FINANCIAL SERVICES FLASH REPORT

Federal Reserve Issues Supplemental Policy Statement on the Internal Audit Function and Its Outsourcing

January 29, 2013

On January 23, the Board of Governors of the Federal Reserve System issued a supplemental policy statement regarding internal audit functions to provide certain financial institutions with additional guidance. This policy supplements internal audit-related interagency guidance that was issued in 2003 and remains in effect.[1] Building upon the 2003 interagency guidance, the supplemental guidance addresses the characteristics, governance and operational effectiveness of an institution's internal audit function. The Federal Reserve's policy statement follows on the heels of the June 2012 revised supervisory guidance issued by the Basel Committee on Banking Supervision for assessing the effectiveness of the internal audit function in banks, which forms part of the Committee's ongoing efforts to address bank supervisory issues and enhance supervision through guidance that encourages sound practices within banks.

The source of the Federal Reserve's supplemental guidance is twofold. First, it derives from supervisory experience of Federal Reserve staff during and following the recent financial crisis, when the staff identified areas for improving internal audit functions at institutions. In effect, the guidance codifies recent regulator oral feedback. Second, the statement reflects certain changes in banking regulations that have occurred since the issuance of the 2003 Policy Statement. The supplemental guidance is available on the regulator's website at http://www.federalreserve.gov/bankinforeg/srletters/sr1301a1.pdf.

What Does the Policy Statement Say?

In building upon the structure provided by the 2003 interagency guidance, which remains in effect, the policy statement addresses the characteristics, governance and operational effectiveness of an institution's internal audit function. While it otherwise follows the same organizational structure as the 2003 interagency guidance, it adds a new section titled "Enhanced Internal Audit Practices" and updates Parts I – IV of the 2003 guidance. The 2003 guidance, as supplemented by the recently issued policy statement, now includes the following areas:

- Enhanced Internal Audit Practices (new in Supplemental Policy Statement section 1)
- Part I – The Internal Audit Function (introduced in 2003 and updated in Supplemental Guidance section 2)

[1] Interagency Policy Statement on the Internal Audit Function and Its Outsourcing, dated March 17, 2003, is available at http://www.federalreserve.gov/boarddocs/SRLetters/2003/SR0305a1.pdf.

- Part II – Internal Audit Outsourcing (introduced in 2003 and updated in Supplemental Guidance section 3)
- Part III – Independence Guidance for Independent Public Accountants (introduced in 2003 and updated in Supplemental Guidance section 4)
- Part IV – Examination Guidance (introduced in 2003 and updated in Supplemental Guidance section 5)

These areas are discussed further below.

Enhanced Internal Audit Practices – This section discusses the enhancements that an institution should incorporate into its internal audit function to address lessons learned from the recent financial crisis. It is intended that these enhanced practices will improve the overall safety and soundness of the institution. The section lists six key areas:

- ***Risk analysis*** – Internal audit should evaluate the effectiveness of all critical risk management functions, (e.g., credit risk) including the institution's overall enterprisewide risk management function. The focus of the analysis is twofold:
  - The nature and extent of monitoring activities that evaluate compliance with applicable laws and regulations and established internal policies and processes within the institution; and
  - Whether monitoring processes are appropriate given the institution's business activities and associated risks.
- ***Thematic macro control issues*** – Internal audit should identify these issues as part of its ongoing risk assessment processes and determine their overall impact on the institution's risk profile. When patterns of thematic macro control issues are identified, internal audit should:
  - Determine whether additional audit coverage is required and, if it is, reflect these issues across the firm in all appropriate auditable areas,
  - Communicate these issues to senior management and the audit committee, and
  - Ensure management establishes effective remediation mechanisms.
- ***Challenging management and policy*** – Internal audit should challenge management to adopt appropriate policies, procedures and effective controls. If policies, procedures and internal controls are ineffective in a particular line of business or activity, internal audit should report specific deficiencies with recommended remediation to senior management and the audit committee. Such recommendations may include restricting business activity in affected lines of business until effective policies, procedures and controls are designed and implemented. Internal audit should monitor management's corrective action and conduct a follow-up review to confirm that recommendations have been addressed.
- ***Infrastructure*** – When an institution designs and implements infrastructure enhancements (e.g., new systems or major systems modifications), internal audit should review major changes to ensure significant internal controls have not been compromised and notify management of potential control issues.
- ***Risk tolerance*** – Internal audit should understand the risks faced by the institution, evaluate the reasonableness of established limits and perform sufficient testing to ensure that management is operating within established limits and other policy restrictions. In addition, internal audit should confirm that the board of directors and

senior management are actively involved in setting and monitoring compliance within the institution's risk tolerance limits.

