Annex

TABLE OF CONTENTS

ANNEX

Guidelines on Advanced Measurement Approach (AMA) for Calculating Operational Risk Capital Charge

1. Introduction

1.1 Operational Risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This includes legal risk[1], but excludes strategic and reputational risks. (For further guidance, refer to **Part A of Appendix 1**).

1.2 The Basel II framework requires banks to hold capital charge for operational risk under Pillar I. It presents three methods for calculating operational risk capital charges in a continuum of increasing sophistication and risk sensitivity: (i) the Basic Indicator Approach (BIA); (ii) The Standardised Approach (TSA)/Alternative Standardised Approach(ASA) ; and (iii) Advanced Measurement Approaches (AMA). Banks are encouraged to move along the spectrum of available approaches as they develop more sophisticated operational risk measurement systems and practices. Internationally active banks and banks with significant operational risk exposures are expected to use an approach that is more sophisticated than the BIA and that is appropriate for the risk profile of the institution.

1.3 The guidelines for calculating operational risk capital charge for BIA, TSA and ASA have been issued separately. This Annex provides guidance on AMA for computing capital charge for operational risk. The guidance is in addition to that contained in 'Guidance Note on Management of Operational Risk' issued by RBI vide its circular No. DBOD.No.BP.BC.39/21.04.118/2004-05 dated October 14, 2005 and wherever there is conflict between the two, the guidance contained in this annex would prevail.

---

[1] Legal risk includes, but is not limited to, exposure to fines, penalties or punitive damages resulting from supervisory actions, as well as ordinary damages in civil litigation, related legal costs and private settlements.

1.4 A bank which has adopted the TSA, the ASA or the AMA, with prior RBI approval, shall not subsequently use a different approach without the prior approval of RBI. If, however, RBI determines that the bank adopting the TSA, ASA or AMA no longer meets the qualifying criteria for the respective approaches, it may require the bank to revert to a simpler approach for some or all of its operations, until it meets the conditions specified by RBI for returning to the more advanced approach.

2. Scope of Application

2.1 The bank adopting the AMA will implement it both at the solo level (including overseas branches) as well as at a consolidated/group-wide level, excluding group companies which are engaged in insurance business.

2.2 RBI recognises, however, that in some cases, it may not be practical for banks to implement the AMA across all of their business activities or across all legal entities which are part of the banking group. This may be the case, for instance, where a bank undertakes a new business activity, has acquired/introduced a new business or has certain immaterial business activities, undertaken either departmentally or through subsidiaries. In such cases, RBI may, on a bank's application, permit a bank to use a combination of the AMA for some part of its operations and the BIA or TSA/ASA for other operations. This approach is referred to as **partial use.** In such cases, the bank shall provide RBI with appropriate written information on the business operations for which the bank proposes to use the BIA or TSA/ASA. Approval for partial use of an AMA will, at a minimum, require that:

(a) all operational risks of the global, consolidated operations of the bank are captured;

(b) all of the operations of the bank that are covered by the AMA meet the qualifying criteria for using an AMA, while those parts of its operations that are using one of the simpler approaches meet the qualifying criteria for that approach;

(c) on the date of the implementation of AMA, a significant part[2] of the operational risks of the solo bank are captured by the AMA; and

(d) the bank provides RBI with a plan specifying the timetable to which it intends to roll out the AMA across all material operations of the bank including that undertaken through subsidiaries.

Subject to the approval of RBI, a bank opting for partial use may determine which parts of its operations will use an AMA on the basis of business line, legal structure, geography, or other internally determined basis. RBI may also impose additional conditions on partial use and additional capital requirements, if deemed appropriate.

2.3 Banks with overseas branches intending to implement AMA should have capability to calculate capital under AMA at global basis, even if the local regulators do not require the overseas branches to adopt AMA.

3. General Requirements for AMA

3.1 A bank should comply with the requirements and the guidelines in this Annex before applying for approval from RBI to adopt the AMA.

3.2 A bank should perform an internal assessment against the requirements and guidelines in this Annex to ascertain its readiness to adopt the AMA before applying for approval from RBI.

3.3 A bank which complies with the requirements in this Annex will not automatically qualify for AMA adoption. RBI has to be satisfied that the intention of the bank in adopting the AMA is to seek continual improvements in its risk management practices. The bank should not regard these standards as an exhaustive checklist to be satisfied in order to adopt the AMA. As part of its approval process, RBI will consider the willingness and ability of the bank

[2] Significant part of Operational Risk would mean part of operations of the bank accounting for more than 50% of the 'average operational losses of the bank for last three years'.

to maintain and improve its systems to ensure the continuing appropriateness of the operational risk capital requirements.

3.4 The overarching principles behind these requirements are as follows:

(i) The process of the bank for deriving operational risk estimates of the AMA elements[3] should generate consistent and predictive estimates of the AMA elements suitable for use under the AMA to calculate minimum operational risk capital requirements; such bank must hold regulatory capital commensurate with the exposure to operational risk.

(ii) Operational risk estimates of the AMA elements should be used pervasively in internal operational risk management and other significant business decisions relating to the operational risk of the bank.

(iii) The bank has set up and is able to maintain a governance framework, including the appropriate organisational structures and control mechanisms, to ensure that it is able to continue to derive consistent and predictive estimates of the AMA elements.

(iv) The bank must have in place a robust operational risk management framework and a conceptually sound operational risk measurement system.

3.5 The AMA methodology should be comprehensive and result in an operational risk capital requirement that reflects the operational risk experience of the bank. The estimate should be fundamentally sound and consistent with the scope of operational risk defined in this Annex.

3.6 A bank shall comply with the requirements, and should meet the guidelines, in this Annex on an ongoing basis.

4. Application to Adopt the AMA

A bank desirous of adopting AMA to calculate its operational risk capital requirement is required to obtain explicit supervisory approval. The bank shall

[3] 'AMA elements' means the internal and relevant external data on operational risk losses, scenario analysis and factors reflecting the business environment and internal control systems

apply in writing to RBI for approval no less than 24 months prior to its AMA adoption date or such other shorter time as may be permitted by RBI. The documents to be submitted to RBI along with application are described in paragraph **16** of these guidelines.

5. Recognised Parallel Run

5.1 A bank intending to adopt the AMA shall conduct a recognised parallel run for at least 18 months, or such shorter period as determined by RBI, after approval of the bank's AMA by RBI.

5.2 RBI will recognise a parallel run only if it is based on an operational risk measurement and management framework assessed by RBI to be sufficiently satisfactory for the parallel run.

5.3 During the recognised parallel run, the bank shall calculate its operational risk capital charge under both the AMA and the prevailing operational risk capital requirements that are applicable to the bank, before adopting AMA. During this period, the operational risk capital charge would be maintained as per the current approach adopted by the bank.

5.4 A bank shall submit to RBI the capital charge calculations for operational risk at both the Solo and Group levels as at the end of each quarter during the recognised parallel run, no later than the 30th day of the following month, even if unaudited and followed up with audited calculations soon after audit is completed.

5.5 If a bank becomes aware during the recognised parallel run that the confirmations made pursuant to paragraph 16.4 and 16.5 are no longer valid or that it no longer complies with any of the conditions or restrictions imposed by the RBI at the time of approving the AMA model, it shall -

(a) inform RBI as soon as practicable;

(b) assess the effect of the situation in terms of the risk posed to the bank;

(c) prepare a plan to rectify the situation and inform RBI of its plan as soon as practicable; and

(d) undertake prompt corrective action in accordance with the plan prepared pursuant to sub-paragraph (c) above.

5.6 During the parallel run, RBI will continue to evaluate the readiness of the bank to adopt the AMA in order to reach a decision, towards the end of the parallel run, on whether to grant or withhold the **final approval** for the bank to adopt the AMA. RBI may withhold such approval if, during the parallel run, it becomes aware of information that materially affects its assessment of the readiness of the bank or if any outstanding issue identified prior to the start of the parallel run has not been addressed. RBI may also require the bank to extend the parallel run to allow more time for the bank to take corrective actions.

6. Prudential Floor

6.1 A bank which migrates to the AMA for operational risk regulatory capital after obtaining RBI approval will also calculate capital charge for operational risk as per existing methodology (BIA or TSA/ASA) for at least three years from the date of migration. (The three year period will exclude the parallel run period during which the capital charge for operational risk will continue to be maintained as per current measurement method i.e. BIA or TSA/ASA). The minimum capital requirement for operational risk during the said three years will be subject to the following prudential floors:

Years →	**Year 1**	**Year 2**	**Year 3**
Prudential Floor (as percentage of minimum capital requirement as per current measurement method i.e. BIA or TSA/ASA)	100	90	80

6.2 RBI will review performance of AMA in banks on an on-going basis and will take a decision on continuance of prudential floors or otherwise after three years of a bank adopting AMA.

7. Calculation of Capital Charge for Operational Risk

7.1 Once the bank has calculated the capital charge for operational risk under AMA, it has to multiply this with (100÷9) and arrive at the notional risk weighted asset (RWA) for operational risk.

7.2 The RWA for operational risk will be aggregated with the RWA for the credit risk and the minimum capital requirement (Tier 1 and Tier 2) for credit and operational risk will be calculated. The available surplus eligible capital (as described in our Master Circular on New Capital Adequacy Framework - NCAF) should be sufficient to meet the capital requirement for market risk.

7.3 The total of eligible capital (Tier 1 and Tier 2) will be divided by the total RWA (credit risk + operational risk + market risk) to compute CRAR for the bank as a whole.

8. Operational Risk Management Framework (ORMF) and Operational Risk Measurement System (ORMS)

8.1 A bank with AMA approval must have in place an ORMF that is sufficiently robust to facilitate quantitative estimates of the bank's Operational Risk Regulatory Capital (ORRC) that are sound, relevant and verifiable. ORMF comprises:

- the organisational structure for management of operational risk;
- governance structures;
- policies, procedures and processes; and
- systems used by the bank in identifying, measuring, monitoring, controlling and mitigating operational risk.

8.2 A bank's ORMS consists of the mathematical and statistical models, technological support systems, data and validation processes used to measure operational risk to estimate the regulatory capital. ORMS is a subset of ORMF. RBI must be satisfied that the bank's ORMF is suitably rigorous and consistent with the complexity of the bank's business. Where

industry risk modelling practices evolve and improve over time, the bank must consider these developments in assessing its own practices. Furthermore, the AMA must play an integral role in the bank's risk management and decision making processes and meet the requirements detailed in subsequent paragraphs, including requirements relating to the Board of Directors (Board) and senior management responsibilities. A bank seeking AMA approval must demonstrate the processes it has undertaken to establish an ORMF. The bank will also be required to demonstrate the processes that are undertaken to ensure the operational risk management framework has continued relevance to the bank's operations.

8.3 Qualitative Standards for the ORMF

A bank must meet the qualitative standards laid down in paragraphs 8.3.1 to 8.3.4 before it is permitted to use an AMA for operational risk capital.

8.3.1 The bank must have an **independent** operational risk management function that is responsible for the design and implementation of the bank's operational risk management framework. The operational risk management function is responsible for codifying firm-level policies and procedures concerning operational risk management and controls; for the design and implementation of the firm's operational risk measurement methodology; for the design and implementation of a risk-reporting system for operational risk; and for developing strategies to identify, measure, monitor and control/mitigate operational risk.

8.3.2 There must be regular reporting of operational risk exposures and loss experience to business unit management, senior management, and to the board of directors. The bank must have procedures for taking appropriate action according to the information within the management reports.

8.3.3 The bank's operational risk management system must be well documented. The bank must have a routine in place for ensuring compliance with a documented set of internal policies, controls and procedures

concerning the operational risk management system, which must include policies for the treatment of noncompliance issues.

8.3.4 A bank shall have, and maintain, rigorous procedures for the development, implementation, and review of the ORMF. Internal and external auditors must perform regular reviews of the operational risk management processes and measurement systems including the verification that the internal validation processes are operating in a satisfactory manner.

8.4 Qualitative Standards for ORMS

8.4.1 The ORMS of a bank should be conceptually sound and implemented with integrity. It should also be sufficiently robust to facilitate quantitative estimates of the operational risk capital requirement of the bank. The bank shall ensure that the ORMS adopted is implemented consistently across the bank and the ORMS should have a reasonable track record in measuring operational risk.

8.4.2 The bank's internal operational risk measurement system must be closely integrated into the day-to-day risk management processes of the bank. This would include ensuring that the output of the ORMS is an integral part of the process of identifying, assessing, monitoring, controlling and mitigating the operational risk of the bank. For example, this output should play a prominent role in risk analysis, managing and reporting, as well as in decision-making, corporate governance and internal capital allocation. Each business line should be able to clearly articulate the drivers of its operational risk and demonstrate how the individual parts of the ORMS are used to supplement its day-to-day decision-making activities. Further guidance in this regard is furnished in **Part C of Appendix 1.**

8.4.3 A bank shall demonstrate, through its internal risk management and decision-making processes that the estimates of the AMA elements produced from internal models do not result in an understatement of risk elements.

8.4.4 A bank shall have techniques for allocating operational risk capital to business lines and for creating incentives to improve the management of operational risk, processes and practices throughout the bank. The bank should be able to demonstrate that the allocation will enhance transparency, risk awareness and operational risk management expertise in the bank.

