Financial Services Authority

Enhancing frameworks in the standardised approach to operational risk

– Guidance Consultation

October 2010

The standardised approach to operational risk enhancing frameworks

A compendium of papers illustrating some of the approaches TSA firms might employ to help them meet the qualitative requirements.

1. Introduction – The standardised approach: enhancing frameworks
2. Operational risk governance and risk management structures
3. Risk identification, measurement, monitoring and reporting
4. The Use Test

1. The standardised approach: Enhancing frameworks

Introduction

1.1 The Financial Services Authority (FSA) is undertaking an initiative designed to examine, review and assess the implementation of the standardised approach (TSA) for operational risk at firms and to establish if any elements in existing frameworks can be improved on or require clarification.

1.2 This work is called: 'The standardised approach: Enhancing frameworks'. As part of this work we have initiated a series of expert groups designed to bring together the FSA and operational risk practitioners at firms to share ideas on current practice, weaknesses, and possible improvements. As well as stimulating discussions and informing the FSA and fellow participants, we are producing this compendium of papers covering various components of a TSA framework.

1.3 These papers are being drafted for the benefit of supervisors of TSA firms, but will also be made available on our website. The compendium outlines key features of the TSA that are of interest, with observations and suggestions to support existing handbook guidance and rules. We use Handbook guidance and other supporting materials to supplement the principles and rules where we think it may help firms to decide what procedures they might wish to consider adopting as good practice. Guidance, and the variety of materials we publish to support the rules and Handbook guidance, is not binding on those to whom the FSA rules apply. Such materials are intended to illustrate ways (but not the only ways) in which firms can comply with the relevant rules. Guidance and supporting materials are potentially relevant to an enforcement case. The extent to which we may take them into account when considering a matter will depend on all the circumstances of the case. Firms are referred to Chapter 2 of our Enforcement Guide for further information about the status of Handbook guidance and supporting materials.

1.4 Our findings will also flow into ongoing work at international level, in the EU and Basel, both of which are considering a number of operational risk topics of relevance to TSA firms at present.

1.5 We are grateful to all those firms and their staff who participated in the expert groups formed to consider the various compendium topics. The quality of contribution was exceptional and the openness with which participants embarked on this process is commended. Each section of the compendium will include details of those firms and individuals who provided such valuable assistance in this process.

Context

1.6 All BIPRU firms are required to meet a set of proportionate general risk-management standards (contained in SYSC 4.1.1R to 4.1.2R and SYSC 7.1.16R), irrespective of the operational risk methodology adopted. In addition, there are also specific qualitative standards for TSA and AMA[1] firms and these are proportionate

1 AMA: Advanced Measurement Approach to operational risk.

for TSA firms. As a consequence of the SYSC[2] general risk management requirements, there should be no significant difference between the qualitative operational risk standards required of a large and complex TSA firm and those for a similarly large and complex AMA firm.

1.7 The waiver approval processes for current AMA firms involved two to three years of close and continuous work with the firm by our Prudential Risk Department and were marked by improvements in the qualitative standards developed by these firms. However, TSA firms have not had the benefit of a similar close and continuous process, and this factor, together with the findings of some ARROW and firm visits and some SREP[3] submissions, has raised concerns about the qualitative standards adopted.

1.8 The lack of any guidance on the appropriate components and form of an acceptable TSA/ASA framework has made it difficult for some firms and supervisors to identify weaknesses in the frameworks adopted. The key message is that, as a result of the general risk management standards contained in SYSC, there should be no significant difference between the qualitative standards applied by a large and complex TSA firm and those required from a similar AMA firm. However, experience suggests that some such TSA firms may experience difficulty if they were to seek AMA approval, further supporting the suggestion that not all TSA firms have reached a satisfactory level of qualitative operational risk management.

Completed compendium sections

1.9 To date, we have facilitated three expert groups and this resultant compendium can be found on our website. These papers cover the following:

I. Operational risk governance and risk management structures

1.10 Topics covered include: the role of the board; risk appetite/tolerance; the role of senior management; the operational risk function; three lines of defence; and behaviour, engagement and risk culture.

II. Risk identification, measurement, monitoring and reporting

1.11 Topics covered include: the tools and techniques used by firms to identify and assess the operational risk inherent in all material products, activities, processes and systems; tracking relevant operational risk data, including loss data; procedures for taking appropriate action in response to information contained in management reports; and how risk exposure is managed, monitored, and reported.

III. The Use Test

1.12 Topics covered include: how the Use Test is integrated into the risk management process; how the output of the risk management process can become an integral part of the process of monitoring and controlling the firm's operational risk profile; how firms determine if they meet the Use Test requirements on an ongoing basis; and the Use Test or experience requirement.

2 SYSC: Senior Management Arrangements, Systems and Controls Sourcebook.
3 SREP: Supervisory Review and Evaluation Process.

Future compendium sections

1.13 We are proposing to undertake the following expert groups as part of this initiative:

I. Policy and documentation

1.14 We expect the policy topics to include: issues addressed in operational risk policies; how policy is communicated and maintained; risk appetite/tolerance; new product approval process; mapping the relevant indicator for business lines and activities policies (see also quantitative requirements); who approves; how frequently policy is reviewed and updated; the requirements placed on documentation; the issues documented; and how firm's satisfy themselves over the quality of documentation and management reporting.

II. Quantitative requirements

1.15 We expect the topics to include: the development of specific criteria for mapping the relevant indicator for business lines and activities; and approaches to business line mapping and relevant indicator mapping.

Summary

1.16 This compendium comprises a series of papers drafted by the FSA to assist firms and supervisors in understanding, assessing and enhancing the adequacy and effectiveness of frameworks introduced to implement the standardised approach to operational risk. The various components of a TSA framework cannot be viewed in isolation and should be reviewed and assessed as a package of closely interwoven elements. Therefore we will focus attention on the 'outcome' generated by the operational risk framework. It is unlikely that a firm with an acceptable operational risk governance and risk management structure, for example, and weaknesses in other TSA elements could be perceived to have an acceptable TSA framework. In addition, weaknesses in one area may well make it impossible for a firm to implement a successful element elsewhere. For example, a firm with poor operational risk reporting and management information is unlikely to be able to demonstrate that the operational risk assessment system is closely integrated into the firm's risk management processes (the 'use' or experience test).

1.17 Implementing operational risk frameworks cannot be viewed as a compliance exercise. Putting the various individual TSA elements in place is only likely to provide an effective framework if the individual elements have been implemented together in a robust, effective and comprehensive manner. The quality of implementation is an important consideration in any assessment of an operational risk framework.

1.18 These papers, and the variety of materials we publish to support the rules and Handbook guidance, are not binding on those to whom our rules apply. Such materials are intended to illustrate some of the ways in which firms can comply with the relevant rules. Irrespective of the techniques and methods adopted, a firm should be able to articulate why they believe the approach they have employed is appropriate.

Challenges

1.19 The process of drafting these papers confirmed the existence of a number of key challenges that cut across the various elements of the TSA methodology. These challenges are being encountered by most TSA firms and resolving these challenges is likely to greatly assist firms in developing more sophisticated operational risk measurement systems and practices. Challenges identified include the following:

i) The importance of tangible, clear and unambiguous board and senior management support and sponsorship for the operational risk management framework and function.

ii) The importance of the board and senior management setting the right cultural tone towards the operational risk framework.

iii) Persuading senior management to invest in improved operational risk frameworks and software. In many instances operational risk functions are required to focus valuable resources managing operational risk data rather than managing operational risk.

iv) The importance of operational risk training and the challenges of ensuring that training is geared to the appropriate level of participant.

v) Embedding the operational risk framework within and across business units, particularly where these cross countries.

For further information

1.20 If you would like more information, or to discuss the contents of these papers, please email andrew.sheen@fsa.gov.uk.

2. Operational risk governance and risk management structures

Introduction

2.1 This paper is one of a series drafted by the FSA to assist firms and supervisors in understanding, assessing and enhancing the adequacy and effectiveness of frameworks introduced to implement the standardised approach to operational risk. While this paper deals with issues related to operational risk governance and risk management structure it is recognised that the various components of a TSA[1] framework cannot be viewed in isolation and must be reviewed and assessed as a package of closely interwoven elements.

2.2 Therefore, it is unlikely that a firm with an acceptable operational risk governance and risk management structure and weaknesses in other TSA elements could be perceived to have an acceptable TSA framework. In addition, weaknesses in one area may well make it impossible for a firm to implement a successful element elsewhere. For example, a firm with poor reporting and management information is unlikely to have an effective governance structure. In addition, implementing operational risk frameworks cannot be viewed as a compliance exercise. Having the various individual TSA elements in place is only likely to provide an effective framework when the individual elements have been implemented together in a robust, effective and comprehensive manner. The quality of implementation is an important consideration in any assessment of an operational risk framework.

2.3 Increasing emphasis is being placed on the risk governance, oversight and management process adopted by firms. The board and senior management play a central role in this process and it is not clear how a firm's governance, oversight and management process can prove effective without the full support and engagement of these bodies, or how the operational risk framework can succeed.

2.4 We expect firms to strengthen their risk governance in response to several regulatory initiatives, including *The Walker Review*[2] and this exercise. We also expect supervisors will ask TSA firms to detail the measures they have taken to assess how suitable their governance arrangements are, any remedial action they have taken as a result and how they are satisfied with their governance arrangements.

2.5 This paper has been drafted for the benefit of supervisors of TSA firms but will also be made available on our website. The paper outlines key features of TSA that are of interest, with observations and suggestions to support existing handbook guidance and rules. We use Handbook guidance and other supporting materials to supplement the principles and rules where we consider it may help firms to decide what procedures to adopt as good practice. Guidance (and the variety of materials we publish to support the rules and Handbook guidance) is not binding on those to whom rules apply. Such materials are intended to illustrate some ways in which firms can comply with the relevant rules.

1 TSA: The Standardised Approach to operational risk.

2 A review of corporate governance in UK banks and other financial industry entities, 26 November 2009, www.hm-treasury.gov.uk/d/walker_review_261109.pdf.

Expert group

2.6 As part of the process of collecting the information necessary to draft this paper, we invited representatives from a number of BIA[3] and TSA firms to participate in an expert group on operational risk governance and risk management structures and a complete list of the 15 firms and their representatives appears in Annex A. A number of the expert group participants made presentations to the group. We are extremely grateful for the quality of debate and discussion in the expert group and for the contribution of participants to the work of the group.

Rules and guidance

2.7 The BIPRU[4] rules require firms to have a well-documented assessment and management system, with clear lines of reporting and responsibility that should be subject to a regular independent review. The requirements are subject to the proportionality principle and are therefore dependant on the size, nature, scale and complexity of the firm.

2.8 There is a fair amount of literature from various sources providing guidance on the topics of governance and risk management. Documents published by the Basel Committee for Banking Supervisors reinforce the importance of the role of senior management when implementing operational risk management frameworks. Furthermore, they emphasise that board members should be qualified for their positions while also being aware of the main operational risks their institution faces.

2.9 The CEBS[5] *Risk Management Consultation Paper* (2009) reinforces the importance of senior management support, as well as the existence of a person responsible for the risk management function across the entire institution (e.g. a Chief Risk Officer (CRO)). This CRO (or equivalent), should be sufficiently senior and independent to be able to challenge the decision-making process of the organisation.