- ***Governance and strategic objectives*** – Internal audit should evaluate governance at all levels of the institution, including the senior management level, and within all significant business lines. Internal audit should also evaluate the adequacy and effectiveness of controls to respond to risks within the organization's governance, operations, and information systems in achieving the organization's strategic objectives. Any concerns should be communicated to the board of directors and senior management.

The above areas (as well as Parts I through IV below) provide clear direction as to how the Federal Reserve will assess the capabilities of an institution's internal audit function. It also demonstrates that the Federal Reserve, like other financial services regulators, is increasingly looking for a dynamic, proactive internal audit function that is serving as a critical, effective challenge for the organization.

The Internal Audit Function, Part I – This section strongly encourages institutions to incorporate professional standards, such as The Institute of Internal Auditors (IIA) guidance, into their overall internal audit architecture and provides additional internal audit guidance not specifically articulated in the IIA guidance.[2] The additional guidance pertains to the characteristics, governance and operational effectiveness of an institution's internal audit function. The supplemental policy includes stronger language around complying with the IIA standards, as the 2003 guidance states institutions are "encouraged to consider," whereas the supplemental policy statement states they are "encouraged to adopt." Elsewhere in the document, the Federal Reserve hammers home the message in stating that it is supplementing the 2003 Policy Statement by "strongly encouraging internal auditors to adhere to professional standards, such as the IIA guidance."

In addition, the regulator clarified certain aspects of the IIA guidance and provided practices intended to increase the safety and soundness of institutions. To illustrate, some examples:

- If the chief audit executive (CAE) reports administratively to someone other than the CEO, the audit committee should document its rationale for the reporting structure.
- Regarding professional staff and competence, the guidance updates this area significantly, including: encouraging a rotational program; performing an annual knowledge gap assessment of the function; filling identified knowledge gaps through rotation, hiring or outsourcing; providing a formal training program and staff evaluation process; and stipulating a minimum of 40 hours of training per auditor per year.
- Regarding objectivity and ethics, auditors should avoid: conflicts of interest, auditing activities in their first year after which they were responsible for such activities, compensation schemes that create inappropriate incentives, and responsibility for the design and operation of internal control systems. An institution's internal audit function should have a code of ethics that emphasizes the principles of objectivity, competence, confidentiality and integrity (e.g., consistent with the code of ethics that was established by the IIA).

[2] Refer to the IIA website at https://na.theiia.org/standards-guidance/Pages/Standards-and-Guidance-IPPF.aspx for the IIA's standards.

- The internal audit charter commentary in the supplemental guidance is not as comprehensive as the recent 2012 Basel guidance on the subject.[3] Generally, it states that the charter must address the responsibility and accountability of the CAE, as well as the function's objectives, scope, management reporting position within the organization, criteria for when and how it may outsource work to outside experts, and responsibility to evaluate the effectiveness of the institution's risk management, internal controls and governance processes.
- Regarding corporate governance considerations, the substance of the supplemental guidance is consistent with the 2003 policy statement; however, there is much commentary regarding the audit committee's responsibilities, which merits careful review. For example, the supplemental guidance states that the audit committee should receive appropriate levels of management information to fulfill its oversight responsibilities and that, at minimum, the committee should receive certain specified data with respect to internal audit that is more granular in description than in the 2003 policy statement. Among other things specified in the guidance, the audit committee should receive: audit results with a focus on areas rated less than satisfactory; audit plan changes, including the rationale for significant changes; audit issue information, including aging, past-due status, root-cause analysis and thematic trends; information on higher-risk issues indicating the potential impact, root cause and remediation status; information on significant industry and institution trends in risks and controls; and an opinion (at least annually) on the adequacy of risk management processes, including effectiveness of management's self-assessment and remediation of identified issues.
- Regarding the internal audit function's processes, the supplemental guidance provides commentary on the risk assessment methodology, including an analysis of cross-institutional risk and thematic control issues and addressing the monitoring activities in place to evaluate the effectiveness of risk management, control and governance processes. The guidance pointed out the need for establishing an audit universe for identifying all auditable entities; conducting a comprehensive assessment of the key risks and critical risk management functions; documentation of risk assessments; development of an internal audit plan; and utilization of formal continuous monitoring through a combination of metrics, management reporting, periodic audit summaries and updated risk assessments to substantiate that established processes are operating as designed. For example, the regulator noted that "common practice for institutions with defined audit cycles is to follow either a three- or four-year audit cycle; high-risk areas should be audited at least every twelve to eighteen months." That said, the regulator also pointed out that, "regardless of the institution's practice, particular care should be taken to ensure that higher-risk elements are reviewed with an appropriate frequency, and not obscured due to their inclusion in a lower risk-rated audit entity."
- The supplemental guidance sets an expectation for a well-designed, comprehensive quality assurance program that ensures internal audit activities conform to the IIA's professional standards and the institution's internal audit policies and procedures. Importantly, the program should include both internal and external quality assessments.

