Risky Business:
Internal Audit Best Practices for Community Banks

Presented by: Angela Roberts & Leonard Wagers
Our Presenters

Angela Roberts, CIA, Clark Schaefer Hackett

Angela is an audit consultant and internal audit specialist in CSH’s Risk Management Services group. This group handles internal audits, internal control evaluations, Sarbanes-Oxley compliance, regulatory compliance, and loan reviews for community banks and financial services institutions.

Angela performs due diligence in audited policy and procedural compliance, and she assembles and provides documentation reviews. Her consulting expertise ranges from regulatory compliance to internal audits for all departments within financial institutions such as lending and deposits. She further specializes in secondary market quality control reviews, loan reviews, NACHA self assessments, BSA, and regulatory report reviews. Prior to joining Clark Schaefer Hackett in 2003, Angela spent 22 years in internal auditing in various financial institutions. She is a Certified Internal Auditor (CIA).
Leonard joined CSH in 2007 with 17 years of experience conducting internal audit and profitability analysis for financial institutions. He is responsible for various tasks including conducting and facilitating an activity-based profitability system for a large regional bank. He has a keen understanding of the industry and goals of financial institutions through his previous experiences and roles in senior management.

Leonard’s expertise and specialties include: operational auditing, compliance auditing, interest rate risk model validations, internal control evaluation and policy and procedure reviews. He is a Certified Public Accountant (CPA), Chartered Global Management Accountant (CGMA) Certified Financial Services Auditor (CFSA), Certification in Risk Management Assurance (CRMA) and Certified Bank Auditor (CBA). He has also served as an adjunct professor at Northern Kentucky University instructing undergraduate and MBA accounting classes.
Internal Audit Best Practices

• Role and Definition of Internal Auditing
• The Three Lines of Defense
• Regulatory Guidance & Expectations
• Key Elements of an Effective IA Program
• Basel Internal Audit Principles
• Internal Audit Outsourcing Considerations
• Resources
“The origin of auditing goes back to times scarcely less remote than that of accounting...Whenever the advance of civilization brought about the necessity of one man being entrusted to some extent with the property of another, the advisability of some kind of check upon the fidelity of the former would become apparent.”

*Accounting historian Richard Brown (1905, quoted in Mautz & Sharaf, 1961)*
“Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.”

_The Institute of Internal Auditors (IIA) definition_
Internal Audit Standards

In 1978, The IIA formally approved the *Standards for the Professional Practice of Internal Auditing (Standards)*, which had the following purposes:

1. Assist in communicating to others the role, scope, performance, and objectives of internal auditing
2. Unify internal auditing throughout the world
3. Encourage improved internal auditing
4. Establish basis for consistent measurement of internal auditing operations
5. Provide a vehicle by which internal auditing can be fully recognized as a profession
Shift to Enterprise Risk Management (ERM)

- Internal audit was traditionally focused on identifying policy violations and encouraging compliance with regulations.
- Focus has shifted towards a more integrated approach to risk management.
- Evolution is a result of changing nature of the market and industry regulations.
- New outlook involves a transition from a document-centric approach to a data-centric approach, allowing internal audit to take advantage of technology that can enhance enterprise risk management (ERM).
Three Lines of Defense in Effective Risk Management & Control

• Published in 2013 by the IIA
• Provides simple and effective way to enhance communication on risk management and control
• Clarifies essential roles and duties
• Provides a fresh look at operations
• Helps assure ongoing success of risk management initiatives
• Is appropriate for any organization
1. Operational Management

- Operational managers own and manage risks
- They are responsible for implementing corrective actions to address process and control deficiencies
2. Risk Management and Compliance Functions

The specific functions will vary by organization and industry, but typical functions in the second line of defense include:

- **Risk Management**
  - Facilitates and monitors the implementation of effective risk management practices by operational management

- **Compliance**
  - Monitors various specific risks such as noncompliance with applicable laws and regulations

- **Controllership**
  - Monitors financial risks and financial reporting issues
3. Internal Audit

