

HOW TO USE THIS MANUAL

The risk based approach to internal auditing has been evolving for decades, yet unfolding events hastened the change. In a 2008 speech at the Federal Reserve Bank of Chicago's Annual Conference on Bank Structure and Competition, Federal Reserve Chairman Ben Bernanke said "...the (recent) turmoil in credit markets underscores some important principles for bank risk management, including the value of proper risk identification and measurement, the need for robust and objective valuation methods, the importance of preparing for liquidity disruptions and the critical role of strong oversight by senior managers." Furthermore, there are new public expectations of directors and senior management. Even for non-public companies, these expectations are still in effect, and the federal regulators will ensure that financial institutions remain above accounting scandals through the issuance and enforcement of regulatory policies and guidance.

In addition, the banking business is changing and becoming more complex and risky. Less than thirty years ago, financial institutions offered fixed-rate mortgages and rate-regulated deposit accounts. Today, there are fixed- and variable-rate loans made to all types of borrowers with risk profiles from A to D. Deposit rates fluctuate daily and pricing decisions may change hourly to reflect market conditions. New products, services, and technologies create new types of risk, demanding enhanced monitoring of activities, as we have learned in the subprime meltdown.

Despite the need for increased scrutiny, regulators and external auditors increasingly rely on the work the internal auditor performs. *Risk Based Auditing for Financial Institutions* will guide you through the more complex expectations the auditing function faces today.

BENEFITS OF USING THIS MANUAL

The benefits you can expect from using the materials provided in the *Risk Based Auditing for Financial Institutions* include the following:

- Significant improvement in the use of audit resources;
- Enhanced view of the value of audit reports as a management tool to prevent losses and to foster risk-managed growth and profits;
- More complete and satisfying work with the auditor as an integral part of the management team;
- Increased audit effectiveness due to the independence of the internal audit function and the Board of Directors' audit committee; and
- Potential for reduced regulatory pressures due to the risk based focus of audits.

INTENDED AUDIENCE

The *Risk Based Audit Manual* is structured to assist auditors who are making the transition to risk based auditing, as well as those auditors who are looking to evaluate ways to enhance the value of their existing risk based audit approach.

If you are currently conducting internal audits using the risk based approach, this manual can serve as a resource for evaluating new ideas and techniques to enhance your program. You should review the discussion below for insight into the content in the chapters, but not be bound by the same building-block approach presented for those making the transition. Each chapter can be used independently to extract questionnaires, risk rating methods, regulations, fraud detection methods, administrative improvement ideas, or outsourcing bid assistance.

For those making the transition to risk based auditing, this manual provides the foundation of this approach in the first four chapters and details of the step-by-step approach, together with forms and examples in the remaining chapters. We suggest that you follow the chapter order to gain the most from this building-block approach to developing and implementing a risk based auditing function in your institution.

Chapter 1: Changing Role of the Internal Auditor. This chapter discusses the transition that has been taking place in the auditing profession, with emphasis on the comparison between traditional control-based internal auditing and a risk-based approach to performing internal audits. Excerpts from this chapter may be useful in developing presentation material to discuss the advantages of risk based auditing with senior management and your Board of Directors.

Chapter 1.1: Implementing Control Self Assessments. CSA is a participative risk-based auditing approach in which project teams, led by management, review risks and controls and assesses methods to reduce risk. The internal auditor assumes the role of facilitator. This chapter describes the procedures for conducting control self assessment sessions.

Chapter 2: Federal Regulators and the Accounting Profession Set the Stage for Risk Based Auditing. In this chapter, the foundation for establishing a risk based audit program continues with a discussion of the banking industry and accounting profession regulations. The regulations discussed in this chapter demonstrate a progressive tightening of controls over the banking industry's financial audits. This trend is expected to continue with banking regulations forthcoming as a direct result of the regulator's desire to conform bank practices to the provisions of the Sarbanes-Oxley Act of 2002.

Chapter 3: Analysis and Impact of the Sarbanes-Oxley Act. The information in this chapter provides details of this important piece of legislation. Although senior management and the board may be well aware of this Act, they may not appreciate its implications on the internal and external audit functions. The materials in Chapters 2 and 3 should help to reinforce the need for strong audit efforts based on risk assessments.

Chapter 3.1: Internal Control Framework. Risk-based audits look closely at internal controls as a basis for risk assessments. Therefore, internal auditors must have a means of determining the adequacy of the controls in place within their institution. Two primary sources for internal control evaluations are the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and the regulators. Although other industry and professional sources such as the AICPA and banking groups also provide guidance on controls, this chapter focuses on COSO's Internal Control Framework and the FDIC's Internal Routine and Controls in the Risk Management Manual of Examination Policies, which recommends using COSO's Framework.

