Supervisory Guidance on Operational Risk Advanced Measurement Approaches for Regulatory Capital

Draft Date: July 2, 2003

Table of Contents

Appendixes

I. Purpose

1. The purpose of this guidance is to set forth the expectations of the U.S. banking agencies for banking institutions that use Advanced Measurement Approaches (AMA) for calculating the operational risk capital charge under the new capital regulation. Institutions using the AMA will have considerable flexibility to develop operational risk measurement systems appropriate to the nature of their activities, business environment, and internal controls. An institution's operational risk regulatory capital requirement will be calculated as the amount needed to cover its operational risk at a level of confidence determined by the supervisors, as discussed below. Use of an AMA is subject to supervisory approval.

2. This draft guidance should be considered with the advance notice of proposed rulemaking (ANPR) on revisions to the risk-based capital standard as published in the Federal Register on July_____ no._____. As with the ANPR, the Agencies are seeking industry comment on this draft guidance. In addition to seeking comment on all specific aspects of this supervisory guidance, the Agencies are seeking comment on the extent to which the supervisory guidance strikes the appropriate balance between flexibility and specificity. Likewise, the Agencies are seeking comment on whether an appropriate balance has been struck between the regulatory requirements set forth in the ANPR and the supervisory standards set forth in this guidance.

II. Background

3. Effective management of operational risk is integral to the business of banking and to institutions' roles as financial intermediaries. Although operational risk is not a new risk, deregulation and globalization of financial services, together with the growing sophistication of financial technology, new business activities and delivery channels, are making institutions'

operational risk profiles (i.e., the level of operational risk across an institution's activities and risk categories) more complex.

4. This guidance identifies the supervisory standards (S) that institutions must meet and maintain to use an AMA for the regulatory capital charge for operational risk. The purpose of the standards is to provide the foundation for a sound operational risk framework, while allowing institutions to identify the most appropriate mechanisms to meet AMA requirements. Each institution will need to consider its complexity, range of products and services, organizational structure, and risk management culture as it develops its AMA. Operational risk governance processes need to be established on a firm-wide basis to identify, measure, monitor, and control operational risk in a manner comparable with the treatment of credit, interest rate, and market risks.

5. Institutions will be expected to develop a framework that measures and quantifies operational risk for regulatory capital purposes. To do this, institutions will need a systematic process for collecting operational risk loss data, assessing the risks within the institution, and adopting an analytical framework that translates the data and risk assessments into an operational risk exposure (see definition below). The analytical framework must incorporate a degree of conservatism that is appropriate for the overall robustness of the quantification process. Because institutions will be permitted to calculate their minimum regulatory capital on the basis of internal processes, the requirements for data capture, risk assessment, and the analytical framework described below are detailed and specific.

6. Effective operational risk measurement systems are built on both quantitative and qualitative risk assessment techniques. While the output of the regulatory framework for operational risk is a measure of exposure resulting in a capital number, the integrity of that

estimate depends not only on the soundness of the measurement model, but also on the robustness of the institution's underlying risk management processes. In addition, supervisors view the introduction of the AMA as an important tool to further promote improvements in operational risk management and controls at large banking institutions.

7. This document provides both AMA supervisory standards and a discussion of how those standards should be incorporated into an operational risk framework. The relevant supervisory standards are listed at the beginning of each section and a full compilation of the standards is provided in Appendix A. Not every section has specific supervisory standards. When spanning more than one section, supervisory standards are listed only once.

8. Institutions will be required to meet, and remain in compliance with, all the supervisory standards to use an AMA framework. However, evaluating an institution's qualification with each of the individual supervisory standards will not be sufficient to determine an institution's overall readiness for AMA. Instead, supervisors and institutions must also evaluate how well the various components of an institution's AMA framework complement and reinforce one another to achieve the overall objectives of an accurate measure and effective management of operational risk. In performing their evaluation, supervisors will exercise considerable supervisory judgment, both in evaluating the individual components and the overall operational risk framework.

9. An institution's AMA methodology will be assessed as part of the ongoing supervision process. This will allow supervisors to incorporate existing supervisory efforts as much as possible into the AMA assessments. Some elements of operational risk (e.g., internal controls and information technology) have long been subject to examination by supervisors. Where this is the case, supervisors will make every effort to leverage off these examination activities to

assess the effectiveness of the AMA process. Substantive weaknesses identified in an examination will be factored into the AMA qualification process.

III. Definitions

10. There are important definitions that institutions must incorporate into an AMA framework. They are:

- *Operational risk:* The risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. The definition includes legal risk, which is the risk of loss resulting from failure to comply with laws as well as prudent ethical standards and contractual obligations. It also includes the exposure to litigation from all aspects of an institution's activities. The definition does not include strategic or reputational risks[1].
- *Operational risk loss:* The financial impact associated with an operational event that is recorded in the institution's financial statements consistent with Generally Accepted Accounting Principles (GAAP). Financial impact includes all out-of-pocket expenses associated with an operational event but does not include opportunity costs, foregone revenue, or costs related to investment programs implemented to prevent subsequent operational risk losses. Operational risk losses are characterized by seven event factors associated with:
  i. *Internal fraud:* an act of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/discrimination events, which involve at least one internal party.
  ii. *External fraud:* an act of a type intended to defraud, misappropriate property or circumvent the law, by a third party.
  iii. *Employment practices and workplace safety:* an act inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity/discrimination events.
  iv. *Clients, products, and business practices:* 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.
  v. *Damage to physical assets:* the loss or damage to physical assets from natural disaster or other events.
  vi. *Business disruption and system failures:* disruption of business or system failures.
  vii. *Execution, delivery, and process management:* failed transaction processing or process management, from relations with trade counterparties and vendors.
- *Operational risk exposure:* An estimate of the potential operational losses that the banking institution faces at a soundness standard consistent with a 99.9 per cent

[1] An institution's definition of operational risk may encompass other risk elements as long as the supervisory definition is met.

confidence level over a one-year period. The institution will multiply the exposure by 12.5 to obtain risk-weighted assets for operational risk; this is added to the risk-weighted assets for credit and market risk to arrive at the denominator of the regulatory capital ratio.

- *Business environment and internal control factor assessments:* The range of tools that provide a meaningful assessment of the level and trends in operational risk across the institution. While the institution may use multiple tools in an AMA framework, they must all have the same objective of identifying key risks. There are a number of existing tools, such as audit scores and performance indicators that may be acceptable under this definition.