[3] The Basel Committee on Banking Supervision issued revised supervisory guidance in June 2012 for assessing the effectiveness of the internal audit functions in banks. Available at http://www.bis.org/publ/bcbs223.htm, the document is based on 20 principles, organized in three sections: (a) supervisory expectations relevant to the internal audit function, (b) the relationship of the supervisory authority with the internal audit function, and (c) supervisory assessment of the internal audit function.

Internal Audit Outsourcing, Part II – This section provides further clarification on the responsibilities of an institution's board of directors and senior management to provide appropriate oversight of internal audit outsourcing and co-sourcing arrangements. The guidance notes that the audit committee and CAE are responsible for the selection and retention of internal audit vendors. In addition, it re-emphasizes the importance of vendor competence, contingency plans for vendors providing significant internal audit services, and comparable quality standards (i.e., the same standards of high-quality work as if the institution maintained an in-house internal audit function).

Independence Guidance for Independent Public Accountants, Part III – This guidance explains certain changes to Section 36 of the Federal Deposit Insurance Act enacted since the issuance of the 2003 Policy Statement. The July 2009 amendments to Section 36 of the Act provide that independent public accountants, subject to the independence standards issued by the American Institute of Certified Public Accountants, the U.S. Securities and Exchange Commission (SEC) and the Public Company Accounting Oversight Board, must comply with the more restrictive of the aforesaid standards. In 2003, the SEC prohibited a registered public accounting firm that is responsible for furnishing an opinion on the consolidated or separate financial statements of an audit client from providing internal audit services to that same client.[4] Therefore, by following the more restrictive independence rules, an institution's external auditor is precluded from performing internal audit services, either on a co-sourced or an outsourced basis, even if the institution is not a public company.

Examination Guidance, Part IV – This section provides additional guidance on the Federal Reserve's supervisory assessment of the overall effectiveness of an institution's internal audit function and considerations relating to potential reliance by Federal Reserve examiners on an institution's internal audit work. The regulator views an effective internal audit function as a vehicle for advancing the institution's safety and soundness and compliance with consumer laws and regulations. Therefore, Federal Reserve examiners will make an overall determination as to whether the internal audit function and its processes are effective or ineffective and whether examiners can potentially rely upon internal audit's work as part of the supervisory review process. If internal audit's overall processes are deemed effective, examiners may be able to rely on the work performed by internal audit, depending on the nature and risk of the functions subject to examination.

Which Financial Services Institutions Are Affected?

This policy statement applies to supervised institutions with greater than US$10 billion in total consolidated assets, including state member banks, domestic banks and savings and loan holding companies, and U.S. operations of foreign banking organizations with greater than US$10 billion in total consolidated assets. This supplemental guidance is also consistent with the objectives of the Federal Reserve's consolidated supervision framework for large financial institutions with total consolidated assets of US$50 billion or more, which promotes an independent internal audit function as an essential element for enhancing the resiliency of supervised institutions. As noted above, because of changes to the Federal Deposit Insurance Act, Section 4 of the document relating to the independence guidance for external auditors also applies to insured depository institutions with total assets of US$500 million or more.

