Finalised guidance

Enhancing frameworks in the standardised approach to operational risk – policies and documentation

November 2011

5. OR policies and documentation

Introduction

5.1. This paper is the next of a series issued by the FSA to assist firms and supervisors in understanding, assessing and enhancing the adequacy and effectiveness of operational risk (OR) frameworks used by firms to implement the standardised approach (TSA) to OR[1]. Policies and documentation (from now on referred to as 'documentation', which includes policies and other document types) underpin all elements of TSA frameworks and in addition serve as a basis for a common language across all components[2], linking them together. Documentation is an integral part of risk controls and can also be viewed as a set of controls itself, addressing risks emanating from 'processes' – one of the main constituents of the OR definition.

5.2. Though we are not prescriptive in the approach to documentation that we ask firms to take, we expect them to be proportionate in the approach they adopt, taking account of their nature, scale and complexity, as it relates to the coverage and the level of details of their documentation.

5.3. The aim of this guidance is to assist supervisors in assessing and challenging firms' documentation and the way it is managed. It also aims to help OR functions at firms to meet TSA requirements for OR. While following the recommendations in this guidance would help make a firm compliant, they are good practice rather than the only way to comply. Although this paper is aimed primarily at TSA firms, the information provided may be of use to other firms and their supervisors. Specifically, the qualitative guidance may also be applicable to firms using the basic indicator approach (BIA) and, possibly, the advanced measurement approach (AMA).

[1] The previous papers (numbered 1 to 4) constitute the '*Enhancing frameworks in the standardised approach to operational risk*' guidance note (http://www.fsa.gov.uk/pubs/guidance/guidance11.pdf).
[2] Components described in the '*Enhancing frameworks in the standardised approach to operational risk*' guidance note

5.4. While this paper has been drafted for the benefit of supervisors of TSA firms we expect that risk management professionals in general will find it useful. The paper uses observations and guidance to support current Handbook guidance and rules. The FSA uses Handbook guidance and other materials to supplement the principles and rules where we think this will help firms to decide what actions they need to take to meet necessary standards. This guidance is not binding – rather it is intended to illustrate the various ways in which firms can comply with the relevant rules.

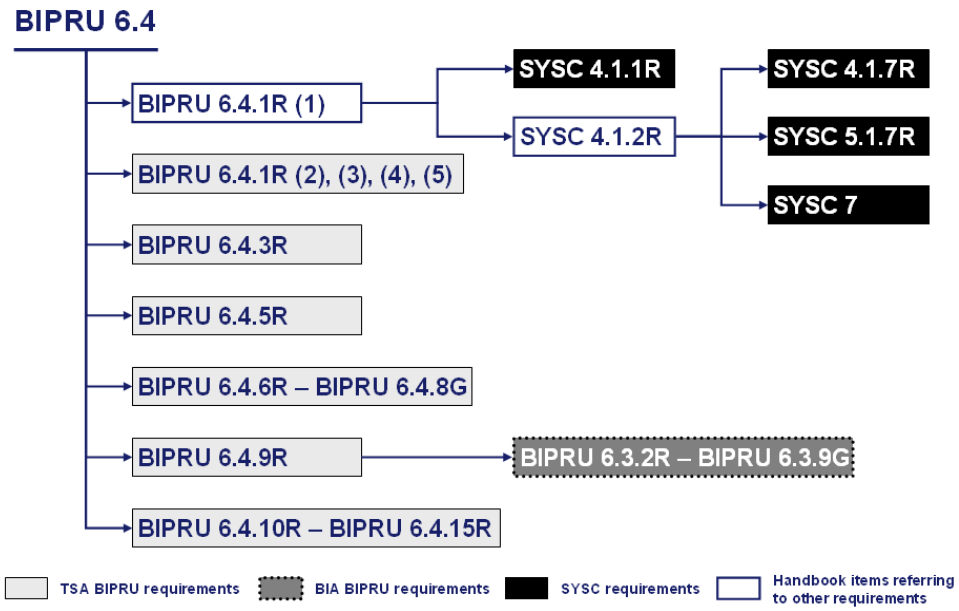
Involvement of stakeholders

5.5. The FSA invited representatives of a number of BIA and TSA firms to participate in an expert group on 'OR policies and documentation'. We held four meetings where a number of participants presented their approaches to documentation. Discussions at these expert group meetings, as well as information provided by the expert group members, form the basis of this document, though other sources of information have been used as well. We are grateful to the expert group contributors and thank them for the quality of debate.

Rules and guidance

5.6. TSA firms must ensure compliance with BIPRU 6.4 and should use this as a starting point for deciding what should be documented. Although this paper's primary focus is on OR, the associated Handbook requirements that TSA firms need to comply with stretch outside the OR domain and cover general risk management. As a result, the scope of this paper has been widened to include documentation outside the direct responsibility of OR functions, but which relates to operational risk – see section 'Scope'.