2.10 Annex B of this paper contains details of the various rules and guidance mentioned above. Firms may find it useful to take full account of these rules and guidance when designing, implementing and testing their operational risk frameworks.

Key characteristics and observations

2.11 This section details elements that TSA firms might wish to employ as part of their risk governance and risk management framework. In drafting this section we have taken account of the various governance documents produced by the BCBS[6] and CEBS, and in some instances we have incorporated elements of that guidance directly into our suggestions.

2.12 While the involvement of the board or its delegates in the risk governance process is likely to be determined by the overall risk management framework of the firm, it is generally accepted that, when a board delegates responsibility to an appropriate

3 BIA: Basic indicator approach to operational risk
4 BIPRU: Prudential sourcebook for banks, building societies and investment firms.
5 CEBS: Committee of European Banking Supervisors.
6 BCBS: Basel Committee on Banking Supervision.

committee (for example, some firms have a Board Risk Committee), it continues to be accountable. Our discussions with the operational risk governance and risk management expert group showed that, for TSA firms with an effective Operational Risk governance and risk management structure, the board's (or its delegate's) responsibilities might include:

i) Approving and periodically reviewing the operational risk framework based on an appropriate definition of operational risk. This framework usually covers the firm's appetite and tolerance for operational risk. Reviews assess industry best practice and, where necessary, ensure the framework is revised accordingly. Reviews of the framework usually occur every 24 months and for many firms an annual review is considered appropriate.

ii) Establishing a senior management structure to implement the firm-wide operational risk management framework and assigning clear lines of management responsibility, accountability and reporting.

iii) Having a clear understanding of operational risk and being aware of the major aspects of the firm's operational risks as a distinct risk category that should be managed. As part of this process, regular reviews of key risks often take place at board level.

iv) Ensuring the operational risk-management framework is subject to effective audit and review by an independent audit function.

v) Understanding the impact of strategic initiatives on the operational risk profile and ensuring that the operational risk impacts of strategic initiatives, new products, processes and systems are evaluated, managed and mitigated.

vi) Promoting:

    a) a risk-focused culture throughout the organisation, with a clear understanding among all staff of their role in managing operational risk;

    b) open communication of the operational risk framework and clear and speedy reporting of operational risk information, including significant operational risk events; and

    c) ongoing risk training to ensure that the operational risk framework is fully embedded throughout the organisation. Our experience suggests that TSA firms often fail to require staff to undertake adequate operational risk training and that the embedding of a robust risk culture suffers as a result.

vii) Satisfying themselves that, for the purposes of risk management, the firm collects and maintains data that is accurate and comprehensive, which supports the principles of sound risk management at all levels of the firm. Actions required to satisfy this requirement might include:

    a) Maintaining a data policy, approved by the board.

    b) Data being sufficiently granular that it supports detailed analysis by risk factor.

c) Data being maintained over a period of time that allows analysis of loss behaviour through the economic and business cycles that are relevant to each risk type (for example, fraud).

d) Data being supported by a data model that allows for aggregation and disaggregation, as required. In particular, firms may wish to avoid their data being constrained by a specific vendor solution, entity identification, product classification, or instrument identification.

e) Data reporting upwards from origination, up to and including the board. Firms are likely to benefit from accurate, timely and clear reporting, aggregated at levels that are relevant to each recipient, and accompanied by value-adding analysis and commentary consistent with the decision-making status of the recipient.

f) Data not being limited to actual losses or incidents, but also including items that allow the firm's management to anticipate potential future problems by using benchmarking and/or trend analysis.

2.13 The board could discuss and approve a risk appetite/tolerance statement that is clear and understood throughout the organisation. We recommend though that firms consider whether their framework should cover the firm's appetite/tolerance for operational risk, as specified through the policies for managing this risk and the firm's prioritisation of operational risk management activities, including the extent of, and manner in which, operational risk is transferred outside the firm.

2.14 The term 'risk appetite' is often taken as a forward-looking view of risk acceptance, while 'risk tolerance' is often considered to be the amount of risk a firm has accepted in the past. In this document the terms are used to capture both aspects – to reinforce a general message that firms might include a forward-looking analysis as part of their risk management and capital assessments. A purely historic approach might be perceived as neither sufficient nor 'interchangeable' with a forward-looking view.

2.15 While some TSA firms have developed statements of this type, this is proving a challenging process in many organisations. Nevertheless, firms have usually expressed an appetite for risk in several forms, including loss data thresholds, RCSA[7] remedial action prompts and KRI[8] thresholds. An effective risk appetite will generally require regularly measuring and reporting risk exposure, as well as using clear and measurable triggers and limits to ensure that a firm does not exceed its risk appetite without taking remedial action. Operational risk appetite statements can provide an important management tool for TSA firms and are frequently used as a means of demonstrating that the operational risk framework is embedded. Risk appetite statements may:

i) take all relevant risks into account, including the firm's risk aversion, the current financial situation and the firm's strategic direction;

ii) encapsulate the various risk appetites in a firm and ensure they are consistent; and

7 RCSA: Risk control self assessment.
8 KRI: Key risk indicator.

iii) detail how the board will monitor management adherence to the risk appetite.

2.16 Generally, in TSA firms with effective operational risk governance and risk management structures, the senior management are responsible for implementing the framework approved by the board and are delegated, by the board, responsibility for developing policies, processes and procedures for managing operational risk. In undertaking these tasks, the requirements placed on the senior management might include:

i) Translating the board-approved operational risk management framework into specific policies, processes and procedures that can be implemented and verified within the different business units.

ii) Managing risks on a day-to-day basis, under the oversight of the management body.

iii) Implementing the operational risk framework through the organisation.

iv) Developing and obtaining approval for policies, processes and procedures for managing and approving operational risk in all new and material products, processes and systems.

v) Ensuring that:

a) all activities are conducted by staff with necessary experience, technical capability and resources;

b) the operational risk management policy is clearly and appropriately communicated to staff in all units;

c) remuneration policies are consistent with the firm's appetite for risk, as expressed in the risk appetite statement; and

d) operational risk staff communicate effectively with staff responsible for credit risk, market risk, compliance and other risks, insurance purchasers and outsourcing arrangers.

vi) Having a full understanding of the nature of the business and activities of the firm.

vii) Considering our SIF[9]/control function requirements.

2.17 The operational risk management function usually plays a key role in identifying, measuring and assessing the risks faced by the firm. Its responsibilities often include oversight of the framework; analysis of the introduction and development of new products, markets, lines of business, processes, systems and significant changes to existing products; and an appropriate involvement in exceptional transactions. The new 'product' approval process might consider the adequacy of the tools and expertise of the operational risk management, information technology, business line and internal control functions to identify, manage, monitor and report the resultant operational risk. Operational risk arising from mergers and acquisitions could be assessed in a similar way. This is particularly

9 SIF: Significant influence function.

important given the confidentiality and timeframe within which mergers and acquisitions are negotiated and the complicated nature of the process.

2.18 In undertaking these tasks, the requirements placed on the senior management of the operational risk management function might include being:

i) Appropriately expert for the risk profile. The board and senior management are often responsible for ensuring that the resources allocated to the risk management function are appropriate and consistent with the risk profile, management and business strategies.

ii) In regular contact with the board and its committees, depending on the delegation of authority and the risk management structure of the firm.

iii) Actively involved in the elaboration of the institution's strategy, to assist and benefit the decision-making process.

iv) Independent from the operational units reviewed by the risk management function. Nevertheless, the function could interact with the operational units and have sufficient access to achieve its objectives.

2.19 Successful risk management functions are usually:

i) empowered and supported by the board and senior management; and

ii) not directly responsible for the audit function, given the audit function's role in challenging the operational framework.

2.20 Responsibility for managing operational risk is not limited to the risk management function. All staff and business line management are responsible for managing operational risk and a firm would benefit from making all staff aware of their accountability for this.

2.21 In general, existing guidelines, papers and principles are not prescriptive on the governing structure of financial institutions. Instead they tend to concentrate on the roles and responsibilities of the key players and avoid discussing the structure created by the firm for its governance process. Nevertheless, it is clear from our discussions with the members of the expert group that a number of common elements exist in many TSA firms' operational risk governance structures. When considering the appropriateness of the adopted operational risk governance and risk management structure the range of issues that should be taken into consideration might include the following:

i) The committee structure – Many organisations with a central group function and separate business units create a Group Operational Risk Committee that reports into a Group Risk Committee, which is a committee established by the board. Depending on the size, nature, scale and complexity of the firm, the Group Risk Committee may receive input from country, business and functional level Operational Risk Committees.

ii) Consideration of the operational risk governance and risk management structure, which could take account of:

a) the composition of any Operational Risk Committees, ensuring that the committee contains a combination of members with either financial experience or risk management, or both;

b) whether the committees are solely dedicated to operational risk, how much time is devoted to this, and what evidence can be provided to testify to the quality of debate and challenge;

c) whether committee members must attend, how many meetings they can miss without censure, whether they can send an alternate and if so whether they require prior agreement of the chair;

d) the frequency of the operational risk governance bodies' meetings (a recent survey of risk governance[10] noted that meetings are not as frequent as had been expected); and

e) whether the meetings of the various committees that form part of the governance structure are timed so issues and events can be escalated in a timely manner.

2.22 Most expert group participants have established senior management Operational Risk Committees to ensure oversight of operational risk. It is interesting to note that some small firms have adopted this approach. In some instances firms have also established Board Risk Committees to oversee the overall risk management process. In some firms, the responsibilities of the board discussed in paragraph 1.15 are carried out by a delegated committee, although the board retains ultimate accountability. Firms adopting the TSA methodology may find it helpful to establish effective Operational Risk Committees and to be able to articulate how they satisfy themselves that the senior committee undertakes an effective role in the operational risk management framework.

2.23 Several expert group participants employ three lines of defence as part of their operational risk governance and risk management structure. A strong risk culture, good communication and understanding and a strong sense of risk awareness can provide comfort when used in conjunction with this approach. While, we have seen different interpretations of its composition the most common approach is for the three lines to comprise the following:

i) The first line is provided by the business units – comprising the business units, support functions and embedded operational risk staff.

ii) The second line is provided by the risk management function – comprising the operational risk management function and the compliance functions. To qualify in this category, the risk management function usually demonstrates the qualities detailed in the operational risk management function section.

iii) The third line is the audit function. A number of TSA firms have outsourced their audit function. The underlying arrangements and effectiveness of an outsourced audit function should be assessed for its suitability.

10 *Risk Governance at Large Banks* by Moody's Global Banking, July 2009

2.24 While a great many firms can point to their structure as evidence of the three lines of defence, firms could strengthen this by producing specific examples showing how they operate satisfactorily. They might also explain how the board and senior management are satisfied that this approach is implemented and operates in an appropriate and acceptable manner.

2.25 One possibility when seeking to determine the effectiveness of a firm's operational risk governance and risk management structure could be to evaluate its impact on behaviour, engagement and risk culture. Any attempt to do so might focus on a number of important elements:

i) Awareness – Every member of staff has an important role to play in the management and mitigation of operational risk within a firm. Supervisors could investigate if staff are aware of their responsibilities with regard to identifying, managing, monitoring and reporting operational risks. Firms could elect to raise awareness of operational risk among staff and embed the operational risk framework into the day-to-day risk management process of the firm.

ii) Culture – The expert group considered a strong risk culture, running through the entire organisation, as essential. For example, it may be better to 'own up' than hide an error, as a no blame culture exists. Such cultures are difficult to achieve without the direct, active and demonstrable sponsorship and support of the board and senior management. A favourable culture is also likely to be achieved if business units are engaged with the governance structure and do not view the arrangements as a constraint.

iii) Challenge – One of the key components of an effective governance structure is challenge throughout the structure – including at board, senior management and committee level. Various mechanisms exist to enable firms to judge the quality and effectiveness of the challenge process – including committee minutes and notes for record.

