**Board of Governors of the Federal Reserve System**
**Federal Deposit Insurance Corporation**
**Office of the Comptroller of the Currency**
**Office of Thrift Supervision**

# Interagency Guidance on The Advanced Measurement Approaches for Operational Risk

June 3, 2011

## Introduction

On December 7, 2007, the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System (Board), the Federal Deposit Insurance Corporation (FDIC), and the Office of Thrift Supervision (OTS) (collectively, the agencies) issued a final rule to implement new risk-based capital requirements in the United States for large, internationally active banking organizations (advanced approaches rule).[1] The advanced approaches rule requires qualifying core banks[2] and permits other qualifying banks to use advanced measurement approaches (AMA) to calculate risk-based capital requirements for operational risk.[3]

The purpose of the AMA is to enhance operational risk measurement and management. The AMA framework requires effective governance, risk capture and assessment, and quantification of operational risk exposure; however, banks have flexibility to develop operational risk measurement and management programs, processes, and tools to meet these requirements that are appropriate relative to banks' activities, business environment, and internal controls. As new methods and tools are developed, the agencies anticipate that the operational risk discipline will continue to mature and converge toward a narrower range of effective risk management and measurement practices.

This interagency guidance discusses certain common implementation issues and challenges, as well as key considerations for addressing these challenges in order to implement a satisfactory AMA framework. This guidance focuses on the combination and use of the four required AMA data elements – internal operational loss event data, external operational loss event data, business environment and internal control factors (BEICFs), and scenario analysis. Given some of the unique challenges with scenario analysis as it relates to the AMA, this data element is discussed in greater detail. Governance and validation also are discussed given their importance in ensuring the integrity of a bank's AMA framework.

[1] See 72 FR 69288. The agencies' advanced approaches rules are at 12 CFR part 3, Appendix C (OCC); 12 CFR part 208, Appendix F and 12 CFR part 225, Appendix G (Board); 12 CFR part 325, Appendix D (FDIC); and 12 CFR part 567, Appendix C (OTS).

[2] For simplicity, and unless otherwise indicated, the advanced approaches rule and this guidance use the term "bank" to include banks, savings associations, and bank holding companies (BHC). The terms "bank holding company" and "BHC" refer only to bank holding companies regulated by the Board and do not include savings and loan holding companies currently regulated by the OTS.

[3] "Core" banks are those banks that must apply the advanced approaches rule under Part I, section 1(b)(1) of the advanced approaches rule.

This guidance addresses certain aspects of the minimum risk-based capital requirements for operational risk and is not intended to address the treatment of operational risk in a bank's internal capital adequacy assessment process.

## Governance

The advanced approaches rule requires that a bank establish an operational risk management function (ORMF) that is responsible for the design, implementation, and oversight of the bank's AMA framework, including operational risk data and assessment systems and operational risk quantification systems and related processes.[4] The ORMF must be independent of business line management.[5] The ORMF also should have an organizational stature commensurate with the bank's operational risk profile.

While a bank has flexibility in determining its governance structure, the agencies will carefully assess independence and organizational stature in those organizational structures where the ORMF reports to a unit other than the bank's independent risk management function.[6] Banks should be prepared to demonstrate that their operational risk governance structures are independent, have appropriate stature within the organization, and are consistent with an effective system of controls and oversight.[7]

Stability of organizational structures facilitates consistent implementation and sustained performance of the AMA. Frequent restructuring of a bank's ORMF could raise supervisory concerns about the effectiveness of a bank's operational risk governance. Having the ORMF structure in place during a bank's parallel run represents one element of a set of sustainable processes that are part of the qualification requirements the bank will need to demonstrate in order to use the advanced approaches rule.[8] While organizational and structural changes may be necessary after qualification to better manage changes in the bank's operational risk profile, supervisors will closely scrutinize significant changes to the ORMF, especially during a bank's parallel run.