8.5 Quantitative Standards for the ORMS

8.5.1 Basic requirements of an AMA Model

8.5.1.1 Given the continuing evolution of approaches for operational risk, Basel II framework does not specify any particular approach, methodology, measurement technique or distributional assumptions used to generate the operational risk measure for the purposes of determining the operational risk capital requirement of a bank. Accordingly, RBI is not specifying the approach, methodology, measurement technique or distributional assumptions used to generate the operational risk measure for the purposes of determining the operational risk capital requirement of a bank. However, the bank shall have a comprehensive AMA and be able to demonstrate that it captures potentially severe 'tail' loss events. The bank shall demonstrate to the RBI that its operational risk measure meets a soundness standard comparable to **a one-year holding period and a 99.9th percentile**, one-tailed confidence interval. An indicative description of statistical distributions used in operational risk modelling is given in para 8.5.5.

8.5.1.2 RBI recognises that the AMA soundness standard provides significant flexibility to a bank in the development of the methodology. This flexibility is intended to encourage the bank to implement a methodology which -

(a) best suits the nature, size and complexity of the activities, operations, business environment, and internal controls of the bank;

(b) has regard to its historical and the industry's experience in respect of operational risk losses and the assessment of its planned future operational risk profile; and

(c) allows for future evolution and innovation where industry practices evolve and improve over time.

8.5.1.3 The bank should also ensure that ORMS is -

(a) comprehensive, consistently implemented and transparent;

(b) independently reviewed by external auditors and validated; and

(c) capturing all material sources of operational risk across the bank, including events that can lead to rare and severe operational risk losses.

8.5.1.4 There may be subjectivity and uncertainty in the ORMF because of the evolving nature of operational risk management and measurement practices. Therefore, the bank shall build in a degree of conservatism into its approach to reflect the evolutionary status of ORMS and its impact on data capture and modelling.

8.5.1.5 A bank's operational risk measurement system must be consistent with the scope of operational risk as defined in paragraph 1 and the loss event types defined in **Appendix 2**. A bank must map its ORRC to the Level 1 business lines detailed in **Appendix 3**. Where the bank's own internal classification of business activities differs to those detailed in that table, the bank may map the ORRC to its own business activities, which in turn must be mapped to those defined in **Appendix 3**. This mapping process must be clearly documented.

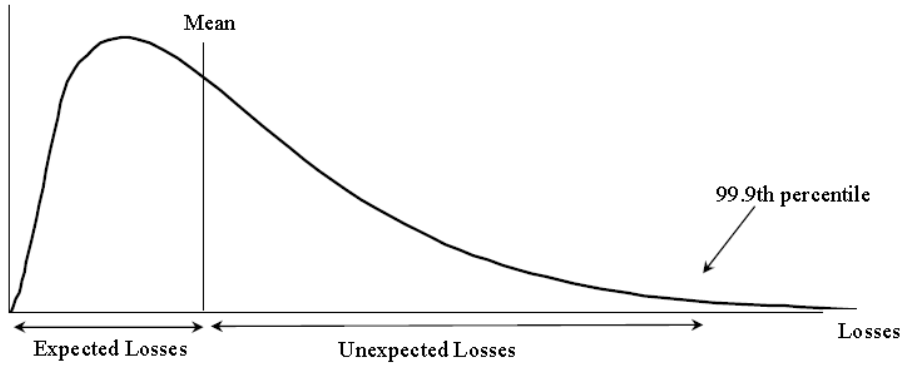
8.5.1.6 The conceptual foundation of operational risk measurement methodology under Basel II framework is based on the view that risk can be quantified through the estimation of specific characteristics of the probability distribution of potential losses over a given time horizon. This approach assumes that a suitable estimate of that probability distribution, or at least of

the specific characteristics to be measured, can be produced. **Figure 1** below illustrates some of the key concepts associated with the framework. The figure shows a probability distribution of potential losses associated with some time horizon (for example, one year). It could reflect, for example, credit losses, **operational losses**, or other types of losses.

The area under the curve to the right of a particular loss amount is the probability of experiencing losses exceeding this amount within a given time horizon. The figure also shows the statistical mean of the loss distribution, which is equivalent to the amount of loss that is “expected” over the time horizon. The concept of “expected loss” (EL) is distinguished from that of “unexpected loss” (UL), which represents potential losses over and above the EL amount. A given level of UL can be defined by reference to a particular percentile threshold of the probability distribution. For example, in the figure UL is measured at the 99.9th percentile level and thus is equal to the value of the loss distribution corresponding to the 99.9th percentile, less the amount of EL. This is shown graphically at the bottom of the figure. The particular percentile level chosen for the measurement of UL is referred to as the “confidence level” or the “soundness standard” associated with the measurement. If capital is available to cover losses up to and including this percentile level, then the bank should remain solvent in the face of actual losses of that magnitude.

Typically, the choice of confidence level or soundness standard reflects a very high percentile level, so that there is a very low estimated probability that actual losses would exceed the UL amount associated with that confidence level or soundness standard.

Figure 1: Probability Distribution of Potential Losses



8.5.1.7 A bank should calculate its regulatory operational risk capital requirement as the sum of expected loss (EL) and unexpected loss (UL). For operational risk EL to be "measured" to the satisfaction of RBI, the bank's measure of EL must be included in the 'EL-plus-UL capital charge' calculated using the AMA model approved by RBI. Banks should endeavour to account for EL by means of provisions to the extent considered appropriate by them, and balance through holding capital. This means that if expected loss has been fully provided for in the books of account through debit to profit and loss account, the same can be deducted from the overall regulatory capital requirement as measured under as per the AMA model i.e. in such a case, the operational risk capital will be required only for unexpected part of losses. If the provisions held against operational losses exceed the EL, the excess would be eligible for inclusion in Tier II capital subject to the limit of 1.25% of risk weighted assets.

8.5.2 Correlation and Dependence in AMA Models

8.5.2.1 Risk measures for different operational risk estimates must be added for purposes of calculating the regulatory minimum capital requirement.

8.5.2.2 Correlation is one measure of the dependency of potential operational risk losses across or within business lines and/or loss event types.

In operational risk, correlations may arise because of the presence of common factors of different nature, either idiosyncratic (e.g. processes, systems, and people) or due to environmental elements that affect several geographical, business, or legal units. These factors can influence the observed frequency or severity of losses in more than one operational risk class. The concept of correlation can be generalized to more complex dependency relationships (e.g., copulas) that recognise differences in dependencies across low- and high-severity operational risk events.

8.5.2.3 Dependence structures could occur as a result of business cycles (i.e., economic difficulties that cause an increase in rogue trading and fraud), bank-specific factors (i.e., a new senior manager changes the control environment across a number of business lines) or cross-dependence of large events (e.g., flooding results in widespread looting and increases the number of fraudulent transactions) or a change in the legal risk associated with certain business practices. Dependence modeling is an evolving area and a wide range of practices in this regard exists in the banking industry. However, choice of dependence approach may have significant impact on the capital estimates. The term dependency would be broadly interpreted to mean any form of dependency (e.g., linear or non-linear, relating to all the data or just to the body or the tail) across two or more operational risk classes, caused by internal and/or external factors. Model documentation should identify and justify assumptions.

8.5.2. 4 A bank may use internally determined correlations/dependence in operational risk losses across individual operational risk estimates, provided it can demonstrate to the satisfaction of RBI that its systems for determining correlations are sound, implemented with integrity, and take into account the uncertainty surrounding any such correlation estimates (particularly in periods of stress).

8.5.2.5 Low-frequency, high-severity events are usually the main drivers of risk estimates used in AMA models. Dependencies between such tail

events should be studied with great care. Given the different nature of tail and body events, different quantitative and qualitative tools could be necessary to determine and estimate the impact that the underlying dependency structures will have on capital.

8.5.2.6 Scenarios are likely to have a significant influence on the amount of capital calculated as per AMA. Scenarios involving multiple risk factors (frequency/severity of losses in different event types) would obviously require assumptions of correlations. For this purpose, the correlations among various risk factors already calculated by the bank based on historical data could form the basis of projections with appropriate adjustment to account for the possibility that the correlations could break down under a stressed scenario.

8.5.2.7. The correlation/dependence assumptions should be validated using appropriate quantitative and qualitative techniques. These should be substantiated by empirical analysis of data where the modeling is primarily based on internal and external data. Validation with quantitative techniques developed for correlations between high-frequency, low-severity events could be difficult to apply to dependencies between tail events. In these cases, the soundness of dependency assumptions that have a material impact on the overall AMA measure should be demonstrated by using, at a minimum, qualitative validation techniques; and, where possible, quantitative techniques and/or some form of stress-test analysis. Qualitative validation may *inter alia* include judgement of business line experts.

8.5.2.8. The bank shall demonstrate to the RBI that its dependence or correlation assumptions are appropriate and reasonably conservative. RBI would expect a greater deal of conservatism in assumptions where the dependence model is not very rigorous. However, a bank cannot compensate the rigor of the model with greater conservatism and a minimum level of rigour has to be demonstrated for all dependence models. The AMA model documentation should identify and justify the assumptions as well as evaluate the AMA model’s sensitivity to these assumptions.

8.5.3 Granularity of AMA

8.5.3.1 The bank should ensure that its ORMS and AMA model are sufficiently ‘granular’ to capture the major drivers of operational risk affecting the shape of the tail of the loss estimates. The granularity of an AMA reflects the degree to which the quantification approach separately models individual operational risk exposures. An Operational Risk Category (ORC) or unit of measure is the level (for example, organisational unit, operational loss event type, risk category, etc.) at which the bank's quantification model generates a separate distribution for estimating potential operational losses. This term identifies a category of operational risk that is homogeneous in terms of the risks covered and the data available to analyse those risks.

8.5.3.2 The least granular approach would be a single ORC (or unit of measure) for all of a bank’s operational risk exposures. An advantage of this approach is that only a single distribution of operational risk losses is estimated, allowing operational risk loss data to be pooled. Pooling helps to address issues related to data paucity. However, this approach may not reflect the true nature of the underlying losses, as losses may arise from different operational risk sources and often are not independent. More granular approaches estimate potential operational risk losses by business line and/or operational risk event type. These approaches provide an ability to capture differences in operational risk exposures across business lines or event types.

8.5.3.3 In general, as operational risk tends to be characterised by different sources, events and effects, granularity could be the tool by which banks recognise such differences in the model. Individual units of measure should be characterised by high levels of homogeneity, with loss events in a given unit of measure distributed fairly identically. Banks should demonstrate that their choice of granularity takes into account use test considerations, and the nature and complexity of business activities and operational losses to which it is exposed. They should seek to identify ORCs within which losses are independent and identically distributed. This choice of granularity should

be adequately supported by quantitative and qualitative analysis. In border line cases, the circumstances could suggest inclusion of particular type of losses in more than one category. In such cases, the sensitivity of the estimation of total annual loss to other ORCs should also be tested. Banks should undertake further statistical or other analysis to support their choice of granularity and the assumptions that choice of granularity implies, and not justify their choice only on the basis of data availability.

8.5.3.4 A very high or very low granularity may raise supervisory concerns. Models with a low granularity may not capture the real sources of operational risk and, therefore, the operational risk profile of the bank. These models imply that all the business lines and units of the bank are affected by operational risk in a similar way - an unrealistic assumption. Additionally, low granularity tends to generate lower operational risk capital outcomes because of an implicit assumption of zero correlation. Therefore, banks that use models with low granularity and assume implicit zero correlations should demonstrate their right choice of granularity.

8.5.3.5 Use of very large number of units of measure may raise issues relating to adequately categorising sources of their operational risk. Also, high granularity may pose other modelling challenges when summing up the operational risk exposure estimates in order to calculate the total bank operational risk capital. In such a case it would also be necessary for banks to demonstrate the transparency required to provide insight into the diversification of the bank's operational risk and into the AMA capital quantification methodology. Though under Basel II, there is a requirement to classify the internal operational risk losses into 8X7 matrix of business lines and loss event types, it need not be applied as a standard for internal operational risk measurement system under AMA. Banks should test the relevance of their choice of classes in order to ensure the homogeneity of the classes and verify that alternative categorisation schemes would not have been better suited to their risk profile and use test considerations. This should be supported, where possible, with statistical tests.

8.5.4 Essential Data Elements of an AMA Model

8.5.4.1 A bank's internal loss data may not be sufficient to model the operational risk exposures faced by the bank as many of the potential risks to which the bank is exposed would not have materialised during the life of the bank. Basel II framework, therefore, requires that a bank's operational risk measurement system must incorporate four key data inputs. These four inputs/elements are

- internal data,
- relevant external operational risk data,
- scenario analysis; and
- business environment and internal control factors (BEICFs).

8.5.4.2 A bank shall include in its ORMS the use of the above four AMA elements, in accordance with the following:

(i) The bank shall have a credible, transparent, well- documented and verifiable approach for weighting the estimates of the AMA elements. The main consideration in the relative use of the four elements would be to ensure that the input data reflects the bank's operational risk profile and operational risk management practices. For example, there may be cases where estimates of the 99.9th percentile confidence interval based primarily on internal and external loss event data would be unreliable for business lines with a heavy-tailed loss distribution and a small number of observed losses. In such cases, scenario analysis, and business environment and control factors, may play a more dominant role in the risk measurement system. Conversely, operational loss event data may play a more dominant role in the risk measurement system for business lines where estimates of the 99.9th percentile confidence interval based primarily on such data are deemed reliable.