IV. Banking Activities and Operational Risk

11. The above definition of operational risk gives a sense of the breadth of exposure to operational risk that exists in banking today as well the many interdependencies among risk factors that may result in an operational risk loss. Indeed, operational risk can occur in any activity, function, or unit of the institution.

12. The definition of operational risk incorporates the risks stemming from people, processes, systems and external events. People risk refers to the risk of management failure, organizational structure or other human resource failures. These risks may be exacerbated by poor training, inadequate controls, poor staffing resources, or other factors. The risk from processes stem from breakdowns in established processes, failure to follow processes, or inadequate process mapping within business lines. System risk covers instances of both disruption and outright system failures in both internal and outsourced operations. Finally, external events can include natural disasters, terrorism, and vandalism.

13. There are a number of areas where operational risks are emerging. These include:

- Greater use of automated technology has the potential to transform risks from manual processing errors to system failure risks, as greater reliance is placed on globally integrated systems;
- Proliferation of new and highly complex products;
- Growth of e-banking transactions and related business applications expose an institution to potential new risks (e.g., internal and external fraud and system security issues);

- Large-scale acquisitions, mergers, and consolidations test the viability of new or newly integrated systems;
- Emergence of institutions acting as large-volume service providers create the need for continual maintenance of high-grade internal controls and back-up systems;
- Development and use of risk mitigation techniques (e.g., collateral, insurance, credit derivatives, netting arrangements and asset securitizations) optimize an institution's exposure to market risk and credit risk, but potentially create other forms of risk (e.g., legal risk); and
- Greater use of outsourcing arrangements and participation in clearing and settlement systems mitigate some risks while increasing others.

14. The range of banking activities and areas affected by operational risk must be fully identified and considered in the development of the institution's risk management and measurement plans. Since operational risk is not confined to particular business lines[2], product types, or organizational units, it should be managed in a consistent and comprehensive manner across the institution. Consequently, risk management mechanisms must encompass the full range of risks, as well as strategies that help to identify, measure, monitor and control those risks.

V. Corporate Governance

Supervisory Standards:

S 1. The institution's operational risk framework must include an independent firm-wide operational risk management function, line of business management oversight, and independent testing and verification functions.

15. The management structure underlying an AMA operational risk framework may vary between institutions. However, within all AMA institutions, there are three key components that must be evident -- the firm-wide operational risk management function, lines of business management, and the testing and verification function. These three elements are functionally

[2] Throughout this guidance, terms such as "business units" and "business lines" are used interchangeably and refer not only to an institution's revenue generating businesses, but also to corporate staff functions such as human resources or information technology.

independent[3] organizational components, but should work in cooperation to ensure a robust operational risk framework.

A. Board and Management Oversight

Supervisory Standards:

S 2. The board of directors must oversee the development of the firm-wide operational risk framework, as well as major changes to the framework. Management roles and accountability must be clearly established.

S 3. The board of directors and management must ensure that appropriate resources are allocated to support the operational risk framework.

16. The board is responsible for overseeing the establishment of the operational risk framework, but may delegate the responsibility for implementing the framework to management with the authority necessary to allow for its effective implementation. Other key responsibilities of the board include:

- Ensuring appropriate management responsibility, accountability and reporting;
- Understanding the major aspects of the institution's operational risk as a distinct risk category that should be managed;
- Reviewing periodic high-level reports on the institution's overall operational risk profile, which identify material risks and strategic implications for the institution;
- Overseeing significant changes to the operational risk framework; and
- Ensuring compliance with regulatory disclosure requirements.

17. Effective board and management oversight forms the cornerstone of an effective operational risk management process. The board and management have several broad responsibilities with respect to operational risk:

- To establish a framework for assessing operational risk exposure and identify the institution's tolerance for operational risk;

[3] For the purposes of AMA, "functional independence" is defined as the ability to carry out work freely and objectively and render impartial and unbiased judgments. There should be appropriate independence between the firm-wide operational risk management functions, line of business management and staff and the testing/verification functions. Supervisory assessments of independence issues will rely upon existing regulatory guidance (e.g. audit, internal control systems, board of directors/management, etc.)

- To identify the senior managers who have the authority for managing operational risk;
- To monitor the institution's performance and overall operational risk profile, ensuring that it is maintained at prudent levels and is supported by adequate capital;
- To implement sound fundamental risk governance principles that facilitate the identification, measurement, monitoring, and control of operational risk;
- To devote adequate human and technical resources to operational risk management; and
- To institute remuneration policies that are consistent with the institution's appetite for risk and are sufficient to attract qualified operational risk management and staff.

18. Management should translate the operational risk management framework into specific policies, processes and procedures that can be implemented and verified within the institution's different business units. Communication of these elements will be essential to the understanding and consistent treatment of operational risk across the institution. While each level of management is responsible for effectively implementing the policies and procedures within its purview, senior management should clearly assign authority, responsibilities, and reporting relationships to encourage and maintain this accountability and ensure that the necessary resources are available to manage operational risk. Moreover, management should assess the appropriateness of the operational risk management oversight process in light of the risks inherent in a business unit's activities. The testing and verification function is responsible for completing timely and comprehensive assessments of the effectiveness of implementation of the institution's operational risk framework at the line of business and firm-wide levels.

19. Management collectively is also responsible for ensuring that the institution has qualified staff and sufficient resources to carry out the operational risk functions outlined in the operational risk framework. Additionally, management must communicate operational risk

issues to appropriate staff that may not be directly involved in its management. Key management responsibilities include ensuring that:

- Operational risk management activities are conducted by qualified staff with the necessary experience, technical capabilities and access to adequate resources;
- Sufficient resources have been allocated to operational risk management, in the business lines as well as the independent firm-wide operational risk management function and verification areas, so as to sufficiently monitor and enforce compliance with the institution's operational risk policy and procedures; and
- Operational risk issues are effectively communicated with staff responsible for managing credit, market and other risks, as well as those responsible for purchasing insurance and managing third-party outsourcing arrangements.

B. Independent Firm-wide Risk Management Function

Supervisory Standards:

S 4. The institution must have an independent operational risk management function that is responsible for overseeing the operational risk framework at the firm level to ensure the development and consistent application of operational risk policies, processes, and procedures throughout the institution.

S 5. The firm-wide operational risk management function must ensure appropriate reporting of operational risk exposures and loss data to the board of directors and senior management.

20. The institution must have an independent firm-wide operational risk management function. The roles and responsibilities of the function will vary between institutions, but must be clearly documented. The independent firm-wide operational risk function should have organizational stature commensurate with the institution's operational risk profile, while remaining independent of the lines of business and the testing and verification function. At a minimum, the institution's independent firm-wide operational risk management function should ensure the development of policies, processes, and procedures that explicitly manage operational risk as a distinct risk to the institution's safety and soundness. These policies, processes and procedures should include principles for how operational risk is to be identified, measured,

monitored, and controlled across the organization. Additionally, they should provide for the collection of the data needed to calculate the institution's operational risk exposure.