## The Four Data Elements

The advanced approaches rule requires that a bank's operational risk data and assessment systems capture operational risks to which the firm is exposed. These systems must include credible, transparent, systematic, and verifiable processes on an ongoing basis that incorporate the four required AMA data elements of (1) internal operational loss event data, (2) external

[4] See section 22(h)(1)(i)(B) of the advanced approaches rule.

[5] See section 22(h)(1) of the advanced approaches rule.

[6] Reporting lines that will raise specific supervisory concerns include those that have the ORMF reporting to functions that are both sources of inherent operational risk and are responsible for managing operational risk. These functions may include both traditional lines of business, as well as corporate functions or officers (e.g., the chief financial officer).

[7] See section 22(j)(3) of the advanced approaches rule.

[8] See 73 FR 44620 (July 31, 2008), interagency "Supervisory Guidance: Supervisory Review Process of Capital Adequacy (Pillar 2) Related to the Implementation of the Basel II Advanced Capital Framework."

operational loss event data, (3) scenario analysis, and (4) BEICFs.[9] The advanced approaches rule also requires that a bank's operational risk quantification systems generate estimates of the bank's operational risk exposure using the bank's operational risk data and assessment systems, and include a credible, transparent, systematic, and verifiable approach for weighting each of the four elements.[10]

***Internal Operational Loss Event Data***

Internal operational loss event data (internal data) under the advanced approaches rule are gross operational loss amounts, dates, recoveries, and relevant causal information for operational loss events occurring at the bank. While the advanced approaches rule provides flexibility in a bank's use and weighting of the four data elements, internal data is a key element in operational risk management and quantification. For quantification, many banks currently use a loss distribution approach (LDA) to estimate their operational risk exposure. When using an LDA, internal data should be used to estimate both the frequency and severity of operational losses.

The advanced approaches rule requires that a bank's operational risk data and assessment systems include a historical observation period of at least five years for its internal data.[11] Banks should carefully consider the benefits of using an observation period longer than the five-year minimum to estimate operational risk exposure, especially in cases where the five-year minimum period contains few extremely large (tail) events. A bank should ensure that the time series used for operational risk exposure estimation includes all relevant internal data, including tail events. The agencies will scrutinize cases in which a bank excludes internal data from the estimation of operational risk severity, particularly the exclusion of tail events. The agencies recognize that banks have different loss histories and that some banks have experienced few tail losses. Therefore, banks also should consider the impact of relevant external operational loss event data (external data) and scenario analysis for producing meaningful estimates of operational risk exposure.

The advanced approaches rule permits a bank to refrain from collecting internal data for individual operational losses below established dollar threshold amounts if the bank can demonstrate to the satisfaction of its primary federal supervisor that the thresholds are reasonable, do not exclude important internal operational loss event data, and permit the bank to capture substantially all the dollar value of the bank's operational losses.[12] Banks should have documented support for their internal data collection threshold(s) that considers information needed to effectively manage operational risk losses at the corporate and business line levels and estimate exposure amounts for each unit of measure (UOM).[13]

---

[9] See section 22(h)(2) of the advanced approaches rule.

[10] See sections 22(h)(2)(ii) and 22(h)(3)(i)(C) of the advanced approaches rule.

[11] See section 22(h)(2)(ii)(A)(1) of the advanced approaches rule. Shorter observation periods may be approved by the bank's primary federal supervisor to address transitional issues such as integrating a new business line.

[12] See section 22(h)(2)(ii)(A)(3) of the advanced approaches rule.

[13] As defined in section 2 of the advanced approaches rule, unit of measure refers to the level (for example, organizational unit or operational loss event type) at which the bank's operational risk quantification system generates a separate distribution of potential operational losses.

The collection and use of legal loss data can pose challenges in the operational risk quantification process that result from factors such as the time lag that often exists between initiation and settlement of legal cases and the practices around discovery. These losses can have a significant impact on a bank's estimate of operational risk exposure. Banks' approaches vary for determining when a legal loss amount is included in their operational risk quantification processes. Some banks incorporate a legal loss amount at the time a legal reserve is created, whereas other banks incorporate legal losses at settlement. The varying treatment of these losses across banks could result in differences in capital requirements for similar exposures. To address these potential differences and ensure that a bank's operational risk capital reflects its risk profile, a bank should include legal losses in its quantification processes using a date no later than the date a legal reserve is established. Banks should have policies that describe their practices for collecting legal loss data and using it in the quantification process.