Figure 1: TSA Handbook requirements relevant to documentation[3]



[3] There are other documentation-related Handbook provisions which, while not referring to TSA, should still be taken into account by TSA firms, e.g. GENPRU 1.2.60R, GENPRU 1.2.61R, GENPRU 1.2.62G.

Additional guidance

5.7. The *Principles for the Sound Management of Operational Risk* issued by the Basel Committee on Banking Supervision (BCBS) in June 2011[4] could be used as a source of additional guidance.

5.8. The Core Principles for Effective Banking Supervision and the Core Principles Methodology (Basel Committee, October 2006), as well as the principles identified by the Committee in the second pillar of Basel II could also be considered when drafting operational risk documentation.

Scope

5.9. As evident from the Handbook structure (Figure 1), in order to meet TSA requirements for OR, firms should consider a wider set of issues including organisational requirements, general risk control, etc., areas which also require documentation. Therefore, the scope of this guidance paper is:

i) Documentation which is the responsibility of OR functions (e.g. operational risk management policy, operational risk management framework, operational risk reporting procedure, operational risk management procedures and guidance, etc.), from now on referred to as *operational risk documentation*.

ii) Any other documentation that supports the operational controls of a firm covering areas, typically owned by other functions or business units, which could be sources of OR (e.g. IT security policy, corporate governance framework, segregation of duties policy, job descriptions and responsibilities, risk management policy, etc.), from now on referred to as *operational risk-related documentation*.

5.10. It should be noted that the distinction between the operational risk documentation and the operational risk-related documentation is rather artificial, given that operational risk spans all of a firm's functional domains. It may not be practicable for firms to focus too much on defining this distinction. Instead, it may be worth ensuring that appreciation of the width of any firm's operational risk goes beyond just these departments, functions, policies and procedures.

5.11. The inclusion of operational risk-related documentation in the scope of this guidance does not imply that OR functions are now responsible for managing such documentation, but rather that OR functions, as part of their oversight responsibilities, could promote the good documentation practices suggested in this guidance in other functions and business units. Other documentation-related Handbook provisions not related to OR, e.g. GENPRU 1.2.60R, GENPRU 1.2.61R, GENPRU 1.2.62G, SYSC 2.2.1R, SYSC 2.2.2G, SYSC 2.2.3G, SYSC 3.2.10G (2), SYSC 3.2.20R, etc., could be referenced for this purpose.

5.12. We could give the following example of the interconnectedness of the OR domain with other areas across the firm both horizontally and vertically. A firm might have an OR management framework that is well-documented, regularly reviewed by internal audit and maintained by

[4] Designed to update and replace the 2003 'Sound Practices' paper.

the OR function. But if the firm does not have an adequate governance policy owned and approved by their Board, or, as a more specific example, documented IT Security procedures owned by the IT function, it is unlikely to meet TSA requirements. In this case the OR management framework will not be able to function without reliance on governance arrangements and could not serve to protect the firm against major loss events without proper controls in all supporting areas, including IT Security, documented in relevant procedures.

5.13. It is also necessary to clarify that the scope of this guidance (not the scope of ownership of OR functions) is limited to the documentation that supports the operation of a firm from a procedural perspective. It excludes documents that are final products, or outcomes, of processes and procedures, as illustrated by some arbitrary examples in Annex 1.

Documentation examples

5.14. The expert group members suggested possible examples of documents that define processes and/or controls required in order to comply with each of the specific sections of the Handbook. Possible documentation examples were mapped to the Handbook requirements and are listed in Annex 2 (for illustration only). Clearly, the examples have to cover both: the operational risk documentation and the operational risk-related documentation. Furthermore, one document could help meet more than one Handbook requirement.

Key features of documentation

5.15. Part of the objective of this guidance paper is to outline examples of key features of typical operational risk documentation and operational risk-related documentation. The contents of the table in Annex 2 can be sorted by 'documentation' examples so as to establish which part of the Handbook requirements each document could potentially support. This could give an indication of key features of some of those documents as illustrated by examples in Annex 3.

5.16. Firms may choose to adopt this or a similar approach when deciding which components or features to include in their documentation. Aligning their own list of documents against the specific TSA Handbook requirements as suggested in Annex 2 should give an indication of key features covered by each respective document. It could be good practice for firms to review the mapping of their documentation to the relevant SYSC and BIPRU sections of the Handbook on a periodic basis to ensure on-going compliance.

5.17. While using this (or similar approaches) it is important to note that a particular feature could be common to several operational risk documents, e.g. the 'organisation and responsibilities of risk management function' documentation requirement could form part of both the OR policy and the OR management framework documents. This may make sense where, using the same example, the policy document would just outline the requirement for an independent risk management function and its responsibilities and the framework document would further detail the function's set up, structure and responsibilities. In another example, a definition of OR may be present in several documents. In any case it is vital to ensure that common documentation components (e.g. definitions, descriptions, formulas, etc.) are and remain consistent across the documentation.