21. Additional responsibilities of the independent firm-wide operational risk management function include:

- Assisting in the implementation of the overall firm-wide operational risk framework;
- Reviewing the institution's progress towards stated operational risk objectives, goals and risk tolerances;
- Periodically reviewing the institution's operational risk framework to consider the loss experience, effects of external market changes, other environmental factors, and the potential for new or changing operational risks associated with new products, activities or systems. This review process should include an assessment of industry best practices for the institution's activities, systems and processes;
- Reviewing and analyzing operational risk data and reports; and
- Ensuring appropriate reporting to senior management and the board.

C. Line of Business Management

Supervisory Standards:

S 6. Line of business management is responsible for the day-to-day management of operational risk within each business unit.

S 7. Line of business management must ensure that internal controls and practices within their line of business are consistent with firm-wide policies and procedures to support the management and measurement of the institution's operational risk.

22. Line of business management is responsible for both managing operational risk within the business lines and ensuring that policies and procedures are consistent with and support the firm-wide operational risk framework. Management should ensure that business-specific policies, processes, procedures and staff are in place to manage operational risk for all material products, activities, and processes. Implementation of the operational risk framework within each line of business should reflect the scope of that business and its inherent operational

complexity and operational risk profile. Line of business management must be independent of both the firm-wide operational risk management and the testing and verification functions.

VI. Operational Risk Management Elements

23. The operational risk management framework provides the overall operational risk strategic direction and ensures that an effective operational risk management and measurement process is adopted throughout the institution. The framework should provide for the consistent application of operational risk policies and procedures throughout the institution and address the roles of both the independent firm-wide operational risk management function and the lines of business. The framework should also provide for the consistent and comprehensive capture of data elements needed to measure and verify the institution's operational risk exposure, as well as appropriate operational risk analytical frameworks, reporting systems, and mitigation strategies. The framework must also include independent testing and verification to assess the effectiveness of implementation of the institution's operational risk framework, including compliance with policies, processes, and procedures.

24. In practice, an institution's operational risk framework must reflect the scope and complexity of business lines, as well as the corporate organizational structure. Each institution's operational risk profile is unique and requires a tailored risk management approach appropriate for the scale and materiality of the risks present, and the size of the institution. There is no single framework that would suit every institution; different approaches will be needed for different institutions. In fact, many operational risk management techniques continue to evolve rapidly to keep pace with new technologies, business models and applications.

25. The key elements in the operational risk management process include:

- Appropriate policies and procedures;

- Efforts to identify and measure operational risk;
- Effective monitoring and reporting;
- A sound system of internal controls; and
- Appropriate testing and verification of the operational risk framework.

A. Operational Risk Policies and Procedures

Supervisory Standards:

S 8. The institution must have policies and procedures that clearly describe the major elements of the operational risk management framework, including identifying, measuring, monitoring, and controlling operational risk.

26. Operational risk management policies, processes, and procedures should be documented and communicated to appropriate staff. The policies and procedures should outline all aspects of the institution's operational risk management framework, including:

- The roles and responsibilities of the independent firm-wide operational risk management function and line of business management;
- A definition for operational risk, including the loss event types that will be monitored;
- The capture and use of internal and external operational risk loss data, including large potential events (including the use of Scenario analysis);
- The development and incorporation of business environment and internal control factor assessments into the operational risk framework;
- A description of the internally derived analytical framework that quantifies the operational risk exposure of the institution;
- An outline of the reporting framework and the type of data/information to be included in line of business and firm-wide reporting;
- A discussion of qualitative factors and risk mitigants and how they are incorporated into the operational risk framework;
- A discussion of the testing and verification processes and procedures;
- A discussion of other factors that affect the measurement of operational risk; and
- Provisions for the review and approval of significant policy and procedural exceptions.

B. Identification and Measurement of Operational Risk

27. The result of a comprehensive program to identify and measure operational risk is an assessment of the institution's operational risk exposure. Management must establish a process

that identifies the nature and types of operational risk and their causes and resulting effects on the institution. Proper operational risk identification supports the reporting and maintenance of capital for operational risk exposure and events, facilitates the establishment of mechanisms to mitigate or control the risks, and ensures that management is fully aware of the sources of emerging operational risk loss events.

C. Monitoring and Reporting

Supervisory Standards:

S 9. Operational risk management reports must address both firm-wide and line of business results. These reports must summarize operational risk exposure, loss experience, relevant business environment and internal control assessments, and must be produced no less often than quarterly.

S 10. Operational risk reports must also be provided periodically to senior management and the board of directors, summarizing relevant firm-wide operational risk information.

28. Ongoing monitoring of operational risk exposures is a key aspect of an effective operational risk framework. To facilitate monitoring of operational risk, results from the measurement system should be summarized in reports that can be used by the firm-wide operational risk and line of business management functions to understand, manage, and control operational risk and losses. These reports should serve as a basis for assessing operational risk and related mitigation strategies and creating incentives to improve operational risk management throughout the institution.

29. Operational risk management reports should summarize:

- Operational risk loss experience on an institution, line of business, and event-type basis;
- Operational risk exposure;
- Changes in relevant risk and control assessments;
- Management assessment of early warning factors signaling an increased risk of future losses;

- Trend analysis, allowing line of business and independent firm-wide operational risk management to assess and manage operational risk exposures, systemic line of business risk issues, and other corporate risk issues;
- Exception reporting; and
- To the extent developed, operational risk causal factors.

30. High-level operational risk reports must also be produced periodically for the board and senior management. These reports must provide information regarding the operational risk profile of the institution, including the sources of material risk both from a firm-wide and line of business perspective, versus established management expectations.

D. Internal Control Environment

Supervisory Standards:

S 11. An institution's internal control structure must meet or exceed minimum regulatory standards established by the Agencies.

31. Sound internal controls are essential to an institution's management of operational risk and are one of the foundations of safe and sound banking. When properly designed and consistently enforced, a sound system of internal controls will help management safeguard the institution's resources, produce reliable financial reports, and comply with laws and regulations. Sound internal controls will also reduce the possibility of significant human errors and irregularities in internal processes and systems, and will assist in their timely detection when they do occur.