(ii) The bank shall determine and justify how the AMA elements are weighted and combined.

(iii) The bank shall demonstrate that it has established a consistent and comprehensive process, and has defined responsibilities for capturing the AMA elements.

(iv) The bank shall have clear standards for the modification of the estimates of the AMA elements. Policies and procedures should address the issue of overriding the data capture systems and should clearly delineate who has authority to override the systems and under what circumstances.

(v) A bank must have in place policies (as part of its operational risk management framework) relating to its AMA data requirements. These policies must be clearly documented and may vary by types of data. Specifically, the policies must address data quality and align with the corporate data management framework.

(vi) A bank must have transparent and verifiable processes for collecting relevant data inputs on an ongoing basis, with associated review and approval processes. These processes must be consistent, timely and comprehensive across the bank.

(vii) Assessments of the appropriateness and relevance of data are to be undertaken on a regular basis and must form the basis of any justification for the exclusion of data from the operational risk measurement system. These assessments must be transparent and clearly documented.

(viii) To maintain data integrity, a bank must have transparent and verifiable processes to review and approve data adjustments as circumstances require. Such adjustments must be well documented. Where the bank makes material adjustments to data, the bank must be able to justify to RBI that these adjustments are made for the purpose of ensuring that data utilised within the model better reflects the environment

in which the bank operates.

(ix) The operational risk data inputs used by a bank in the calculation of its Operational Risk Regulatory Capital (ORRC) must be subject to independent review both initially (that is, at the time the AMA approval is sought) and at **least annually**, to ensure the continued quality of the data and the effectiveness of internal controls. Reviews must include an assessment of the controls surrounding the data collection and maintenance processes, as well as data inspection.

8.5.4.3 Internal Loss Data

(i) The collection, tracking and use of internal loss data is an essential prerequisite to the development and functioning of a credible and robust ORMS.

(ii) Internal loss data is crucial for tying the operational risk measure of a bank to its actual loss experience. This can be achieved, in a number of ways, including using internal loss data as -

(a) the foundation of empirical risk estimates; or

(b) a means of validating the inputs and outputs of the ORMS; or

(c) the link between loss experience and operational risk management and control decisions.

(iii) The bank shall have documented policies and procedures for assessing the ongoing relevance of historical internal loss data, including situations where scaling, judgement overrides or other adjustments may be used, to what extent they may be used and who is authorised to make such decisions. The policies and procedures should identify when an operational risk event becomes an operational risk loss for the purpose of collection within the operational risk loss database and when it is to be

included in the calculation data set. The policies and procedures should provide for consistent treatment across the bank.

(iv) A bank's internal loss data must be comprehensive in that it captures all material losses from all appropriate business activities and geographic locations. The bank must be able to justify that any excluded activities or losses, both individually and in aggregate, would not have a material impact on the overall estimate of the ORRC.

(v) A bank adopting the AMA shall have a minimum five-year observation period of internal loss data requirement whether the internal loss data is used to build the operational risk measure or to validate it. The five-year loss data should be available with the bank for building the operational risk measure or to validate it before making a formal application to RBI for implementing AMA. However, when a bank first moves to an AMA, a 3-year historical data window may be allowed, subject to written approval by RBI.

(vi) When granting a bank approval to adopt the AMA, the RBI may require a bank to apply additional margins of conservatism if it is of the view that the data series of the bank is insufficient.

(vii) A bank shall ensure that its internal loss data collection processes meet the following standards:

a) The bank shall be able to map its internal loss data into the relevant **Level 1** business lines defined in **Appendix 3** and the relevant **Level 1** loss event type categories defined in **Appendix 2** and to provide these data to the RBI upon request.

b) The bank shall document the objective criteria for allocating losses to the specified business lines and loss event type categories. However, it is left to the bank to decide the extent to which it applies these categorisations in its internal operational risk measurement system.

c) The internal loss data of the bank shall be comprehensive in that it captures all material activities and exposures from all appropriate sub-systems, business activities and geographic locations.

d) The bank shall document and be able to explain and justify that any excluded activities or exposures, both individually and in combination, would not have a material impact on the overall risk estimates of the operational risk capital requirement.

e) A bank may record various dates in connection with the internal loss data. However, a consistent choice of relevant date of loss event is important to ensure compliance with the minimum observation period of 5 years laid down in the AMA framework. A bank may choose to use any of the following dates for building the calculation data set, so long as this is followed consistently:

- Date of occurrence
- Date of discovery
- Date of recognizing a contingent liability
- Date of recording the loss/provisions in the books

However, banks should not exclude large losses from the data base simply because they fall outside the observation period. For instance, if a bank uses the date of occurrence for deciding the 5 year period, any large losses which occurred more than 5 years back and are known to the bank, should be included in the calculation dataset.

In case of legal losses, it would be appropriate to model the data with reference to date of making provisions as is the practice generally prevailing internationally.

f) Similarly, in the case of losses where the recoveries take place after a long period of time and the bank is using 'net loss' for modeling, the recoveries after a very long period should be ignored and the data point should not be updated for such recoveries. Banks may document a policy for this purpose and follow that consistently.

(viii) The internal capture of **near miss events** (where no financial loss was incurred), while not generally required to be included in the calculation of operational risk capital requirements data set, could nevertheless be useful in increasing awareness of the operational risk

profile and improving ORM processes. A bank should therefore develop procedures to identify such events. (Refer **Part A of Appendix 1**).

(ix) A bank shall establish one or more appropriate *de minimis* gross loss thresholds which may vary in the bank across business lines or loss event types, for the collection of internal loss data. The bank is responsible for defining the thresholds for an ORC. However, no bank will fix a threshold above **Rs. 50,000** for any of the business classes or loss event types. The bank should be able to demonstrate that the established thresholds meet the following requirements:

(a) The thresholds are reasonable and appropriate for the operational risk management and measurement principles.

(b) The thresholds do not adversely impact the credibility and accuracy of the operational risk measure (i.e. any internal loss data below the *de minimis* gross loss threshold not captured, both individually and in combination, would not have a material impact on the overall operational risk estimates). The bank should have a methodology to satisfy itself and RBI that the exclusions of losses below the thresholds from the statistical modelling does not materially affect the shape of the loss distribution and consequently the measurement of operational risk capital.

(c) The thresholds should result in a significant proportion of the internal operational risk losses being captured.

(d) If a bank experiences a large number of small losses below a threshold such that collectively these form a significant portion of total operational losses, these should be collected and grouped at least for the purpose of operational risk management.

(e) In determining a threshold, the bank should also take into account

- its approach to operational risk management and measurement for regulatory capital purposes;
- the use of the internal loss data for ORM;
- the ability to reconcile the loss data with the accounting data;
- the fact that the threshold for business lines which experience a large number of smaller losses should generally be relatively lower;
- the administrative requirements placed on the business lines and operational risk resources as a consequence of

the data collection and management processes;

- ability to demonstrate that the bank is able to avoid potential biases in the estimation of model parameters, explicitly taking into account the incompleteness of the calculation data set due to the presence of thresholds; and
- the bank is able to calculate expected loss for each risk class.

(x) A bank must include in its operational risk loss database all operational risk related losses in excess of the bank's specified loss threshold(s).

(xi) The bank should decide upfront whether it would model the operational risk losses 'gross of recoveries other than insurance' or 'net of all recoveries'. A conservative treatment would be to model losses based on the gross loss without adjustment for any recovery including insurance recovery. In case a bank decides to adjust the gross loss for recoveries other than insurance, the recoveries should be considered conservatively.

(xii) The Gross Loss should *inter alia* include any direct charges to Reserves due to operational losses, all expenses incurred as a consequence of operational risk events, provisions made, penalty and fines. General maintenance costs, cost of renovations and normal repairs, insurance premiums and costs connected with operational risk losses which are treated as credit risk losses for capital adequacy purpose may be excluded from operational loss database used in AMA model.

(xiii) The amounts lost and recovered before the close of business the same day may not be included in the operational loss data base; it may be treated as near misses. There is general reluctance to report such events. However, reporting of such events is crucial for sound operational risk management. In order to encourage reporting of such near misses, banks may formulate suitable policies e.g. not taking any disciplinary action for the first few incidents and linking the disciplinary action with the amount involved. Detection during the AFIs of banks or

otherwise of incidents of non-reporting of such events will be viewed seriously by RBI.

(xiv) If an operational loss event affects the assets or any other accounts which are subject to mark to market, the amount considered as gross loss would be the amount by which the P&L of the bank is impacted.

(xv) In the case of fixed assets, the gross loss amount would be the replacement cost[4].

(xvi) Banks should also formulate policies for collecting data and information relating to near miss events, operational risk gain events and opportunity costs of operational risk events in terms of loss revenues[5] and use them appropriately in the scenario analysis.

(xvii) Apart from information on gross operational loss amount, the date of the operational loss event, any recoveries of gross operational loss amount, the bank should collect some descriptive information about the drivers or causes of the operational loss event. The level of detail of any descriptive information should be commensurate with the size of the gross operational loss amount. The bank may consider including the following additional information:

- description of loss event;
- loss event type category;
- discovery date of the loss;
- where the loss is reported and expensed;
- event end date;
- management actions;
- adjustments to the loss estimate.

---

[4] Replacement cost would mean the cost incurred by the bank in acquiring the new asset to replace the damaged asset, carrying out major repairs consequent upon the damage, or reconstructing the asset.

[5] Opportunity costs/lost revenues would mean operational risk events that prevent undetermined future business from being conducted (e.g. unbudgeted staff costs, forgone revenue, and project costs related to improving processes), are important for risk management but not for quantification.

(xviii) A bank should be able to identify operational risk events which are covered in the existing insurance policies, in the regulatory capital calculation data set.

(xix) A bank shall develop specific criteria for assigning loss data arising from an operational risk loss event in a centralised function (e.g. information technology department) or an activity that spans more than one business line, as well as from related events over time, in accordance with the following:

(a) when capturing losses that span more than one business line, the bank may decide to assign the entire loss to one business line, for example, where the impact is the greatest, or apportion the loss across several affected business lines. Regardless of the treatment, the method used should be well reasoned and sufficiently documented; and

(b) the bank should have policies in place to describe the identification, capture and treatment, for the purpose of its operational risk loss database and operational risk management and modelling, of a series of operational loss events that are related events over time.

(xx) A bank should have a clear policy that allows for the consistent treatment of loss event classifications (e.g. credit, market or operational risk) across the bank. It is essential for the bank that captures loss events that are treated differently for regulatory capital and management purposes to demonstrate that

(a) loss events are being captured consistently across the bank; and

(b) data systems are sufficiently advanced to allow for this differential treatment of loss events.

(xxi) A bank shall continue to treat operational risk losses that are related to or have characteristics of credit risk, and have historically been included in the credit risk databases of the bank (e.g. collateral management failures) as credit risk for the purposes of calculating the minimum regulatory capital requirement under the Basel framework. These losses will not be subject to the operational risk capital

requirement[6], provided that these losses are subject to the credit risk regulatory capital framework.

(xxii) For the purposes of internal operational risk management, a bank should identify all material operational risk losses consistent with the scope of the definition of operational risk as set out in paragraph 1 and the loss event types listed in **Appendix 2**, including those related to credit risk. Such material operational risk-related credit risk losses should be flagged separately within the operational loss database of the bank. The materiality of these losses may vary between banks as well as within a bank across business lines or loss event types. Materiality thresholds should be broadly consistent with those used by peer banks and set with reference to the credit risk management processes of the bank.

(xxiii) Operational risk losses that are related to market risk must be treated as operational risk for the purpose of calculating the bank' s minimum ORRC.

(xxiv) A bank will be required to implement appropriate processes and controls surrounding the collection of internal loss data so as to ensure that data collected is sufficiently complete and accurate.

8.5.4.4 Relevant External Data

(i) A bank's operational risk measurement system should use relevant external data (either public data or pooled industry data or both), especially when there is reason to believe that the bank is exposed to infrequent, yet potentially severe, operational risk losses.

(ii) Where internal loss data is limited, relevant external data may be a useful input in determining the level of operational risk exposure of a

---

[6] This applies to all banks, including those that may only now be designing their credit risk and operational risk databases.

bank. Even where relevant external data is not an explicit input to the calculation data set of the bank, such data provides a means for the bank to understand industry experience, and in turn, provides a means for assessing the adequacy of its internal loss data. Relevant external data may be used to enhance scenario analysis, fit severity distributions or benchmark operational risk exposure results.

(iii) A bank shall have policies and procedures that provide for the use of relevant external data.

(iv) A bank shall have a systematic and robust process for -

(a) collecting, assessing and incorporating relevant external data into the ORMS;

(b) determining situations for which relevant external data should be used; and

(c) determining the methodologies used to incorporate the data (e.g. scaling, qualitative adjustments or enhancing scenario analysis).

(v) Relevant external data should include data on actual loss amounts, information on the scale of business operations where the event occurred, information on the causes and circumstances of the loss events, or other available information that would assist in assessing the relevance of the loss event to the bank.

(vi) A bank should ensure that the external data used is appropriate, not affected by reporting bias, and relevant to the business and operational risk profile of the bank. The bank should also have a well-defined process to scale the loss amounts as considered appropriate. The scaling process should be systematic, statistically tested and generate outcome consistent with the operational risk profile of the bank.

