27 July 2010

Compendium of Supplementary Guidelines on implementation issues of operational risk

A. INTRODUCTION

1. Given the young and evolutionary nature of operational risk as a risk discipline, one of the biggest challenges institutions face in the implementation of Directives 2006/48/EC and 2006/49/EC (hereafter Capital Requirements Directive, CRD) is the establishment of an operational risk framework which, on the one hand, is able to improve the way operational risks are identified, controlled and mitigated and, on the other hand, correctly reflects the level of operational risk institution is exposed to.

2. The information gathered and the experience gained within the EU supervisory community during the initial phase of the adoption of the new regulatory capital framework provide evidence that the quality of the operational risk management and measurement frameworks of institutions is dependent on their proper recognition and timely resolution of the issues that emerge through the phases of definition, establishment and maintenance of such frameworks.

3. In light of this, after publishing the Guidelines on the validation and assessment of the Advanced Measurement (AMA) and Internal Ratings Based (IRB) Approaches (GL10, April 2006)[1], CEBS has continued to work on issues arising from the implementation of the AMA, Standardised (TSA/ASA) and Basic Indicator (BIA) approaches for operational risk. The period after the publication of the GL10 has proved to be a good test of the principles stated in it and has pointed up areas requiring further clarification and supervisory guidance.

4. Consistently with GL10, this Compendium represents CEBS's current thinking and expectations and aims to promote a higher level of homogeneity and common understanding among competent authorities on several issues that have emerged from implementing operational risk frameworks.

5. Unlike other guidelines, the Compendium is not structured as comprehensive guidance but as a collection of individual guidance papers on particular operational risk implementation issues which will be enlarged and updated on

[1] CEBS Electronic Guidebook, pp. 110 – 273 http://www.c-ebs.org/getdoc/e59e3da6-aea8-43f0-b967-a12e34ff9ef2/2008-09-03-EGB2.aspx

an on-going basis. The focused guidelines are structured as semi-independent documents, allowing their stand-alone use (i.e. each with its own introduction, main body, etc.), but at the same time following an overarching approach and allowing their use in conjunction with other documents, thus contributing to the provision of CEBS's views on wider issues related to operational risk. Before being added to the Compendium the guidance papers are subject to a consultation period in line with the standard CEBS procedure.

6. The main purpose of the individual papers - drafted as guidance to supervisors, but also relevant to institutions - is to support the work of the national authorities in their assessment and review of the operational risk frameworks implemented by institutions. They will thereby help to create a level playing field and to foster the convergent application of the operational risk regulatory framework across the EU.

7. The considerations described in GL10, specifically those regarding the good faith principle (Paragraph 16) and the addressees/scope of application (Paragraphs from 22 to 29) also apply to the guidelines included in the Compendium. As such, bearing in mind the differences in the application of the new regulatory capital framework to the investment firms sector, these guidelines apply to both credit institutions and investment firms and use the term "institutions" to refer to them.

8. The topics are addressed once they become sufficiently relevant to industry practices and there is sufficient experience of them[2]. Depending on the type of topics, the guidelines refer to all institutions subject to the CRD's provisions or only to those institutions adopting a specific approach for calculating operational risk regulatory capital. In applying these guidelines, it is expected that national supervisory authorities will take the principle of proportionality (proportional to the nature, size, scale, and complexity of the institution) into account. Supervisors will also bear in mind that even smaller and less complex institutions that have chosen to apply for the use of the AMA for regulatory purposes have, by doing so, made the choice of complying with the minimum requirements and guidelines envisaged for the AMA.

9. The Compendium, published as part of CEBS's electronic guidebook, is structured into three sections:

   A. Introduction;

   B. Executive summary, which provides essential information on the topics, characteristics and objectives of each published document; and

[2] The chosen approach means that some topics, although deemed relevant in the context of an AMA framework, are not addressed until their level of development within the industry is deemed adequate (for instance, this currently applies, amongst others, to correlation, back-testing and benchmarking). Accordingly, principles and guidelines as expressed in the CRD and GL10 are for the time being considered sufficient to allow a flexible "evolution path" for such elements while respecting minimum supervisory standards. As more knowledge and experience is gained on them within the industry and supervisory authorities, these topics may be covered by CEBS to identify practices, develop a common supervisory view and deliver relevant implementation guidelines.

C. Individual guidance papers for supervisors, categorised according to the potential recipient (All institutions, BIA institutions, TSA/ASA institutions or AMA institutions).

B. EXECUTIVE SUMMARY OF THE PUBLISHED GUIDANCE PAPERS

The scope of operational risk and operational risk loss

10. The guidelines on "The scope of operational risk and operational risk loss" are intended to meet the well recognised need to have definitions of the scope of operational risk and of operational risk loss which are unambiguous and aligned with the prudential criteria so allowing institutions to achieve high standards in terms of capturing and representing their operational risk profile.

11. The paper aims to identify those industry practices for the categorisation of the "scope of operational risk" and the "scope of operational risk loss" which are considered to be consistent with achieving the stated purposes. The document is intended to be a helpful tool for national supervisors in examining, assessing and reviewing the operational risk frameworks developed and implemented by AMA and TSA (or ASA) institutions.

12. The BIA institutions are also encouraged to adopt such practices to make their operational risk frameworks more effective. Greater consistency by all institutions across different jurisdictions in terms of the scope of their operational risk and operational risk loss will contribute to a level playing field and to increase the consistency of the supervisory assessments and review processes.

The use test for AMA institutions

13. The guidelines on "The use test for AMA institutions" originate from the consideration that the use test requirement obliges an AMA institution to ensure that its operational risk measurement system is not solely used for calculating regulatory capital, but is also integrated into its day-to-day business process, embedded within the various entities of the group and used for risk management purposes on an on-going basis.

14. The objective of this paper is to build on the four use test principles outlined in the GL10 both by describing what should be considered to be an appropriate interpretation of the use test by an AMA institution and by identifying what the supervisory expectations are at the beginning and in a "business as usual" scenario for the AMA framework.