2.26 Firms capable of satisfying themselves about the effectiveness of their operational risk governance and risk management structure are also likely to be able to demonstrate to supervisors why they feel that this is the case. In some cases the firm may decide that external observers are best placed to undertake an impartial evaluation of effectiveness, although alternatively in some cases firms decide that this task is best achieved by internal parties, including the internal audit function. The firm is generally in the best position to determine who is best able to evaluate the effectiveness of the operational risk governance and risk management arrangements.

2.27 Supervisors often use a 'vertical slice' through the governance and risk management structure to help understand the workings of the process and procedures and behaviour, engagement and risk culture. This may show how risks and events are escalated within the governance structure and involves tracking the reporting, review and response to a significant operational risk event, from its discovery in a business unit up to the board or most senior risk committee in the firm. Examining the 'vertical slice' could extend to considering how any responses, reactions and decisions are communicated to the original business unit.

2.28 We have observed that firms often benefit from having a clear organisational structure with well defined, transparent and consistent lines of responsibility. This structure works well when it is comprehensive and proportionate to the size, scale and complexity of the firm's activities.

2.29 The operational risk governance and risk management structure is a key component of a firm's assessment and management system for operational risk and it is a specific BIPRU requirement that the assessment and management system for operational risk must be well-documented.

2.30 Regulators and supervisors regularly publish papers, principles and proposals for improving risk governance and risk management – for example, either locally (FSA) or in conjunction with other regulators (CEBS, BCBS, etc). Firms are likely to benefit from ensuring that they remain fully aware of the contents, proposals and recommendations published by regulators and adjust and amend their approaches accordingly.

Challenges

2.31 TSA firms seeking to ensure that their operational risk governance and risk management structures are both appropriate and effective for a firm using the standardised approach and are also proportionate to their size, scale and complexity, face a number of obstacles and supervisors could focus attention on how the firm has approached and resolved these issues, which might include:

i) demonstrating the extent of direct and active board and senior management sponsorship and support;

ii) determining the Operational Risk governance and risk management culture of the firm;

iii) understanding the degree and effectiveness of challenge;

iv) ensuring business engagement with the governance structure; and

v) how the board and senior management have satisfied themselves that the governance structure is effective and appropriate.

Conclusion

2.32 The operational risk governance and risk management structure is a key component of all TSA firms' operational risk framework. However, it may not be sufficient for a firm to be able to point to the existence of a risk governance and risk management structure as much depends on the way in which this process has been implemented. Firm-wide behaviour, engagement and risk culture are key considerations in determining the effectiveness of the risk governance and risk management structure as are the direct, active and demonstrable sponsorship and support of the board and senior management.

2.33 Firms lacking an appropriate and effective structure are unlikely to meet the requirements laid down in BIPRU 6.4 for TSA firms or the general risk management standards in SYSC 4.1.1R to 4.1.2R and SYSC 7.1.16R.

Expert group members:

Industry

Bank of America	Richard Walsh
Bank of Montreal	Christopher Eyles
Bank of NY Mellon	Anna Nicholl
Brewin Dolphin	Barry Howard
Britannia	Graeme Bell
Ford Financial	Robert Pringle
Gatehouse Bank	Reza Zaidi
HSBC	Neil MacKenzie
IG Group	Andrew Bole
	Bjorn Model
Investec	Asim Balouch
	Bharat Thakker
Man Group	Clive Wratten
Nomura	Huw Howell
Northern Rock	Barry Pert
Standard Chartered	Rajit Punshi
	Mark Willis
Vanquis Bank	Rosemary Hilton
	Manish Shah

FSA

Andrew Sheen (Chair)	Operational Risk Policy
Christine Brentani	Operational Risk Policy
Giles Ward	Operational Risk Policy
Anna Jernova	Operational Risk Policy
Liz Meneghello	Operational Risk Policy
David Haberfield	Risk Frameworks & Capital Unit (PRD)
Adrian McCarthy	Risk Frameworks & Capital Unit (PRD)
Brian Thornhill	Asset Managers & Advisers Department

Handbook rules and guidance

Source	Rule/ guidance #	Text
Prudential Sourcebook for Banks, Building Socieites and Investment Firms (BIPRU)	6.4.1R (2)	A *firm* must have a well-documented assessment and management system for *operational risk* with clear responsibilities for the system assigned within the *firm*. The system must identify the *firm's* exposures to *operational risk* and track relevant *operational risk* data, including material loss data.
	6.4.1R (3)	A *firm's operational risk* assessment and management system must be subject to regular independent review.
	6.4.1R (5)	A *firm* must implement a system of management reporting that provides *operational risk* reports to relevant functions within the *firm*. A *firm* must have procedures in place for taking appropriate action in response to the information contained in such reports.
	6.4.2R	A *firm* must comply with the criteria in *BIPRU* 6.4.1R having regard to the size and scale of its activities and to the principle of proportionality.
Senior Management Arrangements, Systems and Controls Sourcebook (SYSC)	4.1.1R	A *firm* must have robust governance arrangements, which include a clear organisational structure with well defined, transparent and consistent lines of responsibility, effective processes to identify, manage, monitor and report the risks it is or might be exposed to, and internal control mechanisms, including sound administrative and accounting procedures and effective control and safeguard arrangements for information processing systems. [Note: article 22(1) of the *Banking Consolidation Directive*, article 13(5) second paragraph of *MiFID*] 3,
	4.1.2R	For a *common platform firm*, the arrangements, processes and mechanisms referred to in SYSC 4.1.1 R must be comprehensive and proportionate to the nature, scale and complexity of the *common platform firm's* activities and must take into account the specific technical criteria described in SYSC 4.1.7 R, SYSC 5.1.7 R and SYSC 7. [Note: article 22(2) of the *Banking Consolidation Directive*]

BCBS and CEBS guidelines

Source	Guidance #	Text
BIS Sound Practices for the Management and Supervision of Operational Risk	Principle 1	The board of directors should be aware of the major aspects of the bank's operational risks as a distinct risk category that should be managed, and it should approve and periodically review the bank's operational risk management framework. The framework should provide a firm-wide definition of operational risk and lay down the principles of how operational risk is to be identified, assessed, monitored, and controlled/mitigated.
	Principle 2	The board of directors should ensure that the bank's operational risk management framework is subject to effective and comprehensive internal audit by operationally independent, appropriately trained and competent staff. The internal audit function should not be directly responsible for operational risk management.

Source	Guidance #	Text
	Principle 3	Senior management should have responsibility for implementing the operational risk management framework approved by the board of directors. The framework should be consistently implemented throughout the whole banking organisation, and all levels of staff should understand their responsibilities with respect to operational risk management. Senior management should also have responsibility for developing policies, processes and procedures for managing operational risk in all of the bank's material products, activities, processes and systems.
	Principle 4	Banks should identify and assess the operational risk inherent in all material products, activities, processes and systems. Banks should also ensure that before new products, activities, processes and systems are introduced or undertaken, the operational risk inherent in them is subject to adequate assessment procedures.
	Principle 5	Banks should implement a process to regularly monitor operational risk profiles and material exposures to losses. There should be regular reporting of pertinent information to senior management and the board of directors that supports the proactive management of operational risk.
	Principle 6	Banks should have policies, processes and procedures to control and/or mitigate material operational risks. Banks should periodically review their risk limitation and control strategies and should adjust their operational risk profile accordingly using appropriate strategies, in light of their overall risk appetite and profile.
CEBS Guidelines on the implementation, validation and assessment of AMA and IRB approaches)	470	Both the management body and senior management should be responsible for approving all material aspects of the overall operational risk framework. They should have a general understanding of the institution's operational risk measurement systems and detailed comprehension of its associated management reports and how operational risk affects the institution. The material aspects of the overall operational risk framework include: activities aimed at identifying, assessing and/or measuring, monitoring, controlling, and mitigating operational risk; proactive risk management strategies and policies; the organisational structure of the control functions; and specifying levels of acceptable risk.
	472	The management body has to exercise effective oversight. Senior management should therefore notify the management body, or a designated committee thereof, of material changes or exceptions from established policies that will materially impact the institution's operational risk measurement systems and management processes.

Source	Guidance #	Text
	473	Both the management body and senior management should be involved, on an ongoing basis, in the oversight of the control procedures and measurement systems adopted by the operational risk management function and Internal Audit, to ensure that they are adequate and that the overall operational risk management and measurement processes and systems remain effective over time.
	474	Senior management should ensure that the following tasks are being addressed: • ensuring the soundness of risk management processes • informing the management body – or a designated committee thereof – of material changes or exceptions from established policies that will materially impact the operations and the operational risk profile of the institution • identifying and assessing the main risk drivers, based on information provided by the operational risk management function • defining the tasks of the risk management unit and evaluating the adequacy of its professional skills • monitoring and managing all sources of potential conflicts of interest • establishing effective communication channels to ensure that all staff are aware of relevant policies and procedures • defining the content of reporting to the management body or to different delegated bodies thereof (e.g. the Risk Committee) • examining reports from Internal Audit on operational risk management and measurement processes and systems and • adequately assessing operational risk inherent in new areas (products, activities, processes, and systems) before they are introduced, and identifying risks tied to new product development and other significant changes to ensure that the risk profiles of product lines are updated regularly.
	475	The operational risk management function designs, develops, implements, and executes risk management and measurement processes and systems.
	476	The Internal Audit should provide an assessment of the overall adequacy of the operational risk framework, as well as of the operational risk management function.

Source	Guidance #	Text
CEBS CP 24 High- level principles for risk management	9	A strong institution-wide risk culture is one of the key elements of effective risk management. One of the prerequisites for creating this risk culture is the establishment of a **comprehensive and independent risk management function under direct responsibility of the senior management**.
	10	The management body is responsible for overseeing senior management, and also for establishing sound business practices and strategic planning. It is therefore of the utmost importance that the **management body have a full understanding of the nature of the business and its associated risks**. At least some members of the management body or, where relevant, the audit committee (or equivalent) should carry out an activity in the area of financial markets or have professional experience directly linked to this type of activity.
	11	**Every member of the organisation must be constantly aware of their responsibilities relating to the identification and reporting of risks** and other roles within the organisation and the associated responsibilities to these roles. The risk culture must extend across all of the organisation's units and business lines. Risk policies must be formulated based on a comprehensive view of all business units, and risks must be evaluated not only from the bottom up, but also across individual business lines.
	12	Institutions must implement a **consistent risk culture and establish sound risk governance, supported by an appropriate communication policy**, all of which must be adapted to the size and complexity of the organisation and the risk profile of the institution or banking group.
	19	The institution should appoint a **person responsible for the risk management function across the entire organisation**, and for coordinating the activities of other units relating to the institution's risk management framework. Normally this person is the Chief Risk Officer (CRO). However, when the institution's characteristics – in particular its size, organisation and the nature of its activity – do not justify entrusting such responsibility to a specially appointed person, the person responsible for internal control can be made responsible for risk management as well.
	20	The **CRO (or equivalent) should have sufficient independence and seniority to enable them to challenge (and potentially veto) the decision-making process of the institution**. Their position within the institution should permit them to communicate directly with the executive body concerning adverse developments that may not be consistent with the institution's risk tolerance and business strategy. When the executive body or the management body considers it necessary, the CRO should also report directly to the management body or, where appropriate, to the audit committee (or equivalent).
	21	The **CRO should have expertise that matches the institution's risk profile**. They should play a key role in making the management body and senior management to understand the institution's overall risk profile.