32. The Agencies are not introducing any new internal control standards, but rather emphasizing the importance of meeting existing standards. There is a recognition that internal control systems will differ among institutions due to the nature and complexity of an institution's products and services, organizational structure, and risk management culture. The AMA standards allows for these differences, while also establishing a baseline standard for the quality

of the internal control structure. Institutions will be expected to at least meet the minimum interagency standards[4] relating to internal controls as a criterion for AMA qualification.

33. The extent to which an institution meets or exceeds the minimum standards will primarily be assessed through current and ongoing supervisory processes. As noted earlier, the Agencies will leverage off existing examination processes, to avoid duplication in assessing an institution's implementation of an AMA framework. Assessing the internal control environment is clearly an area where the supervisory authorities already focus considerable attention.

VII. Elements of an AMA Framework

Supervisory Standards:

S 12. The institution must demonstrate that it has appropriate internal loss event data, relevant external loss event data, assessments of business environment and internal controls factors, and results from scenario analysis to support its operational risk management and measurement framework.

S 13. The institution must include the regulatory definition of operational risk as the baseline for capturing the elements of the AMA framework and determining its operational risk exposure.

S 14. The institution must have clear standards for the collection and modification of the elements of the operational risk AMA framework.

34. Operational risk inputs play a significant role in both the management and measurement of operational risk. Necessary elements of an institution's AMA framework include internal loss event data, relevant external loss event data, results of scenario analysis, and assessments of the institution's business environment and internal controls. Operational risk inputs aid the institution in identifying the level and trend of operational risk, determining the effectiveness of

[4] There are a number of interagency standards that cover topics relevant to the internal control structure. These include, for example, the Interagency Policy Statement on the Internal Audit Function and Its Outsourcing (March 2003), the Federal Financial Institution's Examination Council's (FFIEC's) Business Continuity Planning Booklet (May 2003), the FFIEC's Information Security Booklet (January 2003). In addition, each Agency has extensive

risk management and control efforts, highlighting opportunities to better mitigate operational risk, and assessing operational risk on a forward-looking basis.

35. To use its AMA framework, an institution must demonstrate that it has established a consistent and comprehensive process for the capture of all elements of the AMA framework. The institution must also demonstrate that it has clear standards for the collection and modification of all AMA inputs. While the analytical framework will generally combine these inputs to develop the operational risk exposure , supervisors must have the capacity to review the individual inputs as well; specifically, supervisors will need to review the loss information that is being provided to the analytical framework that stems from internal loss event data, versus the loss event information provided by external loss event data capture, scenario analysis, or the assessments of the business environment and internal control factors.

36. The capture systems must cover all material business lines, business activities and corporate functions that could generate operational risk. The institution must have a defined process that establishes responsibilities over the systems developed to capture the AMA elements. In particular, the issue of overriding the data capture systems must be addressed. Any overrides should be tracked separately and documented. Tracking overrides separately allows management and supervisors to identify the nature and rationale, including whether they stem from simple input errors or, more importantly, from exclusion because a loss event was not pertinent for the quantitative measurement. Management should have clear standards for addressing overrides and should clearly delineate who has authority to override the data systems and under what circumstances.

guidance on corporate governance, internal controls, and monitoring and reporting in its respective examination policies and procedures.

37. As noted earlier, for AMA qualification purposes, an institution's operational risk framework must, at a minimum, use the definition of operational risk that is provided in paragraph 10 when capturing the elements of the AMA framework. Institutions may use an expanded definition if considered more appropriate for risk management and measurement efforts. However, for the quantification of operational risk exposure for regulatory capital purposes, an institution must demonstrate that the AMA elements are captured so as to meet the baseline definition.

A. Internal Operational Risk Loss Event Data

Supervisory Standards:

S 15. The institution must have at least five years of internal operational risk loss data[5] captured across all material business lines, events, product types, and geographic locations.

S 16. The institution must be able to map internal operational risk losses to the seven loss-event type categories.

S 17. The institution must have a policy that identifies when an operational risk loss becomes a loss event and must be added to the loss event database. The policy must provide for consistent treatment across the institution.

S 18. The institution must establish appropriate operational risk data thresholds.

S 19. Losses that have any characteristics of credit risk, including fraud-related credit losses, must be treated as credit risk for regulatory capital purposes. The institution must have a clear policy that allows for the consistent treatment of loss event classifications (e.g., credit, market, or operational risk) across the organization.

38. The key to internal data integrity is the consistency and completeness with which loss event data capture processes are implemented across the institution. Management must ensure that operational risk loss event information captured is consistent across the business lines and

[5] With supervisory approval, a shorter initial historical observation period is acceptable for banks newly authorized to use an AMA methodology.

incorporates any corporate functions that may also experience operational risk events. Policies and procedures should be addressed to the appropriate staff to ensure that there is satisfactory understanding of operational risk and the data capture requirements under the operational risk framework. Further, the independent operational risk management function must ensure that the loss data is captured across all material business lines, products types, event types, and from all significant geographic locations. The institution must be able to capture and aggregate internal losses that cross multiple business lines or event types. If data is not captured across all business lines or from all geographic locations, the institution must document and explain the exceptions.

39. AMA institutions must be able to map operational risk losses into the seven loss event categories defined in paragraph 10. Institutions will not be required to produce reports or perform analysis for internal purposes on the basis of the loss event categories, but will be expected to use the information about the event-type categories as a check on the comprehensiveness of the institution's data set.

40. The institution must have five years of internal loss data, although a shorter range of historical data may be allowed, subject to supervisory approval. The extent to which an institution collects operational risk loss event data will, in part, be dependent upon the data thresholds that the institution establishes. There are a number of standards that an institution may use to establish the thresholds. They may be based on product types, business lines, geographic location, or other appropriate factors. The Agencies will allow flexibility in this area, provided the institution can demonstrate that the thresholds are reasonable, do not exclude important loss events, and capture a significant proportion of the institution's operational risk losses.

41. The institution must capture comprehensive data on all loss events above its established threshold level. Aside from information on the gross loss amount, the institution should collect information about the date of the event, any recoveries, and descriptive information about the drivers or causes of the loss event. The level of detail of any descriptive information should be commensurate with the size of the gross loss amount. Examples of the type of information collected include:

- Loss amount;
- Description of loss event;
- Where the loss is reported and expensed;
- Loss event type category;
- Date of the loss;
- Discovery date of the loss;
- Event end date;
- Management actions;
- Insurance recoveries;
- Other recoveries; and
- Adjustments to the loss estimate.

42. There are a number of additional data elements that may be captured. It may be appropriate, for example, to capture data on "near miss" events, where no financial loss was incurred. These near misses will not factor into the regulatory capital calculation, but may be useful for the operational risk management process.

