycle for a firm's products and activities. It also supports the identification and assessment of operational exposures within the organisation.



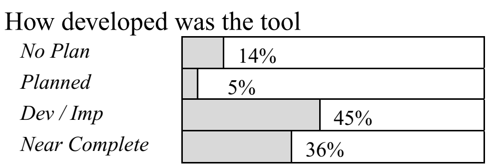



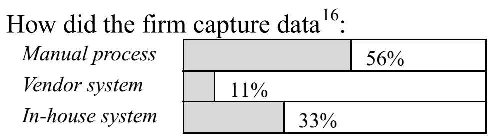

C25 In firms with high-volume process-intensive activities (for example, funds administration), process mapping was often performed as part of an annual accreditation exercise (for example, SAS70 audit or ISO9000 certification process). A few firms had combined this activity with routine 'controls risk self assessments' (see paragraph C29). In these cases, the firms asserted that they maintained the process map on an on-going basis.

C26 Other firms stated that they perceived process mapping to be too resource intensive, and difficult to maintain. So, they felt its use as an OR identification and assessment tool was limited.

*Controls risk assessment*

C27 This category refers to the range of activities performed to identify and qualitatively assess risks and mitigating controls.




C28 Whilst controls risk assessment was a core tool of the OR Framework at most firms, there was considerable variation in practice (for example, the extent to which the assessment focused on *risk* rather than *controls*, by whom it was performed, and how often).

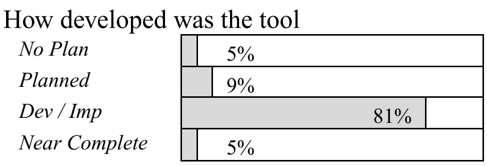
C29 Most often, controls risk assessment referred to a periodic (ranging from quarterly to annual) assessment by business line or senior management in support of the 'Turnbull Reporting' process through the use of tools such as risk workshops and questionnaires. These exercises often allowed management to identify topical risks at a given point in time, but did not necessarily provide a complete risk profile of the organisation.

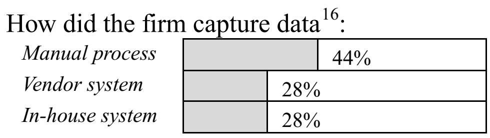
C30 Conversely, at some firms a more detailed 'controls risk *self* assessment' (CRSA) performed on a routine basis (ranging from weekly to quarterly) was used to monitor controls. However, the effectiveness of CRSA varied. For example, in some firms management were requested to assert every quarter that (unspecified) controls were effective or that operational exposures were being controlled. This left open to interpretation which controls and on what basis (i.e. effective for the full quarter or at the time of assertion) management was giving assurance. On the other hand, one firm had implemented a 'positive assurance' framework where all areas had to assert that they had successfully completed identified control activities on a daily, weekly or monthly basis depending on the frequency with which the control was performed.

C31 In a few firms, internal audit, group risk or compliance performed specific risk audits periodically to build a risk profile of a business area or division. Whilst these audits enabled the identification and assessment of risks and mitigating controls, they did not facilitate routine monitoring of operational exposures.

### *Risk indicators*

C32 This category refers to the use of numeric indicators as a proxy to the effectiveness of a control or the likelihood of a risk. As such, the indicators should facilitate the quantitative assessment and monitoring of risk exposures and mitigating controls.




C33 Most firms monitored 'operations/control' indicators (for example. reconciliation breaks, volume of trades, or systems down time) as part of routine management information. However, they had not historically used the indicators in a systematic manner to monitor risks on an individual or aggregate basis.

C34 We noted that a large number of firms were identifying or developing 'risk indicators', although few had made significant progress at the time of our review. Most firms had started by considering the relevance of indicator data that they already gathered, and were therefore focusing on areas where such data was easy to obtain. An issue for firms was getting coverage across the risk categories scoped in the OR Framework.

C35 Other issues that firms faced included separating risk indicators from process indicators, setting appropriate ‘warning’ thresholds to signal the need for intervention, and assessing the predictive capability of the indicators.

