Spring 3-5-2010

A Holistic Information Technology Audit Framework for Small- and Medium-sized Financial Institutions

Petter Lovaas
Dakota State University

DISSERTATION

A HOLISTIC INFORMATION TECHNOLOGY AUDIT FRAMEWORK FOR SMALL- AND MEDIUM- SIZED FINANCIAL INSTITUTIONS

Submitted by

Petter Lovaas

College of Business and Information Systems

In partial fulfillment of the requirements

For the Degree of Doctor of Science

Dakota State University

Madison, South Dakota

Spring 2010

DAKOTA STATE UNIVERSITY

March 5, 2010

We hereby recommend that the dissertation prepared under our supervision by Petter Lovaas entitled "A Holistic Information Technology Audit Framework for small- and medium-sized Financial Institutions" be accepted as fulfilling in part the requirements for the degree of Doctor of Science.

_____

Dr. Wayne Pauli, Dissertation Chair

_____

Dr. Douglas Knowlton, Committee Member

_____

Dr. Patrick Engebretson, Committee Member

_____

Dr. Surendra Sarnikar, Committee Member

ACKNOWLEDGEMENTS

Many thanks go to my dissertation committee: Wayne Pauli, Chair, a true mentor and friend; Douglas Knowlton for his encouragement and guidance; Surendra Sarnikar, for his extensive knowledge and guidance with my methodology work; Patrick Engebretson, for his wisdom in all matters, academic and personal.

My gratitude also goes to Kevin Streff, for giving me the opportunity to gain industry experience and his encouragement to begin my doctoral program; Tom Halverson, for giving me the opportunity to teach; Omar El-Gayer, Director of Graduate Studies, for advising me throughout my program; Lynn Ryan, for her support; Jennifer Mees and Annette Miller, for answering all questions relating to the Graduate School; Erik Osterkamp, for endless conversations on IT auditing and for his encouragement to complete the dissertation.

I would also like to thank my parents and sister Maria for their love and support; Nellie, my companion, for her patience; Ursula Hovet, for her remarkable dedication and understanding; Perry Benson for his advice and patience in listening; and to everyone else who has helped and guided me through this process.

DECLARATION

I herby certify that this project constitutes my own product, that where the language of others is set forth, quotation marks so indicate, and that appropriate credit is given where I have used the language, ideas, expression or writings of another.

I declare that the project describes original work that has not previously been presented for the awarded of any other degree of any institution.

Signed,

_____

Petter Lovaas

ABSTRACT

The Defense-in-Depth (DiD) theory has been accepted by most information security specialists and has been adopted by the Department of Defense (DOD) as a general methodology for improving any organization's information security posture. However, none of today's information technology (IT) audit frameworks incorporate all aspects of the DiD theory (National Security Agency, n.d.).

Banks and other financial institutions are, according to regulations, required to develop an IT audit program to support their respective IT infrastructure, to keep non-public customer information secure, and to conduct a risk-based audit on an annual basis (FDIC, 2000). The regulatory prescribed audit can be conducted either internally or externally. Whether the institution is conducting an internal IT audit or is contracting with an external firm to complete the audit, the question remains the same—how to complete the IT audit successfully.

Because regulators provide little or no guidance to financial institutions, it is difficult to prepare for IT audits. Of the available frameworks, none are customized to provide feedback for both, adequacy and compliance, and none includes the human factors of auditing.

The purpose of this study is to develop a holistic IT audit framework that incorporates the important DiD theory and is customized for small- and medium-sized financial institutions. The newly created framework is based on commonly accepted information security practices, federal regulations, current IT audit frameworks, and has been validated using the design science methodology. Furthermore, implementation using a multiple case study has been completed, and the results have been analyzed. This

research is significant as very little empirical data is available in the IT audit field. The framework is one of the first of its kind to illustrate a blueprint of a risk-based IT audit for small- and medium-sized financial institutions. Portions of this research have been further validated in academic journals and peer-reviewed conference proceedings.

Table of Contents

List of Tables

List of Figures

CHAPTER 1

Introduction

The Information Technology Audit (IT audit) Program Booklet, *The Federal Financial Institutions Examination Council* (FFIEC), states that a well-structured IT audit program is critical for the evaluation of management practices, internal control, and, finally, compliance with bank policy regarding IT. Furthermore, the audit program should be risk-based, promote critical controls, ensure that recommendations are addressed in a timely manner, and keep the Board of Directors current on risk management efforts. Ensuring a sound risk-based IT audit program and audit function may reduce the time examiners spend reviewing regulatory compliance of the bank. Finally, depending on the size and complexity of the institution, the IT audit program should ideally be a continuous process of internal review, coupled with an annual well-structured external IT audit (FFIEC, 2008).