43. Institutions will also be permitted and encouraged to capture loss events in their operational risk databases that are treated as credit risk for regulatory capital purposes, but have an underlying element of operational risk failure. These types of events, while not incorporated into the regulatory capital calculation, may have implications for operational risk management. It will be essential for institutions that capture loss events that are treated differently for regulatory capital and management purposes to demonstrate that 1) loss events are being captured consistently across the institution; 2) the data systems are sufficiently advanced to allow

for this differential treatment of loss events; and 3) credit, market, and operational risk losses are being appropriated in the correct manner for regulatory capital purposes.

44. The Agencies have established a clear boundary between credit and operational risks for regulatory capital purposes. If a loss event has any element of credit risk, it must be treated as credit risk for regulatory capital purposes. This would include all credit-related fraud losses. In addition, operational risk losses with credit risk characteristics that have historically been included in institutions' credit risk databases will continue to be treated as credit risk for the purposes of calculating minimum regulatory capital.

45. The accounting guidance for credit losses provides that creditors recognize credit losses when it is probable that they will be unable to collect all amounts due according to the contractual terms of a loan agreement. Credit losses may result from the creditor's own underwriting, processing, servicing or administrative activities along with the borrower's failure to pay according to the terms of the loan agreement. While the creditor's personnel, systems, policies or procedures may affect the timing or magnitude of a credit loss, they do not change its character from credit to operational risk loss for regulatory capital purposes. Losses that arise from a contractual relationship between a creditor and a borrower are credit losses whereas losses that arise outside of a relationship between a creditor and a borrower are operational losses.

B. External Data

Supervisory Standards:

S 20. The institution must have policies and procedures that provide for the use of external loss data in the operational risk framework.

S 21. Management must systematically review external data to ensure an understanding of industry experience.

46. External data may serve a number of different purposes in the operational risk framework. Where internal loss data is limited, external data may be a useful input in determining the institution's level of operational risk exposure. Even where external loss data is not an explicit input to an institution's data set, such data provides a means for the institution to understand industry experience, and in turn, provides a means for assessing the adequacy of its internal data. External data may also prove useful to inform scenario analysis, fit severity distributions, or benchmark the overall operational risk exposure results.

47. To incorporate external loss information into an institution's framework, the institution should collect the following information:

- External loss amount;
- External loss description;
- Loss event type category;
- External loss event date;
- Adjustments to the loss amount (i.e., recoveries, insurance settlements, etc) to the extent that they are known; and
- Sufficient information about the reporting institution to facilitate comparison to its own organization.

48. Institutions may obtain external loss data in any reasonable manner. There are many ways to do so; some institutions are using data acquired through membership with industry consortia while other institutions are using data obtained from vendor databases or public sources such as court records or media reports. In all cases, management will need to carefully evaluate the data source to ensure that they are comfortable that the information being reported is relevant and reasonably accurate.

C. Business Environment and Internal Control Factor Assessments

Supervisory Standards:

S 22. The institution must have a system to identify and assess business environment and internal control factors.

S 23. Management must periodically compare the results of their business environment and internal control factor assessments against actual operational risk loss experience.

49. While internal and external loss data provide a historical perspective on operational risk, it is also important that institutions incorporate a forward-looking element to the operational risk measure. In principle, an institution with strong internal controls in a stable business environment will have less exposure to operational risk than an institution with internal control weaknesses that is growing rapidly or introducing new products. In this regard, institutions will be required to identify the level and trends in operational risk in the institution. These assessments must be current, comprehensive across the institution, and identify the critical operational risks facing the institution.

50. The business environment and internal control factor assessments should reflect both the positive and negative trends in risk management within the institution as well as changes in an institution's business activities that increase or decrease risk. Because the results of the risk assessment are part of the capital methodology, management must ensure that the risk assessments are done appropriately and reflect the risks of the institution. Periodic comparisons should be made between actual loss exposure and the assessment results.

51. The framework established to maintain the risk assessments must be sufficiently flexible to encompass an institution's increased complexity of activities, new activities, changes in internal control systems, or an increased volume of information.

D. Scenario Analysis

Supervisory Standards:

S 24. Management must have policies and procedures that identify how scenario analysis will be incorporated into the operational risk framework.

52. Scenario analysis is a systematic process of obtaining expert opinions from business managers and risk management experts to derive reasoned assessments of the likelihood and impact of plausible operational losses consistent with the regulatory soundness standard. Within an institution's operational risk framework, scenario analysis may be used as an input or may, as discussed below, form the basis of an operational risk analytical framework.

53. As an input to the institution's framework, scenario analysis is especially relevant for business lines or loss event types where internal data, external data, and assessments of the business environment and internal control factors do not provide a sufficiently robust estimate of the institution's exposure to operational risk. In some cases, an institution's internal loss history may be sufficient to provide a reasonable estimate of exposure to future operational losses. In other cases, the use of well-reasoned, scaled external data may itself be a form of scenario analysis.

54. The institution must have policies and procedures that define scenario analysis and identify its role in the operational risk framework. The policy should cover key elements of scenario analysis, such as the manner in which the scenarios are generated, the frequency with which they are updated, and the scope and coverage of operational loss events they are intended to reflect.

VIII. Risk Quantification

A. Analytical Framework

Supervisory Standards:

S 25. The institution must have a comprehensive operational risk analytical framework that provides an estimate of the institution's operational risk

exposure, which is the aggregate operational loss that it faces over a one-year period at a soundness standard consistent with a 99.9 per cent confidence level.

S 26. Management must document the rationale for all assumptions underpinning its chosen analytical framework, including the choice of inputs, distributional assumptions, and the weighting across qualitative and quantitative elements. Management must also document and justify any subsequent changes to these assumptions.

S 27. The institution's operational risk analytical framework must use a combination of internal operational loss event data, relevant external operational loss event data, business environment and internal control factor assessments, and scenario analysis. The institution must combine these elements in a manner that most effectively enables it to quantify its operational risk exposure. The institution can choose the analytical framework that is most appropriate to its business model.

S 28. The institution's capital requirement for operational risk will be the sum of expected and unexpected losses unless the institution can demonstrate, consistent with supervisory standards, the expected loss offset.

55. The industry has made significant progress in recent years in developing analytical frameworks to quantify operational risk. The analytical frameworks, which are a part of the overall operational risk framework, are based on various combinations of an institution's own operational loss experience, the industry's operational loss experience, the size and scope of the institution's activities, the quality of the institution's control environment, and management's expert judgment. Because these models capture specific characteristics of each institution, such models yield unique risk-sensitive estimates of the institutions' operational risk exposures.