---

[4] The SEC's rules prohibit the accountant from providing any internal audit service outsourced by an audit client that relates to the audit client's internal accounting controls, financial systems or financial statements, *unless it is reasonable to conclude that the results of these services will not be subject to audit procedures during an audit of the audit client's financial statements*. While the Federal Reserve does not refer to this qualifying phrase in the SEC rule, it should be noted that the SEC language does not impose an absolute prohibition on external auditors performing internal audit services.

Notwithstanding the above, the Federal Reserve makes a profound statement regarding the importance of a strong and effective internal audit function in financial services institutions in the "post financial crisis" era. While the regulator has communicated a "bright line" threshold for applying its guidance, history would suggest that the Federal Reserve and other agencies have a tendency to use their guidance in considering circumstances at institutions below the line as well. The regulator has advanced the point of view that an effective internal audit function is a vehicle for advancing the institution's safety and soundness and compliance with consumer laws and regulations.

Why Was the Policy Statement Issued?

The Federal Reserve is providing this supplemental guidance to further its efforts to enhance regulated institutions' internal audit practices and to encourage them to adopt professional audit standards and other authoritative guidance, including those issued by the IIA. The regulator has accumulated supervisory experience during and following the recent financial crisis in which its staff identified areas for improving regulated institutions' internal audit functions. Thus, there was a need to codify lessons learned, recommendations and findings that the Federal Reserve examiners have communicated both orally and in writing to the institutions subject to the regulator's supervision, with the intent of sending a message that there is need for internal audit functions to "up their game" just as risk management and other functions have been encouraged to do.

The focus is on larger institutions because of their complexity, justifying the need for an internal audit function more effectively (a) identifying, evaluating and reporting on risks, (b) adopting a broad focus on governance, risk management and compliance processes and (c) challenging management when it is appropriate to do so. In addition, the regulator re-emphasizes the 2003 policy guidance that the board, audit committee and senior management have important roles to play in enhancing the effectiveness of internal audit. Finally, from a business as well as a regulatory standpoint, any evaluation of the entire enterprise risk management process of a large, complex financial services institution would likely span from board governance to management oversight and consider the three lines of defense. As internal audit is typically viewed as the third line of defense, any assessment of an institution's enterprise risk management would, out of necessity, include internal audit.

What Is the Impact on Financial Services Institutions?

Each institution will need to reassess their internal audit function in light of the supplemental guidance providing clarification of what is expected of an effectively functioning internal audit group, audit committee, board of directors, senior management and CAE. As the regulators will rate the effectiveness of the internal audit function and have signaled they will rely on the work of an effective internal audit function, each financial services institution has a choice – either make the necessary changes and get ahead of the bank examiners by doing the job of auditing themselves or face the consequences of a regulatory audit and the bank examiners factoring in their evaluation of internal audit into their assessment of the institution's safety and soundness and compliance with consumer laws and regulations. There is also a value proposition underlying the Federal Reserve's expectations for a board and senior management group that is truly interested in a balanced approach to managing risk.

A Separate, but Parallel Path – OCC's "Getting to Strong"

While the guidance above was issued solely by the Federal Reserve, since the financial crisis, the Office of the Comptroller of the Currency (OCC) has also been utilizing speeches and examinations to drive internal audit functions to a "strong" rating, signaling "satisfactory" is no

longer adequate for large, complex financial institutions. This is in response to numerous challenges faced by financial institutions, including increasing complexity and velocity of risk facing the bank, including complexity of new bank markets (e.g., derivatives market, mortgage market), changes in new bank products and processes (e.g., fraud prevention, trading platforms), and expansion of risk management at the enterprise and line of business (LoB) levels. In addition, there is compliance with additional laws and regulations in the industry (e.g., Basel, Dodd-Frank, etc.) and the challenge of managing timely remediation of internal control deficiencies and audit recommendations in a continuously changing environment. As noted by a senior deputy comptroller of the OCC[5]:

> … because of the importance of large banks to our economy and the capital markets, we have learned that it is not sufficient to have a "satisfactory" internal audit function. Today, the expectation is that all large banks need to build and maintain strong internal audit functions.