The allocation of the AMA capital

15. The guidelines on "The allocation the AMA capital" describe the range of allocation mechanisms which are currently used by major EU banking groups and outline the range of sound practices in terms of the assessment of allocation mechanisms and home-host related issues.

The Guidelines on operational risk mitigation techniques

1. The “Guidelines on operational risk mitigation techniques” have been built on the provisions of the CRD and the “Validation Guidelines” (GL10 of April 2006) that allow institutions that use the AMA to recognise the mitigating effect of insurance contracts and “Other Risk Transfer Mechanisms” (ORTM) in their AMA capital calculations, subject to certain conditions.

2. The main objective of the paper is to provide supervisory expectations for, and clarification of, specific aspects of insurance within the AMA, namely the eligibility of protection providers, the characteristics of eligible products and the haircuts for uncertainty of coverage.

3. The section on ORTM aims to balance the objective of offering sufficient flexibility for the development of these products with that of enhancing legal certainty regarding their use. The latter is achieved mainly by including an experience requirement for the use of ORTM within the AMA capital calculation. Moreover, supervisors are asked to not accept ORTM as risk mitigants under the AMA framework if these products are held or used for trading purposes, to be aware of the risks assumed by sellers of ORTM protection, and to consider prudential measures if a protection seller acquires significant risk exposures from other institutions.

C. PUBLISHED GUIDANCE PAPERS

LEVEL OF APPLICATION: ALL INSTITUTIONS

Guidelines on the scope of operational risk and operational risk loss

1. Introduction

1. Given the nature of operational risk, its correct classification for management and measurement, as well as supervisory, purposes requires an unambiguous definition of the "scope of operational risk" and appropriate criteria and procedures for identifying and capturing the risk wherever it may occur.

2. The CRD provides little guidance on how to distinguish operational risk from the range of other risks arising within business and support areas.

3. In particular, due to legal considerations, the CRD gives a positive definition of operational risk, the consequence being that it is silent with respect to strategic and reputational risks; risks that are explicitly excluded from the scope of operational risk in the Basel II Accord framework[3]. Despite such differences in the texts, the definition of operational risk within the CRD should be read consistently with that of the Basel Accord, meaning that reputational and strategic risks should be excluded from the scope of operational risk[4].

4. On the other hand the CRD explicitly includes legal risk - as the Basel II Accord does - in the definition of operational risk and this should include every type of legal event triggered by operational risk, regardless of how it is labelled (e.g. compliance risk, environmental risk[5]).

5. With reference to the interaction between operational risk and the other Pillar 1 risk types, for AMA institutions the CRD deals with the boundaries between operational risk and credit and market risks with different treatments for the two types of boundaries. While credit-related operational risk losses are excluded from the operational risk capital requirement (as long as they continue to be treated as credit risk for the purpose of calculating minimum regulatory capital), operational risk/market risk boundary events are included in the scope of operational risk for regulatory capital calculation. The CRD

---

[3] "Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework", November 2005.

[4] In the answer to question n. 210, published on February 26th, 2007 the CRDTG expressed the same view for strategic risk.

[5] The interaction between environmental risk and operational risk has been addressed by the CRDTG in its answer to question n. 18, published on April, 12th, 2006.

does not provide any guidance on how to distinguish between those boundary events which are to be included in the operational risk capital requirement and the "pure market risk" events which are to be excluded from the operational risk requirement.

6. A further aspect that can generate inconsistencies within and across jurisdictions is the interpretation of the "scope of operational risk loss". This issue, which is neither addressed in the CRD nor in the Basel Accord, refers to the types of events, whether or not having a quantifiable loss impact, to be included in the operational risk database and the purposes for which they are included (e.g. for management and/or for measurement purposes).

7. The inclusion or exclusion of some elements/items from the scope of operational risk loss can produce a very different loss outcome, even for institutions with the same risk profile, with unavoidable consequences in terms of management practices and economic and regulatory capital requirements, as well as unknown consequences for the quality and consistency of consortia loss data.

2. Objectives and content

8. The definition of "scope of operational risk" and "scope of operational risk loss" in ways which are unambiguous and consistent with prudential criteria are important in order to achieve high standards in terms of capturing and representing the institution's operational risk profile.

9. Each institution has its individual operational risk profile, and therefore needs to define its individual scope of operational risk and operational risk loss. Having that in mind, this paper aims to identify those industry practices for the categorization of the "scope of operational risk" and the "scope of operational risk loss" which are considered to achieve the stated purposes. These guidelines are meant to be a helpful tool for national supervisors in examining, assessing and reviewing the operational risk frameworks developed and implemented by AMA and TSA (or ASA) institutions.

10. By encouraging the BIA institutions also to adopt such practices, their operational risk frameworks are expected to generate greater effectiveness. Greater consistency amongst institutions in all jurisdictions in terms of their scope of operational risk and operational risk loss contributes to a level playing field and to increasing the consistency of supervisory assessments and review processes.

11. Section 3 covers the scope of operational risk and in particular the issues related to the interpretation of operational risk versus market and strategic risks. The issues related to the interpretation of operational risk versus credit and reputational risks are not included in this document.

12. Section 4 deals more specifically with the scope of operational risk loss. It aims to distinguish between those items arising from an operational risk event that should, at the minimum, be considered to be within the perimeter of the loss and those that can be excluded, provided that specific conditions on the nature of the items or on the environment surrounding them are fulfilled.

3. The “scope of operational risk”

13. This section outlines a number of criteria for assigning a specific event to one of the three risk categories, namely operational, market and strategic risks. Such criteria refer to the most frequently experienced cases and are supplemented with examples that illustrate how to comply with the criteria. The main sources taken into account in setting out the criteria and in choosing the examples are the information gathered from supervisory activities and the standards set by consortia for collecting operational risk data.

14. Such risk categorization is not meant to be comprehensive and is expected to be applied as a general guideline. Different classifications from those outlined in this paper can be envisaged. However, they should refer to individual and limited cases and should be well reasoned and properly documented.