***External Operational Loss Event Data***

External data under the advanced approaches rule are gross operational loss amounts, dates, recoveries, and relevant causal information for operational loss events occurring at organizations other than the bank.[14] External data complement the internal data a bank uses for operational risk measurement and management. External data can provide a bank's senior management and business lines with useful information on potential areas of risk exposure or control failures based on industry loss experience. In addition to its role in the operational risk quantification process, external data can be an important input to a bank's scenario analysis and BEICF processes. For internal risk-management reporting purposes, the inclusion of external data with other data elements can support development of a comprehensive risk profile.

*External Data Sources*

Banks commonly obtain external data from publicly available sources or consortia. Banks should carefully consider the varied characteristics among data from different sources to ensure appropriate alignment of these data with their intended use. Relative to consortia data, publicly sourced data generally contain more descriptive information on individual operational loss events and their underlying causes. This information is particularly useful in assessing the relevance of an event to a particular bank and for conducting analysis of potential losses and control failures. However, one of the challenges with using publicly sourced external data is addressing the inherent reporting bias, which refers to the tendency of publicly reported losses to focus only on larger, more notable losses. Banks should address these biases in their methodologies for incorporating external data into their AMA frameworks.

In contrast, while consortia data typically contain less descriptive or causal information, these data are consistently collected under standard rules and tend to comprise a broader range of operational loss events and associated dollar amounts. As a result, consortia data are not subject to the same reporting bias as publicly sourced information, but banks may face challenges in determining data relevance. In addition, banks face challenges in appropriately scaling both

[14] Section 22(h)(2)(ii)(B) of the advanced approaches rule requires that a bank have a systematic process for determining its methodologies for incorporating external operational loss event data into its operational risk data and assessment systems.

publicly sourced and consortia external data. Regardless of the external data source used, banks should demonstrate that the external data they use are relevant to their risk profiles and appropriate for use in their AMA frameworks.

*External Data Use in Operational Risk Measurement*

As with the other data elements, banks should carefully consider and adequately document how external data are incorporated into their quantification systems. The agencies note that there are significant inherent challenges associated with combining external and internal data in the same model. As such, supervisors will closely scrutinize a bank's approach for combining internal data and external data at the observation level, and will analyze a bank's statistical evidence and rationale for why such an approach is valid.

External data typically are used as a direct input into a severity model based solely on external data. The results of the severity model are then combined with results from an internal data model. When internal and external loss data are modeled separately and then combined to estimate operational risk exposure, banks should have a credible, transparent, systematic, and verifiable process for combining the results from the two models. Any weighting scheme used to combine the results should have well-documented empirical support, including sensitivity analysis that considers the impact of different weighting schemes.

External data may be used in a benchmark approach when a bank can appropriately characterize its operational risk exposure in a base model that uses only internal data. In a benchmark approach, external data is used as a direct input into a model that is separate from the base internal data model. The outcome of the benchmark model is compared to that of the base model and may result in a change in the operational risk exposure estimate generated by the base model. (See the *Scenario Analysis as a Benchmark* discussion below; external data as a benchmark would follow a similar approach.)

While external data can be a useful tool in quantifying operational risk exposure, certain operational losses contained in the raw external data may not be directly relevant for a particular bank's risk profile. A bank may use a number of approaches to address this issue, including external data filtering and scaling methodologies. External data filtering involves the selection of relevant external data based on specific criteria. A bank's filtering processes must be credible, transparent, systematic, verifiable,[15] and should result in objective and consistent selection of data (for example, large losses should not be subjectively excluded). If a bank permits exceptions as part of its external data selection process, the bank should have clear policies and procedures that describe the criteria for such exceptions. The bank also should adequately document and provide its rationale for any exceptions.