(vii) Banks should apply appropriate filtering process to ensure the relevance of data. The filtering process should be applied consistently and any exceptions thereto should be documented and supported with rationale.

(viii) A bank shall regularly review, document and conduct periodic independent reviews on the conditions and practices for the use of relevant external data.

(ix) The use of external loss data must include the consideration of infrequent yet potentially severe operational risk loss events.

8.5.4.5 Scenario analysis

(i) Scenario analysis offers a means to impart a forward-looking element to the process of estimation of operational risk losses. A bank shall use scenario analysis of expert opinions in conjunction with relevant external data to evaluate its exposure to high-severity loss events.

(ii) Scenario analysis is a systematic process of drawing on the knowledge and obtaining expert opinions from experienced business line managers and risk management experts to derive reasoned assessments of the likelihood and impact of plausible high-severity operational losses. For instance, these expert assessments could be expressed as parameters of an assumed statistical loss distribution.

(iii) Scenario analysis is especially relevant for business lines, activities or operational loss event types where internal and relevant external loss data or assessments of the Business Environment and Internal Control Factors (BEICFs) do not provide a sufficiently robust estimate of the exposure of the bank to operational risk. (Please see paragraph 8.5.4.6 for detailed description of BEICFs).

(iv) Scenario analysis should be used to assess the impact of deviations from the dependence or correlation assumptions embedded in the ORM framework, in particular, to evaluate potential losses arising from multiple simultaneous operational risk loss events.

(v) The set of developed scenarios should be comprehensive and capture all material sources of operational risk across business activities and geographic locations.

(vi) A bank shall have a robust process in place for developing scenarios and apply the process consistently across the bank.

(vii) There should be policies and procedures in place for determining the methodologies for incorporating scenario analysis into the ORMS. They should cover key elements of scenario analysis, such as the manner in which the scenarios are generated, the assumptions used, the frequency with which they are updated and the scope and coverage of operational risk loss events they are intended to reflect. The process for conducting scenario analysis and the results should also be clearly documented.

(viii) A bank should ensure that the process by which the scenarios are determined is designed to reduce as much as possible subjectivity and biases. In particular –

(a) The assumptions used in the scenarios should be based, as much as possible, on empirical evidence. These assumptions and processes should be well-documented. Relevant internal and external data available should be used in building the scenario; and

(b) The bank should explain the rationale behind the level at which scenarios are studied and/or the units in which they are studied.

(ix) A bank shall have a process in place for regularly reviewing the developed scenarios and assumptions to ensure that they continue to adequately reflect the operational risk profile of the bank. Scenarios should be regularly validated and re-assessed through comparison to actual loss experience to ensure their reasonableness.

(x) In order to assess the effectiveness of their scenario building process and its outcomes, banks should subject them to one or more of various challenge functions, some of which are indicated below:

- Review by risk control function

- Review by an internal or external auditor
- Review by business peers
- Comparison with other data elements(internal loss data, external loss data, BEICFs)
- Comparison with experience or expertise

(xi) The bank should lay down clear mechanism for mitigating the biases inherent in the scenario building processes.

8.5.4.6 Business Environment and Internal Control Factors ("BEICFs")

(i) In addition to using operational risk loss data, whether actual or scenario-based, a bank's operational risk measurement system must incorporate indicators of the bank's operational risk profile, as well as other information related to the assessment of the bank's internal control framework collectively termed as **Business Environment and Internal Control Factors (BEICFs).** BEICFs are indicators of a bank's operational risk profile that reflect underlying business risk factors and an assessment of the effectiveness of the internal control environment. Like scenario analysis, they provide a forward-looking element to an AMA by considering Business Environment indicators (e.g. the rate of growth, employee turnover, and new product introductions) and Internal Control Factors (eg findings from the challenge process, internal audit results, and system downtime). Accordingly, these factors must be responsive to changes in the bank's operational risk profile and reflect potential sources of operational risk.

(ii) Incorporating BEICFs into an AMA framework endeavours to ensure that key drivers of operational risk are captured and that a bank's operational risk capital estimates are sensitive to its changing operational risk profile. Typically, BEICFs are integrated into the AMA framework as a tool to improve risk management and as a part of the risk measurement

process. When used for risk measurement, BEICFs are used directly (i.e. scorecards) as an input into the modelling process to derive the initial operational risk capital amount, or indirectly as an input to the operational risk modelling. BEICFs are also used as an *ex post* adjustment to corporate level or business line allocations of operational risk capital, based on the underlying change in the business or internal control environment. BEICFs are often indirectly used as an input into the scenario analysis process.

(iii) BEICFs can be used as an input into the scenario analysis process by incorporating an objective measure relating to BEICFs (e.g. RCSA, Scorecards, KRIs) to find what scenarios to make and/or to determine the frequency and severity of individual scenarios.

(iv) Alternatively, BEICFs can be used for identifying material changes to the risk profile (e.g. identification of control weaknesses, or changes to the business environment), and hence 'trigger' a review of the ORC estimate i.e. condense them into an ex-post add-on/ qualitative adjustment factor after capital/ VaR has been calculated. The AMA figure coming from the other 3 elements (i.e. internal loss data, external loss data, and Scenario Analysis) may be adjusted up or down on the basis of the change occurred during the last year to the BEICFs; i.e. banks may calculate the values of each BEICF in a year compared to that of the previous year and determine the year's average change across all the BEICFs. If there is an increase of the volume factors indicating enhancement of risks as a result of changes in business environment and/or a decrease of the control factors, the capital may be adjusted upwards, and vice versa. However, the size of adjustments may be limited to maximum of (+) or (-) 10% of the AMA capital before applying the adjustment.

(v) Each business environment and internal control factor must have reporting thresholds to ensure there is an effective process that can identify key material risks in a transparent manner and enable the bank to react appropriately.

(vi) A bank should be able to justify its choice of each business environment and internal control factor as a relevant driver of operational risk, based on considerations of historical experience and involving the expert judgement of relevant business areas.

(vii) Business environment and internal control factors are required to recognise both improvements and deterioration in the bank's operational risk profile. The operational risk measurement system must capture potential increases in risk due to greater complexity of activities or increased business volume as well as capturing changes in risk due to improvements in internal controls. Changes in the bank's internal processes and risk management procedures should be similarly taken into account.

(viii) A bank must be able to justify the relationship between changes in its measures of operational risk and changes in its business environment and internal control factors. The bank must also be able to justify the relative weighting of the various factors within its operational risk measurement system.

(ix) The framework and application of BEICFs and the outcomes, including the supporting rationale for any adjustments to empirical estimates, is required to be documented and subject to independent review and validation.

(x) Where possible, business environment and internal control factors should be translated into quantitative measures that lend themselves to verification. The bank will be required to compare its estimates of these factors with actual internal operational risk loss experience.

8.5.5 Distributional Assumptions*

8.5.5.1 Distributional assumptions underpin most, if not all, operational risk modelling approaches and are generally made for both operational risk loss

severity and the frequency of operational risk loss events. One of the considerations in a bank's choice of distributions is the existence and size of the threshold above which data are captured and modelled. Modelling of operational risk exposures is still relatively new and a common view of appropriate severity distributional assumptions is yet to emerge. The severity of operational risk loss data tends to be heavy-tailed and methodologies for modelling operational risk must be able to capture this attribute. However, a bank's choice of distribution will have a significant impact on operational risk capital, as will the statistical method used for fitting that distribution. Similarly, a bank's choice of data threshold may significantly impact the appropriateness of the chosen distributions and/or its estimation method, and consequently the bank's operational risk capital.

---

*For further guidance and an overview of the literature on the topic, banks may refer to BCBS Consultative Document titled 'Operational Risk-Supervisory Guidelines for the Advanced Measurement Approaches', December, 2010 and Chernobai,A., Rachev, S.T. and Fabozzi, F.J. :"Operational Risk – A Guide to Basel II Capital Requirements, Models and Analysis" (Wiley Finance, 2007)

8.5.5.2 Generally, the severity and frequency distributions are modelled separately. For estimating severity distributions, range of distributions exists. AMA may use more than one approach to estimate severity of the body, tail and entire distribution. More common distribution used to model severity are lognormal, Weibull, empirical and Generalised Pareto distribution. The Poisson distribution is by far the most widely used distribution for modeling the frequency of operational losses, followed by the negative binomial distribution.

8.5.5.3 Due to being heavy tailed, the severity distributions have greater role in influencing the regulatory capital number than the frequency distributions. Banks should document the process of selection of the distribution to represent both severity and frequency. Typically, the process of selection of an appropriate distribution should begin by Exploratory Data Analysis (EDA)

for each of the ORC to get an idea of the statistical properties of the data and select the most appropriate distribution. This may be followed by use of appropriate techniques to estimate the parameters of the chosen distribution. The quality of fit should be evaluated with appropriate statistical tools. While doing so special attention may be paid to the techniques which are more sensitive to the tail of the distribution.

8.5.5.4 Both graphical and quantitative EDA techniques may be used. Graphical techniques used in EDA include a wide range e.g. histograms, autocorrelation plots, Q-Q plot, density estimate, empirical cumulative distribution function, regression analysis etc.

8.5.5.5 When selecting a severity distribution, positive skewness and leptokurtosis of the data should be specifically taken into consideration. In the case of heavy tailed data, use of empirical curves to estimate the tail region may be inappropriate. In such cases, sub-exponential distributions whose tails decay slower than the exponential distributions may be more appropriate.

8.5.5.6 The determination of appropriate body-tail modelling threshold will be very important when banks model the body and tail of the loss distribution separately. It would also be equally important to ensure that only sound methods are employed to connect the body and tail of the distribution.

8.5.5.7 There exist a number of estimation techniques to fit the operational risk models to historically available operational loss data. These include maximum likelihood estimation, Cramer-Von Mises statistic, the Anderson-Darling statistic, Quantile Distance Estimation method. Banks should use appropriate method (s) taking into consideration the nature of loss data as revealed by EDA.

8.5.5.8 It is difficult to use close-form solutions to generate aggregate distributions of operational losses. Therefore, simulations, numerical or approximation methods may be necessary to derive aggregate loss distributions. Monte carlo-simulations, Fourier Transform-related methods,

Panjer algorithm and Single Loss Approximations may be mentioned in this regard.

8.5.6 Use of Vendor Models

8.5.6.1 Vendor models would be held to the same minimum validation standards as internally developed models for generating frequency and severity distributions. The onus of demonstrating this to the RBI will be on the bank. In cases where the bank uses a vendor-supplied model, the bank shall ensure that it obtains from the vendor and has on record the mathematical and statistical basis of the risk measurement model. The bank shall also ensure that the staff responsible for calculating the operational risk capital requirements using the model understands the model including its mathematical and statistical basis and key assumptions thoroughly. In particular, where vendor models are used, the bank should:

a) document and explain the role of the vendor model and the extent to which it is used within the operational risk measurement system of the bank;

b) demonstrate a thorough understanding of the vendor model;

c) ensure that the vendor model is appropriate for measuring the operational risk of the bank, given the nature of the portfolio and the capabilities of the staff; and

d) have clearly described strategies for regularly reviewing the performance of the vendor model.

8.5.6.2 A bank shall not use a risk measurement model obtained from a third-party vendor that claims proprietary technology as a justification for not providing the documentation or any other details of the model to the bank. The use of such models will not be considered by the RBI as a ground for exemption from complying with the requirements of these guidelines.

8.5.7 Diversification Benefits

A bank may, with the prior approval of RBI, incorporate a well-reasoned estimate of diversification benefits factored in at the group-wide level or at the banking subsidiary level. However, any banking subsidiaries whose host

supervisors determine that they must calculate stand-alone capital requirements may not incorporate group-wide diversification benefits in their AMA calculations (e.g. where an internationally active banking subsidiary is deemed to be significant, the banking subsidiary may incorporate the diversification benefits of its own operations-those arising at the sub-consolidated level- but may not incorporate the diversification benefits of the parent).

9. Risk Mitigation

9.1 A bank may recognise the risk mitigating effect of insurance when calculating operational risk regulatory capital requirements, subject to approval from the RBI. The recognition of insurance mitigation will be limited to 20% of the total operational risk capital requirement calculated under the AMA.

9.2 To recognise insurance as an operational risk mitigant, a bank must be able to demonstrate that the insurance will cover potential operational risk losses included in the operational risk measurement model in a manner equivalent to holding ORRC. This will require that the insurance coverage satisfy the criteria laid down in paragraph 9.2.1 to 9.2.9.

9.2.1 The provider of the insurance policy must have a minimum claims paying ability rating of A or equivalent.

9.2.2 The insurance policy has an initial term of no less than one year. For a policy with residual term of less than one year, the bank shall make appropriate haircuts reflecting the declining residual term of the policy, up to a full 100% haircut for policy with a residual term of 90 days or less.[7]

9.2.3 The insurance policy has a minimum notice period for cancellation of 90 days.

---

[7] Where an insurance policy has an initial term greater than or equal to one year and the residual term is between 90 and 365 days, the amount of insurance recognition will be subject to the following haircut:
(365 - residual term of insurance contract (in days))/275

9.2.4 The insurance policy has no exclusions or limitations triggered by any action of any regulatory authority or, in the case or a failed bank, that preclude the bank, receiver or liquidator from recovering for damages suffered or expenses incurred by the bank, except in respect of events occurring after the initiation of receivership or liquidation proceedings in respect of the bank.