### *Risk workshops*

C36 Whilst a large number of firms had held risk workshops to assist in the identification and assessment of operational exposures, they highlighted the time-intensive nature of this activity and nearly all stated that they were unlikely to repeat such an exercise in the near future. Nevertheless, a number of firms noted that they had gained significant benefit from the workshops in educating business areas and obtaining an understanding of the organisation’s risk profile.

C37 For a number of firms, the initial risk workshop was followed up with periodic (ranging from quarterly to annual) ‘desktop’ reviews of identified risks to update the risk identification / assessment results.

### *New product approval*

C38 Our findings indicated that at most firms, operational exposures were considered as part of their new product approval processes. At a few firms, the central OR function was responsible for coordinating the process.

### *Process/system changes*

C39 At a number of firms, project management was specifically included in the OR Framework. However, it appeared to us that the focus was on risks from the poor management of the key projects, rather than on identifying any operational exposures resulting from process and/or systems changes. A number of firms stated that it was the responsibility of the project to consider and evaluate such risks.

C40 At firms maintaining process maps, they indicated that identification and assessment of risk was part of any updating of the process.

### *Cultural assessment*

C41 Often, firms indicate to us that ‘people risks’ are their major operational exposure. However, they also acknowledge that they find it difficult to assess and monitor exposures in this area. Our findings indicated that this continued to be an area where firms had difficulty, which they had not yet tackled.

C42 Only two firms indicated that they were intending to try to assess risk culture as part of a controls risk assessment exercise. Of these, one firm had performed this through a self-assessment exercise, but had not validated its assessment independently (for example, with Internal Audit) and the other was still planning this exercise.

C43 **PRU** 6.1.15-6.1.23 of CP142 include specific guidance on the firms risk management systems for the identification, assessment and monitoring of OR.

C44 We noted the significant progress firms had made in this area and believe that it will continue. At the time of our review, we observed that firms could not demonstrate to us the comprehensiveness of their tools and methods, and few could demonstrate how they intended to validate the information being produced from them. Whilst this will be essential to the effectiveness of the OR Framework, we recognise that this will develop over time.

C45 We were encouraged that, in practice, firms were performing activities that were consistent with our proposed guidance in CP142.

### Control and mitigation

C46 In general, we did not review the activities firms were performing to control and mitigate their underlying operational exposures as part of this project. However, at some firms the central OR function had been given responsibility for coordinating and/or validating core operational exposures such as business continuity management, information security, project management, and corporate insurance cover.

#### *Accounting for 'expected' operational risk*

C47 'Expected' operational exposures were not generally accounted for as part of the budgeting process, in provisioning, or by pricing into the cost of products. Firms highlighted a number of reasons for this, including not wanting to be perceived as accepting OR (budgeting), accounting regulations (provisioning), or because pricing was largely based on competitors or what the market would pay.

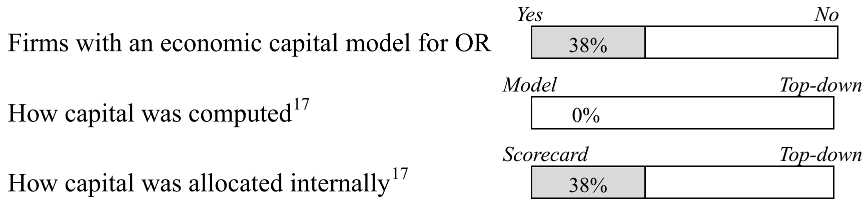
#### *Insurance cover*

C48 No firm had (as yet) mapped their insurance cover to their assessment of operational exposures – insurance cover was more routinely based on broker recommendations, peer comparison, or (at a few institutions) on prior year coverage. However, a few institutions indicated that they intended to compare their risk profile to insurance coverage in the near future.

C49 This is of interest in the context of the revised Accord/RBCD, where the current proposals for the AMA include reductions in regulatory capital requirements where insurance cover has been obtained.

*Economic capital*

C50 Economic capital is more frequently being used by larger organisations as a mechanism that encourages business decisions to be made consistently with overall corporate risk appetite. For example, it is used by firms to compute a risk-adjusted return on capital that can be used in assessing performance and pay.