5.18. Where documents are related (e.g. OR management framework and risk appetite policy) their owners could ensure that the documents are aligned against each other so that they provide consistent views, measures and treatments of the same areas, processes or controls.

5.19. Documentation owners could require their delegates, tasked with documentation creation or updating, to cooperate with colleagues carrying out documentation-related work in other functions and/or business lines, to help establish and maintain alignment and consistency of related documentation. All documentation owners need to understand OR-related elements in their documentation and coordinate documentation maintenance accordingly. Communication of what each department/function/business line is doing in the area of documentation could be vital for this cooperation and coordination.

5.20. Good practice includes common firm-wide terms or references and a set of naming conventions, as well as using mutual references in documents. This helps achieve documentation consistency and improves documentation quality in general.

Documentation hierarchy

5.21. Given the wide array of documents that can be found in all but the smallest firms (see Annexes 2 and 3), it may be practicable to set up several broad levels of documentation, i.e. classify documents by the breadth of their scope and the level of detail. A firm could then set up a structure, or a hierarchy, which could help manage documentation more efficiently.

5.22. Possible documentation hierarchy levels could be:

- Level 1 – typically policies, strategy documents and/or any other documentation covering high-level principles governing activities and/or outlining courses of action thought to be prudent or tactically advantageous.

- Level 2 – control standards documents (a set of requirements for an activity/activities to deliver policy conformance), frameworks (overarching documents linking relevant activities to ensure their consistent execution), methodologies (sets of approaches to activities to deliver required outcomes), etc.

- Level 3 – the lowest level of the documentation hierarchy could include detailed specifications for the execution of activities, conforming to control standards and carried out in accordance with frameworks and methodologies.[5]

5.23. A firm's top-level documents (i.e. Level 1 documents) could be linked together into a firm-wide documentation map, showing the relationship between different domains. For example, an OR policy may branch off the overall enterprise risk policy. Taking the example further, a segregation of duties policy and a business continuity policy may branch off the OR Policy, where a firm decided that segregation of duties and business continuity fall under the remit of OR.

5.24. The FSA is not prescriptive when it comes to the number of hierarchy levels firms decide to introduce, or what type of documents should belong to which level, e.g. whether firms'

[5] See an example in Figure 2

policies should necessarily be at the highest level of the hierarchy. There may be cases, for example, when firms would position framework documents higher than policies.

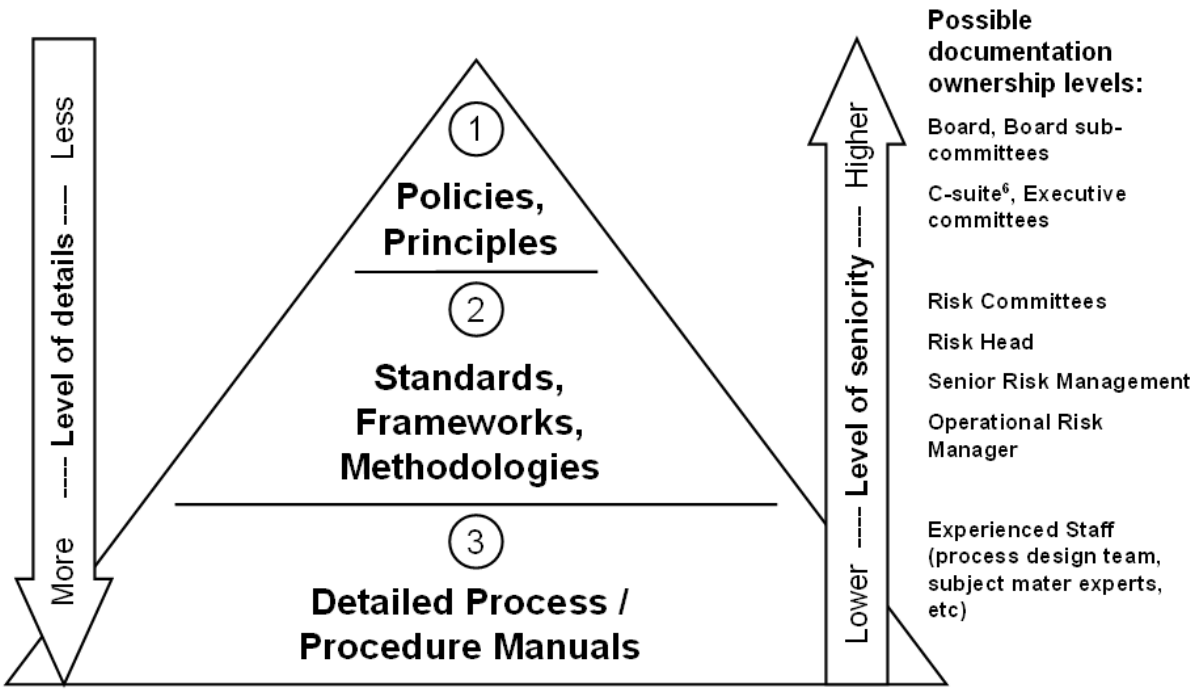
5.25. Instead, it is better for firms to define their own documentation hierarchies. It is also important to agree on documentation naming conventions that establish consistent definitions across a firm for all relevant terms including, but not limited to, 'policy', 'framework', 'methodology', 'manual', etc.