56. While the Agencies are not specifying the exact methodology that an institution should use to determine its operational risk exposure, minimum supervisory standards for acceptable approaches have been developed. These standards have been set so as to assure that the regulation can accommodate continued evolution of operational risk quantification techniques, yet remain amenable to consistent application and enforcement across institutions. The Agencies will require that the institution have a comprehensive analytical framework that provides an

estimate of the aggregate operational loss that it faces over a one-year period at a soundness standard consistent with a 99.9 percent confidence level, referred to as the institution's operational risk exposure. The institution will multiply the exposure estimate by 12.5 to obtain risk weighted assets for operational risk, and add this figure to risk-weighted assets for credit and market risk to obtain total risk-weighted assets. The final minimum regulatory capital number will be 8 percent of total risk-weighted assets.

57. The Agencies expect that there will be significant variation in analytical frameworks across institutions, with each institution tailoring its framework to leverage existing technology platforms and risk management procedures. These approaches may only be used, provided they meet the supervisory standards and include, as inputs, internal operational loss event data, relevant external operational loss event data, assessments of business environment and internal control factors, and scenario analysis. The Agencies do expect that there will be some uncertainty and potential error in the analytical frameworks because of the evolving nature of operational risk measurement and data capture. Therefore, a degree of conservatism will need to be built into the analytical frameworks to reflect the evolutionary status of operational risk and its impact on data capture and analytical modeling.

58. A diversity of analytical approaches is emerging in the industry, combining and weighting these inputs in different ways. Most current approaches seek to estimate loss frequency and loss severity to arrive at an aggregate loss distribution. Institutions then use the aggregate loss distribution to determine the appropriate amount of capital to hold for a given soundness standard. Scenario analysis is also being used by many institutions, albeit to significantly varying degrees. Some institutions are using scenario analysis as the basis for their

analytical framework, while others are incorporating scenarios as a means for considering the possible impact of significant operational losses on their overall operational risk exposure.

59. The primary differences among approaches being used today relate to the weight that institutions place on each input. For example, institutions with comprehensive internal data may place less emphasis on external data or scenario analysis. Another example is that some institutions estimate a unique loss distribution for each business line/loss type combination (bottom-up approach) while others estimate a loss distribution on a firm-wide basis and then use an allocation methodology to assign capital to business lines (top-down approach).

60. The Agencies expect internal loss event data to play an important role in the institution's analytical framework, hence the requirement for five years of internal operational risk loss data. However, as footnote 5 makes clear, five years of data is not always required for the analytical framework. For example, if a bank exited a business line, the institution would not be expected to make use of that business unit's loss experience unless it had relevance for other activities of the institution. Another example would be where a bank has made a recent acquisition where the acquired firm does not have internal loss event data. In these cases, the Agencies expect the institution to make use of the loss data available at the acquired institution and any internal loss data from operations similar to that of the acquired firm, but the institution will likely have to place more weight relevant external loss event data, results from scenario analysis, and factors reflecting assessments of the business environment and internal controls.

61. Whatever analytical approach an institution chooses, it must document and provide the rationale for all assumptions embedded in its chosen analytical framework, including the choice of inputs, distributional assumptions, and the weighting of qualitative and quantitative elements.

Management must also document and justify any subsequent changes to these assumptions. This documentation should:

- Clearly identify how the different inputs are combined and weighted to arrive at the overall operational risk exposure so that the analytical framework is transparent. The documentation should demonstrate that the analytical framework is comprehensive and internally consistent. Comprehensiveness means that all required inputs are incorporated and appropriately weighted. At the same time, there should not be overlaps or double counting.
- Clearly identify the quantitative assumptions embedded in the methodology and provide explanation for the choice of these assumptions. Examples of quantitative assumptions include distributional assumptions about frequency and severity, the methodology for combining frequency and severity to arrive at the overall loss distribution, and dependence assumptions between operational losses across and within business lines.
- Clearly identify the qualitative assumptions embedded in the methodology and provide explanations for the choice of these assumptions. Examples of qualitative assumptions include the use of business environment and control factors as well as scenario analysis in the approach.
- Where feasible, provide results based purely on quantitative methods separately from results that incorporate qualitative factors. This will provide a transparent means of determining the relative importance of quantitative versus qualitative inputs.
- Where feasible, provide results based on alternative quantitative and qualitative assumptions to gauge the overall model's sensitivity to these assumptions.
- Provide a comparison of the operational risk exposure estimate generated by the analytical framework with actual loss experience over time, to assess the reasonable of the framework's outputs.
- Clearly identify all changes to assumptions, and provide explanations for such changes.
- Clearly identify the results of an independent verification of the analytical framework.

62. The regulatory capital charge for operational risk will include both expected losses (EL) and unexpected losses (UL). The Agencies have considered two approaches that might allow for some recognition of EL; these approaches are reserving and budgeting. However, both approaches raise questions about their ability to act as an EL offset for regulatory capital purposes. The current U.S. GAAP treatment for reserves (or liabilities) is based on an incurred-loss (liability) model. Given that EL is looking beyond current losses to losses that will be incurred in the future, establishing a reserve for operational risk EL is not likely to meet US accounting standards. While reserves are specific allocations for incurred losses, budgeting is a

process of generally allocating future income for loss contingencies, including losses resulting from operational risk. Institutions will be required to demonstrate that budgeted funds are sufficiently capital-like and remain available to cover EL over the next year. In addition, an institution will not be permitted to recognize EL offsets on budgeted loss contingencies that fall below the established data thresholds; this is relevant as many institutions currently budget for low severity, high frequency events that are more likely to fall below most institutions' thresholds.

63. An institution's analytical framework complements but does not substitute for prudent controls. Rather, with improved risk measurement, institutions are finding that they can make better-informed strategic decisions regarding enhancements to controls and processes, the desired scale and scope of the operations, and how insurance and other risk mitigation tools can be used to offset operational risk exposure.

B. Accounting for Dependence

Supervisory Standards:

S 29. Management must document how its chosen analytical framework accounts for dependence (e.g., correlations) among operational losses across and within business lines. The institution must demonstrate that its explicit and embedded dependence assumptions are appropriate, and where dependence assumptions are uncertain, the institution must use conservative estimates.