Chapter 3.1A: Methods for Evaluating and Testing Internal Controls. Internal auditors must routinely evaluate the adequacy of internal controls as part of the audit process. However, rarely is much consideration given to the actual design and effectiveness of these controls. This chapter provides insight into how to evaluate and test the design and effectiveness of internal controls. In addition, there is a discussion of what comprises good internal control based on the accounting profession and, in particular, materials from the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Chapter 3.1B: Internal Control Questionnaires (ICQs). Determining the adequacy of internal controls is the most important function the internal auditor can perform. A control evaluation helps the internal auditor to satisfy the audit committee's corporate governance responsibilities. To carry out these corporate governance responsibilities, the internal auditor must analyze operations, evaluate risk, review compliance, confirm information, recommend controls, and assure safeguards. This chapter discusses the types of controls the internal auditor must review and provides sample internal control questionnaires to use in the review process.

Chapter 3.2: Audit Function Quality Assurance Review Procedures. This chapter provides quality assurance work programs and questionnaires to help to assess the internal and external audit functions including outsourced internal audit services. These programs and questionnaires are based on regulatory examination methods, so that positive results from administering the questionnaires should make for a successful examination as, well as reduce audit risk.

Chapter 4: Complying with New Audit Committee Responsibilities. Here is the last piece of the foundation for risk based auditing: the effectiveness of the audit committee of the Board of Directors is crucial to the success of the risk based audit approach. This chapter provides complete justification and the related requirements for establishing an independent audit committee. Consider sharing this information with senior management and the board to demonstrate the need for an audit committee as an integral part of the risk based audit program.

Chapters 5: Overview of the Risk Based Internal Audit Process. This chapter provides a detailed step-by-step approach to developing and implementing a risk based audit function. In addition, examples are provided to demonstrate how the risk based audit approach can be used to determine specific audit procedures and audit tests.

Chapter 5.1: Understanding Enterprise Risk Management (ERM). Risk-based audits require access to management's risk assessments. An important step in that process is understanding how a financial institution approaches enterprise risk management (ERM). This chapter discusses the ERM process, and how risk-based auditors can use this discussion to evaluate the ERM process prior to reviewing management's risk assessments.

Chapter 6: Conducting Risk Assessment Surveys, and

Chapter 7: Risk Assessments and Audit Programs for Banking Products, Services, and Functions. These chapters elaborate on the risk assessment process that is the basis for building the risk based audit plan. Sample questionnaires and ranking systems are included so that you can easily adopt this process to your institution's environment. Chapter 7 also includes a sample risk based audit program for the loan function.

Chapter 7.1: Risk Based IT Audits. Information technology (IT) is an integral part of all financial institution operations. As such, risk based audits must focus on evaluating the programs, systems and controls

that are used to process banking transactions and to store customer information. This chapter on risk based IT audits is based on the Federal Financial Institutions Examination Council's (FFIEC's) *Information Technology Examination Handbook*, so that auditors can ensure their work plans are consistent with regulatory requirements.

Chapter 7.2: Evaluating Residential Real Estate Credit Risk. Credit risk inherent in residential real estate loans requires a sound understanding of prudent underwriting standards for these loans. This chapter discusses residential real estate credit risk issues, including underwriting criteria for making one- to four-family residential real estate term loans, construction loans, land loans, tax lien certificate procedures and home equity loans.

Chapter 7.3: Conducting Loan Quality Reviews. This chapter includes current regulatory guidance requirements for conducting loan reviews and the loan review procedures necessary to comply with regulations as well as loan review related safety and soundness issues that loan review personnel should consider in their overall loan quality review program.

Chapter 7.4: Identifying and Controlling Commercial Real Estate Concentrations. This chapter discusses how commercial real estate (CRE) loans comprise a major portion of many banks' loan portfolios. Demand for CRE lending — a traditional core business for many community banks — has been very strong in recent years, and a growing number of banks have CRE concentrations that are high by historical standards and rising. Growth in land acquisition, development, and construction (ADC) lending has been especially pronounced. The rapid growth in CRE exposures presents credit management challenges for bank management to monitor and control unfamiliar risks. This chapter discusses those risks and how to manage CRE loan portfolios according to regulatory guidance.

