

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.

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.

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.

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 standards¹¹ relating to internal controls as a criterion for AMA qualification.

¹¹ 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 guidance on corporate governance, internal controls, and monitoring and reporting in its respective examination policies and procedures.

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.

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

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.

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.

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 data¹² 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

¹² With supervisory approval, a shorter initial historical observation period is acceptable for banks newly authorized to use an AMA methodology.