- Internal auditors provide the governing body and senior management comprehensive assurance based on the highest level of independence and objectivity within the organization.
- The scope of this assurance, which is reported to senior management and to the governing body, usually covers:
  - A broad range of objectives
  - All elements of the risk management and internal control framework
  - The overall entity, divisions, subsidiaries, operating units, and functions
Internal Audit Best Practices

- Act in accordance with recognized international standards for the practice of internal auditing
- Report to a sufficiently high level in the organization to be able to perform its duties independently
- Have an active and effective reporting line to the governing body
An effective system of internal control and an independent internal audit function form the foundation for safe and sound operations, regardless of an institution's size.

**Board and Senior Management Responsibilities**

The board of directors and senior management are responsible for having an effective system of internal control and an effective internal audit function in place at their institution. They are also responsible for ensuring that the importance of internal control is understood and respected throughout the institution. This overall responsibility cannot be delegated to anyone else. They may, however, delegate the design, implementation and monitoring of specific internal controls to lower-level management and the testing and assessment of internal controls to others.
Structure and Reporting Relationships
Careful thought should be given to the placement of the audit function in the institution's management structure. The internal audit function should be positioned so that the board has confidence that the internal audit function will perform its duties with impartiality and not be unduly influenced by managers of day-to-day operations.
INTERAGENCY POLICY STATEMENT ON THE INTERNAL AUDIT FUNCTION AND ITS OUTSOURCING (March 2003)

Scope
The frequency and extent of internal audit review and testing should be consistent with the nature, complexity, and risk of the institution's on- and off-balance-sheet activities. At least annually, the audit committee should review and approve internal audit's control risk assessment and the scope of the audit plan, including how much the internal audit manager or designated liaison relies on the work of an outsourcing vendor. It should also periodically review internal audit's adherence to the audit plan. The audit committee should consider requests for expansion of basic internal audit work when significant issues arise or when significant changes occur in the institution's environment, structure, activities, risk exposures, or systems.
INTERAGENCY POLICY STATEMENT ON THE INTERNAL AUDIT FUNCTION AND ITS OUTSOURCING (March 2003)

Review of the Internal Audit Function and Outsourcing Arrangements
Examiners will assess the quality and scope of an institution's internal audit function, regardless of whether it is performed by the institution's employees or by an outsourcing vendor.
Examiners will be looking for evidence of the following:

- Internal audit function's control risk assessment, audit plans, and audit programs are appropriate for the institution's activities.
- Internal audit activities have been adjusted for significant changes in the institution's environment, structure, activities, risk exposures, or systems.
- Internal audit activities are consistent with the long-range goals and strategic direction of the institution and are responsive to its internal control needs.
- Audit committee promotes the internal audit manager's impartiality and independence by having him/her directly report audit findings to it.
Examiners will be looking for evidence of the following (continued):

• Internal audit manager is placed in the management structure in such a way that the independence of the function is not impaired

• Institution has promptly responded to significant identified internal control weaknesses

• Internal audit function is adequately managed to ensure that audit plans are met, programs are carried out, and results of audits are promptly communicated to senior management and members of the audit committee and board of directors
Examiners will be looking for evidence of the following (continued):

- Workpapers adequately document the internal audit work performed and support the audit reports.
- Management and the board of directors use reasonable standards, such as the IIA's *Standards for the Professional Practice of Internal Auditing*, when assessing the performance of internal audit.
Generally, insured banks with consolidated assets of more than $500 million are required to establish an audit committee. However, the board of directors may fulfill the responsibilities of the audit committee if the institution is not required by law to establish one. To establish an effective internal audit function, the board of directors (or its audit committee) should establish an audit policy that outlines the framework and standards for which the audit function is expected to operate. The policy and audit committee charter should take into consideration the size and complexity of the bank, with consideration given to the development of the following documents: Audit Committee Charter, Internal Audit Charter, Internal Audit Policy, and Internal Audit Procedures.

