Basel Committee Issues Revised Supervisory Guidance on Assessing the Effectiveness of Internal Audit Functions

August 9, 2012

On June 28, 2012, the Basel Committee on Banking Supervision (Basel Committee) issued revised supervisory guidance for assessing the effectiveness of internal audit functions in banks, entitled “The internal audit function in banks.” This document contributes to the Basel Committee’s ongoing efforts to address supervisory issues and enhance supervision by issuing guidance that encourages sound practices in banks. It replaces the Basel Committee’s 2001 document (“Internal audit in banks and the supervisor’s relationship with auditors”) and incorporates recent developments in supervisory practices.

The Basel Committee’s decision to revise its 2001 document was due, in part, to the recent financial crisis, during which internal audit functions were criticized for their role in the failure to highlight weaknesses in overall risk management. The last several years following the financial crisis continued to highlight industrywide inconsistencies in the role of audit committees, internal audit organization reporting structures, the relationships between bank management and internal audit, and the ongoing quality of internal audit functions.

The revised document specifically builds on the Basel Committee’s “Principles for enhancing corporate governance,” which require banks to have an internal audit function with sufficient authority, independence and resources – as well as access to the board of directors. The Basel Committee believes that an independent, competent and qualified internal audit function is critical to sound corporate governance.

The Basel Committee’s objectives for issuing the 2012 document were to promote and reemphasize the need for a strong internal audit function within banks. Furthermore, the Basel Committee includes appendices (“Annex 1” and “Annex 2”) that provide recommendations to boards of directors/audit committees in the execution of their oversight responsibilities of the internal audit function.

Key changes between the 2012 revised guidance and the 2001 guidance are as follows:

- Increased emphasis regarding the independence of the internal audit function – specifically related to the board of directors’/audit committee’s direct supervisory role.

---

• Emphasis on compliance with The Institute of Internal Auditors (IIA) *International Standards for the Professional Practice of Internal Auditing.*

• Expanded guidance on the relationship between supervisors and the internal audit function – specifically emphasizing communication between the two groups.

The new guidelines also provide perspectives on the relationships between a bank’s management/business units, support functions and internal audit by outlining them in terms of a “three lines of defense” model, as follows:

• **First Line of Defense:** Management and Business Units
  
  Management/business units undertake risk within assigned limits of risk exposure and are responsible/accountable for identifying, assessing and controlling the risks of their business.

• **Second Line of Defense:** Support Functions (Risk Management, Compliance, Legal, Human Resources, Finance, Operations and Technology)
  
  The support functions help ensure that risks in the business units have been appropriately identified and managed, and work closely to help define strategy, implement bank policies and procedures, and collect information to create a bank-wide view of risks.

• **Third Line of Defense:** Internal Audit
  
  Internal Audit independently assesses the effectiveness of processes created in the First and Second Lines of Defense and provides assurance on these processes.

**Overview of the Basel Committee’s Internal Audit Guiding Principles**

The document’s principles fall into three main sections: (1) supervisory expectations relevant to the internal audit function, (2) the relationship of the supervisory authority with the internal audit function, and (3) supervisory assessment of the internal audit function. These principles are the following:  

*Supervisory Expectations*

• **Principle 1: Internal Audit Responsibility** – An effective internal audit function provides independent assurance to the board of directors and senior management on the quality and effectiveness of a bank’s internal control, risk assessment and governance systems/processes, thereby helping the board and senior management protect their organization and its reputation.

• **Principle 2: Independence** – The bank’s internal audit function must be independent of the audited activities, which requires the internal audit function to have sufficient standing and authority within the bank, thereby enabling internal auditors to carry out their assignments with objectivity.

• **Principle 3: Competence** – Professional competence, including the knowledge and experience of each internal auditor and of internal auditors collectively, is essential to the effectiveness of the bank’s internal audit function.

---

• **Principle 4: Integrity** – Internal auditors must act with integrity, including adhering to the bank’s code of ethics and/or an established international code of ethics for internal auditors, such as The IIA’s *International Standards for the Professional Practice of Internal Auditing*.

• **Principle 5: Charter & Authority** – Each bank should have an internal audit charter that articulates the purpose, standing and authority of the internal audit function within the bank in a manner that promotes an effective internal audit function as described in Principle 1.

• **Principle 6: Scope of Activity** – Every activity (including outsourced activities) and every entity of the bank should fall within the overall scope of the internal audit function. Other guidance includes the following:
  
  (i) The internal audit function should evaluate the:
      
      a. Effectiveness and efficiency of internal control, risk management and governance systems in the context of both current and future risks.
      
      b. Reliability, effectiveness and integrity of management information systems and processes (including relevance, accuracy, completeness, availability, confidentiality and comprehensiveness of data).
      
      c. Monitoring of compliance with laws and regulations, including any requirements from supervisors.
      
      d. Safeguarding of assets.
      