9.2.5 The insurance policy may exclude any fine, penalty, or punitive damages resulting from action of any regulatory authority.

9.2.6 The risk mitigation approach and calculations reflect the insurance coverage of the bank in a manner that is transparent in its relationship to, and consistent with, the actual likelihood, impact and severity of operational loss used in the overall determination of the bank of its operational risk capital requirement.

9.2.7 The insurance is provided by a third party. In the case of insurance provided by captive insurers, related corporations and major stake companies of the bank, the exposure has to be laid off to an independent third party, for example through re-insurance that fulfils the requirements as set out in this paragraph.

9.2.8 The bank has in place policies and procedures for determining the risk mitigating effects of insurance within its ORMS. The framework for recognising insurance should be well reasoned and documented.

9.2.9 The bank discloses a description of its use of insurance for the purpose of mitigating operational risk in the policies and procedures.

9.2.10 The methodology of a bank for recognising insurance risk mitigation under the AMA also needs to capture the following elements through appropriate discounts or haircuts in the amount of insurance recognition (Refer to **Part D of Appendix 1**):

(i) the residual term of a policy, where less than one year, as noted above;

(ii) a policy's cancellation terms, where less than one year,

including the possibility that the policy can be cancelled before the contractual expiration;

(iii) the uncertainty of payment, including the willingness and ability of the insurer to pay on a claim in a timely manner and the legal risk that a claim may be disputed; and

(iv) any mismatches in coverage of insurance policies.

9.2.11 A bank should keep the use of insurance under review and recalculate the operational risk capital requirement, if appropriate, in the event that the nature of the insurance or the coverage changes significantly. The bank should notify the RBI of material changes in the coverage of the risk mitigating effect of insurance under the AMA.

9.3 Banks should also follow the guidance contained in BCBS Paper titled 'Recognising the risk-mitigating impace of insurance in operational risk modelling' October 2010.

10. Sensitivity Analysis

10.1 A bank must have in place a comprehensive and rigorous program of sensitivity analysis of its operational risk measurement model. Sensitivity analysis must include consideration of the sensitivity of the bank's ORRC to changes in modelling choices, assumptions and data inputs (including internal data, external data, scenarios and business environment and internal control factors).

10.2 The results of sensitivity analysis undertaken must be reflected in a bank's policies and methodology documentation and be communicated to senior management and the bank's Board, or Board committee, on a regular basis.

11. Internal Validation

11.1 Internal validation encompasses a range of processes and activities that contribute to the internal assessment of a bank of whether it is capable of deriving consistent and predictive estimates of AMA parameters. A bank has

primary responsibility for internal validation and should demonstrate to the RBI that its internal validation is robust and likely to remain so. A bank shall perform an internal validation of the ORMS at least annually.

11.2 The bank should be able to ensure the validity of the ORMS, and its underlying assumptions at the development stage and following significant changes in methodology and assumptions, and it should be able to ensure the validity of the inputs and outputs on an ongoing basis.

11.3 A bank should have the capacity to perform internal validation of the ORMS by its own staff who is not involved in the development of AMA model or execution of a vendor supplied AMA model. However, considering that Indian banks are new to the quantification of operational risk losses, for the present, the internal validation may also be performed by external parties, as long as the bank retains ultimate responsibility. The internal validation function, whether internally or externally performed, should be staffed by qualified persons. However, banks should build the expertise for internal validation by their own staff in due course.

11.4 A bank should establish a clear methodology for internal validation. This methodology should be appropriate for the bank and its ORM framework. The bank should be able to explain and justify its methodology.

11.5 A bank should periodically analyse its internal validation methodology to ensure that it remains appropriate. In particular, certain parts of the ORMS should be revalidated at least **annually** and whenever there is a significant change in the operational risk profile of the bank and in the ORMS methodology or assumptions.

11.6 Internal validation should be clearly documented. This documentation should provide a detailed outline of the internal validation methodology (including its frequency) and outline any identified weaknesses.

11.7 Internal validation techniques should take into account the changing market and operating conditions.

11.8 Internal validation should encompass both quantitative and qualitative estimates of the AMA elements and cover key operational risk processes and

systems.

11.9 Internal validation processes and outcomes should be subjected to independent review by both internal and external auditors.

11.10 The internal validation of the ORMS by the bank should include, at the minimum, the elements described below:

(i) regular comparison of realised outcomes with estimates of the AMA elements, using historical data over as long a period as possible;

(ii) use of appropriate validation methodology and tools, quantitative or otherwise, and comparison with relevant (i.e. in terms of appropriateness, timeliness and time period) external data sources where applicable;

(iii) well-articulated internal validation standards for the input of data into the ORMS to ensure the accuracy, completeness and relevance of the estimates of the AMA elements, data feeds and processes associated with the ORMS, and to distinguish situations where deviations in realised outcomes from estimates of the AMA elements become significant enough to call into question the predictability of the estimates of the AMA elements;

(iv) monitoring the performance and stability of the ORMS and reviewing the inherent statistical relationships and assumptions of the ORMS;

(v) ORMS validation should ensure that the relationship between the inputs and outputs of the ORMS are stable and logical, and that the techniques underlying the ORMS are transparent and intuitive;

(vi) validation of material data above the thresholds to ensure that they are comprehensive, appropriate and accurate. Validation should cover all data types including actual data, constructed data, figures generated by scenario analysis and BE&IC. Particularly for constructed data, validation should ensure that the assumptions are unbiased and the results are realistic; and

(vii) internal validation should include testing and verifying adjustments to operational risk capital requirement estimates, including operational risk exposure as well as assumptions underlying operational risk exposure, AMA models and operational risk regulatory capital

requirement.

12. External Validation

External validation of **ORMS** by third parties may be done in addition to the internal validation by the bank's own staff. In cases where the internal validation has been performed by the external parties, no additional validation by the external parties is required. External validation will also broadly comprise the same elements as indicated in paragraph 11 above. However, external parties will be free to make observations on any other aspect relevant for ORMS they may consider appropriate. In cases where the internal validation is performed by the bank's own staff, the external validation of ORMS may be performed once in two years and as and when there are major changes to the ORMS.

13. Independent Review of ORMF and ORMS by Internal Auditors

13.1 The Internal Auditors of a bank should review the entire ORMF including the ORMS with a special focus on verification of the internal validation processes of ORMS. They should ensure that validation processes are implemented as designed and are effective. It will not be necessary for the internal auditors to perform independent validation of the AMA model, which would have already been carried out by the internal validation unit and /or external parties. In performing their role, the internal auditors of a bank may seek the assistance of other internal or third-party specialists, in cases where the bank's internal audit function is not equipped to carry out the review. However, the overall responsibility will remain with internal auditors.[8] In due course, the bank should endeavour to equip its internal audit function with necessary skills to perform the internal audit independently.

[8] The RBI regards this as a key standard expected of any bank adopting AMA.

13.2 In the event where internal auditor has sought assistance from internal or external specialists in the review process, the specialists involved in performing substantive assessment of internal validation should not be involved in or responsible for -

(a) the design, selection or implementation of the ORMS;

(b) the process for deriving and using estimates of the AMA elements; and

(c) the origination of risk exposures.

13.3 The internal audit of a bank should conduct reviews of the internal validation of the ORM framework of the bank at least **annually**. The review should at least cover aspects of the internal validation related to the operations and processes of the ORMF. The internal audit should conduct checks to attest to the depth, scope and quality of the work of ORMF to ensure that its findings are well founded. In particular, the checks should cover the process of the bank for estimating, documenting and justifying the estimates of the AMA elements used to calculate minimum operational risk capital requirements under the AMA, given that it is an important area which affects regulatory capital requirements. The internal audit should also ensure that the person or group of persons involved in internal validation of the ORMF is independent from those involved in developing that framework and is able to provide objective and effective challenge.

13.4 The internal audit should –

(a) document the scope of its review, its assessment of the ORM framework of the bank and the findings and recommendations in respect of its oversight of internal validation;

(b) proactively discuss its findings and recommendations in respect of its oversight of internal validation with senior management of the bank;

(c) report important findings to the Audit Committee on a timely basis; and

(d) monitor the implementation of the recommendations accepted by the Audit Committee and report incidences of non-implementation to the Audit Committee.

13.5 The Audit Committee of a bank should ensure that the internal auditors are adequately qualified and trained to assume oversight responsibilities of the internal validation process. It is important that the internal auditor is familiar with the strategy and processes of the Bank for identifying, assessing, monitoring, controlling, and mitigating operational risk.

13.6 No person responsible for some or all aspects of the ORM framework within the bank should participate in the oversight of internal validation relating to these aspects.

14. Independent Review of ORMF and ORMS by External Auditors

In addition to internal review, the ORMF and ORMS should be reviewed by the External Auditors also, at least **once in two years**. The aspects covered would be the same as mentioned in paragraph 13. However, if internal review/audit has been carried out with the help of the external parties as indicated in paragraph 13, separate external audit is not necessary. The external auditors which have carried out external validation of the ORMS should not carry out external review of ORMF and ORMS.

15. Sufficient Resources in the Use of the AMA

To effectively manage and measure operational risk throughout a bank, a bank should have sufficient resources in the use of the AMA in the business lines, ORMF, internal validation functions as well as audit areas, so as to sufficiently monitor and enforce compliance with the operational risk policies and procedures. A bank should ensure that there are appropriate, adequate and qualified staff with the necessary experience and technical capabilities and adequate technical resources allocated to support the ORMF.

16. Application for Migration to AMA and RBI's Assessment

16.1 The bank desirous of migrating to AMA will submit a detailed application (as per format to be provided by RBI at the time of receiving a 'letter of intent') long with the following documents:

a. Cover letter requesting approval;

b. Copy of the Board Resolution approving submission of application for migrating to AMA to RBI;

c. Detailed application format duly filled in;

d. Confirmation from the executive officer responsible for risk management in the bank;

e. Confirmation from the executive officer responsible for internal audit in the bank;

f. Documentation of planned operational risk measurement systems (including models used); and

g. Control environment of the operational risk measurement system, implementation procedures, and IT infrastructure.

h. Implementation plan (including Roll-Out)

i. Self-assessment.

16.2 To decide on an application, RBI would need an overview of the models that the bank plans to use and how they will be implemented in the bank's policies and procedures, and detailed information on the construction and calibration of the models, the database, the technological environment, and related policies and procedures, including the bank's control environment. The documents mentioned above are considered to be supporting material. Unless otherwise indicated, the supporting material should be general information about the implementation of the chosen risk measurement approach. The supporting material provides a summary of the institution's current or planned practices in sufficient depth to enable the supervisor to

make an initial supervisory assessment of the application, and to develop a risk-based plan for a more thorough assessment which would entail after the preliminary scrutiny of the application.

16.3 Cover Letter

The cover letter should state that the bank applies for the permission to use the AMA for computing the regulatory capital for operational risk. The letter should also confirm that the material attached to the application is a true and fair. The letter should be signed by the Executive Director of the bank who has the authority to commit the institution.

16.4 Confirmation from the Executive Officer responsible for Risk Management

The written confirmation from the executive officer responsible for risk management in the bank would state that -

(a) the bank has conducted an internal assessment and has ascertained that it fulfils the requirements set out in this Annex;

(b) the use of AMA forms an integral part of the process and system of the bank for managing operational risk;

(c) the bank has carefully considered the implications of the use of AMA on operational risk assessment and capital management;

(d) the bank has a process for continually determining the suitability of its ORMF and its ORMS, taking into account such regulations and guidelines that the RBI may issue from time to time;

(e) the bank has a policies, process to calculate the ORRC requirement for any AMA exposure using the BIA or TSA or ASA within a reasonable timeframe[9] if required by the RBI;

(f) the bank has policies, procedures and controls to calculate its operational risk capital requirement under the AMA accurately and that those policies, procedures and controls are subject to internal audit at least annually; and

(g) the AMA rollout plan of the bank is in accordance with paragraph 2 of this Annex. Where a bank is unable to comply with paragraph 2, it shall demonstrate to RBI that it faces exigencies that are material and relevant;

---

[9] In general, RBI would expect banks to be able to calculate the operational risk capital requirement for any AMA exposure using the BIA or TSA within a 3-month period.

16.5 Confirmation from the Executive Officer Responsible for Internal Audit

16.5.1 The written confirmation from the executive officer responsible for internal audit of the bank would state that -

(a) the auditors agree with the confirmation by the executive officer responsible for operational risk management; and

(b) the bank has conducted an internal and/or external validation (pursuant to this Annex) and has ascertained that it has the systems, processes and controls necessary for adopting AMA[10].

16.6 Documentation of ORMS

16.6.1 For an AMA application, it is essential that the documentation of operational risk measurement systems include at least:

a. A list of all internal documents held by the applicant bank that it considers relevant to the application, including a brief description of their contents.

b. A map of the models to be used. For AMA, this means a statement that explains which operations and/or operational risks are covered by each model.

c. A general description of all the models. This can include a description of the types of data, including the four elements (see paragraph 8.5.4.1 of these guidelines), the definitions, classifications, and methodologies used, and quantitative and qualitative assessments.

d. The allocation of operational risk capital between different entities within the group, and the use of diversification effects.

e. If the institution uses capital relief tools, documentation should be provided on the coverage and measurement of expected loss, the institution's operational risk insurance policy or other risk transfer mechanisms, and the use of correlations.