Documentation ownership

5.26. It is considered good practice for ownership to be clearly established for documentation at all levels of the hierarchy. It is suggested that ownership should be defined by approval. The creation, review and maintenance are generally delegated by owners to lower levels.

5.27. As an example, the Board of directors could approve policies developed by senior management. Senior management could be made responsible for implementing and maintaining policies throughout the organisation. However, the Board would be viewed as policy owners that delegate implementation and maintenance to senior management.

Figure 2: Example illustration of documentation hierarchy and ownership levels



5.28. It is not the intention of this guidance paper to prescribe which management level should own which level of a firm's documentation hierarchy. It is important that a firm organises its ownership structure consistently with its overall governance and that ownership is clearly

[6] CEO, CFO, CRO, COO, etc.

indicated in each document. Additionally, it is good practice for each document's owner to be recorded and tracked in a firm's documentation register (see 5.37).

5.29. It could be good practice to implement a set of controls around documentation ownership, e.g. ensuring that no one is able to change a document without the approval of its owner.

Documentation lifecycle

5.30. Any document has its own lifecycle – creation, review, updating, formal repeal and archiving or, a much less desired outcome, it becomes obsolete and forgotten about. An even worse scenario is when an obsolete or out-of-date document is consulted by a new and inexperienced member of staff to resolve an incident.

5.31. Firms could establish clear processes that define how often documentation is reviewed and updated, conditions for documentation repeal (e.g. approvals, only on replacement, etc.), and communications at all stages of a document's lifecycle.

5.32. A minimum review requirement could be set for all documentation across the firm, e.g. at least annually. However, firms may choose to refine the review requirement depending on the level of documentation hierarchy. Taking the example hierarchy laid out in Figure 2, a guideline for documentation reviews and updates could be:

- Level 1 documentation: reviews and, if necessary, updates may be driven by significant business, regulatory or organisational changes, but not less frequently than annually.
- Level 2 documentation: reviews and, if necessary, updates may be driven by business, regulatory or organisational changes, but not less frequently than annually.
- Level 3 documentation: reviews and, if necessary, updates may be driven by routine changes to products, systems, people and controls, but again there could be specific minimum review requirements for each document where it is practicable to do so.

5.33. Firms may define general review guidelines for each level, as given in the example above. Additionally or alternatively individual documentation owners may override the generic review requirements, or fine-tune specific review frequency requirements, for some or all of their documents.

5.34. In any case, documentation review requirements should be clear. It may be advantageous to specify each document's review requirement directly in the document. Additionally or alternatively each document's review requirements could be recoded and tracked in a firm's documentation register (see 5.37).

5.35. Documentation maintenance should also be made subject to monitoring (see 5.49).

5.36. Firms might also decide on requirements for documentation retention and archiving rules and procedures.

Documentation register

5.37. TSA firms typically have a large number of documents of different types, levels of details and scope. It could be practicable for TSA firms to maintain a central register of all their documentation (including policies).

5.38. Depending on the complexity of the firm's documentation structure and the volume of documentation, the register may be in the form of a simple spreadsheet, a stand-alone database, or even be integrated into the firm's enterprise risk management system.

5.39. The documentation register would contain specific details about each document. Examples of such details, or document attributes, could include some or all of the below:

- Document unique identifier
- Name
- Status (draft, final, archived, etc.)
- Document location (intranet page link, shared directory, etc.)
- Document scope (group-wide, or specific region, business line, function, department, etc.)
- Target audience
- Business criticality rating
- Reference to a corresponding regulatory rule or area (e.g. BIPRU 6.4, CASS, business line mapping, etc.)[7]
- Latest (or current) version number
- Description
- Type (policy, framework, methodology, etc.)
- Level of the documentation hierarchy
- Owner (approver)
- Author
- Creation date
- Last review date
- Next review date
- Repealed date
- Retention period requirement.

5.40. It may also be beneficial to record the name of the business process supported by a particular document. Typically this would be relevant for lower level documentation like processes and procedures, e.g. a 'settlement procedure' document for the 'EMEA equities cash trading' business process. Taking into account the criticality and the scope of the business process a document supports may help in applying a risk-based approach and the principle of proportionality to managing documentation. For example, documentation owners, or their delegates, could ask what risk the firm is exposed to by not having a particular document reviewed at least annually, or by delegating its creation to a less experienced member of staff.