Source	Guidance #	Text
	23	The **risk management function should be actively involved, at an early stage, in the elaboration of the institution's strategy** and decision-making on business activities.
	24	Firms should ensure that the **risk management function is independent from the operational units** whose activities they review. Their position in the organisation should allow them to interact with these units in order to have access to the information necessary for the accomplishment of their mission. However, the risk management function should in all cases be carried out at arm's length from the decision-making function.
	25	**The management of risks should not be confined to the risk management function.** It should be a responsibility of management and staff in all business lines, and they should be aware of their accountability in this respect.
	26	The **management body and senior management should be responsible for allocating resources to the risk management function** in sufficient amounts and quality to allow it to fulfil its missions. These resources should be consistent with the institution's risk management and strategic objectives. They should include adequate personnel (with sufficient expertise and qualifications), data systems and support, and access to internal and external information deemed necessary to the fulfilment of the risk-management's missions.
BIS Enhancing corporate governance for banking organisations	Principle 1	Board members should be qualified for their positions, have a clear understanding of their role in corporate governance and be able to exercise sound judgement about the affairs of the bank.
	Principle 2	The board should approve and oversee the bank's strategic objectives and corporate values that are communicated throughout the banking organisation.
	Principle 3	The board should set and enforce clear lines of responsibility and accountability throughout the organisation.
	Principle 4	The board should ensure that there is appropriate oversight by senior management consistent with board policy.
	Principle 5	The board and senior management should effectively utilise the work conducted by the internal audit function, external auditors, and internal control functions.

3. Operational risk identification, measurement, monitoring and reporting

Introduction

3.1 This paper is one of a series drafted by the FSA to assist firms and supervisors in understanding, assessing and enhancing the adequacy and effectiveness of operational risk frameworks used by firms to implement the Standardised Approach to Operational Risk (TSA). While this paper deals with issues related to risk identification, measurement, monitoring and reporting (IMMR) it is recognised that the various components of a TSA framework cannot be viewed in isolation and should be reviewed and assessed as a package of closely interwoven elements. Therefore, a firm with acceptable IMMR methodologies but with weaknesses in other TSA elements is unlikely to have an acceptable TSA framework. Weaknesses in one area could also make it impossible for a firm to implement a successful element elsewhere. For example, a firm with poor reporting and management information is unlikely to have an effective governance structure. In addition, implementing operational risk frameworks cannot be viewed as a compliance exercise. Having the various individual TSA elements in place is only likely to provide an effective framework when all the individual elements have been implemented in a robust, efficient and comprehensive manner. The quality of implementation is an important consideration in any assessment of an operational risk framework.

3.2 Though we are not prescriptive regarding the approach we ask firms to take, we expect firms to be proportionate in the choices they make for risk identification, measurement, monitoring and reporting.

3.3 The primary aim of this document is to assist supervisors in assessing and challenging some of the methods that firms use to look at their risk exposures. Although this document is aimed at supervisors of firms that use TSA to calculate their operational risk charge, the information provided may be of use to supervisors of other BIPRU[1] firms. We address individual risk identification tools and highlight areas that may be considered good practice, which firms may also find useful. Supervisors may choose to ask TSA firms for detailed analyses of the methodologies used to assess risk exposures, along with any documentation and management information employed. This information can be used to determine whether the overall risk governance architecture is working effectively at the firm.

3.4 While this paper has been drafted primarily for the benefit of supervisors of TSA firms, it is also on our website. The paper outlines key features of TSA that are of interest, with observations and guidance to support existing Handbook guidance and rules. We use Handbook guidance and other supporting materials to supplement the principles and rules where we consider it would help firms to decide what action they need to take to meet the necessary standard. Guidance, and the variety of materials we publish to support the rules and Handbook guidance, are not binding on those to whom our rules apply. Such materials are intended to illustrate ways (but not the only ways) in which firms can comply with the relevant rules.

1 BIPRU: Prudential sourcebook for banks, building societies and investment firms.

Expert group

3.5 We invited representatives of a number of BIA[2] and TSA firms to participate in an expert group on 'Operational Risk Identification, Measurement, Monitoring, and Reporting' and a complete list of the firms and their representatives appears in Annex A of this paper. We held five meetings between June and October 2009, where a number of participants made presentations of their approaches to risk identification, measurement, monitoring and reporting to the group. The information provided at these expert group meetings form the basis of this document, though other sources of information have been used as well. We are extremely grateful for the quality of debate and discussion in the expert group and for the contribution of participants to the work of the group.

Rules and guidance

3.6 The BIPRU 6.4 rules for firms using TSA state that a firm must have a well-documented assessment and management system, which identifies the firm's exposures to operational risk and tracks the relevant data. SYSC 4 and SYSC 7 add to these rules by requiring that firms must have effective processes to identify, manage, monitor and report the risks that they are or might be exposed to (including low-frequency, high severity events). These processes and systems must be proportionate to the nature, scale and complexity of the firm's activities.

3.7 Currently, the main source of guidance for operational risk identification is the Basel Committee on Banking Supervision (BCBS) paper, *Sound Practices for the Management and Supervision of Operational Risk* (Sound Practices, 2003).[3] The Sound Practices paper encourages firms to identify operational risks inherent in all existing products, as well as any new products or services that a firm is planning to undertake. Also, firms' risk profiles should be regularly monitored by relevant staff and reported to senior management. The CEBS[4] Compendium[5] adds that 'near misses'[6] should also be closely monitored and that there should be appropriate procedures to collect such data.

3.8 Annex B of the 'Operational risk governance and management structures' document that forms part of this *TSA: Enhancing Frameworks* Compendium contains a summary of the rules that incorporate risk identification, measuring and monitoring. Firms should take full account of these rules and the associated guidance in the implementation of all aspects of their operational risk framework. TSA firms should be particularly mindful of the qualitative requirements set out in these rules.

2 BIA: Basic Indicator Approach to operational risk.
3 The full paper can be found at: www.bis.org/publ/bcbs96.htm.
4 CEBS: Committee of European Banking Supervisors.
5 The CEBS Compendium of supplementary guidelines on implementation issues of Operational Risk can be found at: www.c-ebs.org/News--Communications/Latest-news/CEBS-Compendium-of-supplementary-guidelines-on-(1).aspx .
6 'Near misses' are Operational Risk-related events that do not necessarily result in an actual loss (or gain) amount.

Key characteristics and observations

IMMR as part of the overall framework

3.9 For all the firms taking part in the expert group, the process of risk identification, measurement, management and reporting (IMMR) was integrated into the overall risk governance framework. It was recognised that it is important that firms can explain how their IMMR procedures fit into their overall risk governance structure and which areas and personnel are responsible for the procedures. Also, where firms employ the three lines of defence model,[7] it was acknowledged that firms should be able to explain how the IMMR process fits in and where responsibilities lie.

3.10 Many risk management frameworks relied on the cultural 'tone-setting' from senior management, which promotes a 'no blame' culture for reporting actual risks and near misses throughout the organisation. Our discussions show that representatives of several expert group firms feel the operational risk function benefits when senior management fully endorse, deploy, review and uphold the IMMR procedures and outcomes at the firm.

3.11 Regarding reporting, many risk managers ensure that information from the IMMR processes goes to the right committees and executive bodies and that any decisions arising from these committees are cascaded down to the areas that collect, control and monitor risk-related information.

3.12 IMMR could be used by board and senior management to monitor whether the firm is operating within its stated risk appetite. Risk indicators can be set to collect data where risk appetite limits are breached. These could be a valuable tool to ensure compliance with risk appetite and risk tolerance levels.

3.13 Firms could benefit from attempting to align their top down risk appetite (often focused on financial returns) with their bottom-up approach (more granular business-related risks and controls) where applicable. While this is a difficult concept, risk indicators could be established that promote this. There is broad industry consensus on the different means that a firm can use to consider its risk appetite for operational risk, including capital, losses and key risk indicators.

3.14 A particular challenge for firms, as well as monitoring existing risk, is how to identify forward-looking risks. One method observed was to develop forward-looking risk indicators, which could be monitored either on a short or longer-term basis. These forward-looking risk indicators attempt to identify trends in the next 12 to 24 months that will drive the level of risk, such as external threats, economic/political conditions or business change.

3.15 The risk identification process can lead to enhancing risk control mechanisms. Firms may decide on a risk mitigation or control strategy for each material risk identified. This information can be captured in a comprehensive risk register that:

7 The three lines of defence model of operational risk control include line management as the first line of defence, the risk control functions as the second line of defence, and the risk assurance functions such as internal or external audit as the third line of defence. Please see the 'Operational risk governance and risk management structures' paper for further information.

i) assigns senior responsibility for control for individual risks;

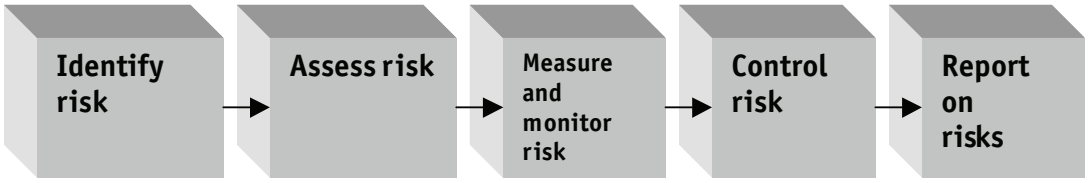
ii) facilitates ongoing and objective assessment of gross risks, performance and effectiveness of associated controls and mitigants; and

iii) provides validation of individual and aggregate (net) exposures relative to the firm's risk appetite (some firms have suggested such validation could be qualitative as well as quantitative).

3.16 The process could identify that there are sufficient controls in place already and/or that management are prepared to accept the level of risk.

3.17 The overall aim of the IMMR process is to ensure management are considering whether the appropriate controls are in place and working effectively to mitigate the risk to an acceptable level (reflecting their risk appetite).

3.18 Expert group members often divided their processes into the various components of the risk management life-cycle and provided an analysis of the elements of each of the stages. Below is an example of such a process. The IMMR process identified below is meant to be iterative and firms could have some system in place to ensure that the process is periodically reviewed and refreshed. The components listed below will be discussed in more detail throughout this paper.



Risk identification and assessment

3.19 Principle 4 in the 2003 BCBS Sound Practices paper states that firms should identify and assess the operational risks inherent in all material products, activities, processes and systems. This implies that firms should also ensure that, before new products, activities, processes and systems are introduced or undertaken, the operational risk inherent in them is subject to adequate assessment procedures.

3.20 The paper also stresses that risk identification is paramount for the subsequent development of a viable operational risk monitoring and control system. Effective risk identification is likely to consider both internal factors (such as the institution's structure, the nature of the institution's activities, the quality of the firm's human resources, organisational changes and employee turnover) and external factors (such as changes in the industry and technological advances) that could adversely affect the achievement of the institution's objectives.