3.1. Operational risk versus market risk

15. When distinguishing between operational risk (events or losses) and market risk (events or losses) the following criteria should be applied:

16. The events (and the related losses) described below should be included in the “scope of operational risk”:

    A. Events due to operational errors;

    B. Events due to failures in internal controls;

    C. Events due to wrong selection of the model, made outside a defined business process/formalised procedure and without a formalized, conscious risk-taking process; and

    D. Events due to wrong implementation of the model.

17. In all these cases, the whole amount of the loss incurred should be included in the “scope of operational risk loss”, unless the position is intentionally kept open after the operational risk event is recognized. In the latter case any portion of the loss due to adverse market conditions after the decision to keep the position open should be ascribed to market risk.

Table 1. Examples to be included in the “scope of operational risk”.

Due to operational errors: *i.* errors during the introduction or execution of orders; *ii.* errors in classification due to the software used by the front and middle office; *iii.* incorrect specification of deals in the term-sheet (errors related to the transaction amount, maturities and financial features);

iv. loss of data and/or misunderstanding of the data flow from the front to the middle and back offices; and

v. technical unavailability of access to the market, for instance making it impossible to close contracts.

Due to failures in internal controls:

vi. failures in properly executing a stop loss; and

vii. unauthorised market positions taken in excess of limits.

Due to model risk:

viii. selection of a model from a range of software without verifying its suitability for the financial instrument to be evaluated and for the current market conditions;

ix. errors in the in-house IT implementation of a selected model; and

x. incorrect mark-to-market valuations and VaR, due for instance to erroneous booking of a trade into the trading system. Market moves in a negative direction resulting in losses.

18. The events (and the related losses) described below should be excluded from the "scope of operational risk":

A. Events due to wrong selection of a model, made through a formalized corporate process where the pros and cons of the model itself are carefully weighed up.

Table 2. Examples to be excluded from the "scope of operational risk".

Due to model risk:

i. losses caused by a pricing model where the potential exposure to the model risk had been previously assessed, for instance by considering potential adjustments to "mark-to-market" transactions[6].

3.2. Operational risk versus strategic risk

19. When distinguishing between operational risk (events or losses) and strategic risk (events or losses), the following criteria should be applied.

[6] If instead potential adjustments to mark-to-market transactions were not included because of a failure/breach in the formalised process, the pertinent losses would fall under the "wrong implementation of the model" case (Paragraph 16 D) and hence they would be considered to be operational risk.

20. The events (and the related losses) described below should be included in the "scope of operational risk":

A. events triggered by legal settlements - e.g. judicial or out of court, arbitration, claims negotiations - or from the voluntary decision of the institution to bear the loss so as to avoid an upcoming legal risk;

B. events stemming from internal inadequacies, failures and errors or from external causes (e.g. external fraud, outsourcer failings) occurring when implementing a project[7].

21. In all these cases, the loss amounts to be recorded in the "scope of operational risk loss" are the specific provisions, costs of settlement[8] and any other expenses incurred as a result of the risk event (e.g. amounts paid to make good the damage, interest in arrears, legal fees and penalties).

Table 3. Examples to be included in the "scope of operational risk".

i. aggressive selling, stemming for instance from individual initiatives, with consequencial breaching of regulations, internal rules or ethical conduct;

ii. expenses stemming from law cases or from interpretations of the regulations which prove to be against industry practice;

iii. refunds (or discounts of future services) to customers caused by operational risk events, before the customers can lodge a complaint but, for example, after the institution has already been required to refund other customers for the same event;

iv. tax related failures/inadequate processes resulting in a loss (e.g. penalties, interest/late-payment charges); and

v. losses related to decisions made by a competent decision-maker but breaching regulations, internal rules or ethical conduct

22. The events (and the related losses) described below should be excluded from the "scope of operational risk":

A. losses incurred by the institution as a result of strategic/senior management decisions or business choices which do not breach any rules, regulations or ethical conduct, or which are not triggered by legal risk.

Table 4. Examples to be excluded from the "scope of operational risk".

[7] This view is consistent with the position of the CRDTG expressed in its answer to the question n. 216 published on April, 17th 2007.

[8] Costs of settlement should not be considered "timing losses" (see Paragraph 27 below).

i. losses related to flawed investment choices in mergers/acquisitions, organizational/management restructuring, etc;

ii. losses related to decisions made by the competent decision making body which are not compatible with the institution's risk tolerance level and deviate from its core business activities, in cases where these decisions did not breach any rules, regulations or ethical conduct;

iii. losses related to implemented but flawed strategies; and

iv. refunds to customers due to business opportunities, where no breach of rules, regulations or ethical conduct occurred.

4. The scope of "operational risk loss"

23. When an operational risk event occurs it may be revealed through different elements/items. Some of them will have a quantifiable impact, and hence be reflected in the financial statements of the institution, others do not affect the books of the institution and are detectable from other types of sources (e.g. managerial archives, incidents dataset).

24. Table 5 below illustrates the types of elements/items, whether or not having a quantifiable impact, which can result from an operational risk event. It should not be considered to be an exhaustive list:

Table 5. Type of elements/items that can result from an operational risk event

1. Direct charges to P&L and write-downs[9]
2. External costs incurred as a consequence of the event[10]
3. Specific provisions taken following the occurrence of a risk event
4. Pending losses[11]

[9] This item includes, inter alia, amounts payable on liabilities caused by an operational risk event and costs to repair or replace assets to their original condition prior to the operational risk event.

[10] External expenses include, among others, legal expenses directly related to the event and fees paid to advisors or suppliers.

[11] "Pending losses" can be defined as losses stemming from operational risk events with a definite and quantifiable impact, which are temporarily booked in transitory and/or suspense accounts and are not yet recognised in the P&L. For instance, the impact of some events (e.g. legal events, damage to physical assets) may be known and clearly identifiable before these events are recognised in the P&L through, say, the establishment of a specific reserve. Moreover the way this reserve is established (e.g. the

5. Timing losses[12]
6. Near-miss events[13]
7. Operational risk gain events[14]
8. Opportunity costs/lost revenues[15]

25. The 1st, 2nd and 3rd elements/items should be included in the scope of operational risk loss for the purpose of managing and/or assessing operational risk and, with reference to AMA institutions, also for calculating the minimum capital requirement for operational risk.