In some cases, such as when a bank's size or business activities differ substantially from those of banks represented in a given external dataset, it may be appropriate for a bank to scale the external data for use in estimating its operational risk exposure. The bank must provide empirical support demonstrating that its scaling methodology is credible, transparent, systematic, and

[15] See section 22(h)(2)(ii) of the advanced approaches rule.

verifiable.[16] If a scaling model developed by a third party (e.g., a vendor) is used by a bank to scale external data, it should be implemented, documented, and validated in the same fashion as an internally developed approach and the bank must document that the incorporation of the scaled data into its quantification processes is credible, transparent, systematic, and verifiable (as is the case for any third-party model). [17]

***Scenario Analysis***

Scenario analysis under the advanced approaches rule is a systematic process of obtaining expert opinions from business managers and risk-management experts to derive reasoned assessments of the likelihood and loss impact of plausible, high-severity operational losses. Scenario analysis may include the well-reasoned evaluation and use of external operational loss event data adjusted, as appropriate, to ensure relevance to a bank's operational-risk profile and control structure. Scenario analysis provides a forward-looking view of operational risk that complements historical internal and external data. The scenario analysis process and its output are key risk-management tools that are especially relevant for assessing potential risks to which the bank may be exposed.

Scenarios are typically developed through workshops that produce multiple scenarios at both the line of business and enterprise levels. Scenario development exercises allow subject matter experts to identify potential operational events and their impacts. Such exercises allow those experts to better prepare to identify and manage the risk exposures through business decisions, risk mitigation efforts, and capital planning. Inclusion of scenario data with other data elements in internal risk-management reporting can support development of a comprehensive operational risk profile of the bank.

There are significant challenges with the development of scenario analysis. Some of these challenges include mitigation of bias and justification for loss frequency and severity estimates. Sound scenario analysis development and output depend on the skill and expertise of facilitators and participants. By its nature, scenario analysis typically includes some degree of bias and subjectivity. Biases in scenario analysis development processes can include overconfidence, motivational bias, availability bias, partition dependence, and anchoring.[18] Scenario analysis should be governed by a consistent process to ensure the integrity of the estimates produced. A sound scenario process should be clearly defined, repeatable, and transparent. It should be responsive to changes in both the internal and external environment. The process should involve appropriate representation of the business lines and subject matter experts, with oversight by the ORMF. Participants should be trained in the scenario generation process, and should receive relevant and detailed background information (including internal and external loss data) that is derived through a systematic selection process.

---

[16] See section 22(h)(2) of the advanced approaches rule.

[17] Ibid.

[18] Additional information about scenario bias can be found on pages 18-19 of *Observed range of practice in key elements of Advanced Measurement Approaches (AMA)*, Basel Committee on Banking Supervision, July 2009. http://www.bis.org/publ/bcbs160b.pdf.

Given the subjective nature of scenario analysis, banks should implement mechanisms for identifying and mitigating biases inherent in scenario development processes. Such mechanisms include carefully structured questions, a well-defined decision-making process, and consideration of a range of possible loss frequencies and severities. Scenario estimates should be supported by high-quality documentation of the reasoning and the rationale underlying the estimates. In addition, banks should implement a robust independent challenge process to ensure that key risks have been captured and scenario estimates are appropriate and well-supported. Banks also should have a process to evaluate and improve upon the results of past scenario workshops.

There are significant challenges in using scenario analysis data as a direct input to the modeling process given the subjective nature of scenario analysis data. For example, it is difficult to mix synthetic (scenario) data and observational (internal and external) data elements in a credible manner. Supervisors will closely scrutinize a bank's approach to mixing internal and scenario data at the observation level, and will review statistical evidence confirming that such an approach is valid. In addition, to address the inherent subjectivity involved in scenario analysis development, banks should have sufficiently transparent processes that explain the judgments used in the development and weighting of scenario analysis data. A bank may consider indirect methods for the use of scenario analysis in its operational-risk quantification systems, including using scenario analysis to develop benchmark models or to adjust operational risk exposure estimates as described below.