[7] This may help in identifying all documents that would need to be reviewed following a specific rule change in the FSA Handbook, or a change in a specific area e.g. business line mapping, or CASS rules, etc.

5.41. The documentation register could be reviewed regularly with notifications sent to document owners when reviews are due; it could be updated once review confirmations are received from document owners.

5.42. The OR function does not necessarily need to be the owner of the firm's documentation register. Instead, it could promote this approach as good practice and treat it as an additional OR control that requires documentation register owners to ensure the register is kept up to date by the corresponding documents' owners.

5.43. In terms of the actual physical storage, firms could also consider creating a central library where at least core documentation (i.e. the level one documents – policies, principles, etc.) could be stored (soft and hard copies), which could facilitate their maintenance. Firms may decide that lower level documents such as procedures could be retained at desk level and need not be held centrally.

Identifying critical documentation

5.44. It is recommended that firms identify all the policies and documents that are absolutely critical to the operation of the firm, as opposed to documents playing more of a supplementary role. Such business critical documentation could be marked accordingly to ensure that it gets priority for reviews, updates and relevant communications. If practicable, firms may choose to additionally classify all their documentation by business criticality and record each document's criticality rating in the documentation register. Identifying critical documentation should not mean that all other documentation could be left mismanaged or forgotten about.

Subject matter expertise

5.45. Owners of documents should ensure that the right subject matter experts are involved in writing, reviewing and updating their documents. The higher the business criticality of the document – the more experienced its authors and/or reviewers should be.

Communication and training

5.46. Policies and documentation cannot operate in a vacuum. Dedicating efforts to creating and maintaining policies and documentation may not in itself be enough to meet TSA requirements. It is not enough when communicating a new policy rollout, or a framework update, etc. to just place the new or updated document in a shared directory or on an intranet page, hoping staff will adjust their day-to-day work routines accordingly.

5.47. Depending on the level of a document in the documentation hierarchy and/or its criticality to the business, further measures to ensure that it is able to support operation of corresponding controls effectively (and meet TSA requirements) may range from just issuing a communication memo to initiating a full-fledged communication programme followed by mandatory training to be undertaken by all the relevant staff. It could be recommended that all new joiners in a firm should attend training that covers relevant documentation.

5.48. As an additional communication measure, some firms practise covering new policies or updates of new policies at the corresponding risk management fora as part of promoting the importance of documentation in embedding the risk culture in their organisations.

Monitoring of documentation

5.49. Accurate documentation supports the smooth running of firms' processes. Firms should consider implementing measures to monitor at least their most important documents to ensure they are:

i) being complied with (typically for high level documents like policies); and

ii) reviewed at agreed intervals and upon relevant business changes, and updated when necessary.

5.50. Compliance with policies and similar documentation could be monitored through some standard OR management framework tools[8] like risk and control self-assessments (RCSA), key control indicators (KCI), etc.

5.51. The information in the documentation register may help in monitoring the status of documentation reviews. Firms could use this information to set KCI – one of the possible ways in which to monitor the status of their documentation reviews. Key risk indicators (KRI) could also be used.

5.52. Possible examples of KCI/KRI for documentation monitoring could include:

i) number of overdue documentation reviews;

ii) number of audit points that are either directly related, or could be traced back, to documentation;

iii) number of incidents (e.g. loss events, accidental gains, near misses) with improper/missing documentation, etc. as their root cause.

5.53. The outcomes of documentation monitoring could be presented as part of reporting packs at relevant risk management fora to help enforce documentation management requirements (like the regular review requirement), and made available to audit.

5.54. It could be argued that monitoring should primarily be focused on the controls themselves, rather than the documentation that describes those controls. However, controls monitoring is already assumed and is not the subject of this guidance paper. Monitoring of documentation could serve as a very useful proactive control capable of highlighting possible issues before they materialise as process failures.

Location of documentation

5.55. It is important to ensure that relevant staff can access the documents they need easily. Typically larger firms end up creating very complex and heterogeneous documentation directories on their intranet pages and/or shared folders. This may create a risk that members

[8] See the 'Operational Risk Identification, Measurement, Monitoring and Reporting' section of the 'Enhancing frameworks in the standardised approach to operational risk' guidance note (http://www.fsa.gov.uk/pubs/guidance/guidance11.pdf).

of staff are not able to locate and access the required procedure document when required, or resort to using a wrong version of the document.

5.56. To mitigate this risk firms, depending on their size and complexity, may choose implementing measures ranging from accurately recording and updating the location of each document in a simple documentation register, to rolling out a proper documentation management solution, possibly even integrated with an enterprise risk management system.

5.57. Irrespective of the approach chosen, documentation owners should ensure, possibly through delegation, that documentation maintenance includes updating the version numbers and location (e.g. in the documentation register and/or a documentation management system) of documents so that there is no ambiguity around the location of a document and its current version.