26. "Pending losses", where recognised to have a relevant impact, should be immediately included in the scope of operational risk loss for the purpose of calculating the capital requirement of AMA institutions; this can be done through the recognition of their actual amount in the loss data base or a pertinent scenario analysis. AMA institutions should include these losses in the scope of operational risk loss for management purposes too.

27. In general "timing losses" may be excluded from the scope of operational risk loss. However "timing losses" due to operational risk events that span two or more accounting periods and give raise to legal risks (e.g. "timing losses" due to some of the causes and examples mentioned in paragraph 20 A and table 3) should be included in the scope of operational risk loss for the purpose of calculating the capital requirement of AMA institutions. AMA institutions should include these losses in the scope of operational risk loss for management purposes too.

---

date of recognition) can vary between institutions or countries by reason of the adoption of different accounting regimes (e.g. IAS/IFRS or other regimes).

[12] "Timing losses" can be defined as the negative economic impacts booked in a fiscal period, due to events impacting the cash flows (lower cash in / higher cash out) of previous fiscal periods. Timing impacts typically relate to the occurrence of operational risk events that result in the temporary distortion of an institution's financial accounts (e.g. revenue overstatement, accounting errors and mark-to-market errors). While these events do not represent a true financial impact on the institution (net impact over time is zero), if the error continues across two or more accounting periods, it may represent a material misstatement of the institution's financial statements. This in turn may result in legal censure of the institution from its counterparts, customers, supervisory authorities, etc.

[13] As stated in GL10, Paragraph 524, the term "near-miss event" can be used to identify an operational risk event that does not lead to a loss.

[14] As stated in GL10, Paragraph 525, the term "operational risk gain event" can be used to identify an operational risk event that generates a gain.

[15] The term "opportunity costs/lost revenues" can be used to identify an operational risk event that prevents undetermined future business from being conducted (e.g. unbudgeted staff costs, forgone revenue, project costs related to improving processes).

28. The “near-miss events”, “operational risk gain events” and “opportunity costs/lost revenues” are also important for management purposes - in particular for promptly detecting failures/errors in processes or internal control systems - and, if appropriate, for the measurement purposes of AMA institutions. Institutions, consistently with their size, complexity, type of business are encouraged to develop criteria and procedures for collecting such items.

LEVEL OF APPLICATION: BIA INSTITUTIONS

None

LEVEL OF APPLICATION: TSA/ASA INSTITUTIONS

None

LEVEL OF APPLICATION: AMA INSTITUTIONS

Guidelines on the use test for AMA institutions

1. Introduction

1. In accordance with Annex X, Part 3, Section 1.1, paragraph 2 of the CRD, AMA institutions are required to meet the principle that: *"The credit institution's internal operational risk measurement system shall be closely integrated into its day-to-day risk management processes*."

2. This requirement, known as the "use test", obliges an AMA institution to ensure that its operational risk measurement system is not solely used for calculating regulatory capital, but is also integrated into its day-to-day business process, embedded within the various entities of the group and used for risk management purposes on an on-going basis.

3. The requirement expects the inputs and outputs of an AMA institution's operational risk measurement system to contribute to, and be an integral part of, its risk management processes, including at business line level.

4. By requiring the information incorporated in the model to be used in the decision making process and to support and improve operational risk management within the organisation, the requirement aims to promote the use of appropriate and consistent information that fully reflects the nature of the business and its risk profile. For these reasons, supervisors expect the AMA framework to be updated on a regular basis and to evolve as more experience in management and quantification of operational risk is gained.

5. The objective of this paper is to make progress on the four use test principles outlined in the GL10 by describing what should be considered to be an appropriate interpretation of the use test by an AMA institution and by identifying what the supervisory expectations are at the beginning and in a "business as usual" scenario of the AMA framework.

2. Use Test Assessment

6. Almost all EU supervisors have set minimum criteria for assessing compliance with the use test requirement. There are a number of factors which drive the supervisory process and assessment with many of these often being conducted against the four use test principles outlined in paragraph 496 of the GL10. Most supervisors have incorporated the four principles in national legislation, rules or assessment procedures. These principles are:

   - "*The purpose and use of the AMA should not be limited to regulatory purposes.*

   - *The AMA should evolve as the institution gains experience with risk management techniques and solutions.*

- *The AMA should support and enhance the management of operational risk within the organisation.*

- *The use of an AMA should provide benefits to the organisation in the management and control of operational risk.*"

7. The assessment of the use test requirement is an important part of the AMA validation process. The fulfilment of this requirement for an institution is a condition for the supervisory approval of the use of the AMA framework and needs to be assessed by the institution and validated by the competent authority. It also requires that - in the case of the use of an AMA at consolidated level - the parent's AMA framework has been rolled out to the subsidiaries and that the subsidiaries' operational risk and controls are incorporated in the group-wide AMA calculations.

8. The majority of the supervisors assess compliance with this requirement on a case-by-case basis taking into account all the surrounding factors and circumstances that include, but are not limited to, the institution's size, nature, structure and complexity, the regulatory expectations of current and future AMA standards and the current standard and evolution of the AMA process.

9. The supervisory expectations on the industry's answer to the use test requirement are strictly connected to the underlying timeframe: at the beginning of the implementation of the AMA or in a "business as usual" context.

10. In particular, in a "business as usual" context, the objective of the supervisory validation and review process of the use test requirement is to assess the following aspects:

    - the extent to which the operational risk framework is integrated into the business and is used in day-to-day risk management;

    - the use of the risk measurement system in the management of operational risk across different business lines within the organisational structure;

    - management processes and reporting; and

    - the use of model inputs and outputs, as well as the information received from the operational risk management process in the decision-making process and any associated remedial action.

