The Seven-Step Process to Risk Based Auditing

Designed to evaluate controls and modify the scope of an audit, risk based auditing is paramount to an efficient and successful audit plan.

E. Michael Thomas, CIA, CPA, CBA, CFE, CRP
Executive
Crowe Chizek and Company LLC

AN IMPORTANT TOOL in the internal auditor's toolbox, risk based auditing effectively serves the three primary roles of internal auditing by providing feedback on the adequacy of internal control, providing a source of information for monitoring risk, and providing identification and communication of best practices among industries and operating lines of business.

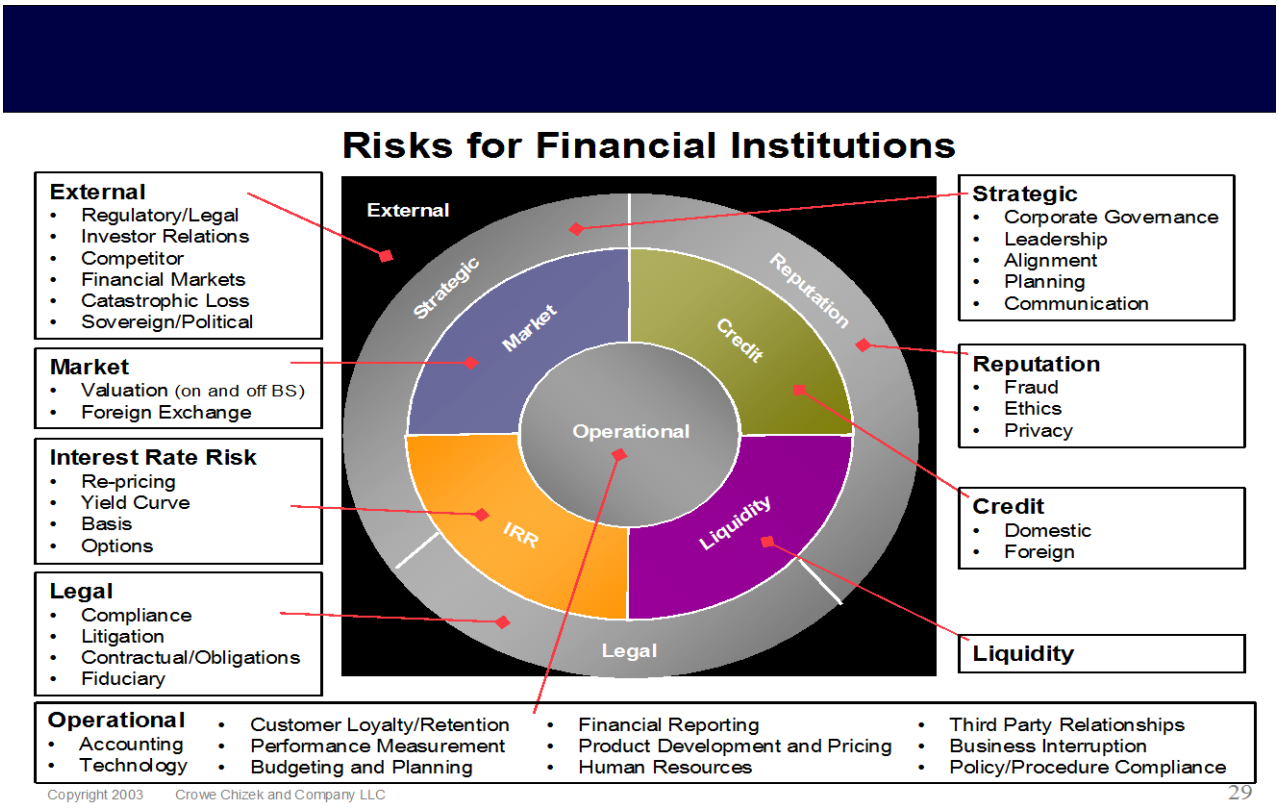
The primary focus of the risk based audit — to validate that the internal control environment is functioning as planned, that assets are adequately safeguarded, and that the organization is operating in conformance with established policies — is the same as traditional auditing, including communicating the results of the control assessment to executive management and the audit committee. The difference is the focus on the scope of the audit procedures designed to achieve these goals, which is set through the risk assessment and audit planning processes.