3.21 In addition to identifying the most potentially adverse risks, firms will wish to assess their vulnerability to them. Effective risk assessment allows the firm to better understand its risk profile and effectively target risk management resources.

3.22 The first stage of such a process would involve the firm identifying the main risks to which it is or might be exposed and to set up indicators or other monitoring mechanisms. Risks could be looked at in the context of the overall business strategy and might not necessarily be considered in isolation. Some firms may choose to assess the quantitative impact of their material risks. These can also link into (or help inform) the firm's risk appetite. The following tools can be used for this stage:

i) **Risk and Control Self-Assessments (RCSA):**[8] Most firms conduct some sort of RCSA, which can include: i) different business areas holding workshops to assess where they are exposed to risks; ii) business heads being asked to fill in risk register templates or questionnaires; or iii) a hybrid or combination of these two approaches. Overall, by assessing its operations and activities, a firm is seeking to establish where the main risks in that area lie. The process is internally driven (though it can be led by an external third party) and often incorporates checklists and/or workshops to identify the strengths and weaknesses of the operational risk environment. Often, the most effective RCSA processes address inherent risks as well as the controls to mitigate them.

   RCSA's could include the following elements: risk description, risk event type, risk owner, impact and likelihood (probability) for gross (or inherent) risk, control, control owner, impact and likelihood for net (or residual risk), control effectiveness, and a remedial action plan (if appropriate). The assessment of gross risk pre-controls is often difficult for firms to undertake and some firms may benefit from thinking in terms of how much could be lost if key controls don't work as expected.

   It is important for firms using this tool to have a process in place that keeps RCSAs up-to-date and relevant over time.

ii) **Business process mapping:** With this methodology, firms identify all the steps within specific business processes or procedures (for example, the life-cycle of booking and settling a trade) to determine where areas of weaknesses might lie. This may result in controls being tightened in these areas. In addition, key risk indicators could be set up to monitor weak points in processes so that actions can be taken before weaknesses turn to breaking points. Firms might take a risk-based approach about which business processes should be mapped in this way and to what detail.

iii) **Scenarios analysis:** Scenario analysis often involves carrying out workshops in different areas of the firm where expert judgement is used to ascertain different risks to which the area might be exposed. The main difference between scenario and RCSA workshops is that the scenario workshops are meant to investigate the 'unexpected' or potentially catastrophic losses to which the firm may be exposed while the RCSA workshops tend to focus on the expected losses. Firms could envisage further reaching scenarios of potential events beyond their own distress. Firms could use internal data and external data to facilitate the thinking around the scenarios and to inform and verify the quantification of the

8 In actuality, RSCA's span across multiple stages of the process and can link into scenario analyses and will cover the risk control assessment.

risks. These can include extreme, but plausible events and are often focused on low frequency, high severity events. Scenarios tend to be forward looking.[9] It is generally felt important that enough time is allocated for the running of the workshops to ensure effective outcomes. Firms using the scenario processes are unlikely to be able to demonstrate the integrity of the scenarios if the outputs from the scenario planning workshops are not clearly documented.

Scenarios exercises could include: the description of the scenario, including the cause; key controls; use of internal and external data; control failures implicit in the scenario; frequency; and impact, including the worst case loss and impact and any remedial actions. The impact figures of catastrophic events on a firm's financial position are often assessed using scenarios. Scenarios can also be used to generate frequency and impact figures for modelling purposes. It is up to firms to identify the appropriate number of scenarios to use.

It is also important to look out for scenario biases, such as:

- **Partition dependence:** where respondents' knowledge is distorted by discrete choices of buckets within which their responses have to be represented.
- **Availability:** where participants recall recent events.
- **Anchoring:** where different starting points yield different estimates.
- **Motivational:** where the misrepresentation of information due to respondents' interests are in conflict with the goals and consequences of the assessment.
- **Overconfidence:** where small data samples are applied to the whole population.

3.23 To assist in the risk identification process, firms could use the results of internal and external audit reports and other available public data. Firms could also consider any regulatory reports received (e.g. from ARROW and/or SREP assessments and supervisory correspondence) and any other published FSA guidance, statements or notices.

3.24 The risk assessment phase provides a good opportunity for firms to ensure that adequate controls and mitigants are in place to manage the risks and whether existing controls might require improving.

3.25 Firms demonstrating good practice in their use of the risk identification and assessment exercises/tools, tend to employ these tools on an annual basis and more frequently as required if material changes to business areas occur.

Risk measurement and monitoring

3.26 The next stage of the IMMR process involves the firm setting up specific risk indicators and thresholds for measuring the identified risks to which the firm is exposed.[10] To meet the requirements of SYSC 4.1.1R firms should also ensure that

9 It is possible for the same risks to appear under both RCSAs and scenarios, once for the expected loss element and, secondly, for the unexpected loss component.

10 It is important that the definitions and scales utilised within risk capture and risk measurement systems are consistent throughout the firm and can be easily understood by those who are expected to work with or record data into these systems.

they have a risk monitoring procedure in place. Some of the elements of this risk measurement and monitoring phase could include:

i) Key Risk Indicators (KRIs), Key Performance Indicators (KPIs) and/or Key Control Indicators (KCIs)[11]

These are statistics and/or metrics that can provide insight into a firm's risk position. These indicators tend to be reviewed on a periodic basis (generally monthly) to alert firms to changes that are indicative of risk concerns. Such indicators may include the number of failed trades, staff turnover rates, and the frequency and/or severity of errors and omissions. Firms could establish thresholds per indicator and many usually monitor them on a red/amber/green (RAG) basis. Many firms employing this tool ensure that staff understand the implications, escalation process and actions to be taken when risk indicators go into the amber or red zones. Firms could benefit from having a robust process for changing KRI thresholds, with appropriate gatekeepers having ownership for individual KRIs. KRIs are usually periodically reviewed to assess their relevance.

ii) Early warning indicators/Emerging risk indicators

Firms could identify appropriate indicators that provide early warning of an increased risk of future losses. Such indicators are usually forward-looking and reflect potential sources of operational risk, such as rapid growth, the introduction of new products, employee turnover, transaction breaks, system downtime, etc. With the setting of appropriate thresholds linked to these indicators, an effective monitoring process can enable the firm to act upon these risks appropriately.

iii) Loss data

Firms could maintain a loss data base, which captures details of actual operational losses at the firm, as well as near misses. Data collected could include: the cause, the event, the date the event took place, the severity, the amount of the loss, the effect, the risk owner, control failures, the control owner, any recoveries of gross loss amounts, lessons learnt and any remedial actions. Material exposures to losses could also be identified.

iv) Risk monitoring

Firms often implement a process to regularly monitor operational risk profiles and material exposures to losses as an integrated part of the firm's activities. An effective monitoring system can allow for the quick detection and correction of deficiencies in the firm's processes and procedures and can allow for enhancements of the risk-management process. In turn, these actions can substantially reduce the potential frequency and/or severity of a loss event. The frequency of monitoring could reflect the risks involved and the nature of changes to the operating environment. Internal audit and/or the risk management functions could periodically assess compliance with the monitoring activities.

11 Some firms may also monitor Key Control Indicators (KCIs). Key indicators can be used to both provide insight regarding the level of risks occurring as well as for monitoring what is happening to the risks.

3.27 Many risk measurement and monitoring processes capture both existing and forward-looking risks, with firms proactively setting up and refreshing suitable risk indicators, as well as establishing appropriate time-frames for monitoring the information obtained from the indicators and their effectiveness.

Risk control

3.28 Firms should have effective processes to manage operational risks. These policies could be implicitly and/or explicitly linked with the risk appetite of the institution.

3.29 Risk appetite statements could contain a mix of qualitative and quantitative factors and be capable of being communicated, measured and applied to key risk-generating areas of a firm. The risk-measurement tools above could be used to assist firms in ensuring that quantitative aspects of the firm's risk appetite are not breached.

3.30 In our view, firms may wish to consider periodically reviewing and analysing their risk-control strategies and adjusting their operational risk appetite accordingly, in light of changes to their business models/activities and/or size.

Such analysis could help the institution to identify and distinguish between:

i) which risks[12] it is willing to accept as business as usual and hold capital against or factor into business performance and/or margins;

ii) the risks for which it is willing to invest in controls and mitigants;

iii) which risks could be transferred through insurance;[13] and

iv) which risks it should avoid altogether.

3.31 In many firms, the board of directors and senior management are responsible for establishing a strong internal control culture in which control activities are an integral part of the regular activities of the institution.

3.32 As mentioned previously, the tools used under the risk identification section, such as RSCA workshops and scenario analysis workshops often provide good opportunities for firms to assess and ultimately strengthen their controls around risks that have been identified.

3.33 Each cyclical review of the IMMR processes could allow for the review of the control effectiveness as well.

Risk reporting

3.34 The SYSC rules require firms to have effective risk reporting and this process may involve senior management receiving regular reports reflecting the up-to-date status of operational risk issues at the firm. The operational risk reports may contain internal financial, operational, and compliance data, as well as external market information about events and conditions that are relevant to decision-making. Reports are usually distributed to appropriate levels of management and to areas of

12 These could include risks that are unmitigated and/or residual risks following mitigation or controls.

13 Where insurance is used as a mitigant, it is essential that the firm undertake a robust gap analysis of the insurer and the policy.

the firm on which areas of concern may have an impact. Reports that fully reflect any identified problem areas and motivate timely corrective action of outstanding issues are often most effective. To ensure the usefulness and reliability of these reports, management could regularly verify the timeliness, accuracy, and relevance of reporting systems and internal controls in general. Management may also wish to use reports prepared by external sources (external auditors, regulators) to assess the usefulness and reliability of internal reports. Reports could be analysed with a view to improving existing risk management performance, with a focus on the implications of operational risk breaches on the business. The management information (MI) reports can also potentially be used to inform and instigate the development of new risk management policies, procedures, and practices and could be used to monitor compliance with risk appetite levels.

3.35 To be of most benefit, the MI is likely to be in a form that the users can readily understand, challenge and act on. It can be useful, for example, to have a high-level summary of the top risks at the firm in the form of a risk dashboard. Some firms also find it useful to provide a heat map summary of their risk ranking in such a way to show which risks are of higher or lower probability and of higher and lower impact. This type of report can be developed for each business area as well as the firm as a whole and can be supported by underlying reports providing more detail. It can be important for the reports to identify in a clear and easy-to-understand manner any concentration of risks that might pose a threat to the business and reasons for any movements in risk rankings.

3.36 It may also be important to ensure that trend analysis is available for the various KRIs and that KRIs are appropriately aggregated when amassing data upwards from smaller business areas to larger regional areas, for example. In our view it is beneficial that senior management challenge KRI data that never changes as this may mean that the KRIs are not measuring true areas of risk, thresholds are not set at the correct level or controls may be continually failing. The MI reports may want to highlight any operational risk themes that may be developing.

3.37 Overall, it can be important that the recipients of the reports understand what the operational risk appetite is at the firm and what the governance procedures are for changing the information that is set in the reports. Some members of the expert group argued that it is important to be able to demonstrate effective operational risk challenge within all decision-making processes.