11. Additional factors to be considered in a "business as usual" context are the overarching elements essential to well-implemented and functioning risk management processes, some of which are highlighted in paragraph 496 of GL10, namely:

    - the incentive that the operational risk framework provides for better risk management by increasing transparency, risk awareness and operational risk management expertise;

- the relationship between business strategy and operational risk management, including approval of new products, systems and processes;

- the use of model inputs and outputs in action plans, business continuity, internal audit working plans, budgeting decisions, mitigation plans and insurance management; and

- the definition of an appropriate operational risk tolerance.

12. For these purposes it can be useful to verify, on the one hand, the regular use of model inputs and output by business line management, the capacity to achieve operational risk objectives, and the use of the inputs/output in terms of capital assignment and, on the other hand, the role senior management plays in the strategic implementation phase and in the on-going monitoring activity of the overall operational risk framework.

13. The senior management is also expected to ensure the quality of the inputs and output of the model as well as whether there is sufficient buy-in from the business. Part of the senior management's work should aim especially to understand the operational risk management process and the relevant aspects of the model with reference to the business units. It is therefore imperative that senior management be regularly updated on the operational risk framework, including its strengths and weaknesses, or on adjustments to the model itself, and on any significant shifts in the institution's operational risk exposure without needless delay.

14. Home-host considerations affect the assessment process where AMA EU banking groups' applications are concerned. As the assessment and contribution of the host and home supervisors will be influenced by a number of factors, supervisors determine their assessment process on a case-by-case basis. Key factors influencing the assessment process include whether the supervisor is acting as home or host supervisor, the size and local impact of the subsidiaries, and the contribution of the subsidiary towards the AMA's design, implementation and process.

15. These factors shape the contribution of the home and host supervisors. In some cases much reliance is placed on the home supervisor's assessment process, for example the group model is usually audited by the home supervisor. In other cases a greater contribution will be required from the host supervisor, e.g. local implementation and the local use test requirement will often be reviewed by the host, or by the host together with the home supervisor. The size and impact of the subsidiary must be assessed from both the home and host perspectives. A subsidiary may require less consideration from the home supervisor if it contributes a negligible proportion to the group's size or income; yet the subsidiary may have a sizeable market share in the host's jurisdiction.

16. Supervisors expect advances in some aspects of the elements of operational risk management which are in their infancy at the beginning of the AMA framework process. Therefore, provided that these elements meet a minimum standard as a condition for granting approval to use the AMA itself, supervisors are in general prepared to offer some flexibility on the

development, implementation and advancement of some of the key elements.

17. In particular, the factors reflecting the business environment and internal control systems are those where some supervisors show this flexibility. However supervisors will encourage institutions to continuously advance and improve various areas of their operational risk framework, both those that meet current standards and those that do not. Supervisors expect the less developed areas to advance and improve significantly over the near term, and equally the developed areas are also expected to improve and advance as the quantification of operational risk management becomes more sophisticated.

18. Supervisors want the evolution of the operational risk framework to include more widespread use of the inputs and outputs of the framework. Furthermore, supervisors anticipate an improvement in the quality of inputs, which should in turn, enhance the modelling process and output. These will allow for enhanced use of model inputs and outputs for risk management purposes.

3. Final remarks

19. It is clear that meeting the use test requirement is a difficult task for institutions. Where institutions were asked to postpone their application, the use test requirement was often an area that needed further development. This resulted in supervisors having to inform institutions that greater effort was required from them to meet the use test requirement and subsequently having to conduct extra visits to the institution or reviews to assess its progress.

20. Supervisors have been successful in informing the industry that the use test requirement is a key driver for enhancing not only the quality of the modelling process but also of the management process. Supervisors want clear evidence that the modelling process supports and advances operational risk management in the institution; accordingly it should be adaptable to the changing dynamic of the institution so that it can continuously enable the institution's operational risk exposure to be determined.

21. As operational risk frameworks advance, the inputs should become more relevant and bespoke and therefore more reflective of the institution's business, strategy and exposure to risk. As the institution's operational risk framework becomes more sensitive and more closely aligned to its operational risk profile, the institution will be better equipped to provide evidence that it meets the use test requirement.

22. For the sake of completeness, it is worth mentioning that institutions adopting the Standardised Approaches (TSA or ASA) for operational risk capital purposes, in accordance with Annex X, Part 2, Section 4, paragraph 12(b) of the CRD, have to meet the principle that: "*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 process of monitoring and controlling the credit institution's operational risk profile*".

23. This provision poses the question how TSA or ASA institutions meet this principle, given that the difference between the use test requirement for AMA and TSA/ASA institutions is the element to be integrated into their risk management and businesses processes: the “measurement system” for AMA institutions and the “assessment system” for TSA/ASA institutions.

24. As more experience with the implementation of TSA/ASA requirements is gained within the industry and supervisory authorities, this topic may be taken up by the CEBS to identify the range of practices, develop a common supervisory view and produce a guidance paper to be included in the Compendium of Supplementary Guidelines.

Guidelines on the allocation of the AMA capital

1. Introduction

1. EU institutions usually adopt a group-wide model to calculate operational risk capital requirements at a consolidated level, taking into account internal and external data, scenario analysis and business environment and internal control factors. This practice is in line with the CRD, which does not require a stand-alone AMA calculation at the solo-level. Simultaneously, this practice resolves the current difficulties that institutions face - due to the scarcity of relevant information - of building the consolidated capital charge starting from the contributions of the individual operating segments within the group. Furthermore, large banking groups usually adopt a group-wide risk management approach so that a group risk model is consistent with the risk management system.

2. Accordingly, banking group-wide capital requirements provide the basis for the calculation of solo or sub-consolidated capital requirements for the entities within the group, using an allocation mechanism and, in some cases, adjustments to ensure that subsidiaries have sufficient amounts of capital.

3. Starting from the description of the range of allocation mechanisms which are currently used by major EU banking groups, the objective of this paper is to outline sound practices in terms of assessments of allocation mechanisms and home-host related issues.

2. Observed range of allocation mechanisms

4. EU banking groups often use BIA or TSA figures such as gross income as the key for allocation. Nevertheless, some institutions use other indicators, or a combination of them, as the basis for determining the capital charge for the subsidiaries, which tends to reflect, on the one hand, the size of the institution (e.g. FTE, assets) and, on the other hand, its internal loss experience.