C51 Our findings indicated that methods for the computation and allocation of economic capital for OR were still being developed. In general, whilst firms had developed methods for allocating capital, none had developed a model for computing what the overall level of OR capital should be. As a result, firms used a 'top-down' approach to the calculation of OR economic capital – i.e. based on an assessment by senior management. For example, one firm computed its OR capital as the difference between economic capital held for market and credit risk, and the aggregate capital held by the firm to maintain its credit rating.

C52 A few firms had made some progress in developing models for allocation of economic capital. These based the allocation on a formulaic 'scorecard' using 'bottom-up' risk assessment inputs – such as control risk assessment scores and internal audit ratings. Firms also ensured that allocation did not become a 'zero-sum game' (i.e. a business area only gained at the expense of another business line) by holding some capital centrally – ensuring that incentives were maintained.

C53 At the time of our review, no firm indicated that they were using OR capital as a significant input to the pay of business line management. This was perhaps because of the developmental nature of the model, or that other factors (such as revenue earned) were perceived to be more important.

C54 **PRU** 6.1.24 and **SYSC 3A** of CP142 include specific guidance on the control of OR.

C55 Firms are actively considering how to centrally control and mitigate OR, and we expect further developments in this area. An area of interest for us here is the comparison of industry practice on the control of OR to the proposed revised Accord/RBCD criteria – for example, on the treatment of expected losses, insurance, and economic capital.

17 Results for firms with an economic capital model for OR

# Our project approach

The OR project was initiated under our ARROW consumer and industry-wide framework (CIWF)[R1]. The primary input into the project was a programme of short discovery visits between May 2002 and January 2003. We supplemented the information from these discovery visits with findings from other firm-specific risk assessment and mitigation visits, discussions with software vendors and consultants and the review of published surveys.

The objective of the discovery visits was to better understand the firm's approach to OR management. Our review focused on:

- the governance and management framework;
- the operational risk management function, and qualitative aspects of operational risk management;
- risk modelling and any quantitative aspects of operational risk management;
- interaction of operational risk management with key interested parties such as internal audit, compliance, legal, information security, business continuity management, human resources and operations; and
- the implementation of regulatory requirements on operational risk

We have included below both the list of visit topics that we sent to firms, and the pre-visit documentation we requested they send us before the visit.

# A Visit topics

The questions below are provided to help the firm prepare for the discovery visit and provide a framework for our discussions. The FSA recognises that some of these questions may not be applicable to the firm, and that participation may be required from several different areas to be able to fully cover these topics. The FSA would prefer the agenda for the visit to be based on organisational reporting lines that are appropriate to the firm, and the OR management framework implemented at the firm.

## Background & Governance

Definition

- What is the firm's definition of operational risk? Are there any exclusions?
- Has the firm categorised its operational exposures (this does not necessarily mean into Basel categories)?

OR Management Framework

- Why has the firm invested in an OR management framework?
- How long has the firm's OR management framework been in place?
- What are the key components of the firm's OR management framework?
- Given that OR management is the responsibility of most senior management and control functions, how has the firm established and communicated individual responsibilities?
- Is the firm satisfied with its OR management framework? Are any significant changes to this framework planned? If so, what is the project / programme structure to manage this transition?
- Given that market and credit risk management is well established, what is the status of OR management in the firm?
- Is there an internal economic capital model? How is OR represented in this model?

Governance Structure (the Board)

- Is there a Board approved strategy and policy statement for OR?
- Has the Board set out a view on its appetite for OR?
- Is there a Board Member responsible for OR?
- What management information does the Board receive?
- How are OR issues escalated to the Board?
- Does the firm formally comply with any corporate governance standards (eg. Turnbull)?

Governance Structure (Management)

- Who is the Approved Person for the Risk assessment function (CF14)?
- How are OR responsibilities allocated (this may be along business lines, by legal entity, or on a geographical basis)?
- What is the management reporting structure for OR (including the background and reporting lines for key individuals)?
- Is there an OR Committee?
- Does the firm have a centralised OR management function (this may be at Group, business line, or subsidiary level)?
- What is the remit of this function, and how is it resourced?

Validation

- Who is responsible for reviewing the adequacy and correct implementation of the OR Framework (eg. Internal Audit)?