  (ii) The head of internal audit is responsible for establishing an annual internal audit plan that can be a part of a multiyear plan, subject to the board of directors/audit committee’s approval. The plan should be supported by a robust risk assessment.
      
  (iii) The internal audit function’s budget should be sufficiently flexible to adapt the internal audit plan to the bank’s changing risk profile.

• **Principle 7: Adequate Coverage** – The scope of the internal audit function’s activities should ensure adequate coverage of matters of regulatory interest (i.e., risk management, regulatory capital adequacy and liquidity control functions, regulatory and internal reporting functions, the regulatory compliance function, and the finance function) within the audit plan.

• **Principle 8: Established Internal Audit Function, Part I** – Each bank should have a permanent internal audit function, which should be structured consistent with Principle 14 when the bank is within a banking group or holding company.

• **Principle 9: Board of Directors Role** – The bank’s board of directors has the ultimate responsibility for ensuring that senior management establishes and maintains an adequate, effective and efficient internal control system and, accordingly, the board should support the internal audit function in discharging its duties effectively.

• **Principle 10: Audit Committee Role** – The audit committee, or its equivalent, should oversee the bank’s internal audit function.

• **Principle 11: Head Internal Audit Role** – The head of the internal audit department should be responsible for ensuring that the department complies with sound internal
auditing standards and with a relevant code of ethics, such as The IIA’s *International Standards for the Professional Practice of Internal Auditing.*

- **Principle 12: Reporting Structure** – The internal audit function should be accountable to the board, or its audit committee, on all matters related to the performance of its mandate as described in the internal audit charter.

- **Principle 13: The Internal Audit Function as the Third Line of Defense** – The internal audit function should independently assess the effectiveness and efficiency of the internal control, risk management and governance systems and processes created by the business units and support functions and provide assurance on these systems and processes.

- **Principle 14: Established Internal Audit Function, Part II** – To facilitate a consistent approach to internal audit across all the banks within a banking organization, the board of directors of each bank within a banking group or holding company structure should ensure that either:
  
  (i) The bank has its own internal audit function, which should be accountable to the bank’s board and should report to the banking group or holding company’s head of internal audit; or
  
  (ii) The banking group or holding company’s internal audit function performs internal audit activities of sufficient scope at the bank to enable the board to satisfy its fiduciary and legal responsibilities.

- **Principle 15: Impact of Outsourcing on the Board of Directors** – Regardless of whether internal audit activities are outsourced, the board of directors remains ultimately responsible for the internal audit function.

**Supervisory Authority**

- **Principle 16: Supervisory Communication** – Supervisors should have regular communication with the bank’s internal auditors to:
  
  (i) Discuss the risk areas identified by both parties.
  
  (ii) Understand the risk mitigation measures taken by the bank.
  
  (iii) Understand weaknesses identified and monitor the bank’s responses to these weaknesses.

**Supervisory Assessment**

- **Principle 17: Ongoing Assessment** – Bank supervisors should regularly assess whether the internal audit function has sufficient standing and authority within the bank and operates according to sound principles.

- **Principle 18: Assessment Issue Communication** – Supervisors should formally report all weaknesses they identify in the internal audit function to the board of directors and require timely remedial actions.

- **Principle 19: Assessment Impact** – The supervisory authority should consider the impact of its assessment of the internal audit function on its evaluation of the bank’s risk profile and on its own supervisory work.
Principle 20: Assessment Corrective Action – The supervisory authority should be prepared to take informal or formal supervisory actions requiring the board and senior management to remedy any identified deficiencies related to the internal audit function within a specified timeframe and to provide the supervisor with periodic written progress reports.

Summary

Protiviti believes that the Basel Committee’s guiding principles represent a codification, so to speak, of leading practices for bank internal audit functions observed around the world. Overall, many of the above principles have also been addressed by other regulatory and/or association bodies, including but not limited to the United States (U.S.) Commodity Futures Trading Commission, the U.S. Dodd-Frank Act, the U.S. Federal Financial Institutions Examination Council (i.e., interagency guidance) and The Institute of Internal Auditors.

While many bank internal auditors essentially follow the above principles today due to experience, lessons learned from the financial crisis and a knowledge-sharing culture that exists in the industry, many other institutions were discredited by regulatory bodies in the recent financial crisis where there were clear lapses in sound internal practices – including inadequate internal audit reporting structures, ineffectively developed internal audit plans and ineffective execution of such plans, and a lack of professional competency within the internal audit function. Overall, Protiviti supports the Basel Committee’s issuance of these guiding principles as a measure to further encourage consistency among bank internal audit functions around the world.
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

Carol Beaumier
Executive Vice President – Global Industry Programs
Global Leader – Financial Services Industry Practice
+1.212.603.8337
carol.beaumier@protiviti.com

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

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

Michael Klinger (Germany)
Managing Director
+49.69.96.37.68.155
michael.klinger@protiviti.de

Lindsay Dart (United Kingdom)
Managing Director
+44.207.3890.448
lindsay.dart@protiviti.co.uk