5-2009

A Comprehensive Information Technology Risk Assessment Audit Framework for Small- and Medium-Sized Financial Institutions

Petter Lovaas
Dakota State University, lovaasp@pluto.dsu.edu

Kevin Streff
Dakota State University, kevin.streff@dsu.edu

A Comprehensive Information Technology Risk Assessment Audit Framework for Small- and Medium-Sized Financial Institutions

Petter Lovaas
Dakota State University
lovaasp@pluto.dsu.edu

Kevin Streff
Dakota State University
kevin.streff@dsu.edu

ABSTRACT

Information technology audits are vital information management programs for banks and financial institutions. A plethora of laws and regulations exists, requiring financial institutions to develop an information technology audit program to support its information technology infrastructure and keep non-public customer information secure. Furthermore, banks are required to complete a risk-based audit on an annual basis to comply with regulators. This research combines two previously identified frameworks, the Comprehensive Risk-Based Auditing Framework (CRBA) and Small to Medium Entity Risk Assessment Model (SMERAM), to further develop the audit process to include the critical risk assessment process and to ensure that the audit is risk- based. Having a sound risk-based audit program will improve the overall information security posture for banks and financial institutions. Furthermore, this research utilizes an example to demonstrate the process.

Keywords

Information technology auditing, information security, small- and medium-sized financial institutions, risk assessment, risk-based auditing, risk assessment auditing.

INTRODUCTION

In the Information Technology Audit Program (IT audit) Booklet, The Federal Financial Institutions Examination Council (FFIEC) states that:

> A well-planned, properly structured audit program is essential to evaluate risk management practices, internal control systems, and compliance with corporate policies concerning IT-related risks at institutions of every size and complexity. Effective audit programs are risk-focused, promote sound IT controls, ensure the timely resolution of audit deficiencies, and inform the board of directors of the effectiveness of risk management practices. An effective IT audit function may also reduce the time examiners spend reviewing areas of the institution during examinations. Ideally, the audit program would consist of a full-time, continuous program of internal audit coupled with a well-planned external auditing program (FFIEC, 2008).

Furthermore, the FFIEC IT Handbook documents that a sound, risk-based audit should include and cover the following areas:

- Identify areas of greatest IT risk exposure to the institution in order to focus audit resources;
- Promote the confidentiality, integrity, and availability of information systems;
- Determine the effectiveness of management's planning and oversight of IT activities;
- Evaluate the adequacy of operating processes and internal controls;
- Determine the adequacy of enterprise-wide compliance efforts related to IT policies and internal control procedures; and
- Require appropriate corrective action to address deficient internal controls and follow up to ensure management promptly and effectively implements the required actions. (FFIEC, 2008)

Banks and financial institutions are, according to regulations, required to develop an information technology audit program to support its information technology infrastructure, to keep non-public customer information secure, and to conduct a risk-based audit on an annual basis. This audit can be conducted either internally or externally. Whether the institution is conducting its own IT audits, or contract for it externally, the question is the same—how to complete the audit successfully. Because regulators provide little or no guidance to financial institutions, it is difficult to prepare for audits. Of the audit models on the market today, none are customized to provide feedback for both, adequacy and compliance, and none include the human factors of auditing, particularly aimed toward small- and medium-sized financial institutions. A framework that combines these will increase the bank's important information security posture.

This paper will discuss what is considered a risk-based IT Audit and how it can be successfully implemented in small- and medium-sized financial institutions. Furthermore, this research will summarize previous research completed on the audit frameworks on the market today, and discuss some of their shortcomings. Finally, this paper will discuss a new and innovative approach to risk-based auditing based on the Comprehensive Risk-Based Audit (CRBA) Framework (Lovaas, Streff, Podhradsky, 2009).

LITERATURE REVIEW

The time when information technology audits were basically a controls review is over. Today federal examiners are responsible for much more, including evaluating the value of the information technology audit function as it relates to specific functions, such as the institution's ability to report and detect important risk factors to the board of directors as well as to senior management (Patel, 2006).