64. Management must document how its chosen analytical framework accounts for dependence (e.g., correlation) between operational losses across and within business lines. The issue of dependence is closely related to the choice between a bottom-up or a top-down modeling approach. Under a bottom-up approach, explicit assumptions regarding cross-event dependence are required to estimate operational risk exposure at the firm-wide level. Management must demonstrate that these assumptions are appropriate and reflect the institution's current

environment. If the dependence assumptions are uncertain, the institution must choose conservative estimates. In so doing, the institution should consider the possibility that cross-event dependence may not be constant, and may increase during stress environments.

65. Under a top-down approach, an explicit assumption regarding dependence is not required. However, a parametric distribution for loss severity may be more difficult to specify under the top-down approach, as it is a statistical mixture of (potentially) heterogeneous business line and event type distributions. Institutions must carefully consider the conditions necessary for the validity of top-down approaches, and whether these conditions are met in their particular circumstances. Similar to bottom-up approaches, institutions using top-down approaches must ensure that implicit dependence assumptions are appropriate and reflect the institution's current environment. If historic dependence assumptions embedded in top-down approaches are uncertain, the institution must be conservative and implement a qualitative adjustment to the analysis.

IX. Risk Mitigation

Supervisory Standards:

S 30. Institutions may reduce their operational risk exposure results by no more than 20% to reflect the impact of risk mitigants. Institutions must demonstrate that mitigation products are sufficiently capital-like to warrant inclusion in the adjustment to the operational risk exposure.

66. There are many mechanisms to manage operational risk, including risk transfer through risk mitigation products. Because risk mitigation can be an important element in limiting or reducing operational risk exposure in an institution, an adjustment is being permitted that will directly impact the amount of regulatory capital that is held for operational risk. The adjustment is limited to 20% of the overall operational risk exposure result determined by the institution using its loss data, qualitative factors, and quantitative framework.

67. Currently, the primary risk mitigant used for operational risk is insurance. There has been discussion that some securities products may be developed to provide risk mitigation benefits; however, to date, no specific products have emerged that have characteristics sufficient to be considered capital-replacement for operational risk. As a result, securities products and other capital market instruments may not be factored in to the regulatory capital risk mitigation adjustment at this time.

68. For an institution that wishes to adjust its regulatory capital requirement as a result of the risk mitigating impact of insurance, management must demonstrate that the insurance policy is sufficiently capital-like to provide the cushion that is necessary. A product that would fall in this category must have the following characteristics:

- The policy is provided through a third party[6] that has a minimum claims paying ability rating of A[7];
- The policy has an initial term of one year[8];
- The policy has no exclusions or limitations based upon regulatory action or for the receiver or liquidator of a failed bank;
- The policy has clear cancellation and non-renewal notice periods; and
- The policy coverage has been explicitly mapped to actual operational risk exposure of the institution.

69. Insurance policies that meet these standards may be incorporated into an institution's adjustment for risk mitigation. An institution should be conservative in its recognition of such policies, for example, the institution must also demonstrate that insurance policies used as the basis for the adjustment have a history of timely payouts. If claims have not been paid on a timely basis, the institution must exclude that policy from the operational risk capital adjustment.

[6] Where operational risk is transferred to a captive or an affiliated insurer such that risk is retained within the group structure, recognition of such risk transfer will only be allowed for regulatory capital purposes where the risk has been transferred to a third party (e.g., an unaffiliated reinsurer) that meets the standards set forth in this section.
[7] Rating agencies may use slightly different rating scales. For the purpose of this supervisory guidance, the insurer must have a rating that is at least the equivalent of A under Standard and Poor's Insurer Financial Strength Ratings or an A2 under Moody's Insurance Financial Strength Ratings.

In addition, the institution must be able to show that the policy would actually be used in the event of a loss situation; that is, the deductible may not be set so high that no loss would ever conceivably exceed the deductible threshold.

70. The Agencies will not specify how institutions should calculate the risk mitigation adjustment. Nevertheless, institutions are expected to use conservative assumptions when calculating adjustments. An institution should discount (i.e., apply its own estimates of haircuts) the impact of insurance coverage to take into account factors, which may limit the likelihood or size of claims payouts. Among these factors are the remaining terms of a policy, especially when it is less than a year, the willingness and ability of the insurer to pay on a claim in a timely manner, the legal risk that a claim may be disputed, and the possibility that a policy can be cancelled before the contractual expiration.

X. Data Maintenance

Supervisory Standards:

S 31. Institutions using the AMA approach for regulatory capital purposes must use advanced data management practices to produce credible and reliable operational risk estimates.

71. Data maintenance is a critical factor in an institution's operational risk framework. Institutions with advanced data management practices should be able to track operational risk loss events from initial discovery through final resolution. These institutions should also be able to make appropriate adjustments to the data and use the data to identify trends, track problem areas, and identify areas of future risk. Such data should include not only operational risk loss event information, but also information on risk assessments, which are factored into the operational risk exposure calculation. In general, institutions using the AMA should have the

[8] Institutions must decrease the amount of the adjustment if the remaining term is less than one year. The institution

same data maintenance standards for operational risk as those set forth for A-IRB institutions under the credit risk guidance.

72. Operational risk data elements captured by the institution must be of sufficient depth, scope, and reliability to:

- Track and identify operational risk loss events across all business lines, including when a loss event impact multiple business lines.
- Calculate capital ratios based on operational risk exposure results. The institution must also be able to factor in adjustments related to risk mitigation, correlations, and risk assessments.
- Produce internal and public reports on operational risk measurement and management results, including trends revealed by loss data and/or risk assessments. The institution must also have sufficient data to produce exception reports for management.
- Support risk management activities.

73. The data warehouse[9] must contain the key data elements needed for operational risk measurement, management, and verification. The precise data elements may vary by institution and also among business lines within an institution. An important element of ensuring consistent reporting of the data elements is to develop comprehensive definitions for each data element used by the institution for reporting operational risk loss events or for the risk assessment inputs. The data must be stored in an electronic format to allow for timely retrieval for analysis, verification and testing of the operational risk framework, and required disclosures.

74. Management will need to identify those responsible for maintaining the data warehouse. In particular, policies and processes will need to be developed for delivering, storing, retaining, and updating the data warehouse. Policies and procedures must also cover the edit checks for data input functions, as well as the requirements for the testing and verification function to verify data integrity. Like other areas of the operational risk framework, it is critical that management

---

must have a clear policy in place that links the remaining term to the adjustment factor.

ensure accountability for ongoing data maintenance, as this will impact operational risk management and measurement efforts.

XI. Testing and Verification

Supervisory Standards:

S 32. The institution must test and verify the accuracy and appropriateness of the operational risk framework and results.

S 33. Testing and verification must be done independently of the firm-wide operational risk management function and the institution's lines of business.