The process begins with formal annual planning, planning updates before audit segments begin, and periodic feedback from management and the audit committee regarding report content expectations. The audit scope is adjusted based on all of these factors, and allows the internal auditor a keen ability to understand management and audit committee concerns regarding risk and audit coverage and to react quickly to these concerns. A seven-step process outlining an effective risk based approach can easily be adapted in all internal audit environments.

Step One: Understanding the Business Environment

The key to effective risk based auditing is for the internal auditor to begin the planning process by gaining a thorough understanding of the business process for the area under review. In combination with feedback from management and the audit committee, business objectives are developed, specific risks that could cause management not to meet those business objectives are identified, and controls established by management to mitigate these risks are evaluated. These business objectives, risks, and controls should also be reviewed in relationship to the entity-wide business objectives, risks, and controls to assist in developing comprehensive corporate decisions.

A thorough understanding of risk — both global and specific to a business process — allows the internal auditor to focus on an area's risk factors. In the financial services and banking industry, these risks include traditional areas of risk — credit, interest rate, liquidity, market, operational, legal/regulatory, strategic, and reputational risk — as well as non-traditional risk such as performance risk measurement, human resource development and retention, customer loyalty and retention, product/service development, and ethics/integrity.



Step Two: Preliminary Risk Assessment

The purpose of the preliminary risk assessment is to determine the level of risk and adequacy of controls in the various functional processes of a business unit. The assessment focuses on the business profile, management structure, organizational changes, and specific concerns of management and the audit committee to determine the areas of greatest risk. It also serves to aid the internal auditor in evaluating the control design to determine the desired audit scope. Many corporations have incorporated an automated risk assessment application into their risk based

approach, which uses artificial intelligence to link audit planning, risk assessment, analytical review, internal controls review, and selection of audit procedures into one fully integrated, automated process. The risk assessment determines how well each function's control design mitigates inherent risk. At the conclusion of this assessment, the internal auditor evaluates the results and assigns a low, moderate, or high risk rating to the individual business processes.

In the financial service industry, specifically banking institutions, the rated risk factors are categorized into three broad categories: financial, business, and operational risk. These broad categories are then weighted to determine aggregate risk, such as commercial lending which would be weighted more heavily in financial risk, while wire transfer operations would be more heavily weighted in operational risk. An understanding of these risk definitions is required to effectively review the associated risks and control requirements.

Financial Risk

Financial risk includes four key categories: credit, interest rate, market, and liquidity risk.

Credit risk — which is most closely associated with lending activities in the financial services industry — is the risk to an institution's earnings and capital when a customer fails to meet the terms of any contract or otherwise fails to perform as agreed. Credit risk encompasses a broad range of financial institution activities, including items reflected both on and off the balance sheet, as well as from any activity where the institution is dependent on issuer, borrower, or counter-party performance. For example, an investment security portfolio has inherent credit risk, (i.e. the risk that the issuer of a security may default) as do counter-parties in derivative contracts.

Interest rate risk focuses on the impact to earnings and capital arising from economic movement in interest rates. The focus is on the change in value in an investment portfolio (e.g. portfolios held-to-maturity and available-for-sale) and the potential impact to a company's interest earnings, as well as the economic perspective of the market value of portfolio equity. Interest rate risk should be evaluated for re-pricing risk, basis risk, yield curve risk, and options risk.

Interest rate risk definitions:

- Re-pricing risk represents the risk associated with the differences in timing of cash flows and rate changes with an institution's products.
- Basis risk represents the risk associated with changing rate relationships among varying yield curves associated with an institution's products.
- Yield curve risk is associated with changing rate relationships over an institution's maturity structure.
- Options risk is associated with interest-related options, which are embedded in an institution's products.

Market risk focuses on the impact to earnings and capital arising from changes in market factors — interest rates, market liquidity, volatility — that affects the value of traded instruments. Market risk includes items reflected both on and off the balance sheet, focusing primarily on mark-to-market portfolios (e.g. accounts revalued for financial statement presentation) such as trading accounts and certain derivatives. Foreign exchange, which is a separate risk category, can also be classified as having market risk.

Liquidity risk, which is frequently monitored along with interest rate risk and price risk, if applicable, is evaluated through management's asset/liability management process. Liquidity risk, including both on and off balance sheet activity, focuses on the impact to earnings and capital resulting from an institution's inability to meet its obligations as they become due in the normal course of business without incurring significant losses. It also includes the management of unplanned decreases or changes in funding sources, as well as managing changes in market conditions that could affect an institution's ability to liquidate assets in the normal course of business without incurring significant losses.