5. In a few cases, allocation keys - which could be considered more risk sensitive than adopting gross income or BIA/TSA figures - are used namely:

   - the marginal contribution to AMA capital requirements based, inter alia, on stand-alone calculations, expected shortfall, Shapley method, etc; or

   - the risk exposure at local level measured by business environment and internal control factors or by scenario-generated data or actual losses.

3. Assessments of allocation mechanisms

6. The use of an allocation mechanism to determine the regulatory minimum capital charge for operational risk for a subsidiary is conditional on the approval of the AMA framework and needs to be approved itself. It also requires that the parent's AMA framework has been rolled out to the

subsidiary and that the subsidiary's operational risks and controls are incorporated in the group-wide AMA calculations.

7. Annex X, Part 3, point 3 of the CRD states that, "when an AMA is intended to be used by the EU parent credit institution and its subsidiaries, or by the subsidiaries of an EU parent financial holding company, the application shall include a description of the methodology used for allocating operational risk capital between the different entities of the group". The description should include the relevant documentation on the allocation mechanism and any supporting data, as appropriate.

8. Most supervisory authorities do not set explicit restrictions on the allocation mechanisms which can be used. When deciding on the appropriateness of an allocation method those supervisors examine the choice of the underlying allocation indicators, bearing in mind the early stage of the development of risk-sensitive allocation mechanisms.

9. However, even if simpler allocation methodologies can be accepted as a starting point, AMA banking groups are strongly encouraged – with a view to the overall improvement of the risk sensitivity of their risk measurement framework - to introduce over time capital allocation mechanisms that more appropriately reflect the operational risk profiles of each relevant subsidiary and, to the extent possible, that are more equitable between the subsidiaries themselves.

10. The implementation of more risk-sensitive allocation mechanisms at local level could be a way to provide comfort to host supervisors on the appropriateness of the capital figures. One of the main issues is that, as diversification effects are generally determined on a consolidated basis and allocation mechanisms act on the already diversified capital, capital figures allocated to some subsidiaries may not reflect in an appropriate way their actual operational risk and the contribution of such subsidiaries to the diversified consolidated capital. This may result in some host supervisors imposing supplementary capital requirements on subsidiaries, which do not affect the consolidated capital regulatory figure.

11. An institution intending to use an allocation mechanism is expected to demonstrate its feasibility. Moreover, the adequacy of the allocation key(s) should be assessed by taking into account the size and the complexity of the subsidiaries. It is sound practice for institutions to compare at least the results of different allocation mechanisms and analyse the varying results considering the risk profile of the entities.

12. Supervisors expect that institutions will regularly review the AMA framework, including their adopted allocation mechanism. The allocated AMA capital should be relevant and adequate at all times, meaning that it should reflect the evolving operational risk profiles of the subsidiaries.

4. Home-host issues regarding allocation mechanisms

13. In the case of cross border banking groups, the use of an allocation mechanism is subject to the approval of both the home and host supervisors and has to be addressed within the joint decision on the AMA application.

Relevant host supervisors are all the supervisory authorities within the EU which supervise subsidiaries whose capital requirements are calculated (or included in the roll-out plan) according to the AMA adopted by a banking group located in another Member State.

14. The home supervisor coordinates the approval process with all relevant host supervisors, given that the level of participation of the relevant host supervisors will differ from case to case. If there are specific information needs, they should be agreed between the home supervisor and host supervisors at an early stage in the approval process to give the institution and the home supervisor sufficient time to provide that information without endangering timely approval. In any case, complete documentation of the allocation methodology and its validation results is needed and will be provided by the home supervisor to the host supervisor on request. Host supervisors may perform their own on-site examinations, and they will in these cases inform the home supervisor of the results.

15. A change in the capital allocation mechanism should be considered as a model change. Even if a new application may be not necessary, a change to the allocation methodology should be based on a joint decision.

16. The results of on-going validation can be discussed during the regular contacts between the institution and its supervisors as part of the supervisory review process.

GUIDELINES ON OPERATIONAL RISK MITIGATION TECHNIQUES

1. Introduction

1. Institutions can employ a variety of risk transfer instruments to manage and mitigate their operational risk. These take the form of insurance contracts and "Other Risk Transfer Mechanisms" (ORTM). The Capital Requirements Directive (CRD) allows institutions that use the AMA to recognise the mitigating effect of these instruments in their AMA capital calculations, subject to certain conditions.

2. The conditions that apply to insurance providers and contracts are set out in Annex X, Part 3, Paragraphs 26 to 29 of the CRD[16]. As for ORTM, Annex X, Part 3, Paragraph 25 of the CRD states that the impact of ORTM shall be recognised only if the institution can demonstrate to the satisfaction of the competent authorities that a noticeable risk mitigation effect is achieved.

3. The Guidelines on the Implementation, Validation and Assessment of AMA and IRB Approaches (the "Validation Guidelines"), issued by CEBS in April 2006, provide only limited additional guidance on these instruments for transferring operational risk. In particular, Paragraph 578 of the Guidelines states that the supervisory authorities expect appropriate standards for the recognition of ORTM, while Paragraph 579 states that outsourced activities should not be considered to be part of ORTM.

4. The main objective of this paper is to provide more complete guidance on the recognition of insurance within the AMA capital calculation. In particular, after addressing in Section 2 general conditions for the recognition of operational risk mitigation instruments, Section 3.1 deals with the eligibility of protection providers and the characteristics of eligible products and Section 3.2 covers the issue of haircuts for uncertainty in coverage.

5. The treatment of ORTM is discussed in Section 4. For several reasons - the most important being the relatively brief experience of institutions and supervisors with this type of protection – CEBS has decided to issue only a limited number of specific guidelines at this stage, and to refer instead, in general, to CRD requirements and CEBS guidelines for insurance, and to relevant sections of the CRD framework for credit risk mitigation (in particular, Part 1, "Eligibility", and Part 2, "Minimum Requirements", of Annex VIII of the CRD). Therefore the guidelines provided on ORTM aim to ensure convergence of supervisory practices in the area of ORTM by providing a framework which is consistent with the one for insurance products. This also adds to the legal security needed to develop ORTM for the purposes of risk management and capital alleviation within the AMA.