Other

3.38 Firms could establish a risk identification and control process for new products and services and consider them in the context of their agreed risk appetite and systems and controls capabilities. A new product-approval process could encompass the use of RCSAs, scenarios, and the development of KRIs ahead of any formal sign-off process. Firms could also identify how the risk information related to the new products/services can be captured by any MI.

3.39 Firms could also establish policies for managing the risks associated with outsourcing activities.

3.40 Firms will wish to provide training to staff engaged in the IMMR processes. Training could be geared at the various stages of the IMMR process – for example, certain staff could be trained on how to identify risks that need to be reported. Selected members of staff may also need to be trained on how to record information related to the firm's risk events in the firm's loss database. Training may also need to be tailored for scenario workshop participants. In these circumstances it may prove beneficial for training programmes to be kept up-to-date as new developments occur, and to be reviewed periodically.

Challenges

3.41 The presentations and discussions by the expert group members highlighted a number of challenges surrounding IMMR. These are listed below:

i) Several participants stressed that a culture supportive of operational risk management at the firm was particularly important for ensuring that risks were adequately identified and reported on a timely basis. Senior management support for operational risk policies and procedures was particularly important where firms were trying to increase the reporting of risk incidents and to move away from a 'blame culture'.

ii) Most participants stressed the importance of operational risk training in IMMR. Some firms mentioned that they sometimes found challenges in ensuring that staff training on operational risk was geared at the right level for the various types of staff at the firm. Also important is for operational risk personnel to understand the various businesses in which they are involved in monitoring risks and setting risk indicators.

iii) Sometimes the RCSA scoring can be quite subjective and it is important to ensure that a healthy degree of challenge takes place to ensure the integrity of the data. Also, it is sometimes difficult to obtain a uniform approach across business units and in different countries. Sometimes local regulation plays a role in the differentiation.

iv) Several expert group participants felt that where the operational risk data is feeding to business area capital figures and remuneration, it is vital to prevent 'gaming the system' by the manipulation of the results of subjective risk assessments.

v) Challenges also occurred when new operational risk tools were being rolled out across the business. One firm stressed the importance of getting appropriate buy-in at the business unit level, ensuring that tools were user-friendly and making the framework fit-for-purpose for everyone across jurisdictions and business units. Participants stressed that it took time to ensure that the new tools were properly embedded.

vi) Firms experienced challenges in combining and consolidating IMMR processes across two (or more) firms following a merger or acquisition.

vii) Firms highlighted the importance of finding the right balance between spending time monitoring risks and spending time reporting risks. Also, firms found that if they had more operational risk staff, they could do much more in terms of IMMR.

viii) Firms highlighted the importance of ensuring that the information in the MI was timely and did not result in stale information. They felt it was important to have ways of highlighting serious risk breaches that occurred between the MI reporting cycles. Also important was the ability to be forward-looking rather than purely reactive.

ix) Many firms highlighted the challenges in quantifying risk appetite and in setting appropriate thresholds and limits. One issue discussed was how the thresholds around KRIs can be manipulated to show more or less red KRIs and the challenges associated with management expectation and linking KRIs to the firm risk appetite, stressing the importance of an appropriate governance system around the KRI process. Also, some firms found it challenging to identify what the correct number of KRIs or scenarios should be for their particular firm.

Conclusion

3.42 Overall, we are not prescriptive in the approach to IMMR that we ask firms to take. However, to satisfy SYSC 4.1.1R, all firms should be able to demonstrate that they have gone through a robust process to identify key risks to which they are exposed. Robust controls should also be established. Firms should set up a methodology to monitor those risks. Operational risk reporting is also essential and may be appropriately tailored for the specific senior management to which it is geared. Risk managers may be required to justify the approach they have taken – for example, in how they determine the risk identification tools that are used and how they ensure the support and engagement of business area managers in identifying, reporting and controlling risks.

3.43 Firms lacking appropriate and effective risk Identification, Measurement, Monitoring and Reporting (IMMR) arrangements are unlikely to meet the requirements laid down in BIPRU 6.4 for TSA firms or the general risk management standards in SYSC 4.1.1R to 4.1.2R and SYSC 7.1.16R. Firms could benefit from ensuring that they are familiar with the BIPRU and SYSC requirements.

Expert group members (as at October 2009)

Industry

Abbey	David Burrill
Bank of America	Richard Walsh
Bank of Montreal	Scott Matthews
	Gary Olivier
Credit Suisse	Jennifer Dax
Goldman Sachs	Sofia Zimmar
HSBC	Mike Constantinou
	Emma Frew
IG Index	Andrew Bole
	Bjorn Model
Investec	Bharat Thakker
	Alex Cox
Northern Rock	Fraser McNeill
Pershing	John Phillips
Shore Capital	Michael Van Messel
SMBCE	Toshio Mano
Standard Chartered	Rajit Punshi
	Mark Willis

FSA

Christine Brentani (Chair)	Operational Risk Policy
Andrew Sheen	Operational Risk Policy
Giles Ward	Operational Risk Policy
Anna Jernova	Operational Risk Policy
Liz Meneghello	Operational Risk Policy
Philip Umande	Risk Frameworks & Capital Unit (PRD)
Brian Thornhill	Asset Managers & Advisers (RFD)

4. The Use Test

Introduction

4.1 This paper is one of a series drafted by the FSA to assist firms and supervisors in understanding, assessing and enhancing the adequacy and effectiveness of frameworks introduced to implement the standardised approach (TSA) to operational risk. While this paper deals with issues related to the 'use' test it is recognised that the components of a TSA framework cannot be viewed in isolation and should be reviewed and assessed as a package of closely interwoven elements. As such, a firm that can demonstrate its framework is fully embedded but has weaknesses in other TSA elements, is unlikely to have an acceptable TSA framework. In addition, weaknesses in one area could make it impossible for a firm to implement a successful element elsewhere. For example, a firm with poor reporting and management information is unlikely to be able to demonstrate effective 'use'. Only when the individual TSA elements have been implemented together in a robust, effective and comprehensive manner is there likely to be an effective framework. The quality of implementation is an important consideration in any assessment of an operational risk framework.

4.2 It is a requirement of the Capital Requirements Directive (CRD) that Advanced Measurement Approach (AMA) and TSA firms' internal operational risk assessment or measurement systems are closely integrated into their risk management processes (through the Use Test). However, the Use Test for operational risk is not elaborated in the CRD to the same degree as the IRB[1] Use Test and this has led to uncertainty about what needs to be done. As a result, both CEBS[2] and the FSA have published a number of papers and guidance to assist both supervisors and industry. However, to date, these have been aimed primarily at AMA firms.

4.3 Feedback from industry indicated that applying the Use Test to TSA firms was distinct from AMA firms. As a result, this paper has been produced to provide guidance on how to apply the Use Test to TSA firms. In drafting this paper, we have used the term 'Use Test' to refer to the requirement for the operational risk framework to be closely integrated into a firm's risk management processes. This process is sometimes referred to as 'embedding' or 'experience' and in some instances these terms better capture the essence of the requirement.

4.4 This paper has been drafted for the benefit of supervisors of TSA firms but will also be made available on our website. The paper outlines key features of TSA that are of interest, with observations and suggestions to support existing handbook guidance and rules. We use Handbook guidance and other supporting materials to supplement the principles and rules where we think it may help firms to decide what procedures they might wish to consider adopting as good practice. Guidance, and the variety of materials we publish to support the rules and Handbook guidance, is not binding on those to whom our rules apply. Such materials are intended to illustrate ways (but not the only ways) in which firms can comply with the relevant rules.

1 IRB: Internal-rating based approach to credit risk.
2 CEBS: Committee of European Banking Supervisors.

Expert group

4.5 A group comprising operational risk experts from a number of BIA and TSA firms was formed and the membership is shown in Annex A. The group had a number of meetings during which the experts gave presentations on the Use Test and discussed the most relevant issues. We are extremely grateful for the quality of debate and discussion in the expert group and for the contribution of participants to the work of the group. The views expressed in this paper draw on the valuable input of this group.

Rules and guidance

4.6 Firms using the TSA or AMA methodologies are required to comply with the Use Test, which requires that:

- For TSA firms: 'The Operational Risk assessment system must be closely integrated into the risk management processes of the credit institution. Its output must be an integral part of the processes of monitoring and controlling the credit institution's Operational Risk profile'.

  BIPRU 6.4.1 R (4) CRD, Annex X, Part 2, Paragraph 12 (b)

- For AMA firms: 'The credit institution's internal Operational Risk measurement system shall be closely integrated into its day-to-day risk management process'.

  BIPRU 6.5.6 R (2) CRD, Annex X, Part 3, Paragraph 2

  The key element of the Use Test is therefore that the risk assessment system is closely integrated into the firms risk management processes. However, to understand what the Use Test means for TSA firms, it is useful to look at how the TSA requirement differs from the AMA requirement; the key differences[3] are:

  - Measurement vs. assessment – because TSA firms do not have to produce a quantitative (modelled) capital estimate, the TSA Use Test refers to 'assessment' as opposed to 'measurement'. However, this does not preclude TSA quantitative measurement and clearly 'measurement' would constitute an 'assessment' – but not vice versa.

  - 'Its output must be… integral...to monitoring and controlling the…risk profile': the second sentence in the TSA Use Test definition is not included in the AMA requirement. It emphasises that, while a TSA firm's risk assessment system may not produce a quantitative figure as an output, it would, however, produce some output. The output, whatever its form, must be used for and form part of the monitoring and controlling of the firm's risk profile – so the output must be actionable. For example, the output from a risk and control self assessment (RCSA) might be used as a basis for decision making.

3 A third difference is that the AMA Use Test must be integrated into the 'day-to-day management' but no such provision is included in the TSA requirement. However, this does not mean a TSA firm's Use Test should not or need not be integrated on a day to day basis; its temporal integration should be appropriate.

4.7 Proportionality: In addition, while there is no principle of proportionality in relation to the Use Test for AMA firms, for TSA firms:

- 'A firm must comply with the criteria in BIPRU 6.4.1 R [which includes the Use Test] having regard to the size and scale of its activities and to the principle of proportionality.'

  BIPRU 6.4.2 (BCD Annex X, Part 2 point 12 (part))

4.8 This means that compliance with the Use Test will not only depend on 'size and scale' but also any other relevant factors, such as the nature or complexity of the firm (the Principle of Proportionality).

4.9 However, some consideration needs to be taken in applying the principle of proportionality to the Use Test. The proportionality principle in BIPRU 6.4.2 applies to all the qualitative requirements in BIPRU 6.4.1 – such as the requirement to measure, monitor, identify and report – and, in our view, adjustment for the nature, scale, complexity etc. may be more readily applicable to these other obligations than the Use Test. Because it may be easier to integrate a risk assessment system and 'monitor and control its risk profile' in a small, less complex firm, there is no obvious reason why the degree of integration and the monitoring and control should be any less or any more onerous due to the size or complexity of the firm.

4.10 As a benchmark, and due to the integration requirement on both TSA and AMA firms, a TSA firm of a similar nature, scale and complexity to another firm that has an AMA waiver would benefit from applying the Use Test to the same degree. If such a firm were to seek to move from TSA to AMA standards they would only need to meet the requirements that result from the additional modelling and risk measurement components.