16.6.2 The list of documents referred to above is intended to be a comprehensive list of all the institution's internal documentation underlying its

[10] In areas where a bank does not fully meet RBI's expectations, it should conduct self assessments to identify the key shortcomings and develop comprehensive action plans to address them before supervisory validation begins. Such action plans should include identifying the personnel responsible for specific actions, resource needs and a schedule for completion.

validation process (including documentation on external vendor models, if used) that the institution judges to be relevant to its application. RBI may request more detailed information, either in the initial application or at a later stage, to allow an effective assessment of the application. These documents, like all internal documentation, have to be made available to RBI upon request.

16.7 Control Environment

The documentation of the control environment, implementation procedures, and the Informational Technology (IT) infrastructure should include, at a minimum:

(a) An overview of the internal governance of the institution (i.e., the role and responsibilities of management, the functions of committees involved in governance of operational risk management function, and the role of Internal Audit).

(b) The planned use of operational risk measurement systems (how, in practical terms, banks plan to use different models in the operating activity).

(c) The responsibilities of the parties involved in modelling.

(d) An overview of the validation process.

(e) General information on the institution's IT structure, as far as AMA approach is concerned.

(f) Internal Audit and External Audit reports, as the case may be.

(g) ORMS validation report submitted by the internal validation unit (wherever applicable)

(h) ORMS validation report submitted by the external party (wherever applicable)

16.8 Implementation Plan

16.8.1 Banks intending to move to an AMA will submit a meaningful implementation plan (including rollout), to RBI as part of the application pack. The implementation plan is a commitment on the part of the bank to

implement the AMA on the specified dates for all of the operations for which it is seeking approval to use the AMA.

16.8.2 The implementation plan should contain internal rules with detailed provisions regarding time and content in regard to the following:

(a) Development of operational risk management processes, in particular for data collection;

(b) Development of the measurement methodology;

(c) Implementation of the IT infrastructure which is used for operational risk management and measurement purposes;

(d) Training of staff, including management staff; and

(e) The ‘use test.’

16.9 Self Assessment

16.9.1 The bank should carry out a self-assessment of its state of readiness based on the standards and minimum requirements set out in this Annex. It should develop an action plan to fill identified gaps and deficiencies, and a schedule for achieving compliance.

16.9.2 The self-assessment should begin with a global assessment, from a consolidated perspective, of how the various models fit together within the bank or the group, as the case may be. This global assessment should cover the suitability of the organizational structure in terms of internal governance, the adequacy of resources devoted to the operational risk measurement system, comparability across the group with respect to data and methodology, and consistency in IT organization.

16.9.3 The self-assessment should also cover all the aspects of the operational risk measurement system: methodology, quality of data, quantitative and qualitative validation procedures, internal governance, and technological environment. The self-assessment could be conducted by staff from an independent risk assessment function with the support, if necessary,

of auditors or a combination of all the resources including also the participation of external auditors and consultants.

16.10 Other Aspects

16.10.1 RBI may grant approval for a bank to adopt the AMA, subject to such conditions or restrictions as may be deemed necessary. The AMA approval may specify how the AMA is to apply in relation to a bank, including approvals under other paragraphs of this Annex. RBI's prior written approval is required for any material changes to the operational risk measurement model. Prior notification to RBI is also required for material changes to other components of the operational risk management framework.

16.10.2 Once a bank has obtained AMA approval, it shall continue to employ the AMA on an ongoing basis unless the AMA approval is revoked or suspended for some or all of the bank's operations. A return, at the bank's request to the lower approaches (BIA or TSA/ASA) will generally only be permitted in exceptional circumstances.

16.10.3 RBI may, at any time, suspend or revoke its approval to a bank to adopt the AMA, or impose any additional conditions if it determines that:

a. the bank has not fulfilled any of the conditions or restrictions specified in these guidelines or in any approval granted pursuant to paragraph 7.1.1; or

b. it is appropriate, having regard to the particular circumstances of the bank, to impose such additional conditions or order such suspension or revocation.

16.10.4 RBI may, at any time, in writing, require a bank with AMA approval to reduce its level of operational risk or increase its capital if RBI considers that the bank's ORRC is not commensurate with the bank's operational risk profile.

17. Merger of an AMA bank with a non-AMA Bank

17.1 Operations of one of the banks are considered immaterial

a) More than 80% AMA and less than 20% non-AMA

The merged entity will not be required to have a definite time-bound roll out plan for implementing AMA for the entire organization. However, it would make an endeavor to complete this as early as possible. Until that time, the operational risk capital will be calculated as AMA capital with the BIA/TSA capital of the other entity as add-on. Wherever the add-ons are difficult to calculate, suitable proxies/scaling factors may be applied by the bank with the approval of their Board of Directors.

b) More than 80% Non-AMA and less than 20% AMA

The merged entity may compute operational risk capital based on BIA/TSA for the entire organisation, depending upon the approach followed by the non-AMA bank before merger.

17.2 Operations of both the banks are material

Where neither of the banks has gross income/assets less than 20% of the gross income/assets of the merged entity at the time of merger, the merged entity will have to submit a definite plan to roll out AMA across the entire organization. The following methodology will be followed by the merged entity until the AMA for the entire organisation is approved by RBI.

(i) Identical business lines

a) If the non-AMA bank has operational loss data(for a minimum period of one year), it can be merged with the data of the respective business lines of the AMA bank and the frequencies and severities can be calculated based on this dataset, pending detailed re-modelling of the parameters based on the combined data during the roll-out period.

b) If the non-AMA bank does not have operational loss data, the AMA capital of the merged entity may be calculated as under:

(Total gross income of the merged entity/Gross income of the AMA bank and the non-AMA bank on the date of merger)* (Capital of the AMA bank as per AMA methodology + capital of the non-AMA bank as per BIA/TSA, on the date of merger)

(ii) The business lines which are not identical

The capital for business lines which were on AMA will continue to be calculated as per AMA. The capital for business lines which were not on AMA will continue to be calculated as per BIA/TSA. This will have to be done even if the merger at the level of branches results in the same branch carrying out various activities falling in the ambit of different business lines. For calculating BIA/TSA capital for non-identical business lines in such situations the bank will have to apportion the gross income between AMA and Non-AMA operations. If a bank is not able to do this, it may use any appropriate scaling/adjustment to the satisfaction of RBI.

(iii) Calculation of total operational risk capital

The total capital of the merged entity will be calculated as the **higher** of {the sum of (a), (b) and (c) below} OR {as per BIA}:

a) Capital of the **identical business lines** as per **(i)**

b) Capital of the **non-identical business lines belonging to the pre-merged AMA bank**, based on AMA methodology

c) Capital of the non**-identical business lines belonging to the pre-merged non-AMA bank** based on BIA/TSA

18. Additional Disclosures under Pillar 3

The following Table would be added as an additional disclosure requirement for AMA banks under Pillar 3. It would appear as **Table DF 9a** in the Pillar 3 disclosures presently required in terms of the updated Master Circular on New Capital Adequacy Framework.

Operational risk **Qualitative disclosures** (a) In addition to the general qualitative disclosure requirement, the approach(es) for operational risk capital assessment for which the bank qualifies. (b) Description of the AMA, if used by the bank, including a discussion of relevant internal and external factors considered in the bank's measurement approach. In the case of partial use, the scope and coverage of the different approaches used. (c) For banks using the AMA, a description of the use of insurance for the

purpose of mitigating operational risk

Appendix 1

Supplementary Guidance

A. Scope of Operational Risk and Operational Risk Loss

1. Introduction

1.1 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.

1.2 The Guidelines on AMA provide some guidance on how to distinguish operational risk from the range of other risks arising within business and support areas. With reference to the interaction between operational risk and the other Pillar 1 risk types, for AMA institutions, the boundaries between operational risk and credit and market risks are dealt with in para 8.5.4.3 (xx) to (xxiii) of the **Annex** 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.

1.3 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

2.1 The definition of "scope of operational risk" 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 bank's operational risk profile.

2.2 Each bank 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 guidance note 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.

2.3 By encouraging the BIA/TSA/ASA institutions also to adopt such practices, their operational risk frameworks are expected to generate greater effectiveness.

2.4 Para 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 guidance. However, some examples distinguishing operational losses from the credit and reputation-related losses are given in paragraphs 3.5 and 3.6. It also distinguishes 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"

3.1 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.

3.2 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 these guidelines can be envisaged. However, they should refer to individual and limited cases and should be well reasoned and properly documented.

3.3 Operational Risk versus Market Risk

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

(i) 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.

3.3.2 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 to, for instance, erroneous booking of a trade into the trading system. Market moves in a negative direction resulting in losses.

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

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.

3.4 Operational risk versus strategic risk

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

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

i. 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; and

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

3.4.3 In all these cases, the loss amounts to be recorded in the "scope of operational risk loss" are the specific provisions, costs of settlement* 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 2 Examples to be included in the "scope of operational risk"

i. aggressive selling, stemming for instance from individual initiatives, with consequential 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.

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

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.

---

*Costs of settlement are not to be considered to be timing impacts (see below).

@Refunds to customers would reduce the income for the bank, and hence would be an operational loss.

Table 3: Examples to be excluded from the "scope of operational risk".

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.

3.5 Operational Risk versus Credit Risk

Operational risk losses relating to credit risk will be treated as credit risk for the purposes of calculating the banks minimum capital requirements (Pillar 1), with the exception of fraud perpetrated by parties other than the borrower. Examples of operational risk losses related to credit risk that would be included in the AMA measurement: Card skimming; ID theft; and credit card fraud.

Examples of operational risk losses related to credit risk that would not be included in the AMA measurement (generally losses that arise from the purported exercise of a credit delegation):

a) procedural failure: where processing errors prevent recovery on a loan or actually enable a loss, as where a cash advance is made on a credit facility that was earlier cancelled by the loan officer;

(b) Fraud: loans obtained in a fraudulent transaction or in relation to money laundering, including collusion with staff (i.e. internal fraud). Note that this involves the borrower and is therefore not excluded;

(c) Legal issues: loan documents may contain legal defects (invalid clauses, ambiguous terms, etc.) e.g. the root cause of the loss was credit default; however

the guarantees or collateral is not properly managed. In this circumstance the loss is greater due to an operational risk event;

(d) collateral failure: failure to properly apply for loan insurance, failure to make a public filing needed to 'perfect' a security interest, failure to monitor collateral and make timely collateral calls, and incorrect valuations. In such cases, only the difference between the collateral value and the default amount is reported is the operational risk loss; and

(e) failure of a service provider: incorrect rating/valuation provided, resulting in incorrect decisions being made

3.6 Operational Risk versus Reputational Risk

In contrast to the boundary issues pertaining to operational risk and credit risk which forms part of Pillar I, reputational risk forms a part of Pillar II and arises due to a number of other risks. For example, a large credit risk loss, market risk loss, operational risk loss, or strategic risk may result in a reputational risk loss. Further, while the financial loss in the former case is captured in the Pillar I, the reputational risk loss (pillar 2) would generally be more aligned to a loss of income, or inability to obtain funding, etc. As a result, the reputational risk and operational risk boundary is difficult to define. Usually, reputational risk results in loss of future income which is not considered part of the loss definition for operational risk. One way of differentiating between the operational risk and reputational risk could be to visualize whether the event could lead to loss of income via loss of future business or otherwise. In the case of former, the effects from the perspective of implication of capital adequacy may be treated as reputational effects and analysed under Pillar II.

Other activities which may have reputational risk implications are sponsorship of securitization structures, the sale of credit exposures to securitization trusts, and sponsorship of money market mutual funds, in-house hedge funds, and private equity funds.

3.7 Miscellaneous Issues

3.7.1 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).

3.7.2 Table 4 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 4 : Type of elements/items that can result from an operational risk event

1. Direct charges to P&L and writedowns[1]
2. External costs incurred as a consequence of the event[2]
3. Specific provisions taken following the occurrence of a risk event
4. Pending losses[3]
5. Timing Losses[4]
6. Near-miss events[5]
7. Operational risk gain events[6]
8. Opportunity costs/lost revenues[7]

3.7.3 The 1st, 2nd and 3rd elements/items in Table 4 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 banks, also for calculating the minimum capital requirement for operational risk.

3.7.4 "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 banks; this can be done through the recognition of their actual amount in the loss data base or a pertinent scenario analysis. AMA banks should include these losses in the scope of operational risk loss for management purposes too.

3.7.5 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 rise to legal risks (e.g. “timing losses “due to some of the causes and examples mentioned in paragraph 16 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.

3.7.6 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.

---

[1] 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.

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

[3] “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 provision. Moreover the way this provision is established (e.g. the 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).

[4] “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.

[5] The term “near-miss event” can be used to identify an operational risk event that does not lead to a loss.

[6] The term “operational risk gain event” can be used to identify an operational risk event that generates a gain.

[7] 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).

Comment [f1]:

Comment [f2]:

B. Use Test for AMA Banks

1. Introduction

1.1 As per Para 8.4.2 of these guidelines, the bank's internal operational risk measurement system must be closely integrated into the day-to-day risk management processes of the bank. This requirement, known as the "use test", obliges an AMA bank 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.