Review of OR Management Framework

- Has the firm commissioned a review (either internal or external) of its OR management framework recently?
- Has the firm participated in any industry-wide surveys on OR recently?

OR Experience

- What are the firm's main operational exposures?
- Have there been any significant OR issues recently? How were they managed?

External Disclosure

- Does the firm have a policy on disclosure? What has it disclosed to the market on OR?

## Qualitative

Risk culture

- Is the firm aware of its risk culture?
- How does the firm manage its human resources to control its operational exposures?
- Does the firm incentivise OR management?
- Has the firm identified any link between compensation structures and operational exposures?

Risk appetite, tolerances, and thresholds

- Does the firm have a defined risk appetite for identified operational risk exposures?
- Has the firm defined its tolerance for particular operational exposures (ie. accepted a certain level of OR losses as a cost of doing business)? If so what are its thresholds (ie. losses acceptable upto a certain limit)?
- Does the firm distinguish between expected and unexpected OR losses operational exposures?
- How (if at all) does the firm aggregate its operational exposures?

Identification

- How does the firm identify its operational exposures (this may include analysis of products, activities, processes and systems, peer comparison, etc)? How often is the identification exercise carried out?

Evaluation (measurement)

- How does the firm evaluate (or measure) its exposures (this may include the use of actual loss experience, key risk indicators, controls risk self assessment etc)? How often is the evaluation exercise carried out?

Monitoring

- How does the firm monitor its operational risk exposures, and actual loss experience? How and what is escalated?

Control

- Does the firm have a formal strategy for controlling its operational exposures (through mechanisms for risk mitigation, transference, and acceptance)?
- How does the firm review the adequacy of its control mechanisms for managing its overall exposure to OR?
- Is there an OR provisioning policy?

## Quantitative

Loss Data

- Does the firm collect OR loss data (and data on other risk indicators)? How long has this data been collected?
- Over what threshold is this data collected?
- Is the data ‘cleaned’ (in relation to credit or market loss)?
- Does the firm make a distinction between expected and unexpected losses?
- Does the firm include indirect losses in its loss data?

Data Integrity

- What tools does the firm use to collate information on operational exposures and losses?
- How is information on key risk indicators and actual loss information input and validated?
- What security procedures are used to protect the data?

Modelling OR

- Does the firm use any sophisticated qualitative or quantitative measurement models?
- For quantitative models, what distribution approaches are applied and to what degree of ‘fit’?
- Is external data used and if so how?
- Is scenario testing applied?
- What confidence level is applied?
- For qualitative models, how is this approach validated and benchmarked?

## Interactions

Interactions

- How does the OR function interact with areas responsible for:
  - Human Resources
  - Credit and Market Risk management
  - Internal Audit
  - Compliance
  - Legal
  - Information Security
  - Business Continuity Management
  - Outsourcing
  - Insurance
- Are there any other regular formal or informal interactions?

Business lines

- What role do the business units (such as front and back office functions) have in OR management?
- What is their relationship to the central OR function?
- Are there OR officers in the business units?
- Are expected OR losses priced into products?
- Is there an OR review process for new products, processes and systems (or for one-off transactions)?

Internal Audit

- What role does Internal Audit have in OR management?
- What is their relationship to the central OR function?

Compliance

- What is the firm's appetite and tolerance for regulatory (and statutory) risk? How does it set thresholds for managing this risk?

## Implementation

CP142

- Does the firm believe it can easily comply with the draft Handbook policy as outlined in CP142?

Revised Accord/RBCD

- What issues is the firm considering with regards to the revised Accord/RBCD?
- What stage is the firm considering aiming for?

## B Pre-Visit Documentation requested

- Details of the OR management framework, including relevant organisational charts and the mandate of any central OR management function
- Relevant Strategy & Policy statements outlining the firm's approach to OR and corporate governance
- Relevant Board and senior management MIS pack on OR
- Relevant OR disclosure material (to the market)
- Information provided to industry bodies on OR (for example, as part of a survey)
- Relevant internal/external reports on the OR management framework
- TOR and membership of any committees that regularly consider OR (e.g. Executive Committee, ALCO, Risk Committee) and a copy of the minutes from the most recent meeting
- Details of any tools, methodologies, or frameworks for the evaluation of OR
- Details of the firm's insurance strategy

**Annex 3**

# References

We identify below a number of references that firms may wish to review in developing their approach to the implementation of an OR Framework.