A risk-based IT audit should

- Identify the institution's data, application and operating systems, technology, facilities, and personnel;
- Identify the business activities and processes within each of those categories;
- Include profiles of significant business units, departments, product lines, or systems, and their associated business risks and control features, resulting in a document describing the structure of risk and controls throughout the institution;
- Use a measurement or scoring system that ranks and evaluates business and control risks for significant business units, departments, and products;
- Include board or audit committee approval of risk assessments and annual risk-based audit plans that establish audit schedules, audit cycles, work program scope, and resource allocation for each area audited;
- Implement the audit plan through planning, execution, reporting, and follow-up; and
- Include a process that regularly monitors the risk assessment and updates it at least annually for all significant business units, departments, and products or systems. (FFIEC, 2008)

Risk-based internal auditing (RBIA) is considered the methodology that the internal audit department utilizes to ensure that risks are being managed and assures that the residual risk falls within appropriate levels. Basically, risk- based auditing ensures that the organization is within its acceptable level of risk after controls are put into place. The board of directors in any organization is ultimately responsible for this acceptable risk level (Griffiths, 2006).

According to Griffiths, in order for any risk-based audit framework to be implemented successfully in an organization, the board of directors and upper management must ensure that the institution has identified all risks for each asset, and through a risk assessment process, that controls have been implemented to reduce the risks for each asset, depending on its criticality level, and falls within the acceptable risk level the board has determined and approved. Ensuring a comprehensive risk management process is critical to any organization, and will define the responsibilities of management, external audit processes, internal audit, and any other functions that provide assurance (Griffith, 2006).

One of the major aspects of conducting and planning an IT compliance audit involves selecting the framework utilized. The financial sector requires very specific regulatory guidelines for conducting an information technology audit (Beaumier, 2007). There are several standards that can be utilized to assist in complying with these standards. Even if an organization has more than one regulator to comply with, standards, such as the International Organization for Standards (ISO) 27002, will help compliance with these regulations (Greene, 2006). Because guidance from regulators is scarce, audit frameworks can be utilized for more specific guidance on conducting an audit. Some of the most accredited frameworks on the market are the *Committee of Sponsoring Organizations* Enterprise Risk Management (COSO ERM) framework and the Control Objectives for Information and related Technology (COBIT). Although they offer some similarities when conducting a compliance audit, none of these frameworks are identical. There are, however, some key areas that must be addressed and are a part of all of frameworks (Beaumier 2007):

- Board of director and senior management oversight
- Risk identification and assessment

- The Compliance organization itself
- Policies and procedures
- A system of internal controls
- Training
- Self-monitoring and remediation
- A customer complaint process
- Reporting and record keeping
- Board of directors and management reporting

As identified in previous research, most of these frameworks fall short of regulatory requirements for small- and medium-sized financial institutions (Lovaas, Streff, Podhradsky, 2009). The ISO 27002 standard is often referred to as "mile wide, and inch deep" (Privacy Rights Clearinghouse, 2008). The ISO standards cover many topics, but none in depth. Utilizing the COSO framework will leave the auditor to rely heavily on the reviews of policies and procedures to ensure that the audit complies with the framework. The goal of a COSO audit is to ensure that the organization and its management have in place appropriate internal controls and ensure a strategic view. The process extends through monitoring and decisions relating to financial reporting and internal control (Singleton, 2008). In addition, the auditor will balance the audit findings and make a final overall evaluation that outlines the level of risk in the five areas of the COSO model. Even within the model, strengths in certain elements may mitigate weaknesses in other elements (Singleton, 2008). Because no standard exists in auditing the soft controls, in practice utilizing the COSO framework may not be as easy as it seems (Simmons, 1997).

Another audit framework more often utilized by IT auditors is the COBIT framework. "COBIT is a comprehensive IT governance framework that has achieved international recognition and usage because it deals with every aspect of IT" (Financial Service Technology, 2009). The intent of information technology governance and the aim behind COBIT is to ensure that information technology and organizational needs are met and that information technology extends the organization's strategies and objectives (Martin, 2008).

In essence, the COSO framework is designed to provide guidance on addressing internal control needs throughout an organization, and does not necessarily directly relate back to IT. COBIT, on the other hand, is designed to be very open, and allows the organization to address specific information technology control issues.