*Scenario Analysis as a Benchmark*

In a scenario benchmark model, scenario analysis data are used as a direct input into a model that is separate from the primary (base) operational-risk quantification model (such as a model based on internal and/or external data). The outcome of the benchmark model may result in an adjustment to the operational-risk exposure estimate generated by the base model.[19] When scenarios are used for benchmarking, it is critical to demonstrate the credibility of the benchmark model through validation and appropriate documentation. In addition, the bank should be able to show that: (i) scenario output can be credibly and transparently translated into an estimate of operational-risk exposure for the bank's units of measure; and (ii) for a given UOM, the risk exposure can be appropriately estimated using internal and relevant external data.

The method chosen for comparing the results from the benchmark scenario model with those of a base model should incorporate a range of possible outcomes, such as the calculation of a confidence interval around the point estimate of the base model. While values that lie in the confidence interval may differ numerically from the point estimate, those differences may be small enough that they do not provide convincing evidence of an inaccurate point estimate. Thus, scenario analysis may be used either to select a different outcome from within this range or, more generally, to select among candidate distributions (or models) that reasonably fit a given collection of data and therefore are considered statistically indistinguishable and equally valid.

When using scenario analysis as a benchmark, there are two possible results:

[19] While this discussion focuses on the use of scenario analysis as a benchmark, the principles could equally apply to the use of external data as a benchmark.

i. A scenario benchmark result that falls within the confidence interval generated by the base model generally would not be viewed as statistically different from the base model and the estimate of operational risk exposure would equal the output of the benchmark model. Supervisory scrutiny would increase as the benchmark result moves toward the limits of the confidence interval or as the confidence level increases (for example, a 95 percent versus a 90 percent confidence interval).

ii. A scenario benchmark result that falls outside of the confidence interval should prompt the bank to thoroughly investigate the credibility of the results of both the base model and the benchmark model. The investigation may conclude that the base model and/or benchmark model are flawed and a correction to one or both of the models is warranted. A bank's process for modifying the model(s) to address deficiencies must be credible, transparent, systematic, and verifiable in accordance with the requirements of the advanced approaches rule.[20]

If the review and investigation of the base model and the scenario analysis benchmark model indicates that the methodologies of both appear sound but a discrepancy between the outcomes persists, then the bank should consider alternative means for incorporating scenario analysis into its operational-risk quantification process. For example, a bank may consider using scenario analysis data to adjust its operational-risk exposure estimates. However, supervisors expect significant support and documentation for this approach. Such a qualitatively based adjustment to the results of the base model may be appropriate in limited instances (e.g., if internal and external data do not provide a sufficient number of relevant large loss results). When using a scenario-based adjustment, banks should provide the rationale for adjusting their exposure estimate as well as evidence that:

i. The methodology is credible, transparent, systematic, and verifiable;

ii. Adjustments to quantified exposure estimates are subject to an independent review and approval process that confirms whether key judgments and any resulting changes to exposure estimates are credible; and

iii. The original model and its outcomes are statistically sound prior to any adjustment and the size of the adjustment is appropriate.

The agencies recognize that, in principle, a credible process could produce both upward and downward qualitative adjustments. A qualitative reduction in exposure estimates may be acceptable only in extremely limited circumstances. As such, a downward adjustment generally is not consistent with a conservative risk assessment. As with upward adjustments, a bank should provide the rationale for a downward adjustment and ensure that the adjustment meets the three criteria above. Furthermore, the magnitude of any adjustment to the quantitatively estimated operational-risk exposure should always be governed and justified by policy thresholds that conform to conservative risk assumptions.

*Scenario Analysis as the Base Model*

[20] See section 22(h)(3) of the advanced approaches rule.