When defining what constitutes a "strong" internal audit function, we believe there are four core elements, as depicted below, many of which parallel or are similar to the Federal Reserve supplemental policy release:

Each of these elements is discussed further below.

Accountability/Effective Challenge – This element – accountability and effective challenge to the LoBs – is the key to a strong audit function. "Accountability" is substantiated in numerous ways, including holding LoB management accountable for negative audit findings and lack of timely resolution of issues, considering audit results in performance evaluations and compensation decisions, and completing follow-up reviews in a timely manner and retesting to confirm that management's corrective action is thorough.

When issues are identified, there is an effective process for driving change by identifying the root cause and formulating the appropriate solution to correct the problem. Major findings are communicated to the board and senior management succinctly in periodic reports summarizing the root cause of problems, issues that cut across multiple functions and businesses, adequacy of policies and procedures, near misses and potential or emerging issues, ongoing perpetual problems, recommendations for process improvements, and the status of outstanding issues. Audit reports should include comments on the efficacy of business unit self-assessments, emerging issues and appropriateness of risk levels relative to both the quality of the control environment and to the established risk appetite.

This element is augmented by the support of the three core elements below:

Stature/Independence – The stature of the audit function refers to the alignment of the function, independent of LoB and financial functions, with the objective of supporting the accountability of management and the board. The audit committee plays a vital role in heightening the stature of the audit function by setting a rigorous "tone at the top" regarding the independence accorded to the function. The key is that internal audit is independent by virtue of its direct reporting line to the board and the board's support in executing the audit plan and

[5] "Auditing the Auditors," Scott D. White and Lisa R. Adinolfi-Tejera, *FSA Times*. This article is available at http://www.theiia.org/fsa/2012-features/auditing-the-auditors/.

remediation of audit findings and recommendations. The role of internal audit is clarified and integrated with other functions (e.g., corporate risk management, policy development, new product and service deployment, strategy-setting, etc.). This is illustrated in the Federal Reserve release requiring a clear explanation of an internal audit administrative reporting line other than to the CEO.

Competence/Talent – Strong audit management and staff with an appropriate level of technical and strategic expertise commensurate with the company's complexity and risk profile are essential for ensuring that the function performs to expectations. This is directly addressed in the Federal Reserve release. Sufficient depth is required within the audit team in order to enable succession and continuation of quality coverage during times of change and/or adversity. Audit management must possess strong technical, analytical and communication skills. Audit committee members must possess specific knowledge of audit and risk management practices, commensurate with the complexity and risk profile of the bank.

Scope and Frequency – Internal audit should monitor the business in a periodic, continuous, and forward-looking manner, with the board and management actively setting expectations and evaluating performance of the function. This process creates a robust view of the institution that can be fully relied on by regulators and the board. The audit committee's engagement with the internal audit function must be robust in terms of setting expectations, approving the overall plan, evaluating performance, willingness to change, and the frequency and quality of communications, including discussions of emerging issues. For example, the audit committee and its chair should have ongoing interaction with the CAE separate and apart from formally scheduled meetings so that the committee remains current on any concerns

Suggested Action Steps

Every institution is different in terms of where it stands against regulatory expectations. With that in mind, a potential approach to addressing this guidance could be some combination of the following:

(1) Assess the institution's internal audit function against (a) the 2003 policy guidance as supplemented by the recent policy statement, (b) the June 2012 Basel guidance on internal audit and (c) the IIA standards.

(2) Identify any potential gaps that may exist from the assessment per (1) that should be addressed.

(3) Discuss the gaps with the audit committee chair and the audit committee, prioritize the gaps, and obtain audit committee approval and management funding to proceed. Considerations in "getting to strong" would include, but would not be limited to:

- Appropriately structure the internal audit department to maintain its independence and strengthen its stature within the organization
- Evaluate overall corporate governance over the system of internal controls and the audit function
- Enhance existing risk assessment methodologies, including:
  - Identification of cross-institutional and thematic macro control issues, and evaluation of their impact on the institution's risk profile and resultant audit plan
  - Addressing the processes and procedures for evaluating the effectiveness of risk management, control and governance processes