Ultimately, all audit frameworks discussed in this section follow the IT audit Life Cycle outlined by Hunton, Bryant, and Bagranoff. It indicates that all audit frameworks include the following:

- Planning
- Risk Assessment
- Prepare Audit Program
- Gather Evidence
- Form Conclusions
- Deliver Audit Opinion
- Follow Up (Hunton, Bryant, Bagranoff, 2004).

SUMMARY OF PROBLEM

Because no comprehensive risk-based audit framework, particularly designed for small- and medium- sized financial institutions exists, the CRBA framework has been developed. It includes vulnerability assessments, penetration testing, internal auditing, social engineering, and, finally, an external audit. Combining all of these processes ensures an innovative, ongoing audit framework designed to fully satisfy regulators and most of all the needs that small- and medium- sized financial institutions have in complying with regulatory requirements. Figure 1 shows and explains the CRBA framework (Lovaas, Streff, Podhradsky, 2009).

"An appropriate assessment of risk is the foundation of a high quality audit" (AccountingWeb, 2008). Previous research has suggested that a new innovative Risk Management Program can help with risk management for small- and medium- sized financial institutions (SMERAM) (Podhradsky, Streff, Engebretsen, Lovaas, 2009). SMERAM helps determine if they are compliant with regulatory requirements and for each asset fall within the acceptable risk level that will depend on the size and complexity of the financial institution. "Each institution has its own acceptable risk level, which is derived from its legal and regulatory compliance responsibilities, its threat profile, and its business drivers and impacts" (Harris, 2006). SMERAM further helps to complete a valid risk assessment that is both, an adaptive and integrated part, of the entire information security program (Podhradsky, Streff, Engebretsen, Lovaas, 2009). The SMERAM process includes nine steps outlined in Table 1.

Table 1. SMERAM Risk Assessment Process

1. Inventory assets, vendors, and service providers	4. Determine Inherent Risk. Which assets represent risk to the bank?	7. Demonstrate compliance, reporting, improve the process
2. Develop priorities, protection profile (Confidentiality, Integrity, Availability-Volume)	5. System Controls. What system safeguards does the bank want to implement?	8. Organizational Controls. What safeguards does the bank want to implement?
3. Identify Threats. What are the threats to each asset?	6. Determine Residual Risk. What is the risk after applying controls?	9. Document Information Security Program and establish an effective set of IT policies

A comprehensive risk assessment process and information technology audit process is vital to any comprehensive information security program when considering small- and medium- sized financial institutions. "The two major pillars of the program include the IT Risk Assessment and the IT Audit. The IT Risk Assessment evaluates the use of technology to identify appropriate compensating controls, while the IT Audit evaluates the compliance and adequacy of these controls" (Streff, Lovaas, Podhradsky, 2009).

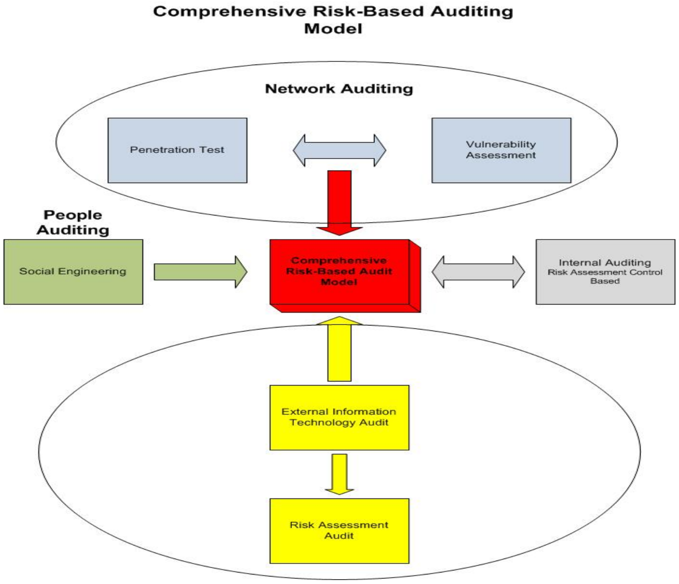
Comprehensive Risk-Based Auditing Model
Network Auditing
Penetration Test
Vulnerability Assessment
People Auditing
Social Engineering
Comprehensive Risk-Based Audit Model
Internal Auditing Risk Assessment Control Based
External Information Technology Audit
Risk Assessment Audit

Figure 1. CRBA Framework

SOLUTION AND MODEL

As indicated previously, Information Technology auditing is critical to any small- and medium- sized financial institution. Furthermore, banks are required to complete a risk-based audit on an annual basis. Combining the CRBA framework with the SMERAM model will create a risk-based audit program. As indicated in Figure 2, part of the external audit process includes the risk assessment audit. Figure 2 further develops the external audit process by adding threats and controls already developed from the risk assessment for part of the on-site audit process.