In rare cases, a bank may have insufficient internal data and relevant external data to derive an operational-risk exposure estimate for a UOM. Provided that the bank has documented and demonstrated that insufficient data exist, a bank may consider using a scenario-based approach. In this approach the other three data elements must be inputs into the scenario analysis process.[21] However, the bank also should continue its efforts to collect internal and external data in order to address the paucity of data.

***Business Environment and Internal Control Factors***

BEICFs under the advanced approaches rule are indicators of a bank's operational-risk profile that reflect a current and forward-looking assessment of the bank's underlying business-risk factors and internal control environment. BEICFs are forward-looking tools that complement the other data elements in the AMA framework in developing a comprehensive risk profile. BEICF tools should provide balanced assessments of both the risk in the business environment and the quality of internal controls. The ORMF should be actively involved in the development and ongoing monitoring of BEICF tools to ensure a systematic assessment of risk across the organization. The ORMF should ensure the process is designed such that significant risks can be appropriately aggregated and monitored. Business line management should implement and use BEICFs as a component of day-to-day operational-risk management.

Common BEICF tools include risk and control self assessments, key risk indicators, and audit evaluations. Banks should consider the benefits of using consistent BEICF indicators across all lines of business. Such an approach may facilitate aggregation and reporting of operational-risk drivers, the effectiveness of the internal control environment, and BEICF assessments.

Banks should have a clear structure and associated policies around the reporting of the results of the BEICF assessment process. BEICF reporting within business lines should be appropriate for the activities and risks assumed by the particular business. Business line reporting should include both the identified risks and the corresponding controls aimed at mitigating those risks. Senior management and board reports should include information on significant risks and controls for material business lines and for the enterprise.

Banks also may use these assessments in operational-risk quantification. BEICFs are typically incorporated in the quantification process as indirect inputs to inform other data elements such as scenario analysis, or as inputs to determine ex post adjustments to operational-risk exposure estimates. When BEICF assessments are used to make ex post adjustments, banks should have a credible, transparent, systematic, and verifiable approach that demonstrates how BEICF outputs translate into exposure estimate adjustments. Ex post adjustments may result in an increase or decrease in operational-risk exposure estimates at the enterprise or business line level. Given the inherent subjectivity of BEICF-related adjustments, banks should have clear policy guidelines that limit the magnitude of both upward and downward adjustments. Over time, the direction and magnitude of any such adjustments should be compared to internal data, conditions in the business environment, and changes in the effectiveness of controls to ensure appropriateness.

[21] See section 22(h)(3)(i)(c) of the advanced approaches rule.

The advanced approaches rule requires that a bank periodically compare the results of its prior BEICF assessments against its actual operational losses in the intervening period.[22] For example, banks may consider a comparison of the frequency and severity of internal losses to the assessment of risks and internal controls in order to assess the reliability of these tools. Such comparisons may indicate that a bank should recalibrate the existing assessment tools or consider using other more effective tools. When comparing legal losses to BEICF assessments, banks should ensure that the comparison reflects the business and internal control environment that was in effect at the time the legal loss events occurred.

## Independent Review

### *Validation*

The advanced approaches rule requires that a bank validate, on an ongoing basis, its advanced systems.[23] For operational risk, advanced systems refer to a bank's operational-risk management processes, operational-risk data and assessment systems, and operational-risk quantification systems. Validation of a bank's AMA framework must include: (i) an evaluation of the conceptual soundness of the advanced systems (including developmental evidence supporting the advanced systems), (ii) an ongoing monitoring process that includes verification of processes and benchmarking, and (iii) an outcomes analysis process that includes back-testing.[24] Validation is a process encompassing a variety of activities that may be performed by different individuals and/or groups throughout the organization over time.

Banks should develop formal policies that implement validation of the AMA framework. The scope of validation and the methodologies employed should be consistent with the materiality and complexity of the risks being managed. A bank's validation process must be independent of the advanced systems' development, implementation, and operation, or be subject to an independent review of its adequacy and effectiveness.[25] As a general matter, a bank should ensure that individuals who perform the validation activities are not biased in their assessments due to their involvement in the development, implementation, or operation of the processes or products undergoing validation.