75. The operational risk framework must provide for regular and independent testing and verification of operational risk management policies, processes and measurement systems, as well as operational risk data capture systems. For most institutions, operational risk verification and testing will primarily be done by the audit function. Internal and external audits can provide an independent assessment of the quality and effectiveness of the control systems' design and performance. However, institutions may use other independent internal units (e.g. quality assurance) or third parties. The testing and verification function, whether internally or externally performed, should be staffed by qualified individuals who are independent from the firm-wide operational risk management function and the institution's lines of business.

76. The verification of the operational risk measurement system should include the testing of:

- Key operational risk processes and systems;
- Data feeds and processes associated with the operational risk measurement system;
- Adjustments to empirical operational risk capital estimates, including operational risk exposure;
- Periodic certification of operational risk models used and their underlying assumptions; and

[9] In this document, the terms "database" and "data warehouse" are used interchangeably to refer to a collection of data arranged for easy retrieval using computer technology.

- Assumptions underlying operational risk exposure, data decision models, and operational risk capital charge.

77. The operational risk reporting processes should be periodically reviewed for scope and effectiveness. The institution should have independent verification processes to ensure the timeliness, accuracy, and comprehensiveness of operational risk reporting systems, both at the firm-wide and the line of business levels.

78. Independent verification and testing should be done to ensure the integrity and applicability of the operational risk framework, operational risk exposure/loss data, and the underlying assumptions driving the regulatory capital measurement process. Appropriate reports, summarizing operational risk verification and testing findings for both the independent firm-wide risk management function and lines of business should be provided to appropriate management and the board of directors or a designated board committee.

Appendix A
Supervisory Standards for the AMA

S 1. **The institution's operational risk framework must include an independent firm-wide operational risk management function, line of business management oversight, and independent testing and verification functions.**

S 2. **The board of directors must oversee the development of the firm-wide operational risk framework, as well as major changes to the framework. Management roles and accountability must be clearly established.**

S 3. **The board of directors and management must ensure that appropriate resources are allocated to support the operational risk framework.**

S 4. **The institution must have an independent operational risk management function that is responsible for overseeing the operational risk framework at the firm level to ensure the development and consistent application of operational risk policies, processes, and procedures throughout the institution.**

S 5. **The firm-wide operational risk management function must ensure appropriate reporting of operational risk exposures and loss data to the board of directors and senior management.**

S 6. **Line of business management is responsible for the day-to-day management of operational risk within each business unit.**

S 7. **Line of business management must ensure that internal controls and practices within their line of business are consistent with firm-wide policies and procedures to support the management and measurement of the institution's operational risk.**

S 8. **The institution must have policies and procedures that clearly describe the major elements of the operational risk management framework, including identifying, measuring, monitoring, and controlling operational risk.**

S 9. **Operational risk management reports must address both firm-wide and line of business results. These reports must summarize operational risk exposure, loss experience, relevant business environment and internal control assessments, and must be produced no less often than quarterly.**

S 10. **Operational risk reports must also be provided periodically to senior management and the board of directors, summarizing relevant firm-wide operational risk information.**

S 11. **An institution's internal control structure must meet or exceed minimum regulatory standards established by the Agencies.**

S 12. **The institution must demonstrate that it has appropriate internal loss event data, relevant external loss event data, assessments of business environment and internal controls factors, and results from scenario analysis to support its operational risk management and measurement framework.**

S 13. **The institution must include the regulatory definition of operational risk as the baseline for capturing the elements of the AMA framework and determining its operational risk exposure.**

S 14. **The institution must have clear standards for the collection and modification of the elements of the operational risk AMA framework.**

S 15. **The institution must have at least five years of internal operational risk loss data[10] captured across all material business lines, events, product types, and geographic locations.**

S 16. **The institution must be able to map internal operational risk losses to the seven loss-event type categories.**

S 17. **The institution must have a policy that identifies when an operational risk loss becomes a loss event and must be added to the loss event database. The policy must provide for consistent treatment across the institution.**

S 18. **The institution must establish appropriate operational risk data thresholds.**

S 19. **Losses that have any characteristics of credit risk, including fraud-related credit losses, must be treated as credit risk for regulatory capital purposes. The institution must have a clear policy that allows for the consistent treatment of loss event classifications (e.g., credit, market, or operational risk) across the organization.**

S 20. **The institution must have policies and procedures that provide for the use of external loss data in the operational risk framework.**

S 21. **Management must systematically review external data to ensure an understanding of industry experience.**

S 22. **The institution must have a system to identify and assess business environment and internal control factors.**

S 23. **Management must periodically compare the results of their business environment and internal control factor assessments against actual operational risk loss experience.**

[10] With supervisory approval, a shorter initial historical observation period is acceptable for banks newly authorized to use an AMA methodology.

S 24. **Management must have policies and procedures that identify how scenario analysis will be incorporated into the operational risk framework.**

S 25. **The institution must have a comprehensive operational risk analytical framework that provides an estimate of the institution's operational risk exposure, which is the aggregate operational loss that it faces over a one-year period at a soundness standard consistent with a 99.9 per cent confidence level.**

S 26. **Management must document the rationale for all assumptions underpinning its chosen analytical framework, including the choice of inputs, distributional assumptions, and the weighting across qualitative and quantitative elements. Management must also document and justify any subsequent changes to these assumptions.**

S 27. **The institution's operational risk analytical framework must use a combination of internal operational loss event data, relevant external operational loss event data, business environment and internal control factor assessments, and scenario analysis. The institution must combine these elements in a manner that most effectively enables it to quantify its operational risk exposure. The institution can choose the analytical framework that is most appropriate to its business model.**

S 28. **The institution's capital requirement for operational risk will be the sum of expected and unexpected losses unless the institution can demonstrate, consistent with supervisory standards, the expected loss offset.**

S 29. **Management must document how its chosen analytical framework accounts for dependence (e.g., correlations) among operational losses across and within business lines. The institution must demonstrate that its explicit and embedded dependence assumptions are appropriate, and where dependence assumptions are uncertain, the institution must use conservative estimates.**

S 30. **Institutions may reduce their operational risk exposure results by no more than 20% to reflect the impact of risk mitigants. Institutions must demonstrate that mitigation products are sufficiently capital-like to warrant inclusion in the adjustment to the operational risk exposure.**

S 31. **Institutions using the AMA approach for regulatory capital purposes must use advanced data management practices to produce credible and reliable operational risk estimates.**

S 32. **The institution must test and verify the accuracy and appropriateness of the operational risk framework and results.**

S 33. Testing and verification must be done independently of the firm-wide operational risk management function and the institution's lines of business.