Included in the Risk Assessment Audit step are several details. The initial step is to scope between 5-10 assets, selected for audit by the financial institution. An asset is considered to be anything of value to the bank, and could be physical equipment, software, or services. This number will depend on the size and complexity of the institution. These assets are considered high-risk assets within the organization. A predetermined set of controls will be added to the asset. Furthermore, all of these controls will be checked on-site. For medium- to high- rated assets the process works the same, except only the predetermined critical controls will be checked during the on-site audit. Finally, no auditing will be done on low- risk assets.

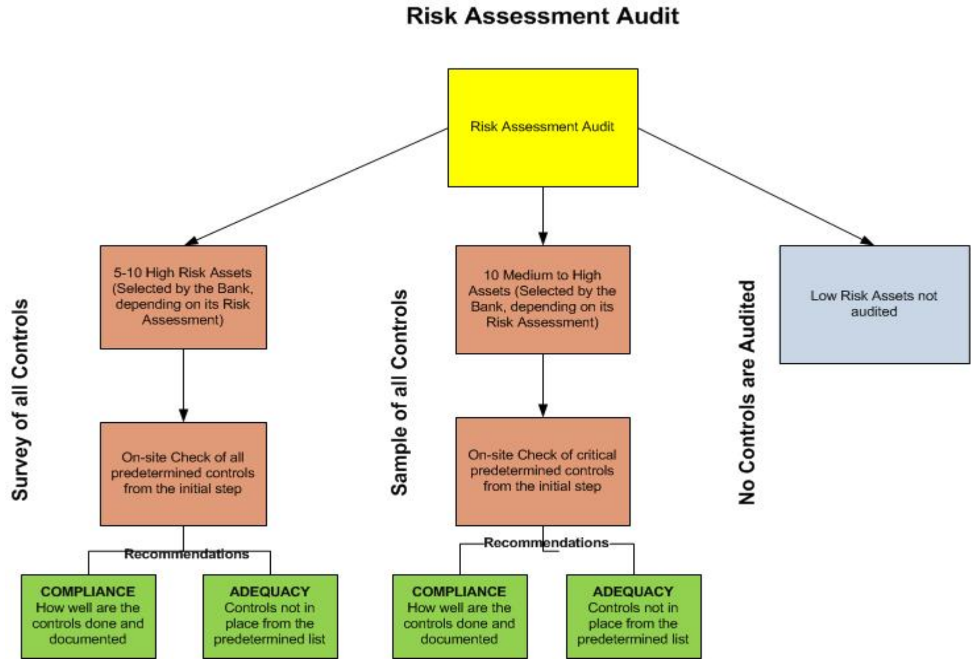
Risk Assessment Audit
Risk Assessment Audit
5-10 High Risk Assets (Selected by the Bank, depending on its Risk Assessment)
10 Medium to High Assets (Selected by the Bank, depending on its Risk Assessment)
Low Risk Assets not audited
Survey of all Controls
Sample of all Controls
No Controls are Audited
On-site Check of all predetermined controls from the initial step
On-site Check of critical predetermined controls from the initial step
Recommendations
Recommendations
COMPLIANCE How well are the controls done and documented
ADEQUACY Controls not in place from the predetermined list
COMPLIANCE How well are the controls done and documented
ADEQUACY Controls not in place from the predetermined list

Figure 2. Risk Assessment Audit

EXAMPLE

Secure Banking Solutions LLC has developed a Risk Assessment tool based on the SMERAM Risk Assessment Process previously discussed in this paper. This research will use this process as an example for developing the audit work papers. It will look at two examples, one high- and one medium- risk asset. The reason is to illustrate the risk-based process as it relates to checking the controls. There are several other threats and controls that will also be a part of the audit, but for example purposes only data loss as a threat is considered here. Table 2 shows a list of all controls associated with each asset. They are rated high, medium, and low. Because the Core Banking System (CBS) is considered a high- risk asset for all banks, it is used in this example. The second asset, again for example purposes, is a web server. For the CBS, all controls are verified on-site, while for the web server, samples of the controls are verified.