Guidance

4.11 Most Use Test guidance has been aimed at AMA firms with an expectation that read across to TSA firms could be easily made. Nonetheless, feedback from the expert groups and our supervisory activities is that TSA firms require specific guidance on how to apply the Use Test. However, where possible, this paper follows the AMA guidance to ensure continuity between the regimes and emphasise that the lessons learnt from AMA can be relevant to TSA firms.

4.12 The primary guidance on the Use Test is provided in CEBS *Guidelines on the implementation, validation and assessment of Advanced Measurement (AMA) and Internal Ratings Based (IRB) Approaches* (see guideline GL10), which outlines four broad principles by which firms could evidence meeting the Use Test. We think these principles are equally applicable to and helpful for TSA firms (substituting 'risk assessment' for 'AMA'), and are:

- the risk assessment system should not be limited to regulatory purposes;
- the risk assessment system should continually evolve as the institution develops experience of risk management techniques and solutions;

- the operational risk framework brings together the assessment and management of operational risk within an organisation; and
- the use of an operational risk assessment system should provide tangible benefits to the organisation.

4.13 We have also published three papers on the Use Test:

- *The Use Test* July 2005.[4]
- *Operational Risk Management Practices* October 2007.[5]
- *Operational Risk: The 'Use Test'* June 2008 (FSA Use Test Paper).[6]

4.14 These were principally aimed at AMA firms and this paper builds on the framework in our Use Test paper to explain the key characteristics and observations that apply to TSA firms.

4.15 Annex B sets out the rules and guidance referred to above in more detail.

Key characteristics and observations

4.16 This next section outlines the observations drawn from the expert groups on the Use Test and develops a framework that could be used to apply to TSA firms in meeting their Use Test requirements. The basic framework is outlined before more detailed discussion of how it may apply to firms.

4.17 The general approach to the Use Test for TSA firms outlined in BIPRU 6.4.1 comprises four main components:

> 'The operational [a] risk assessment system must be [b] closely integrated into the firm's risk management processes. Its output must be an integral part of the process of [c] monitoring and controlling the firm's [d] operational risk profile.'

4.18 So the process of meeting the Use Test can be divided into a three stage process:

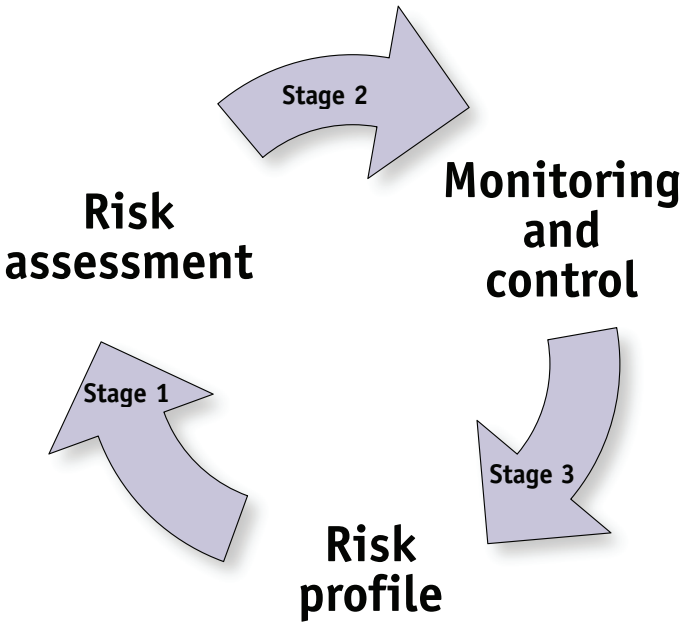
- Stage 1: Risk profile → Risk assessment: The firm's operational risk profile should be evaluated by its risk assessment system.
- Stage 2: Risk assessment → Monitoring and control: the output of the risk assessment system should feed into the monitoring and control of the firm's operational risk.
- Stage 3: Monitoring and control → Risk profile: the resulting monitoring and control should result in an improved risk profile within the firm's risk appetite or tolerance; the actions taken should genuinely and demonstrably enhance risk profile and not be merely superficial.

4.19 Integration: The overarching requirement is that the risk assessment system be closely integrated with risk-management process.

4 www.fsa.gov.uk/pubs/international/orsg_use_test.pdf
5 www.fsa.gov.uk/pubs/international/or_practices_oct07.pdf
6 www.fsa.gov.uk/pubs/international/orsg_8sep08.pdf

4.20 The process illustrated in Figure 1 aims to highlight a number of issues that arose in the expert group. Firstly, whereas the AMA Use Test is focused on a single output – the measurement of regulatory risk capital – TSA firms do not have a single unifying output, but rather use a variety of risk assessment outputs to manage their risk profile.

Figure 1: The Use Test



4.21 Secondly, there is a concern that some firms perceive the Use Test as a linear process leading from inputs to an output that only needs be repeated once or intermittently. The cycle in the figure is intended to emphasise that the Use Test is an ongoing process of continuous monitoring, management and improvement.

4.22 A key concern of industry and supervisors is not just how to apply the Use Test, but also what evidence can be provided to demonstrate that it is being met. This next section expands on the framework above by explaining what inputs, outputs and actions firms may find helpful to fulfil the Use Test while the boxes alongside the text provide examples of evidence firms might provide to supervisors to assess whether a firm meets the Use Test. This evidence is intended to be non-prescriptive and non-exhaustive.

Stage 1: Risk profile → Risk assessment

4.23 The first stage of the Use Test cycle is the firm's assessment of its risk profile. This typically involves the gathering of risk profile metrics – the inputs. The four components used by AMA firms to measure risk may be a good starting point, but TSA firms are not required to use all the four components and may use a wider variety of inputs, as shown below. Practices vary among TSA firms though; some place greater reliance on inputs that are quantitative in nature while others rely on a more qualitative assessment system. The next section outlines the inputs that a firm might use to assess its risk profile.

i) **Internal loss data and incidents:** Gathering internal loss data is a key element by which firms can assess their risk profile (and monitor and control of that risk profile). Frequency and severity of events can be used to assess risk profile, while reviews of events can be used to monitor the effectiveness of the risk-assessment system and devise appropriate controls through. For example, root-cause analysis and remedial action, such as risk mitigation plans. Internal data may also complement other elements to the risk assessment process – for example, by informing scenario analysis, scaling external data and in risk and control self assessments.

ii) **Scenarios:** Scenarios are a useful means by which firms can assess their risk profile and inform the monitoring and management of operational risks. Scenarios may also provide an assessment output in a form that is tractable and engages management and can therefore be helpful in ensuring that the output is actionable.

iii) **External loss data and events:** External data can help firms assess their risk profile. However, for some firms, particularly smaller firms, the cost, applicability and scaling of external data may decrease its utility, particularly if they have a non-quantitative approach to risk assessment. Nonetheless, external events may be useful for engaging senior management on the impact of particular risks, as well as complementing other parts of the risk-assessment process, such as scenarios.

iv) **Business Environment and Internal Control Factors (BEICFs):** BEICFs include changes to laws and regulations, changes to internal rules, policies and procedures, new business, products and processes. How this data is processed, filtered and ultimately used may be useful in demonstrating how a firm assesses its risk profile. In some cases, the BEICFs may be an output that can feed into a firm's risk monitoring process. (KRIs, RCSA and audit reports can be considered part of the BEICF element but are considered separately in this document).

v) **Key Risk Indicators (KRIs):** KRIs can include gathering data on such indicators as occurrence of errors, system unavailability, staff turnover, outstanding training, etc. KRI trends and ratings may also be useful tools for assessing the firm's risk profile. More significantly, KRIs straddle the area between risk assessment and control and monitoring. Since they are an inherently actionable output they may be very useful in demonstrating that the outputs of the risk assessment system are used.

Stage 1: Risk profile → Risk assessment

Evidence could include:

- manner and frequency with which the risk assessment of the risk profile is used within the bank;
- evaluation and validation of the quality of the inputs and risk assessment;
- the choice of appropriate range and types of inputs to assess the risk profile; and
- established mechanisms to evaluate the quality of risk profile inputs – for example, BEICFs are compared to actual loss data.

vi) Risk and Control Self-Assessments (RCSA): Many firms conduct some sort of RCSA. Assessment through RCSAs of a firm's operations and activities to identify where risks lie may be an important means of identifying risks. It is important that this input is integrated into the firm's risk-management process.

vii) Audit reports: Audit reports and in particular audits of operation risk may be useful inputs in assessing a firm's operational risk profile.

Stage 2: Risk assessment → Management, monitoring and control

4.24 The second stage of the Use Test cycle is to incorporate the outputs of the risk-assessment process in the monitoring and control process. The TSA risk assessment system will typically be multi-faceted and produce a variety of outputs that feed into the management monitoring and control of risk. Some may be quantifiable outputs, such as economic capital, while others produce qualitative outputs, such as heat maps. Most risk-assessment systems will comprise a combination of both.

4.25 It is important to appreciate the outcome that the risk-assessment system is attempting to achieve – namely an assessment of the risks that the entity faces as a result of which the firm can understand what its risk profile is and identify appropriate responses in terms of monitoring and control.

4.26 Two recent reports, *A review of corporate governance in UK banks and other financial industry entities*[7] (the Walker Review) and *The Turner Review: A regulatory response to the global banking crisis*[8] both have implications for ensuring adequate linkages between risk assessment and risk governance, monitoring and control. These reviews highlighted two key themes:

- **Culture:** The Walker Review observed that many of the deficiencies in board risk management 'related much more to patterns of behaviour than to organisation' and recommended an improved greater culture of 'challenge'.
- **Board attention to risk:** The Walker Review also observed that, 'board-level engagement in the high-level risk process should be materially increased with particular attention to the monitoring of risk and discussion leading to decisions on the entity's risk appetite and tolerance'.

4.27 The significant read across to the Use Test of both of these issues is highlighted below. The reports may also be useful in promoting the need to implement the Use Test to senior management.

4.28 The elements linking risk assessment and the management, monitoring and controls process are expanded on below, with potential evidence that may be adduced in the box alongside.

i) **Management reporting:** Management reporting of the operational risk assessment is useful in demonstrating the link between risk assessment and management, monitoring and controlling risks, as highlighted by the Turner and Walker reports. However, reporting alone is unlikely to demonstrate use

7 www.hm-treasury.gov.uk/d/walker_review_consultation_160709.pdf
8 www.fsa.gov.uk/pubs/other/turner_review.pdf

– firms may consider how the reporting can be and is used, and may focus on clarity, quality and accuracy. There is some debate about whether reports should be detailed or pithy. A case for either can be made, but in both cases firms may consider whether the format is appropriate for management to understand, challenge and act on. To facilitate this, steps to educate senior management may be useful. Documentation, such as minutes, may help demonstrate whether management understands, has challenged and/or has acted on (or chosen not to act on) management reports.

