

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

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 impacts 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. The data warehouse<sup>16</sup> 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.

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 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.

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.

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

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.

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

<sup>16</sup> 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.