Other considerations

5.58. It is good practice to require documentation owners to ensure that their documents:

i) have clarity of purpose and content;

ii) are easy to understand by their audience;

iii) use consistent language (terminology, acronyms, etc.) across the firm;

iv) are of appropriate length (not too long and not too short); and

v) are of appropriate complexity.

5.59. To minimise issues around confidentiality, firms may consider developing and implementing a confidentiality classification system, defining controls for documentation access (e.g. who can read it or read and modify, etc.), applying confidentiality markings to documents and enforcing these measures through policies. It may be pragmatic not to apply this to documents of the lowest confidentiality rating. Each document's confidentiality rating could also be reflected in the firm's documentation register where firms choose to implement one. At the same time, however, it could be worth remembering that some operational risk and operational risk-related documentation might need to be available and easily accessible to all staff if firms are to have an appropriate risk culture.

5.60. Some firms use a dispensation approval process to enforce high-level documents like policies, e.g. specifying that there will be no dispensation from a policy without the approval of the corresponding level of management. Depending on the criticality of a document, the related dispensations can be time-limited and monitored by senior management and audit.

5.61. Additionally firms may choose to consider some of the standards published by the BSI[9]. The BSI supports the implementation of framework approaches to operational risk through its work and development of national and international standards and has developed a number of voluntary standards designed to assist firms and supervisors in the financial services sector

[9] British Standards Institute - the UK's National Standards Body

when implementing best practice and assessing the effectiveness of operational risk. These standards, both specifications and guidance, are designed to assist firms when managing operational and regulatory risk and form part of the risk control processes. The list of relevant standards is in Annex 4.

Conclusion

5.62. Documentation forms an integral part of managing OR and serves as a very important prerequisite to the effective operation of controls. Just as section BIPRU 6.4, containing TSA requirements for OR, refers to sections of the Handbook outside of the OR domain (e.g. SYSC), it may make sense for OR functions in firms not only to ensure the good management of documentation they are directly responsible for, but, as part of their usual oversight responsibilities, to also promote good documentation practices across their firms in general, e.g. through raising awareness and highlighting any concerns over documentation practices that they observe.

5.63. Overall, we are not prescriptive in the approach to documentation that we ask firms to take. However, to help satisfy TSA OR requirements, firms could demonstrate that they have all their important processes documented to the appropriate levels of detail and that their documentation is well-managed through the application of the principles of well-defined ownership, documentation hierarchy and lifecycle, as well as establishing relevant controls over documentation management.

5.64. Although harder to demonstrate, it is recommended that firms meet the requirement of what may be called a 'use test' for documentation, i.e. ensuring that documentation really works for the firm by being of good quality, regularly communicated, well-understood and actually used by the relevant staff as well as evolving with the firm's business and continuing to reflect the environment the firm operates in.

5.65. Firms should apply the principle of proportionality and adopt a risk-based approach when choosing to implement a particular way of managing documentation, e.g. how complex the documentation hierarchy and ownership structure should be, or whether to apply documentation management principles, like the regular reviews requirement, to all documentation across the firm, or to the documentation identified as business critical only, etc.

Annex 1: Some examples to clarify the scope of this guidance

Documentation examples that are in scope of this guidance	Out of scope of this guidance
Position limits setting policies; Position limits	Position limits breaches reports
Anti-money laundering (AML) and know-your-client (KYC) procedures	Client AML and KYC records
IT security manuals; IT security breach procedure	IT security breaches logs
IT application recovery procedures	List of IT application incidents
Procedure document, prescribing safekeeping of legal documents	Legal contracts
OR reporting process document	OR reports
Business continuity planning (BCP) testing procedures	Results of BCP testing

Annex 2: Possible documentation examples mapped to the Handbook requirements (for illustration purposes only)

Handbook Item	Handbook Item Summary	Documentation examples that may cover Handbook requirements could include, but are not limited to:
BIPRU 6.4.1R (2)	Clear responsibilities for OR assessment and management system	Firm-wide job descriptions and responsibilities document including OR function responsibilities and OR management responsibilities of staff other than the OR function Terms of Reference
	OR assessment and management system identifying exposures to OR and tracking relevant OR data, including material loss data	OR Management Framework Data/Information Management Policy Event (Loss Event/Incident) Management Policy Loss Database Reporting Procedure Risk Data/Information Collection Procedures Risk Profiling Process
	Well-documented assessment and management system for OR	Internal capital adequacy assessment process (ICAAP) Key Risk Indicators Procedure Manual OR Appetite / Tolerance Policy OR Management Framework OR Management Procedures and Guidance
BIPRU 6.4.1R (3)	Regular independent review of OR assessment and management system	OR Management Framework specifying requirements for regular reviews of adequacy and effectiveness of OR management policies and procedures OR Management Policy Audit Plan
BIPRU 6.4.1R (4)	Integration of OR assessment system into risk management processes	Overall Risk Management Framework specifying links to OR Management Framework overall Risk Management Policy making references to OR Management Policy
BIPRU 6.4.1R (5)	Procedures for taking action in response to OR reports information	Escalation Policy OR Appetite / Tolerance Policy OR Management Procedures and Guidance OR Reporting Procedure
	System of management reporting that provides OR reports	OR Reporting Procedure
BIPRU 6.4.3R	Division of activities into business lines	Business Lines Mapping Policy
BIPRU 6.4.5R	Calculating OR capital requirement for each business line	OR Capital Calculation Methodology
BIPRU 6.4.6R - 6.4.8G	TSA ORCR calculation rules	OR Capital Calculation Methodology
BIPRU 6.4.9R	Relevant indicator rule (TSA ORCR calculation)	OR Capital Calculation Methodology
BIPRU 6.3.2R - 6.3.9G	Relevant indicator definition (BIA ORCR calculation)	OR Capital Calculation Methodology
BIPRU 6.4.10R - 6.4.15G	Business line mapping rules	Business Lines Mapping Policy OR Capital Calculation Methodology