Stage 2: Risk assessment → Management, monitoring and control

Evidence could include:

- demonstration that the board understands the risk assessment system through training briefings, minutes, etc;
- documentation of escalation and resultant remedial processes or actions;
- demonstrable monitoring of trends in risk assessment inputs and outputs;
- that senior management require and analyse a proper risk assessment for new products and significant investments;
- demonstrable buy-in from the governance committees and business units;
- a risk appetite statement showing how the appetite or tolerance is set, its form, and the escalation and remedial processes;
- documentation showing senior management has considered action on its receipt of information from the risk assessment system;
- remuneration is affected in a transparent manner by actual loss experience and/or the evolution of risk indicators and scores;
- operational Risk capital calculations are allocated to business units;
- capital outputs are used to generate risk adjusted performance measures, eg RAROC;
- management information flows from business units to the board and vice versa.

ii) **Governance:** An appropriate governance structure may be useful for showing how the risk assessment process feeds into risk management, monitoring and control. But again, as highlighted by the Walker and Turner reports, it is important to consider not simply the governance structure but how it operates. Firms should ensure that their risk-assessment outputs feed into and are integrated into the firm's governance arrangements, such as the relevant committees, and that this structure results in the appropriate actions being taken to monitor and control those risks. Showing that the relevant committees, management and the board have understood the outputs, challenged if necessary and acted on where appropriate is crucial. Clear documentation may help in this case.

iii) **Risk appetite:** The Walker Report highlighted that a firm's risk appetite and risk appetite statement may be an important link between the assessment of risk and the decision about what actions it takes in light of any changes in this assessment. There are a wide range of interpretations of operational risk appetite

and risk tolerance.[9] Whichever approach is adopted, demonstrating its influence on risk management can be critical. For example, explaining and documenting how risk appetite is set and its form (whether a threshold, warning line or limit), how it relates to trigger points for risk ratings and the escalation procedure where appetite is breached, can be useful in demonstrating the links between risk assessment and risk management and control.

iv) **Performance and incentives:** The alignment of incentives and the performance measures with the firm's risk appetite may help create a culture of accountability that rewards success and rectifies mistakes in the risk management process. This may be an element in demonstrating the Use Test, and complements the Walker and Turner observations that the culture and way in which individuals operate within a risk management structures are at least as important as the structure its self.

v) **Capital calculations:** All firms produce capital calculations as a result of their risk assessment – typically an economic capital and a Pillar 2 capital calculation within the ICAAP. These tangible outputs can show that the risk assessment is being conducted. It may be equally important to show where the output is used to monitor and control operational risk. For example, it may be used as a basis for allocating capital to products, business lines, business units, legal entities and geographical locations or performance appraisals may be dependent on this output. The BIS paper *Principles for home-host supervisory cooperation and allocation mechanisms in the context of AMA*[10] contains a number of useful principles on the allocation of capital.

vi) **Not limited to regulatory purposes – Commercial rationale**: The first principle of the GL10 paper is that the purpose of the risk assessment is not limited to regulatory purposes. Where the operational risk assessment process is also used – for example, to inform business decisions or in product development – this can be a useful means of ensuring that senior management are aware of and involved in the operational risk assessment process.

Stage 3. Management, monitoring and control → Risk profile

4.29 One of the most challenging areas is closing the loop between the actions taken to manage, monitor and control risk and assessing their effect on the firms risk profile. This stage ensures that the Use Test process is evaluable, effective and addresses the second GL10 principle, namely that 'The risk assessment system should continually evolve as the institution develops experience of risk management techniques and solutions'. Some regulators refer to the Use Test as the 'use and experience test' or simply the 'experience test' to emphasis this. Implementing Stages 1 and 2 may provide one off evidence of use. The third stage of evaluating outcomes can ensure that the Use Test is developed as a meaningful and dynamic process.

4.30 How to implement and demonstrate this link is challenging. Firms may need to reflect on how their risk assessment system can link changes in management

9 See www.fsa.gov.uk/pubs/international/ora_4apr07.pdf for a discussion of this issue.
10 See www.bis.org/publ/bcbs135.pdf?noframes=1

monitoring and the control of risks with changes in risk profile. This third stage of the Use Test could be met by the following:

i) **Historical documentation**: Historical documentation of past risk assessments and changes to risk monitoring, management and control may be critical to making this link. With some forms of monitoring and risk assessment, trends in the risk profile resulting from changes in the risk management, monitoring and control may provide useful evidence.

ii) **Event studies**: Firms may want to analyse and document particular events that have resulted in changes to management, monitoring and control and whether these have resulted in changes to risk profile.

iii) **Audits**: Internal and external audits may be useful for demonstrating the effects of management monitoring and control on a firm's risk profile.

iv) **Supervisory review process**: ARROW, ICAAP and Supervisory Review and Evaluation Process (SREP) progress may also be a means of proving the evolution of the firms risk assessment system – for example, by showing how particular identified risks have been controlled and monitored.

Stage 3: Management, monitoring and control → Risk profile

Evidence may include:

- how the institution ensures that the nature and balance of inputs into the risk assessment system are relevant and fully reflect the nature of the business;
- how the risk measurement system becomes more responsive and robust;
- how decisions for improving processes and controls are made;
- trends in risk assessment calculations and allocations and their links to monitoring and control actions;
- audits and the supervisory review process;
- the review and modification of the risk appetite or tolerance.

Challenges

4.31 The Use Test has proved to be difficult for firms, both AMA and TSA, to understand, implement and demonstrate to supervisors. Our understanding is that the Use Test has not received the attention it warrants from TSA firms and this paper is intended to address this shortfall. Particular challenges that we anticipate include the following:

i) **Evolution and experience**: Firms have often treated the Use Test as a one-off regulatory requirement – however, it should evolve as the institution gains experience with risk management techniques and solutions. This is likely to prove challenging to demonstrate to supervisors and ensuring that the relevant process are structured and documented could be crucial to demonstrating fulfilment of this criteria.

ii) **Ongoing:** Firms should be able to meet the Use Test on an ongoing basis. As a result, it may be important to consider changes in staff, structure, products, business practices etc, alongside the evolution of the Use Test.

iii) **Diversity:** There may be a greater variety of approaches to risk assessment by TSA firms than AMA firms for whom the capital measurement objective and more prescriptive rules may help ensure greater conformity. TSA firms by contrast use a variety of approaches with some taking a more qualitative and others a more quantitative approach. With more diverse practices it may be challenging for firms to understand what good practice is and more challenging for supervisors to resist imposing inappropriate one size fits all requirements on firms.

iv) **Proportionality:** There is potentially some uncertainty about the application of the proportionality principle to the Use Test for TSA firms. Paragraphs 3.07-10 discuss this area but differences may nonetheless arise between firms and supervisors on how this provision should be interpreted and applied.

Conclusion

4.32 To date, the majority of guidance on the Use Test has been aimed at AMA firms. However, TSA firms have experienced problems in understanding and implementing the Use Test and demonstrating to supervisors that they have done so. This paper aims to address these concerns.

4.33 By successfully implementing the Use Test firms should reap wider benefits; for example, some key supervisory concerns highlighted in the Turner and Walker reports may be addressed through the Use Test. In addition, successful implementation of the Use Test may help assist firms in meeting wider operational risk regulatory requirements as well as providing commercial benefits.

Expert group members

Industry

Bank of America	Richard Walsh
Bank of Montreal	Scott Matthews
Brewin Dolphin	Barry Howard
HSBC	Mike Constantinou
Mitsubishi UFJ Securities	Tim Vaughan
Nationwide	Lisa White
Nomura	Huw Howell
Standard Chartered	Rajit Punshi
Sumitomo Mitsui Banking Corporation Europe	Toshio Mano

FSA

Operational Risk Policy	Giles Ward (Chair)
Operational Risk Policy	Christine Brentani
Operational Risk Policy	Andrew Sheen
Operational Risk Policy	Anna Jernova
Operational Risk Policy	Liz Meneghello
Risk Frameworks & Capital Unit (PRD)	David Haberfield

Handbook rules and guidance

Source	Rule #	Text
BIPRU	6.4.1R(4)	A firm's operational risk assessment system must be closely integrated into the firm's risk management processes. Its output must be an integral part of the process of monitoring and controlling the firm's operational risk profile.
	6.4.2R	A firm must comply with the criteria in BIPRU 6.4.1R having regard to the size and scale of its activities and to the principle of proportionality.
SYSC	7.1.16R	A BIPRU firm must implement policies and processes to evaluate and manage the exposure to operational risk, including to low-frequency high severity events. Without prejudice to the definition of Operational Risk, BIPRU firms must articulate what constitutes operational risk for the purposes of those policies and procedures. [Note: annex V paragraph 12 of the Banking Consolidation Directive]

BCBS and CEBS guidelines

Source	Guidance #	Text
BIS Standards	Principle 3	Senior management should have responsibility for implementing the operational risk management framework approved by the board of directors. The framework should be consistently implemented throughout the whole banking organisation, and all levels of staff should understand their responsibilities with respect to operational risk management. Senior management should also have responsibility for developing policies, processes and procedures for managing operational risk in all of the bank's material products, activities, processes and systems.
	Principle 6	Banks should have policies, processes and procedures to control and/or mitigate material operational risks. Banks should periodically review their risk limitation and control strategies and should adjust their operational risk profile accordingly using appropriate strategies, in light of their overall risk appetite and profile.
	Principle 9	Supervisors should conduct, directly or indirectly, regular independent evaluation of a bank's policies, procedures and practices related to operational risks. Supervisors should ensure that there are appropriate mechanisms in place which allow them to remain apprised of developments at banks.

Source	Guidance #	Text
CEBS GL10 (AMA)	4.3.2	Annex X, Part 3, Paragraph 2 of the CRD requires the institution's internal operational risk measurement system to be closely integrated into its day-to-day risk management process ('Use Test'). The Use Test for the AMA is not elaborated in the CRD to the same extent as the Use Test for the IRB approach. The operational risk measurement system of an institution must have certain key elements. These elements must include the use of internal data, external data, scenario analysis, and factors reflecting the business environment and internal control systems (Annex X, Part 3, Paragraph 9 of the CRD). The following section establishes a framework of four broad principles which industry would have to consider, at a minimum, to satisfy the Use Test. For each principle, typical examples of actions that could be undertaken are also provided. The examples illustrate ways to comply with the principles, and are not meant to be either binding or exhaustive. The following section establishes a framework of four broad principles which industry would have to consider, at a minimum, in order to satisfy the Use Test. For each principle, typical examples of actions that could be undertaken are also provided. The examples illustrate ways to comply with the principles, and are not meant to be either binding or exhaustive.

Source	Guidance #	Text
		Principles and examples 1. The purpose and use of the AMA should not be limited to regulatory purposes. Evidence of meeting the Use Test could include, but is not limited to: • Providing evidence that the risk measurement system is used to manage operational risk exposures across different business lines within the organisation structure. • Providing evidence of how inputs, estimations, predictions, or outputs from the risk measurement system are used in the decision-making process, for example as an element in strategic and tactical decision-making. 2. The AMA should evolve as the institution gains experience with risk management techniques and solutions. Evidence of meeting the Use Test could include, but is not limited to: • Providing evidence of how the institution ensures that the nature and balance of inputs into the risk measurement system are relevant and fully reflect the nature of the business. • Providing evidence of how the risk measurement system becomes more responsive and robust. 3. The AMA should support and enhance the management of operational risk within the organisation. Evidence of meeting the Use Test could include, but is not limited to: • Providing evidence how decisions for improving processes and controls are made. • Providing evidence that operational management objectives and activities are communicated within the organisation. 4. The use of an AMA should provide benefits to the organisation in the management and control of operational risk. Evidence of meeting the Use Test could include, but is not limited to: • Providing evidence that senior management has considered action on its receipt of information from the risk measurement system. • Providing evidence that the AMA increases transparency, risk awareness, and operational risk management expertise, and creates incentives to improve the management of operational risk throughout the organisation.

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