[16] Except where noted otherwise, all references to Articles and Annexes of the CRD are references to Directive 2006/48/EC.

Supervisors should bear in mind, however, that stricter conditions could be necessary for the recognition of ORTM within the AMA framework, reflecting differences in the type of protection provided by these instruments, as compared with insurance contracts, and the peculiarities of operational risk relative to credit risk.

6. Finally, institutions and supervisors should keep in mind that – depending on how the ORTM are structured and how they are classified in the institution's accounts – they can entail additional risks (such as credit risk and market risk) for the institution buying or selling protection and that these carry regulatory capital implications of their own.

7. CEBS will continue its dialogue with the industry on the development of ORTM and will closely monitor their use as instruments for operational risk mitigation. As institutions and supervisors gain more knowledge and experience with the use of these instruments for risk management purposes and capital calculation and a range of best practices is identified, CEBS will supplement and/or review these guidelines, and may also recommend adjustments to the relevant regulatory requirements under the CRD framework.

2. General conditions for risk mitigation techniques

8. Annex X, Part 3, Paragraph 29 of the CRD, as amended in July 2009 through the Comitology procedure (the so-called CRD II), states that "the capital alleviation arising from the recognition of insurances and other risk transfer mechanisms shall not exceed 20% of the capital requirement for operational risk before the recognition of risk mitigation techniques". The new provisions introduced by the CRD II will have to be applied by 31 December 2010 and in the interim supervisors should apply the 20% limit on capital alleviation to both insurance contracts and ORTM, which together should not exceed the 20% limit.

9. Paragraph 580 of the Validation Guidelines states that institutions should review their use of insurance and ORTM and recalculate the operational risk capital charge if the nature of the insurance or the coverage of ORTM changes significantly. If a material loss is incurred which affects the insurance coverage, or if changes in insurance or ORTM contracts create major uncertainty as to their coverage, institutions should recalculate the AMA capital requirement with an additional margin of conservatism, for example by applying haircuts in the modelling exercise. The AMA capital requirement should also be recalculated if there is a major change in the operational risk profile of the institution.

10. Paragraph 581 of the Validation Guidelines requires institutions to notify their competent authorities of material changes in the coverage of insurance or ORTM. Supervisors will closely monitor the features of insurance products and ORTM and their impact on the coverage of operational risk.

3. Specific conditions for the use of insurance

3.1. Eligibility of providers and characteristics of the products

11. According to Annex X, Part 3, Paragraph 26 of the CRD, in order for insurance to be recognised for capital purposes, the insurance provider must be authorised by a regulator to provide insurance contracts or re-insurance contracts. The EU "single passport" provides an explicit mechanism for mutual recognition of EU-regulated undertakings, enabling an EU Member State to accept the authorisation granted by another EU Member State without itself having to verify that the undertaking is appropriately authorised. However, consideration should be given to recognising the risk-mitigating effect of insurance contracts provided by an undertaking authorised by a non-EU regulator if that undertaking satisfies prudential requirements that are equivalent to those applied in the EU and meets the standards set in Paragraphs 26 to 29[17].

12. The Basel II regulatory framework allows banks to recognise the risk-mitigating impact of insurance if the insurer has a minimum claims paying ability rating of A (or equivalent). However, the CRD sets a less stringent standard. Paragraph 26 requires insurers to have a "minimum claims paying ability rating by an eligible ECAI which has been determined by the competent authority to be associated with a credit quality step 3 or above under the rules for the risk weighting of exposures to credit institutions under Articles 78 to 83". EU supervisors are governed by the CRD, and should therefore allow ratings equivalent to credit quality step 3 or better [18], based on the long-term claims paying ability rating of the insurer.

13. Paragraph 27(a) requires that insurance contracts must have an initial term of no less than one year. This should be interpreted as requiring the parties to contract for at least one year. The "residual term" should refer to the period remaining on the contract at a given point in time.

14. Paragraph 27(d) states "that the risk mitigation calculations must reflect the insurance coverage in a manner that is transparent in its relationship to, and consistent with, the actual likelihood and impact of loss used in the overall determination of operational risk capital." The mapping of insurance contracts to operational risk losses (or operational risk sub-categories) should be performed at a sufficiently granular level to demonstrate the relationship between the actual and potential likelihood and magnitude of operational risk losses and the level of insurance coverage. All the information sources available to the institution, including (internal and external) loss data and scenario estimates, should be used for this aim. Calculations should reflect the level of coverage, for example through the determination of a probability of coverage.

---

[17] All references to Paragraphs 26-29 in these Guidelines refer to Annex X, Part 3 of Directive 2006/48/EC.

[18] This view is supported by the response of the CRD Transposition Group (CRDTG) to question n. 95, published in August 2006.

15. Paragraph 27(e) states that insurance may be recognised for capital purposes only if it is provided by a third-party entity, i.e. an independent entity outside the group of the institution seeking insurance protection. When making this assessment, supervisors should have a complete grasp of the institution's group structure so as to be able to assess whether the operational risk has in fact been transferred outside the group to an entity in which neither the institution nor any other entities within its group has a relevant interest. In analysing the group structure, supervisors should consider the group definitions given by the CRD, national financial services acts, and corporate group law (where applicable). An institution should also take reasonable steps to ensure that neither it nor any of its subsidiaries is knowingly re-insuring contracts that cover operational risk events that were the object of the initial insurance arrangement entered into by the institution.

3.2. Haircuts for uncertainty of coverage

16. Institutions that use insurance instruments to transfer operational risk should analyse the various factors that create uncertainty in the effectiveness of the risk transfer. They should reflect these uncertainties in their capital calculations through appropriate haircuts.

17. Haircuts should be calculated conservatively. It is up to each institution to determine the appropriateness of the haircuts it applies. The CRD provides little detail on how haircuts should be applied, leaving institutions with considerable discretion to develop methods that suit their structure. Supervisors should assess these haircuts carefully, balancing the discretion provided by the CRD against the need to ensure that the general intent of the rules is not circumvented[19].