Handbook Item	Handbook Item Summary	Documentation examples that may cover Handbook requirements could include, but are not limited to:
SYSC 4.1.1R	Governance arrangements	Board & Risk Management Committee Structure Chart Delegated Authorities Policy Enterprise-wide risk management Policy Governance Policy Terms of Reference
	Internal control mechanisms (administrative and accounting procedures and safeguard arrangements for information processing systems)	Data Privacy Controls Manual Information Security Policy Segregation of Duties Policy Trading Book Policy
	Organisational structure	Job Descriptions & Responsibilities Maintenance Procedure for Organisation Charts
	Processes to identify, manage, monitor and report risks	OR Management Framework Risk Assessment Methodology Risk Management Policy
SYSC 4.1.7R	Business continuity policy	Business Continuity Procedures Business Continuity Policy Crisis Management process
SYSC 5.1.7R	Segregation of duties and prevention of conflicts of interest	Conflicts of Interest Policy Departmental Conflicts of Interest Procedures Segregation of Duties Policy
SYSC 7.1.2R	Risk management policies and procedures, procedures for risk assessment	Risk Management Framework Risk Management Policy Risk Management Procedures and Guidance Risk Control Self Assessment Process
	Risk tolerance	OR Tolerance Methodology
SYSC 7.1.3R	Arrangements, processes and mechanisms to manage the risk in light of level of risk tolerance	Detailed function- and business-specific OR and controls procedures Key Risk Indicators Procedure Manual OR Management Framework OR Management Policy Risk Appetite / Tolerance Policy OR Management Procedures and Guidance
SYSC 7.1.5R (1)	Monitoring adequacy and effectiveness of risk management policies and procedures	Assurance framework document OR Management Framework specifying requirements for regular reviews of adequacy and effectiveness of OR management policies and procedures
SYSC 7.1.5R (3)	Monitoring adequacy and effectiveness of measures to address deficiencies in risk management policies, procedures, arrangements, processes, mechanisms	OR Reporting Procedure OR Management Framework defining the three lines of defence model Risk Management Policy requiring independent audit of risk management frameworks, including OR Management Framework
SYSC 7.1.6R (1)	Establishing and maintaining risk management function that implements risk management policies/procedures	Corporate Governance Framework Governance Policy Risk Management Framework Risk Management Policy
		Organisation Charts

Handbook Item	Handbook Item Summary	Documentation examples that may cover Handbook requirements could include, but are not limited to:
SYSC 7.1.6R (2)	Establishing and maintaining risk management function that provides reports/advice to senior personnel	Corporate Governance Framework Governance Policy OR Management Framework OR Management Policy Organisation Charts Terms of Reference
SYSC 7.1.8G (1)	Documenting organisation and responsibilities of risk management function	Board & Risk Management Committee Structure Chart Corporate Governance Framework Governance Policy Job Descriptions & Responsibilities Organisation Charts Risk Management Policy Terms of Reference
	Documenting risk management framework setting out how risks are identified, measured, monitored and controlled	Detailed function- and business-specific OR and controls procedures Key Risk Indicators Procedure Manual Risk Appetite / Tolerance Policy OR Management Procedures and Guidance Risk Assessment Methodology Risk Control Self Assessment Process Various OR procedure documents (Internal / External Loss data collection, Risk and Control Assessments, Key Risk Indicators, etc.)
SYSC 7.1.8G (2)	Clarification of term 'risk management function'; it is not a controlled function itself, but part of the systems and controls function to set and control risk exposure	Job Descriptions & Responsibilities OR Management Framework OR Management Policy Organisation Charts Risk Management Policy
SYSC 7.1.16R	Defining OR	OR Management Framework including the definition of Operational Risk OR Management Policy including the definition of OR Terms of Reference
	Implementing policies and processes to evaluate and manage the exposure to OR	Detailed function- and business-specific OR and controls procedures Key Risk Indicators Procedure Manual Risk Control Self Assessment Process Scenario & Stress Testing Procedures