1.2 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.

1.3 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, RBI expects 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.

1.4 The objective of this guidance note is to describe what should be considered to be an appropriate interpretation of the use test by an AMA bank 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

2.1 Following four principles will be used by RBI for this purpose:

- 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.

2.2 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 bank 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.

2.3 RBI will 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.

2.4 The supervisory expectations on 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.

2.5 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.

2.6 Additional factors to be considered in a "business as usual" context are the overarching elements essential to well-implemented and functioning risk management processes, 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.

2.7 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.

2.8 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.

2.9 Home-host considerations affect the assessment process in case of banking groups' applications are concerned. Key factors influencing the assessment

process would include whether the RBI 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.

2.10 RBI expects 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, RBI is in general prepared to offer some flexibility on the development, implementation and advancement of some of the key elements.

2.11 In particular, the factors reflecting the business environment and internal control systems are those where supervisors show this flexibility. However RBI 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. RBI 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.

2.12 RBI expects 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. It is clear that meeting the use test requirement is a difficult task for banks. The use test requirement is a key driver for enhancing not only the quality of the modelling process but also of the management process. RBI expects clear evidence that the modelling process supports and advances operational risk management in the bank; accordingly it should be adaptable to the changing dynamic of the bank so that it can continuously enable the bank's operational risk exposure to be determined.

4. As operational risk frameworks advance, the inputs should become more relevant and therefore more reflective of the bank's business, strategy and exposure to risk.

As the bank'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.

C. Additional Guidance on Operational Risk Management Framework (ORMF)

1. Independent Operational Risk Management Function (ORM Function)

The bank shall have an ORM Function that is responsible for the design, selection, monitoring and ongoing development of the ORMF of the bank, including the operational risk management and measurement processes and ORMS. The ORM Function is also responsible for ensuring consistency of implementation of the ORMF across all business lines.

1.1 A bank shall ensure that the ORM Function has reporting lines and responsibilities that are structurally and functionally independent from the personnel and management functions responsible for originating exposures and of the activities that contribute to the operational risk profile. All roles and responsibilities of people and functions involved in operational risk management shall be clearly defined and documented.

1.2 The ORM Function should codify, establish and ensure the consistent application of appropriate bank-wide policies and procedures concerning operational risk management, for all material business activities, processes and systems.

1.3 The ORM Function is also responsible for the design and implementation of the operational risk measurement methodology of a bank, risk monitoring and reporting system as well as the development of strategies to identify, assess, monitor, control and mitigate operational risk.

1.4 The ORM Function should assess industry best practices with a view to improving the activities, processes and systems of a bank.

1.5 The ORM Function should have oversight and supervision responsibilities for any systems used in the AMA, and have ultimate responsibility for the ongoing assessment of the performance of and alterations to the ORMS. The ORM Function

should review and document any changes to the operational risk policies and procedures and the ORMS, including the reasons for the changes.

1.6 The ORM Function should be responsible for the process related to the definition, documentation, collection and application of the estimates of the AMA elements needed to calculate the operational risk exposure of a bank. The ORM Function should ensure the reliability and consistency of the estimates of the AMA elements, including implementing procedures to verify that definitions are consistently applied across business lines and geographic areas. In this regard, the bank should implement internal standards for the estimates of the AMA elements and associated remedial actions to be taken when such standards are not met.

1.7 The ORM Function should periodically review and consider the effects of loss experience, external market changes, other environmental factors, and the potential for new or changing operational risks associated with new products, activities or systems on the ORMF.

1.8 The ORM Function should produce, review and analyze operational risk data and reports.

1.9 The ORM Function should be responsible for verifying the fulfilment of the AMA qualifying criteria, and, in particular, ensuring the ORMS is closely integrated into the day-to-day risk management processes and operations.

1.10 Where a bank has a central operational risk unit and some of the staff managing the operational risk of the bank is located in other business units, business lines, geographical groups or legal entities, the bank should ensure that the staffs follows the guidelines set by the central operational risk unit. There should be clear responsibilities and reporting lines for the staff.

1.11 The person responsible for internal validation of the ORMF should not be the person responsible for the design or implementation. Where any person or group of persons of the ORMF is involved in the validation work relating to the ORMF designed or implemented by another person or group of persons of the same unit, the bank should ensure that there is no conflict of interest, and that the person or group of persons involved in the validation work can provide objective and effective

challenge to the person or group of persons responsible for the design or implementation of the ORMF.

1.12 The ORM Function should be responsible for ensuring appropriate regular reporting of relevant bank-wide operational risk information to the Board and senior management.

1.13 The evaluation of the performance and remuneration of the ORMF should take into consideration how well operational risks are managed (e.g. reliability, consistency and predictability of estimates of the AMA elements and other risk estimates).

1.14 An ORMF should specifically cover the following aspects:

(i) establish a process to identify the nature and types of operational risk and their causes and measure their resulting effects on the bank;

(ii) identify the appetite for operational risk of the bank and specified levels of acceptable risk;

(iii) provide the overall operational risk strategies;

(iv) set out the responsibilities of the Board, senior management, business unit management and persons that have responsibility for managing operational risk;

(v) include operational risk management policies and procedures that clearly describe the major elements and activities of the ORM framework;

(vi) ensure that effective operational risk management and measurement processes are adopted;

(vii) ensure that proper organisational structure of control and reporting functions is in place;

(viii) include independent review and internal validation processes and procedures, as well as independent oversight of the internal validation function; and

(ix) include review and approval process for significant policy and procedural changes and exceptions.

2. Documentation of ORMF

2.1 A bank shall have a process for ensuring compliance with its ORMF in the form of a documented set of policies and procedures in place to identify, assess, monitor, control and mitigate operational risk.

2.2 A bank should consider and review the adequacy and completeness of its documentation for managing its operational risk, including how documentation is developed, maintained, and distributed (referred to as "documentation" in this Part). As part of the design and implementation of the ORMF, the importance of documentation should be emphasised. The RBI would expect to see evidence of this as part of the AMA application and ongoing supervision of the bank.

2.3 The level of documentation should be commensurate with needs and culture of the bank and should be appropriate to the operational risk it takes and its operational risk management and measurement process. The documentation should explain the approach that has been adopted and the rationale for that approach.

2.4 Documentation should be timely and up to date.

2.5 Documentation should cover the following broad areas:

(i) internal governance – clearly documented reporting lines;

(ii) internal control – decision-making processes should be clear and transparent; and

(iii) compliance – clear records to ensure compliance with all relevant requirements.

2.6 Documentation should comprise the following elements:

(i) a definition of operational risk that is consistent with the definition set out in this Annex, and loss event types that will be monitored;

(ii) roles and responsibilities of the Board, senior management, business unit management and ORMF, including documented levels of approval and authorisation to ensure accountability to an appropriate level of management;

(iii) outline of the operational risk reporting framework, the type of information to be included, treatment and resolution of non-compliance issues;

(iv) situations where exceptions and overrides can be used and the approving authorities for such exceptions and overrides; and

(v) internal validation and oversight of internal validation processes and procedures.

3. Documentation on All Material Aspects of ORMS

3.1 Documentation on the ORMS should be comprehensive and provide a level of detail sufficient to ensure that the approach of a bank to determine its ORMS is transparent and capable of independent review and validation.

3.2 Documentation on the ORMS should include the following:

(i) rationale for the development, operation and assumptions underpinning its framework, including the choice of inputs, distributional assumptions, and the weighting across qualitative and quantitative elements;

(ii) overview of the analytical approach (e.g. description of the model or statistical technique used, ORMS inputs and outputs, how different inputs are combined and weighted, and steps taken to ensure the integrity of the data used in the estimation process);

(iii) the assumptions and specifications underpinning the ORMS and their rationale and limitations;

(iv) details and rationale for establishing thresholds and their use;

(v) the analytics and relevant theory behind all calculations;

(vi) details of the parameters and assumptions of the ORMS including the justification for their use and the process undertaken for checking and validating those assumptions;

(vii) justification for the weighting of estimates of the AMA elements.

(viii) comparison between the operational risk exposure estimate and actual loss experience over time, to assess the framework's performance and the reasonableness of its outputs;

(ix) an explanation of how the bank ensures that the ORMS achieves the soundness standard ;

(x) details of any explicit and implicit dependence structures utilised in the ORMS, including evidence supporting their use;

(xi) details of the proposed methodology for measuring and accounting for expected loss; and

(xii) details of the methodology relating to the use of insurance for risk mitigation, including how the level of insurance mitigation is derived and the types of insurance contracts utilised.

4. Oversight of the ORMF

4.1 Board oversight

4.4.1 The Board has ultimate responsibility for the overall operational risk profile and ORMF of a bank.

4.4.2 The Board has ultimate responsibility for the continuing appropriateness of the ORMS of a bank, the process for deriving estimates of the AMA elements, the use of the ORMS and estimates of the AMA elements. This includes responsibility for the adequacy of control processes in respect of these areas. Accordingly, a bank should equip the Board with a general understanding of the objectives and basis of the ORMS of the bank, and the process for deriving and using estimates of the AMA elements. The information provided to the Board should be adequate for the Board to be able to perform its roles effectively.

4.4.3 The Board should establish the appetite for operational risk for the bank. The Board is responsible for the implementation of sound fundamental risk governance principles that facilitate the identification, assessment, monitoring, controlling and mitigation of operational risk.

4.4.4 The Board should be informed of significant changes to and controls in respect of, the ORM framework. The Board should also be informed of significant deviations from established policies and procedures, weaknesses in the design and operation of the ORMS of the bank, the process for deriving estimates of the AMA elements, the use of the ORMS and estimates of the AMA elements.

4.4.5 The Board should ensure that there are comprehensive and adequate written policies and procedures relating to the oversight and control of the ORM framework of the bank, the design and operation of its ORMS, the process for deriving estimates of the AMA elements, the use of the ORMS and estimates of the AMA elements. At a minimum, these policies and procedures would include the following -

(i) the roles and responsibilities of the Board, senior management, business unit management and other personnel involved in the design and approval of the ORM framework of the bank, ORMS and the process for deriving and using estimates of the AMA elements;

(ii) the internal control processes and independent oversight of the design and operation of the ORM framework of the bank, the ORMS, the process for deriving estimates of the AMA elements, the use of the ORMS and estimates of the AMA elements;

(iii) the matters which the bank considers material and approval levels for these matters; and

(iv) the frequency and level of detail of reporting to the Board and senior management on the ORM framework of the bank, the ORMS and the estimates of the AMA elements used by the bank to calculate minimum operational risk capital requirements under the AMA.

4.4.6 The Board should ensure that the ORMS of a bank is closely integrated into the day-to-day risk management processes.

4.4.7 The Board should understand significant risks and strategic implications and how operational risk affects a bank.

4.4.8 The Board and senior management should assign responsibilities and reporting relationships to encourage and maintain accountability and ensure that the necessary resources are available to manage operational risk. This includes evaluating and ensuring that the staff responsible for any aspect of the ORM framework, the ORMS, operational risk control and internal validation, are adequately qualified and trained to undertake their respective roles.

4.4.9 The Board should review the scope and frequency of the independent review program to ensure its continued effectiveness.

5. Senior Management Oversight[8]

5.1 Senior management should exercise active oversight over the ORMF. Senior management should translate the ORMF into specific policies and procedures that can be implemented and verified within the business lines, products and activities of a bank.

[8] The RBI expects the involvement of senior management in respect of these areas, as set out in para 5 to exceed the level of involvement by the Board.

5.2 Senior management and staff in the ORMF should meet regularly to discuss the performance of the ORMF, areas needing improvement and the status of efforts to improve previously identified deficiencies.

5.3 Senior management should inform the Board of issues and changes or deviations from established policies that will significantly impact the operations of the ORMF, including the operational risk profile and capital allocated to operational risk on a regular and timely basis.

5.4 Senior management should ensure the continuing appropriateness and effectiveness of the ORM framework, the ORMS, the process for deriving estimates of the AMA elements, the use of the ORMS and estimates of the AMA elements. Senior management should articulate its expectations and provide guidance for the technical and operational aspects in respect of these areas.

5.5 Senior management should have a good understanding of the design and operation of the ORMS, the process for deriving estimates of the AMA elements, the use of the ORMS and estimates of the AMA elements. Senior management should also have a good understanding of the operational risk policies and procedures of the bank. Senior management should approve these areas and also the differences between documented procedures and actual practices, if any.

5.6 Senior management should also ensure, on an ongoing basis, that the ORMS and the process for deriving and using estimates of the AMA elements -

(a) provide for a meaningful assessment of the operational risk exposures of the bank and generate consistent and predictive estimates of the AMA elements suitable for use to calculate minimum operational risk capital requirements; and

(b) are consistent with all applicable rules and regulations as well as established internal policies and procedures.

5.7 Senior management should assess operational risk inherent in new areas (e.g. products, activities, processes and systems) before they are introduced, and identify

risks tied to new or existing product development and significant changes in order to ensure that the risk profiles of product lines are updated regularly.

5.8 Senior management should ensure effective communication of the operational risk management approach of the bank to staff. When all staff are aware of relevant policies and procedures and understand their responsibilities with respect to operational risk management, this will ensure consistent treatment of operational risk across the bank. Senior management should also ensure that operational risk issues are communicated to appropriate staff responsible for managing credit, market and other risks, as well as those responsible for purchasing insurance and managing third-party outsourcing arrangements.