18. The following sub-sections introduce guidelines on haircuts for insurance coverage, distinguishing them on the basis of the pertinent elements of uncertainty, namely: maturity, cancellation and uncertainty of payment and mismatches in coverage.

a) Maturity

19. Paragraph 27(a)[20] requires institutions with insurance contracts that have less than a year to run, to apply appropriate haircuts reflecting the declining residual term of the policy. This requirement is consistent with the required 99.9 % confidence interval over a one year period and is to be applied within each AMA capital calculation. Supervisors may waive this requirement if the institution has in place a replacement contract that provides insurance cover on equivalent terms or if the current insurance contract has an

[19] For example the calculation of the haircuts by simple ex-post adjustments may fail to capture the relevant uncertainties of the insurance coverage.

[20] As noted earlier, all references to Paragraphs 26-29 in these Guidelines refer to Annex X, Part 3 of Directive 2006/48/EC.

automatic renewal provision and no cancellation notice has been given[21]. However, institutions and supervisors need to be cautious about assuming that institutions can renew their policies on equivalent terms, conditions, and coverage, as some risks covered by the policy may not be included when the policy is renewed [22].

b) Cancellation

20. Paragraph 28(b) requires institutions to capture policy cancellation terms, when exercisable in less than one year, through haircuts. In some jurisdictions, national insurance regulations or national law grants insurance providers the right to cancel insurance policies. In the case of renewable policies, the renewal assumptions should also take into account the ability of the insurer to cancel the policy during the term or at the renewal date.

c) Payment uncertainty and coverage mismatches

21. Paragraph 28(c) requires institutions to apply haircuts for payment uncertainty and for mismatches in the coverage of insurance policies.

- Payment uncertainty is the risk that the insurance provider will not make the payments expected by the institution in a timely fashion. This can result, for example, from disputes due to differences in the interpretation of contractual language, from counterparty default or from unanticipated delays in payment (for example, arising from the claims protocol or the evaluation and settlement processes). Institutions, if necessary, should consider and fully document data on insurance payouts by loss type in their loss databases and set haircuts accordingly. Supervisors should also familiarise themselves with customary claims payment delays which can often exceed one year.

- A haircut for counterparty default should be assessed on the basis of the credit quality of the insurance company responsible under the given contract, even if its parent institution has a better rating or the risk is transferred to a third party. Insurers with a lower claims paying ability should attract a higher haircut than insurers with a higher credit quality.

- A coverage mismatch occurs when the coverage of the insurance contract does not match the operational risk profile of the institution,

[21] For example, if an insurance contract for two or more years has a clause providing that the parties will negotiate a new two-or-more-year contract before the expiry of the first year, the contract revolves every year, ensuring that there is always at least one year outstanding on the contract. If, in addition the coverage of the policy does not change with renewal, a haircut need not to be applied.

[22] For example, the insurer may retain the right to increase the premium, and there is the risk that the premium may be increased to an unacceptably high level if there is a significant loss by the institution (or the industry) which prompts the insurer to revise its pricing. Furthermore, insurers may decide to cease writing business for certain types of risks, as the result of high losses or other industry or legal developments.

such that the cover does not provide the desired mitigating effect and some events are not covered. In particular coverage mismatches of medium to large losses due for instance to high deductibles and limits, or to the exhaustion of policy limits, should be correctly captured and appropriately incorporated into the AMA model by making use of all the available sources (loss data and scenario estimates) and specific data analysis and simulation exercises.

4. Specific conditions for the use of ORTM

22. Paragraph 25 states that ORTM may be recognised for capital purposes only if the institution can demonstrate to the satisfaction of its competent authority that it achieves a noticeable risk mitigating effect. Supervisors expect buyers of ORTM protection for which capital alleviation is claimed to use such instruments for risk management, and should not accept ORTM as risk mitigants under the AMA framework if they are held or used for trading purposes. Supervisors should monitor the use of such products closely and assess the intent of the institution in purchasing such instruments when evaluating their risk mitigating effect.

23. Institutions should have experience in using ORTM products before they are allowed to recognise these products in their AMA capital calculations. This requirement is intended to encourage institutions to collect data from internal and external sources on the probability of coverage and the timeliness of payment for ORTM instruments. This is particularly necessary for product types or classes with novel characteristics, and is not necessarily required for every product.

24. While ORTM reduces the operational risk exposure of the protection buyer, it increases the risk exposure of the protection seller. It is essential that the protection seller should be financially sound, both in terms of solvency and liquidity. Supervisors should be aware of the risks assumed by sellers of ORTM protection and should consider prudential measures if a protection seller acquires significant risk exposures from other institutions. Consideration should be given also to the possibility that the seller of some forms of ORTM protection may be subject to insurance regulation under national insurance regulations.

25. Supervisors should assess the institution's use of ORTM in AMA capital calculations on a case by case basis, considering the eligibility of the protection seller (regulated or unregulated entity) and the nature and characteristics of the protection provided (funded protection, securitisation, guarantee mechanism or derivatives).

26. Such assessments should be based on the relevant requirements of Paragraphs 26 to 28 and the specific conditions set out in Section 3 of the present Guidelines. Supervisors should also take into consideration relevant sections of the requirements for recognition of credit risk mitigation in Part 1 ("Eligibility") and Part 2 ("Minimum Requirements") of Annex VIII of the CRD.

27. When considering these requirements and conditions, supervisors should bear in mind that stricter qualifying criteria may be required for the eligibility of ORTM providers and the type of ORTM products for the following reasons:

- the peculiarities of operational risk relative to credit risk (e.g., absence of underlying assets, greater role of unexpected losses);
- the lack of an efficient, liquid, and structured market for analogous products which thus far have been traded outside the banking sector (e.g., catastrophe bonds, weather derivatives); and
- the difficulty in assessing the legal risk of ORTM, even when the terms and conditions of the contracts are clearly and carefully spelt out.