Business Risk

Legal and regulatory, strategic, and reputation risk are classified as business risk.

Legal and regulatory risk — also known as compliance risk — is the impact of unenforceable contracts, lawsuits, or adverse judgments that can disrupt or otherwise negatively affect an institution's operations or condition. Regulatory risk arises from violations or nonconformance with laws, rules, regulations, prescribed practices, or ethical standards. These risks — which are not limited to consumer protection laws — include exposure to litigation from all aspects of financial institution activities.

Strategic risk involves the risk to earnings and capital arising from adverse business decisions or improper implementation of those decisions. This definition is more than an analysis of the written strategic plan, and focuses on how plans, systems, and implementation affect franchise value. It also incorporates how management analyzes external factors that affect the strategic direction of an institution.

Reputation risk arises from negative public opinion that affects an institution's ability to establish new relationships or services, or continue servicing existing relationships. Reputation risk is the potential effect the public's opinion could have on an institution's franchise value.

Operational Risk

Operational risk is present on a daily basis through an institution's processing of transactions and is pervasive in all products and services an institution provides. It is defined as the impact to earnings and capital from problems encountered in processing transactions and is a function of operating processes, internal controls, management information systems, and employee integrity.

Step Three: Develop a Three-Year Audit Plan

Based on the preliminary risk assessment that places the auditable business processes within a risk matrix based on low to high risk, a three-year audit plan is established. With certain adjustments based on management and audit committee input or regulatory requirements, low risk areas would be audited every three years, moderate risk areas audited every other year, and high-risk areas audited every year. The three-year audit plan should be revisited each year during the update phase of the risk assessment process and adjustments should be made based on new or changed risk factors. This methodology allows the internal auditor flexibility in a changing risk environment.

Example Three-Year Audit Plan for a Bank

Audit Cycle/Area	Aggregate Risk from Risk Assessment Matrix	Audit Frequency (1, 2, or 3 year rotation)	Year 2003	Year 2004	Year 2005
LENDING OPERATIONS					
Commercial Loans		2	✓		✓
Consumer Loans		2		✓	
Real estate Loans		2	✓		✓
Credit Administration		1	✓	✓	✓
Secondary Marketing		3		✓	
TREASURY MANAGEMENT					
Securities		2	✓		✓
Cash Management		3			✓
Asset/Liquidity Management		2	✓		✓
Wire Transfer		1	✓	✓	✓
Automated Clearing House		1	✓	✓	✓
Borrowings and Repurchase Agreements		3		✓	
ACCOUNTING AND FINANCIAL REPORTING					
General Accounting		2	✓		✓
Financial Reporting		2		✓	
DEPOSIT OPERATIONS		2		✓	
BRANCH OPERATIONS		2	✓		✓
BANK ADMINISTRATION					
Human Resources		2	✓		✓
Payroll		3		✓	
Purchasing		3		✓	
Insurance Coverage		2	✓		✓

Step Four: Complete the Secondary Risk Assessment

In this stage, which is performed during the scheduled audit, the internal auditor determines the effectiveness of the control design. Through in-depth interviews, walk-throughs and other observations, the internal auditor determines if the controls established by management in the control design are in fact operating as designed.

The secondary risk assessment allows the internal auditor to more accurately tailor the audit approach to current risks by providing for alteration of the audit plan. For example, in the preliminary risk assessment the internal auditor may have noted that there were adequate segregation of duties and physical controls in place. Based on these circumstances the preliminary risk assessment could have placed the overall risk for the area at the moderate level. If, during the secondary risk assessment, the internal auditor learns that segregation of duties and physical controls were not actually in place, the overall risk for the area could be elevated to the

high level. As such, the audit plan and scope would need to be revised to include a higher level of substantive testing in response to the higher overall risk in the area.

Step Five: Execution of the Internal Audit Program

After making adjustments to the audit scope based on the results of the secondary risk assessment, the audit plan is finalized and audit fieldwork can begin. A standard audit program guides the audit process, and determines which audit procedures should be performed based on the secondary risk assessment rating. Naturally, the higher the risk assessment, the more detailed the audit procedures to be performed.

The following audit program is an example of applying the results of the secondary risk assessment to the actual audit procedures, using low (L), medium (M), or high (H) risk as the basis for the audit scope.