Chapter 7.5: Evaluating Fair Lending Risks. This is an overview of federal fair lending laws, including types of illegal discrimination. The analyses that examiners use to detect possible discrimination and how the analyses are used in examinations is also discussed. Institutions should prepare for these compliance exams and risk based auditors should ensure the preparation efforts are designed to adequately protect the institution from fair lending violations. In addition to federal laws, some states also have laws against credit discrimination. However, because federal banking agencies do not enforce state laws regarding credit discrimination, this chapter focuses only on federal fair lending laws.

Chapter 7.6: How to Identify, Measure, Monitor, and Control Interest Rate Risks. If you are going to audit your institution's IRR philosophy and policy, you need to understand the risks the institution is facing. Unfortunately for most, the risks are not obvious — ALM managers have to find them in the institution's asset and liability accounts and make certain assumptions about these risks. ALM managers also have to know where the institution is in the interest rate cycle and make an assumption about which direction interest rates will go in the future. Chapter 7.6, "How to Identify, Measure, Monitor, and Control Interest Rate Risks," helps risk-based auditors understand how ALM managers carry out their interest rate risk management responsibilities, thus providing a basis for auditing the ALM function.

Chapter 7.7: Risk Based Audits of Liquidity. This chapter provides risk assessments and audit procedures related to the development of risk-based audit programs for financial institution liquidity management. Risk based auditors must evaluate the institution's liquidity risks related to the adequacy of liquidity sources to meet present and future needs, and the ability of the institution to meet liquidity needs without adversely affecting operations or an institution's reputation. Chapter 7.7 also addresses risks associated

with concentrating correspondent relations to ensure compliance with the *Interagency Policy Statement on Correspondent Concentration Risks*.

Chapter 7.8: Risk Based Audits of Payment and Settlement Systems. This chapter addresses the risks related to payment and settlement systems. According to the Federal Reserve, the basic risks in payment and settlement systems are credit risk, liquidity risk, operational risk, and legal risk. These risks arise between financial institutions as they settle payments and other financial transactions and must be managed by institutions, both individually and collectively. This chapter provides risk assessments and audit procedures related to these risks to assist auditors in a risk-based evaluation and in updating their audit programs. In addition, this chapter provides a discussion of risk issues related to the expanded use of mobile banking with an emphasis on mobile banking device and application risks

Chapter 7.9: Risk Based Audits of Risk Management and Insurance. Rising insurance premiums and the possible inability to obtain coverage at any cost have changed the traditional role of insurance. Obtaining coverage for every insurable risk has been replaced by a risk management approach. This chapter discusses insurance risk management program issues and provides risk based auditors with an audit program and internal control review program to address this important risk.

Chapter 7.10: Risk Based Audits of Director Duties and Responsibilities. Directors are placed in positions of trust by the bank's shareholders, and both statute and common law place responsibility for the management of a bank firmly and squarely on the board of directors. This chapter provides a risk based audit approach to ensuring that directors are carrying out their duties and responsibilities according to safe and sound banking principles in compliance with applicable laws and regulations.

Chapter 7.11: Conducting a Risk Assessment of Cloud Computing. Cloud computing represents a significant strategic issue that the regulatory agencies expect institutions to evaluate carefully because all IT security issues must be considered according to FFIEC guidelines. This chapter provides guidance on conducting a risk assessment of cloud computing.

Chapter 7.12: Conducting ERM Risk Assessments. The Committee of Sponsoring Organizations (COSO) has presented guidance on "Enterprise Risk Management — Integrated Framework." Chapter 7.12 explains this guidance and how it applies to financial institutions.

Chapter 8: Risk Based Audit for Fraud Detection. No internal audit program is complete without coverage of fraud. This chapter provides practical guidance on how to identify situations where fraud may be present and what risk assessment factors should be used to determine which areas of your institution should be subject to a risk based audit. Sample fraud cases with the related controls and audit procedures that were used to detect the fraud are also included.

Chapter 9: Internal Audit Administration — Making a New Start with Risk Based Auditing. To ensure that your institution's management is receptive to the risk based audit approach, this chapter provides the tools to help you develop and communicate effective audit programs, workpapers, and reports. Audit communications become part of the strategic planning process to make sure the institution is setting proper risk priorities based on annual updates of risk assessments.

Chapter 10: Outsourcing the Internal Audit Function. Recognizing that some institutions will choose to outsource the internal audit function, this chapter provides a sample request for proposals (RFP) to use when arranging for bids from accounting or consulting firms offering this service.

Chapter 11: Conducting a Risk Based Audit — A Case Study. This chapter provides a review of how a risk based audit, using the techniques discussed throughout this manual, would take place in an institution.