Table 2. Threat and Control Table

Threats and Controls for Core Banking System		Threats and Controls for Web Server	
Threat:	Control:	Threat:	Control:
Data Loss		Data Loss	
H	Security Information and Event Management	H	Security Information and Event Management
H	Unique User Accounts	H	Data Loss Prevention
M	Activity Logs	H	Activity Logs
M	Activity Log Monitoring	M-H	Activity Log Monitoring
L	Acceptable Use Notification	L	Acceptable Use Notification
M	Data Loss Prevention	M	Website Filtering
		M	Unique User Accounts
		L	Firewall: Egress Filtering

Once all the controls have been documented, a work paper can be developed. For the CBS, all of the controls are verified for both, compliance and adequacy. The bank is in compliance if it has implemented the controls, done it well, and has enforced it. If the bank looks at the access logs on a monthly basis, but no documentation exits to verify the monitoring, a recommendation for further documentation will be included in the audit report. For adequacy purposes, the controls that the bank does not have in place will be recommended in the audit report. For the web server, that in this example is considered a medium- rated asset, a sample of the controls will be audited. More emphasis will be put on the high- rated controls; however, a sample of the most important controls in the medium and low category will also be audited.

Table 3 shows an example work paper that the auditor will take on-site to document findings. It allows the auditor to document all findings while completing the onsite audit.

CONCLUSION AND FUTURE RESEARCH

This paper has looked at and documented requirements put forth by regulators for financial institutions as it relates to information technology auditing. The research has investigated some of the most commonly used audit models currently on the market. Furthermore, the researchers have suggested that these frameworks lack an important aspect of information security. By suggesting a new framework, CRBA, and combining this framework with the SMERAM risk management process, the research has suggested a new and innovative risk-based audit module that allows the board of directors and upper management to audit the areas that are most critical. Easily utilized work papers will simplify the external audit process.

Further research is required to validate this new model, and the researchers intend to test this new and innovative model in three small- and medium- sized financial institutions. Testing will ensure that the process works as intended. Furthermore, this critical testing will validate the model, and if necessary, corrections can be made to the model. Finally, the researchers intend to further expand the model to ensure that it is more comprehensive and includes additional regulatory requirements for small- and medium- sized financial institutions.

Table 3. Risk Assessment Audit Work Papers

Risk Assessment Audit for XYZ Bank

Threats and Controls for Core Banking System		Method of Audit	Request Information	Compliance	Adequacy	Notes	Exception / Recommendation
Threat:	**Control:**						
Data Loss							
H	Security Information and Event Management	Physical Check		The Bank has acquired software (GFI Events Manager) to monitor and report security events on the CBS. However, the software has not yet been installed.	The Bank should, in a timely manner, install and implement the SIEM software acquired.		1
H	Unique User Accounts	Physical Check		All user accounts on the CBS are considered unique. They consist of the first four letters of last name, the two- digit start month, and two- digit start year.	NA		
M	Activity Logs	Physical Check					
M	Activity Log Monitoring	Documentation	CBS Activity Logs, and documentation	The Bank is monitoring the activity logs on a needs basis. No formal process or documentation exists to support the Banks Logging and Monitoring Program.	The Bank should create a formal process to ensure that activity logs are reviewed and monitored on a regular basis.		1
M	Acceptable Use Notification	Physical Check					
M	Data Loss Prevention	Physical Check					
Threats and Controls for Web Server							
Threat:	**Control:**						
Data Loss							
H	Security Information and Event Management	Physical Check					
H	Data Loss Prevention	NA					
H	Activity Logs	Physical Check					
M-H	Activity Log Monitoring	Documentation	Web Server Activity Logs, and documentation				
M	Acceptable Use Notification	NA					
M	Website Filtering	Physical Check					
M	Unique User Accounts	NA					
L	Firewall: Egress Filtering	Physical Check					