5.9 Senior management should ensure steps are taken by staff at all levels to closely integrate the ORMS of the bank and practices into the day-to-day risk management processes and operations of the bank.

6. Business Unit Management Oversight

6.1 Business unit management is responsible for the day-to-day management of operational risk within each business line and for the appropriateness and effectiveness of operational risk policies and procedures and controls within their area of operation.

6.2 Business unit management should ensure that internal controls and practices within their business lines are consistent with bank-wide policies and procedures to support the management and measurement of the operational risk of the bank.

6.3 Implementation of the ORM framework within each business line should reflect the scope of that business and its inherent operational complexity and operational risk profile.

7. Regular Reporting to the Board, Senior Management and Business Unit Management

7.1 A bank shall ensure that there is regular and comprehensive reporting of its operational risk profile, risk exposures and loss experience to the Board, senior management and business unit management, to enable them to understand,

assess, monitor and control operational risk and losses, and other corporate risk issues. These reports would also serve as a basis for related mitigation strategies and could create incentives to improve operational risk management throughout the bank.

7.2 The content, depth, frequency and format of reporting should depend on the recipient and how the information will be used. It should also be consistent with the level of risk and commensurate with the nature, size, risk profile and degree of complexity of the business operations of the bank.

7.3 Regular reports to the Board, senior management and business unit management of a bank should include the following:

(i) the operational risk profile and type of exposures of the bank giving rise to operational risk (e.g. description of key operational risk events and drivers);

(ii) estimates of regulatory and economic capital and changes in regulatory capital requirements and economic capital over time;

(iii) information on, including changes to, the inputs (e.g. estimates of the AMA elements) and outputs of the ORMS and the approach of the bank to managing and measuring operational risk;

(iv) appropriate indicators that provide early warnings of potential operational risk-related losses or increased risk of future losses and management assessment of these factors;

(v) risk reduction and risk transfer strategies (e.g. the effect of any expected loss deductions, cost benefit analysis of the mitigation and corrective actions on the business line (as listed in **Appendix 3**) or exposures to loss event types (as listed in **Appendix 2)** and losses);

(vi) reports from Internal Audit and ORMF on material issues with respect to the ORM framework of the bank; and

(vii) results of internal validation.

7.4 A bank shall have a process in place for taking appropriate action according to the information within management reports. This should include escalation procedures for key operational risk issues to facilitate the taking of appropriate action between formal reporting cycles.

7.5 A bank should document the outcomes of independent reviews, exception reporting including identified problem areas and timely corrective action on outstanding issues.

8. Independent Regular Review of the ORMF

8.1 A bank's ORM Framework should be subject to effective and comprehensive independent review both initially at the time the AMA approval is sought, and thereafter on an ongoing basis, to ensure the continued integrity of the framework. Such reviews shall be conducted by functionally independent, appropriately trained and competent personnel, and shall take place at regular intervals or when a material change is made to the framework. There should be two reviews: (i) internal review by the bank's own audit staff **annually**; and (ii) external review by external auditors **once in two years**. However, before submitting the application for approval of AMA, the bank should have preferably carried out both the reviews.

8.2 For the purposes of paragraph 8.1, 'functionally independent' means that:

(i) the relationship between the party or parties conducting the reviews and the bank's business areas is such that opportunities for the independent party or parties to improperly influence the operational risk management framework are minimised; and

(ii) the party or parties conducting the reviews must not be involved in the development, implementation or operation of the operational risk measurement system, or be part of, or report to the operational risk management function.

It is not necessary that the same party undertake all aspects of the review.[9]

8.3 The bank should develop procedures for reviewing the ORMF that covers all significant activities (including any outsourced activity) that would expose the bank to material operational risk. The procedures should be regularly updated and include the following areas:

(i) assessing the overall adequacy and effectiveness of the ORM framework, including the activities of the business lines and of the ORMF;

(ii) ensuring consistency of the AMA methodology across the business lines of the Bank;

---

[9] In most cases, the independent reviews could be facilitated by a bank's internal audit function but may require the engagement of independent parties outside of this function

(iii) complying with the standards relating to the ORM framework and the policies and procedures of the bank, as well as adhering to the overarching principles set out in paragraph 3.4 of the guidelines;

(iv) developing internal processes for identifying, assessing, monitoring, controlling and mitigating operational risk;

(v) defining the scope of operational risks captured by the ORMS and assessing whether the ORMS captures all material activities and exposures from all appropriate sub-systems and geographic locations;

(vi) assessing the reasonableness of any assumptions made in the ORMS;

(vii) integrating the ORMS into the day-to-day risk management processes. The bank should ensure that the ORMS is an integral part of the process of monitoring and controlling the bank's operational risk profile and the information plays a prominent role in risk reporting, management reporting, internal capital allocation and risk analysis. (For further guidance, refer to **Part B** of this **Appendix**).

(viii) The bank should have techniques for allocating operational risk capital to major business lines and for creating incentives to improve the management of operational risk throughout the firm;

(ix) ensuring the integrity of the ORMS, including the appropriateness, accuracy and adequacy of technical documentation supporting the ORMS and management reports;

(x) implementing new products, processes and systems which expose the bank to material operational risk;

(xi) dealing with issues such as the adequacy of the IT infrastructure, data collections, data input processes and data maintenance; and

(xii) conducting specific examinations in order to assess the degree of independence of the ORMF.

D. Miscellaneous Aspects

1. Model Uncertainty

If the dependence or correlation assumptions are uncertain, a bank shall be conservative and implement an appropriate adjustment to the AMA model to take that uncertainty into account. RBI envisages that a bank would have a formalised framework to manage the model risks inherent in its ORRC calculation. Such a framework would include the monitoring, mitigation and accounting for known uncertainties related to modelling choices, assumptions, parameters and input data. An assessment of the model uncertainties would typically be conducted at least once a year and involve the following steps:

(a) acknowledging in the model documentation all assumptions, choices and parameters, implicit or explicit in the model and their limitations to ensure that no implicit assumption or choice in the model is left unchallenged and consequently becomes a potential source of unmanaged model risk;

(b) eliciting from academic research and industry practice a sufficiently comprehensive set of alternatives for each modelling choice, assumption and parameter. This includes the monitoring of academic research and industry practice on an ongoing basis for innovations in operational risk measurement approaches;

(c) supporting the criteria used for selecting the most appropriate alternative for each modelling choice, assumption and parameter, with peer-reviewed academic publications;

(d) identifying, assessing and documenting all residual model risks, as well as the corresponding sensitivity of the ORRC across the full range of uncertainty to a reasonably high level of confidence; and

(e) applying conservatism to the model inputs, outputs and/or calculation commensurate with the model risks and sensitivity as outlined in (d).

2. Insurance Coverage

2.1 This section provides further guidance on the use of insurance as a risk mitigant by a bank and how RBI envisages such insurance would be treated for the purposes of meeting the requirements in the **Annex**. In order for insurance to be recognised for these purposes, banks may have to negotiate certain terms and conditions with their insurance providers, specifically for periods of insurance, restriction exclusions and the notification period for cancellation.

2.2 In terms of the requirement in paragraph 9.2.10.(iv) of the **Annex**, RBI recognises that banks, or their captive insurers, will generally have either a deductible or a self-insured retention amount which, in effect, provides less than 100 per cent insurance by a third party. In such cases, a bank could include this cover in its operational risk measurement model through the use of a haircut.

2.3 In capturing the characteristics of its insurance policies through haircuts to the amount of insurance recognition, a bank would typically consider the ability and willingness of the insurer to pay claims in a timely manner. If the assessment concludes that there are concerns regarding the ability to pay in a timely manner, the bank could determine an appropriate haircut to adjust the amount of insurance that is recognised.

2.4 Banks should identify any mismatches in the coverage of insurance policies, which can occur in many ways leading to uncertainty in payment. Mismatches in insurance coverage vis-a-vis the operational risk profile of a bank would normally depend upon on the specific insurance policy terms and conditions, exclusions, deductibles and limits.

Appendix 2

Detailed Loss Event Type Classification

Event-Type Category (Level 1)	Definition	Categories (Level 2)	Activity Examples (Level 3)
Internal fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/ discrimination events, which involves at least one internal party	Unauthorised Activity	Transactions not reported (intentional)
			Transaction type unauthorised (with monetary loss)
			Mismarking of position (intentional)
		Theft and Fraud	Fraud / credit fraud / worthless deposits
			Theft / extortion / embezzlement / robbery
			Misappropriation of assets
			Malicious destruction of assets
			Forgery
			Kite flying
			Smuggling
			Account take-over /
			Tax non-compliance / evasion
			Bribes / kickbacks
			Insider trading (not on firm's account)
External fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party	Theft and Fraud	Theft/Robbery
			Forgery
			Kite flying
		Systems Security	Hacking damage
			Theft of information (with monetary loss)

Employment Practices and Workplace Safety	Losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity / discrimination events	Employee Relations	Compensation, benefit, termination issues
			Organised labour activity
		Safe Environment	General liability (slips and falls, etc.)
			Employee health & safety
			Workers compensation
		Diversity & Discrimination	All discrimination types
Clients, Products & Business Practices	Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product.	Suitability, Disclosure & Fiduciary	Fiduciary breaches / guideline violations
			Suitability / disclosure issues (KYC, etc.)
			Retail customer disclosure violations
			Breach of privacy
			Aggressive sales
			Account churning
			Misuse of confidential
			Lender liability
		Improper Business or Market Practices	Antitrust
			Improper trade / market
			Market manipulation
			Insider trading (on firm's account)
			Unlicensed activity
			Money laundering
		Product Flaws	Product defects (unauthorised, etc.)
			Model errors
		Selection, Sponsorship & Exposure	Failure to investigate client per guidelines
			Exceeding client exposure
		Advisory Activities	Disputes over performance of advisory activities
Damage to Physical Assets	Losses arising from loss or damage to physical assets from natural disaster or other events.	Disasters and other events	Natural disaster losses
			Human losses from external sources (terrorism, vandalism)
Business disruptio	Losses arising from disruption of business or	Systems	Hardware

			Software
			Telecommunications
			Utility outage / disruptions
Execution, Delivery & Process Management	Losses from failed transaction processing or process management, from relations with trade counterparties and vendors	Transaction Capture, Execution & Maintenance	Miscommunication
			Data entry, maintenance or loading error
			Missed deadline or responsibility
			Model / system mis-operation
			Accounting error / entity attribution error
			Other task mis-performance
			Delivery failure
			Collateral management failure
			Reference Data Maintenance
		Monitoring and Reporting	Failed mandatory reporting obligation
			Inaccurate external report (loss incurred)
		Customer Intake and Documentation	Client permissions / disclaimers missing
			Legal documents missing / incomplete
		Customer / Client Account Management	Unapproved access given to accounts
			Incorrect client records (loss incurred)
			Negligent loss or damage of client assets
		Trade Counterparties	Non-client counterparty misperformance
			Misc. non-client counterparty disputes
		Vendors & Suppliers	Outsourcing
			Vendor disputes

Appendix 3

Mapping of Business Lines

Level 1	Level 2	Activity Groups
Corporate Finance	Corporate Finance	Mergers and acquisitions, underwriting, privatisations, securitisation, research, debt (government, high yield), equity, syndications, IPO, secondary private placements
	Government Finance	
	Merchant Banking	
	Advisory Services	
Trading & Sales	Sales	Fixed income, equity, foreign exchanges, credit products, funding, own position securities, lending and repos, brokerage, debt, prime brokerage and sale of Government bonds to retail investors. .
	Market Making	
	Proprietary Positions	
	Treasury	
Payment and Settlement*	External Clients	Payments and collections, inter-bank funds transfer (RTGS, NEFT, EFT, ECS etc.), clearing and settlement
Agency Services	Custody	Escrow, securities lending (customers) corporate actions, depository services
	Corporate Agency	Issuer and paying agents
	Corporate Trust	Debenture trustee
Asset Management	Discretionary Fund Management	Pooled, segregated, retail, institutional, closed, open, private equity
	Non-Discretionary Fund Management	Pooled, segregated, retail, institutional, closed, open
Retail Brokerage	Retail Brokerage#	Execution and full service
Retail Banking	Retail Banking	Retail lending including trade finance, cash credit etc. as defined under Basel II and also covering non fund based and bill of exchange facilities to retail customers, housing loans, loans against shares, banking services, trust and estates, retail deposits@, intra bank fund transfer on behalf of retail customers.
	Private Banking	Private lending (personal loans) and private/bulk deposits@, banking

		services, trust and estates, investment advice
	Card Services	Merchant/commercial/corporate cards, private labels and retail
Commercial Banking	Commercial Banking	Project finance, corporate loans, cash credit loans, real estate, export and import finance, trade finance, factoring, leasing, lending, guarantees including deferred payment and performance guarantees, LCs, bills of exchange, take-out finance, interbank lending other than in call money and notice money market.

* Payment and settlement losses related to a bank's own activities would be incorporated in the loss experience of the affected business line.

The Indian retail brokerage industry consists of companies that primarily act as agents for the buying and selling of securities (e.g. stocks, shares, and similar financial instruments) on a commission or transaction fee basis.