Annex 3: Possible key features of some typical OR documentation

Some Operational Risk documentation examples	Possible key features of documentation examples might include:	Relevant Handbook Item
Business Lines Mapping Policy	Business line mapping rules	BIPRU 6.4.10R - 6.4.15G
	Division of activities into business lines	BIPRU 6.4.5R
		BIPRU 6.4.3R
OR Appetite / Tolerance Policy	Arrangements, processes and mechanisms to manage the risk in light of level of risk tolerance; definitions of risk appetite / risk tolerance	SYSC 7.1.3R
	Risk management framework setting out how risks are identified, measured, monitored and controlled	SYSC 7.1.8G (1)
	Procedures for taking action in response to OR reports information	BIPRU 6.4.1R (5)
OR Appetite / Tolerance Procedures	Arrangements, processes and mechanisms to manage the risk in light of level of risk tolerance	SYSC 7.1.3R
	setting level of risk tolerance	SYSC 7.1.2R
OR Capital Calculation Methodology	Business line mapping rules	BIPRU 6.4.10R - 6.4.15G
	Calculation of OR capital requirement for each business line	BIPRU 6.4.5R
	Division of activities into business lines	BIPRU 6.4.3R
	Relevant indicator definition	BIPRU 6.3.2R - 6.3.9G
	Relevant indicator rule	BIPRU 6.4.9R
	TSA ORCR calculation rules	BIPRU 6.4.6R - 6.4.8G
OR Management Framework	Arrangements, processes and mechanisms to manage the risk in light of level of risk tolerance	SYSC 7.1.3R
	Clear responsibilities for OR assessment and management system	BIPRU 6.4.1R (2)
	Clarification of term 'risk management function'; it is not a controlled function itself, but part of the systems and controls function to set and control risk exposure	SYSC 7.1.8G (2)
	Arrangements concerning the segregation of duties and prevention of conflicts of interest	SYSC 5.1.7R
	Defining OR	SYSC 7.1.16R
	Organisation and responsibilities of risk management function	SYSC 7.1.8G (1)
	Establishing and maintaining risk management function that implements risk management policies/procedures	SYSC 7.1.6R (1)
	Establishing and maintaining risk management function that provides reports/advice to senior personnel	SYSC 7.1.6R (2)
	Integration of OR assessment system into risk management processes	BIPRU 6.4.1R (4)
	Monitoring adequacy and effectiveness of measures to address deficiencies in risk management policies, procedures, arrangements, processes, mechanisms	SYSC 7.1.5R (3)
	Monitoring adequacy and effectiveness of risk management policies and procedures	SYSC 7.1.5R (1)
	OR assessment and management system must be subject to regular independent review	BIPRU 6.4.1R (3)

Some Operational Risk documentation examples	Possible key features of documentation examples might include:	Relevant Handbook Item
	Procedures for taking action in response to Operational Risk reports information	BIPRU 6.4.1R (5)
	Processes to identify, manage, monitor and report risks	SYSC 4.1.1R
	Risk management policies and procedures, procedures for risk assessment	SYSC 7.1.2R
	TSA OR capital charge calculation rules	BIPRU 6.4.6R - 6.4.8G
OR Management Policy	Arrangements, processes and mechanisms to manage the risk in light of the level of risk tolerance	SYSC 7.1.3R
	Clear responsibilities for OR assessment and management system	BIPRU 6.4.1R (2)
	Clarification of term 'risk management function'; it is not a controlled function itself, but part of the systems and controls function to set and control risk exposure	SYSC 7.1.8G (2)
	Defining OR	SYSC 7.1.16R
	Organisation and responsibilities of risk management function	SYSC 7.1.8G (1)
	Establishing and maintaining risk management function that implements risk management policies/procedures	SYSC 7.1.6R (1)
	Establishing and maintaining risk management function that provides reports/advice to senior personnel	SYSC 7.1.6R (2)
	Governance arrangements	SYSC 4.1.1R
	Integration of OR assessment system into risk management processes	BIPRU 6.4.1R (4)
	OR assessment and management system must be subject to regular independent review	BIPRU 6.4.1R (3)
	Procedures for taking action in response to OR reports information	BIPRU 6.4.1R (5)

Annex 4: BSI operational risk standards and their mapping to the FSA Handbook

BS 10012: 2009 Data Protection (SYSC 4.1.1.R)

BS 25999-1:2006 Business Continuity Management. Code of Practice (SYSC 4.1.7R)

BS 25999-2:2007 Business Continuity Management. Specification (SYSC 4.1.7R)

BS 27000 Series: Information technology. Information security management (SYSC 4.1.1.R)

BS ISO 31000:2009 Risk Management. Principles and Guidelines (SYSC 7.1.2R)