REFERENCES

1. Accounting Web (2008). *PCAOB proposes seven new risk assessment auditing standards*. Retrieved April 3, 2009 from http://www.accountingweb.com/cgi-bin/item.cgi?id=106299&d=883&h=884&f=882&dateformat=%o%20%B%20%Y
2. Beaumier, Carol (2007). How to Audit Compliance in the Financial Services Industry: A Primer. Retrieved November 2008 from http://www.knowledgeleader.com/KnowledgeLeader/Content.nsf/Web+Content/HIHowtoAuditComplianceinFSI!OpenDocument
3. FFIEC, 2008. *Audit Handbook*. Retrieved March 15, 2008 from http://www.ffiec.gov/ffiecinfobase/booklets/audit/audit.pdf
4. Financial Services Technology (2009). *Performing COBIT Assessments*. Retrieved February 1, 2009 from http://www.usfst.com/pastissue/article.asp?art=272028&issue=228
5. Greene, Sari S. (2006). *Security Policies and Procedures; Principles and Practices*. New Jersey: Pearson.
6. Griffiths, David (2006). Risk-*Based Internal Auditing: Three views on Implementation*, retrieved April 1, 2009 from http://www.internalaudit.biz/files/implementation/Implementing%20RBIA%20v1.1.pdf
7. Harris, Shon (2006). *How to Define an Acceptable Level of Risk*. Retrieved April 21, 2009 from http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci1177563,00.html#
8. Hunton, J.E, Bryant, S.M, Bagranoff, N.A (2004). *Core Concepts of Information Technology Auditing*. New Jersey: Wiley
9. Lovaas, P. and K. Streff. A *Comprehensive Information Technology Audit Framework for Small- and Medium-Sized Financial Institutions*. Hawaii International Conference on Business, June 12-15, 2009, Honolulu, Hawaii
10. Martin, Alyssa G. (2008). *Assess Your IT Controls*. Retrieved January 30, 2009 from http://www.creditunionmagazine.com/Assess_Your_IT_Controls_823.html
11. Patel, Ray (2006). *Regulators Are Becoming More Focused on Information Technology Audits*. Retrieved April 2, 2009 from http://www.plantemoran.com/Industries/FinancialInstitutions/CreditUnions/Resources/Credit+Union+Advisor/2006+Spring+Issue/Regulators+Are+Becoming+More+Focused+on+Technology+Audits.htm
12. Podhradsky, A., Streff, K., Engebretson, P., Lovaas, P. (2009). *An Innovative Information Technology Risk Assessment Model for Small and Medium-Sized Financial Institutions*. Hawaii International Conference on Business, June 12-15, 2009, Honolulu, Hawaii.
13. Privacy Rights Clearinghouse (2008). *A Chronology of Data Breaches*. Retrieved November 10, 2008, from http://www.privacyrights.org/ar/chrondatabreaches.htm
14. Simmons, Mark R. (1997). *COSO Based Auditing*. Retrieved January 30, 2009 from http://www.cwu.edu/~atkinsom/coso.htm
15. Singleton, Tommie (2008). *The COSO Model: How IT Auditors can use it to Measure the Effectiveness on Internal Controls (Part 2)*. Retrieved January 30, 2008 from http://www.isaca.org/Content/NavigationMenu/Students_and_Educators/IT_Audit_Basics/IT_Audit_Basics_The_COSO_Model_How_IT_Auditors_Can_Use_IT_to_Measure_the_Effectiveness_of_Internal_C.htm
16. Singleton, Tommie (2007). *What Every IT Auditor Should Know About Auditing Information Security*. Retrieved January 16, 2009 from http://www.isaca.org/Content/NavigationMenu/Students_and_Educators/IT_Audit_Basics/What_Every_IT_Auditor_Should_Know_About_Auditing_Information_Security.htm
17. Streff, K., Lovaas, P., Podhradsky, A. (2009). *A Progressive Information Security Management Model for Small- and Medium-Sized Financial Institutions*. Hawaii International Conference on Business, June 12-15, 2009, Honolulu, Hawaii