	Essential Control Point: Access to blank loan disbursement checks is restricted to authorized individuals.		
Risk	**Audit Procedures:**	**W/P Ref.**	**Done By**
LMH	1. Through inquiry and observation, determine whether access to blank loan disbursement checks is restricted to authorized individuals as follows: a.) Checks are stored in a locked cabinet or vault. b.) Access is restricted under dual control or to one individual. c.) Only authorized individuals are in possession of the key or combination to the locked cabinet or vault. (Consider performing this procedure during walk through of disbursement process.)		
MH	2. Through inquiry of bank personnel, determine whether logs or subsidiary records are maintained to monitor the issuance of checks by sequential number and to indicate the individual(s) who accessed the supply.		
MH	3. Through inquiry of bank personnel, determine whether periodic inventories of blank check supplies are performed. Review documentation for evidence of periodic inventories and determine whether the inventories were performed under dual control or by an individual who does not have regular access to the check supply.		
H	4. Obtain check logs and review for evidence of individual(s) who accessed the check supplies.		
H	5. Perform an inventory of blank checks.		

During audit fieldwork and prior to the exit meeting, all potential audit issues should be fully discussed with operating personnel and line management. This “exiting as you go” process serves three valuable purposes. First, it allows the internal auditor to ensure the facts are accurate, which prevents unnecessary audit work and strengthens the internal auditor’s credibility. Secondly, operating personnel and line management can begin correcting problems, which will positively demonstrate to senior management their ability to address issues. This also

allows no surprises at the formal exit interview. Lastly, if there are disagreements to items other than facts, such as the overall risk or the recommended solution, the internal auditor is aware before the formal exit and can react accordingly.

Step Six: Conduct a Formal Exit Meeting

A formal exit meeting should be conducted with both operating and senior management prior to leaving the field to present issues noted during the audit, as well as best practice suggestions for improving controls, efficiency, and operational performance. Minor exceptions or findings can be discussed verbally, which may not be included in the audit report.

The formal exit meeting is also the opportunity for the internal auditor and management to discuss recommendations for improvement and to clear any factual issues that are still in question. The internal auditor should be sure to give management credit for actions already taken and offer consultative advise on those issues that are unresolved.

Step Seven: Reporting and Communication

After the conclusion of the exit meeting, a report draft is issued to operating management to solicit corrective action plans. The draft report should include findings and recommendations ranked as high, moderate, or low risk. High risk indicates management should immediately remedy the situation to prevent significant risk of loss; moderate risk indicates that timely remedy by management is suggested; and low risk indicates that there does not appear to represent an immediate risk but improvements are still possible.

The report is issued in draft form to allow continued communication between the internal auditor and operating management in the areas of relative importance of the audit results and recommended solutions. At this phase of the process, there should be no disagreements as to the facts in the report as these should have been agreed to during the fieldwork and exit meeting stages.

Management action plans (MAPs) should document specific actions to address the findings and recommendations, with management assignments of who is responsible for the plan and a date when the actions should be concluded. In reviewing MAPs, the internal auditor should determine that the identified risk will be adequately addressed and the completion timetable is reasonable.

A final report is issued to include the internal auditor's findings and recommendations, as well as management's action plans. This report should be distributed to all applicable operating, senior and executive management, as well as to members of the audit committee. The internal auditor should regularly meet with the audit committee in person to discuss the audit reports and solicit any necessary feedback.

The internal auditor will periodically provide a monitoring report that management and the audit committee can utilize to track critical internal audit findings, follow up on the results, and review at a glance the effectiveness of risk management and the resolution of all significant findings. Follow up reporting should continue until the issue is satisfactorily resolved. This communication is often the source of appropriate changes in audit scope to address risk changes.

Focus is on Risk

The seven-step process to risk based auditing encompasses the attributes of business knowledge, macro-risk assessment, strategic audit planning, and detailed risk assessment necessary to effectively and efficiently deploy audit resources. If performed properly, the seven-step process will allow the internal auditor to focus on the areas of risk proportionate to the potential exposure to the company. The cycle of continually assessing risk, efficiently planning audit activities, and effectively performing, delivering, and reporting audit activities will result in overall lower risk to the organization.

Mike Thomas is an executive in the Montgomery Ala. office of Crowe Chizek, offering internal audit, IT audit, loan review and compliance outsourcing services to the financial services industry. Mike has over twenty-five years of broad-based experience, specializing in internal audit within the financial services industry.