## FSA Regulatory Approach and Risk Assessment Framework

An overview of our regulatory approach and ARROW risk assessment framework can be found at: http://www.fsa.gov.uk/approach/.

R1 *Building the New Regulator Progress Report 2*, February 2002
http://www.fsa.gov.uk/pubs/policy/bnr_progress2.pdf

R2 *The firm risk assessment framework*, February 2003
http://www.fsa.gov.uk/pubs/policy/bnr_firm-framework.pdf

## Governance

There have been a number of reviews of corporate governance in the UK. The findings of these reviews have been incorporated into a *Combined Code* that forms part of the listing rules issued by the UK Listing Authority (a division of the FSA). The more recent Higgs and Smith Reports are currently being considered and do not currently form part of the *Combined Code*.

R3 *Combined Code on Corporate Governance*, FSA, May 2000
http://www.fsa.gov.uk/pubs/ukla/lr_comcode.pdf

R4 *Review of the role and effectiveness of non-executive directors* (The Higgs Report), The Department of Trade and Industry, Jan 2003
http://www.dti.gov.uk/cld/non_exec_review/pdfs/higgsreport.pdf

R5 *Audit Committees – Combined Code Guidance* (The Smith Report), Financial Reporting Council, Jan 2003
http://www.frc.org.uk/publications/content/ACReport.pdf

[R6] *Position Statement: The Role of Internal Audit in Risk Management*, The Institute of Internal Auditors – UK and Ireland, June 2002
http://www.blindtiger.co.uk/IIA/uploads/-38c9a362-ed71ce5fa5--7770/PositionStatementRiskManagement.pdf

## International Developments on the Capital Adequacy Framework

Details of the revised Basel Capital Accord are on the Bank for International Settlements website at: http://www.bis.org/index.htm.

[R7] *Sound Practices for the Management and Supervision of Operational Risk*, Feb 2003
http://www.bis.org/publ/bcbs96.pdf

[R8] *The 2002 Loss Data Collection Exercise for Operational Risk: Summary of the Data Collected*, March 2003
http://www.bis.org/bcbs/qis/ldce2002.pdf

[R9] *Consultative Document: The New Basel Capital Accord* (CP3), April 2003
http://www.bis.org/bcbs/cp3full.pdf

Details of the Risk Based Capital Directive are on the European Commission Services website at: http://europa.eu.int/comm/internal_market/regcapital/index_en.htm.

[R10] *Third Consultative Paper: Review of Capital Requirements for Banks and Investment Firms* (CD3), July 2003
http://europa.eu.int/comm/internal_market/regcapital/cp3/2003-consultpaper3_en.htm

Details of the Solvency 2 project, including the scope and timetable, are on the European Commission Services website at:
http://europa.eu.int/comm/internal_market/insurance/solvency_en.htm#solvency2.

[R11] *Prudential Supervision of Insurance Undertakings*, Dec 2002
http://europa.eu.int/comm/internal_market/insurance/docs/solvency/solvency2-conference-report_en.pdf

Details of our activity on the capital adequacy framework, and in particular the terms of reference, membership and minutes for the Operational Risk Implementation Advisory Group (ORIAG) are at:
http://www.fsa.gov.uk/international/1_caf.html.

[R12] *CP189: Report and First Consultation on the Implementation of the New Basel and EU Capital Adequacy Standards*, July 2003
http://www.fsa.gov.uk/pubs/cp/189/index.html

[R13] *ORIAG Working Paper*, January 2003
http://www.fsa.gov.uk/international/ORIAG_wp_jan03.pdf

A conference on *Leading Edge Issues in Operational Risk Measurement* was hosted by The Basel Committee on Banking Supervision Risk Management Group in May 2003. The agenda and presentations are at:
http://www.newyorkfed.org/pihome/news/speeches/2003/con052903.html.

**ISBN: 0117047368**

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.