Federal Reserve Bank of Atlanta
Overview of the Components of an Effective Internal Audit Function
**Key Elements of an Effective IA Program**

- **Staffing** - The internal audit function should be competently supervised and staffed by people with sufficient expertise and resources to identify the risks inherent in the institution's operations and assess whether internal controls are effective.

- **Risk Assessment** - A control risk assessment (or risk assessment methodology) documents the internal auditor's understanding of the institution's significant business activities and their associated risks. These assessments typically analyze the risks inherent in a given business line, the mitigating control processes, and the resulting residual risk exposure of the institution. They should be updated regularly to reflect changes to the system of internal control or work processes, and to incorporate new lines of business.
Key Elements of an Effective IA Program

- **Internal Audit Plan** - An internal audit plan is based on the control risk assessment and typically includes a summary of key internal controls within each significant business activity, the timing and frequency of planned internal audit work, and a resource budget.

- **Internal Audit Program** - An internal audit program describes the objectives of the audit work and lists the procedures that will be performed during each internal audit review.

- **Internal Audit Report** - An audit report generally presents the purpose, scope and results of the audit, including findings, conclusions and recommendations. Workpapers that document the work performed and support the audit report should be maintained.
Internal Audit Exception Tracking - Management responses to audit findings should be documented and tracked for adequate follow-up.

- Is there documentation detailing the coverage, findings, and follow-up of control weaknesses?
- Does management give appropriate and timely attention to material control weaknesses once identified?
- Is line management held accountable for unsatisfactorily or ineffectively following up on control weaknesses?
BASEL Internal Audit Principles

Highlights from the BASEL Report:

• Every activity (including outsourced activities) and every entity of the bank should fall within the overall scope of the internal audit function (*princ. 6*)

• The scope of the internal audit function’s activities should ensure adequate coverage of matters of regulatory interest within the audit plan (*princ. 7*)

• Each bank should have a permanent internal audit function (*princ. 8*)

• 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 (*princ. 13*)
Internal Audit Outsourcing

Outsourcing Considerations

• Many organizations are turning to outsourcing arrangements to satisfy internal audit needs due to:
  – Increasing complexities
  – Time constraints
• Outsourcing arrangements take many forms
• Some enter into these arrangements to enhance the quality of their control environment by obtaining the services of a vendor with the knowledge and skills to critically assess and recommend improvements to their internal control systems
Internal Audit Outsourcing

Outsourcing Considerations

• Directors and senior management should ensure that the outsourced internal audit function is competently managed.

• Small institutions that do not employ a full-time audit manager should appoint a competent employee who ideally has no managerial responsibility for the areas being audited to oversee the outsourcing vendor's performance under the contract.
  – This person should report directly to the audit committee for purposes of communicating internal audit issues.
Outsourcing Considerations

- To clearly distinguish its duties from those of the outsourcing vendor, the institution should have a written contract with provisions that:
  - Define the expectations and responsibilities under the contract for both parties
  - Set the scope and frequency of, and the fees to be paid for, the work to be performed by the vendor
  - Set the responsibilities for providing and receiving information, such as the type and frequency of reporting to senior management and directors about the status of contract work
  - State that outsourced internal audit services provided by the vendor are subject to regulatory review and that examiners will be granted full and timely access to the internal audit reports and related workpapers prepared by the outsourcing vendor.
INTERAGENCY POLICY STATEMENT ON THE INTERNAL AUDIT FUNCTION AND ITS OUTSOURCING


The IIA - The Three Lines of Defense in Effective Risk Management and Control

BASEL COMMITTEE ON BANKING SUPERVISION The Internal Audit Function in Banks (2012)
http://www.bis.org/publ/bcbs223.pdf

Federal Reserve Bank of Atlanta
Overview of the Components of an Effective Internal Audit Function
https://www.frbatlanta.org/banking/publications.aspx
Thanks for joining us.

Angela Roberts  
Audit Manager  
Clark Schaefer Hackett  
(513) 338-8262  
aroberts@cshco.com

Leonard Wagers  
Audit Manager  
Clark Schaefer Hackett  
(513) 338-8274  
lwagers@cshco.com