### *Validation of Governance and Data Elements*

The validation of conceptual soundness consists of an evaluation of the developmental evidence supporting the risk measurement and management framework, including the underlying systems, processes, and tools. Validation should consider whether the conceptual framework, governance, measurement and monitoring systems, management reporting, and controls are appropriate for the firm's size, complexity, and business activities.

---

[22] See section 22(h)(2)(ii)(D) of the advanced approaches rule.

[23] See section 22(j)(4) of the advanced approaches rule.

[24] Ibid.

[25] Ibid.

A bank must have a process for ongoing monitoring to assess whether all aspects of the AMA framework have been implemented effectively, remain appropriate, and are performing as intended.[26] Ongoing monitoring activities should include ensuring that: (i) the capture of internal and external data is accurate and complete, (ii) scenario and BEICF data are well supported and structured to limit bias, (iii) risk monitoring and management is effective, and (iv) appropriate remediation is undertaken if deficiencies exist. Validation also must incorporate outcomes analysis. Outcomes analysis must include comparisons of data elements, such as BEICFs, with actual loss experience or scenario analysis results with internal and external data.[27]

### *Validation of Quantification Systems*[28]

Validation should ensure that the bank's operational-risk quantification systems generate credible estimates of the bank's operational-risk exposure that reflect the operational-risk profile of the bank. Validation of the conceptual soundness should include validation of model inputs (including the selection and any transformations of data elements), outputs, assumptions, and the methodology. Ongoing validation of the AMA quantification system must evaluate the conceptual soundness of the system and be conducted to ensure that the approach and its underlying theory and logic remain sound and appropriate for the bank's range of business activities and the variety of operational loss events to which it is exposed.[29] This includes periodic evaluation of the appropriateness of the assumptions, parameters, inputs, outputs, and methodology, as well as comparisons of the AMA model and its results to other models. Outcomes analysis also must be conducted to compare model results with actual outcomes and losses.[30]

### *Internal Audit*

The advanced approaches rule requires a bank to have an internal audit function independent of business-line management that at least annually assesses the effectiveness of the controls supporting the bank's advanced systems and reports its findings to the bank's board of directors (or a committee thereof).[31] Such controls include a bank's validation processes. As a practical matter, there may be overlap between a bank's validation and audit activities. As mentioned above, the advanced approaches rule requires that a bank's validation process must be independent of the advanced systems' development, implementation, and operation or that the validation process be subjected to an independent review of its adequacy and effectiveness. Consistent with the rule, staff in the ORMF may perform validation work, provided that this work is reviewed by an independent party. This validation work may be supported by additional validation efforts within a bank's lines of business. For example, some banks validate internal

[26] See section 22(j) of the advanced approaches rule.

[27] See section 22(h)(2)(ii)(D) of the advanced approaches rule.

[28] This guidance draws on existing supervisory guidance on model validation, including the *Supervisory Guidance on Model Risk Management* issued by the Office of the Comptroller of the Currency and the Federal Reserve Board of Governors on April 4, 2011.

[29] See section 22(j)(4)(i) of the advanced approaches rule.

[30] See section 22(j)(4)(iii) of the advanced approaches rule.

[31] See section 22(j)(5) of the advanced approaches rule.

loss data for a given business unit using an independent party within that same business unit, supplemented with a review by the ORMF.

Some banks use the internal audit function to validate non-quantitative aspects of their advanced systems. This could present a conflict of interest--or at least the appearance thereof--in that a bank's internal audit function is expected to assess the controls, including validation, related to the advanced systems. Where internal audit staff is reviewing work that it or other audit staff performed, there is the potential that the objectivity of the review will be compromised. The agencies expect that those who conduct the validation work will not be responsible for reviewing the controls associated with the validation work they completed. In instances where internal audit staff reviews validation work that was performed by other, distinct internal audit staff, the bank should be prepared to demonstrate that such an arrangement does not compromise the independence of the review. Any such arrangement would be subject to heightened supervisory scrutiny.