- Ensuring a mechanism exists, and is operating effectively, for updating the risk assessment, given changes in market conditions, laws and regulations, business processes or activities, and systems
- Determining the adequacy of processes for understanding and evaluating risk tolerances
- Communicating to the audit committee and senior management
- Considering a risk control self-assessment performed by management

– Ensure the audit committee is receiving timely and appropriate data in accordance with the policy guidance[6]

– Implement a retrospective review process (i.e., if an adverse event occurs at an institution, a postmortem and "lessons learned" analysis should be conducted to ensure that appropriate action is taken to improve processes and remediate identified issues); internal audit should evaluate management's postmortem and "lessons learned" analysis following the occurrence of adverse events and close calls and, in certain instances, perform its own analysis

– If applicable, reassess reliance on co-sourcing and outsourcing arrangements to perform internal audit activities and ensure that a contingency plan is in place in the event of temporary or permanent disruption

– Ensure compliance with auditor independence requirements by precluding engagement of the external auditor to provide internal audit services

(4) Based on the prioritization per (3), define a plan to address the priority gaps over a reasonable time frame.

(5) Discuss the plan per (4) with the regulators to ascertain its adequacy for improving the internal audit function.

(6) Execute against the plan and report at each audit committee meeting on the progress against the remediation plan.

(7) Critically evaluate the scope and effectiveness of existing quality assurance processes within the internal audit function. Regulators are increasing expectations on the robustness of quality assurance functions and the pervasiveness of coverage, along with evidence of applying "lessons learned" in one audit area or business function across the financial institution's audit process.

While the above plan would provide a significant step forward, an appropriate comprehensive plan would result from a careful assessment of the Federal Reserve's and other regulatory expectations; the audit committee's expectations; the strategy, businesses and risk profile of the institution; and the current capabilities of the internal audit function.

[6] As noted earlier: Among other things, this data includes audit results with a focus on areas rated less than satisfactory; audit plan changes, including the rationale for significant changes; audit issue information, including aging, past-due status, root-cause analysis and thematic trends; information on higher-risk issues indicating the potential impact, root cause and remediation status; information on significant industry and institution trends in risks and controls; and an opinion (at least annually) on the adequacy of risk management processes, including effectiveness of management's self-assessment and remediation of identified issues.

Summary

In its release, the Federal Reserve (and as discussed herein, over the past several months through different means, the OCC) has re-emphasized what is expected from an effectively functioning internal audit group, audit committee, board, senior management and CAE by clarifying a number of matters and presenting additional guidance. The OCC has also emphasized its expectations of a "strong" internal audit function, creating the need for institutions to reassess the capabilities, positioning and stature of their existing functions.

Without a doubt, internal audit is an area that is significantly affected by both "heightening expectations" across regulatory bodies as well as regulatory and legislative mandates under the Dodd-Frank Act, Basel capital accords and Federal Reserve policies. Internal audit functions face a significant challenge in answering the call to advance the financial services institution's safety and soundness and compliance with consumer laws and regulations, particularly given the regulatory reform issues, evolving markets, a changing competitive landscape, margin pressures, capital and liquidity issues, and increased stakeholder expectations in the industry. Regulators have raised the bar for internal audit functions to audit, and express an opinion on, both the readiness design of risk management systems and the effectiveness of the enterprise's risk management function. This is a new requirement for some internal audit groups, requiring some of them to access additional expertise and skill sets. The next 12 to 24 months will provide both a challenge and an opportunity as CAEs and audit committees align the function with the new realities.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit. Through our network of more than 70 offices in over 20 countries, we have served more than 35 percent of FORTUNE® 1000 and Global 500 companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Protiviti is a wholly owned subsidiary of Robert Half International Inc. (NYSE: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

Contacts

Cory Gunderson
Managing Director – U.S. Financial Services Practice Leader
Global Leader – Risk and Compliance Solutions
+1.212.708.6313
cory.gunderson@protiviti.com

Scott Jones
Managing Director
+1.213.327.1442
scott.jones@protiviti.com

Rick Magliozzi
Managing Director
+212.603.8363
frederick.magliozzi@protiviti.com

Michael Thor
Managing Director
+1.312.476.6400
michael.thor@protiviti.com

protiviti®
Risk & Business Consulting.
Internal Audit.