The FFIEC IT Audit Handbook also sets forth certain requirements that a sound, risk-based audit should include. Some of the handbook's core ideas include that institutions must identify assets and develop a method for identifying the risks to each IT asset. This method should promote confidentiality, integrity and, finally availability. Furthermore, the IT Audit should also cover management activities and evaluate the adequacy of both policy and controls implemented by the bank.

Banks and other financial institutions are, according to regulations, required to develop an IT audit program to support its IT infrastructure, to keep non-public customer

information secure, and to conduct a risk-based audit on an annual basis (FDIC, 2000). This audit can be conducted either internally or externally. Whether the institution is conducting an internal IT audit or is contracting for it externally, the question remains the same—how to complete the IT audit successfully.

Because regulators provide little or no guidance to financial institutions, it is difficult to prepare for IT audits. Of the models on the market today, none is customized to provide feedback for both, adequacy and compliance, and none includes the human factors of auditing. Human factor auditing is a method an auditor may use to gain access to sensitive areas or information, also called social engineering. This method tests the employees to ensure knowledge of policies and procedures, and can provide critical training to ensure Information Assurance (IA). A framework that combines these will increase the bank's important information security posture. Through research, several other general issues have emerged with any type of audit, not simply IT audits. The most common concern is insufficient information when evidence is gathered to make adequate recommendations. Any organization should pay special attention to audit trails and, in particular, electronic records created by IT systems, such as system logs. These should be prioritized and stored appropriately as they become extremely important when conducting an IT audit (Burnelli, 2004).

The second most common audit issue deals with framework design errors, e.g., the auditor's failure to accurately calculate the inherent risk and adjust the audit program accordingly (Beasley, Carcello, Hermanson, & Neal, Spring 2009).

Most risk-based audits are heavily based on policies and procedures or network auditing. The National Security Agency (NSA) published a strategy called "Defense-in-

Depth (DiD)" that outlines the "best practices" for IA (See Figure 1). It integrates people, operations, and technology capabilities to establish IA protection across multiple layers and dimensions. A hacker, who attempts to penetrate or break down one security barrier, encounters these additional layers of defense, Defense-In-Depth (National Security Agency, n.d.). DiD is considered by most experts as a "best practice" for information security, and has been incorporated into various information security fields, such as network protection (Kelly, 2006).

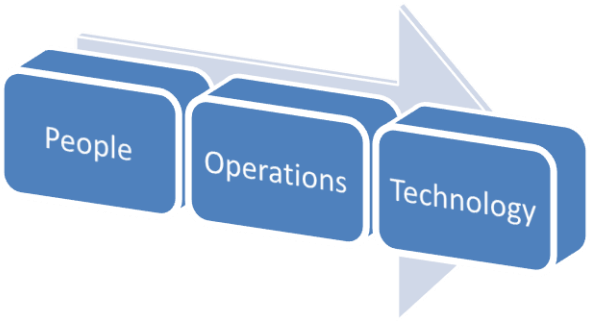

Figure 1: Defense-In-Depth

Purpose of Study

The DiD framework has been accepted by most information security specialists and has been adapted by the Department of Defense (DOD) as a general methodology for improving any organization's information security posture. However, none of today's IT Audit frameworks incorporates all aspects of the DiD strategy (National Security Agency, n.d.).

The purpose of this study is to develop a holistic IT audit framework that incorporates this important DiD concept. Furthermore, to develop such a framework, three research steps have been developed:

1. Identify shortcomings of existing IT audit frameworks, in particular, relating to small- and medium-sized financial institutions.
2. Develop a holistic risk-based IT audit framework, incorporating Defense-in-Depth, specifically designed for small- and medium-sized financial institution, based on current research and methods. (See Figure 1.)
3. Test and evaluate the artifact.

Requirements

The research has some inherent requirements to allow it to be designed specifically for small- and medium-sized financial institutions (SMEFIs). The framework has to:

1. Follow the Defense-In-Depth concept, including the following key areas: people, technology, and operations.
2. Comply with regulatory requirements.
3. Incorporate both, adequacy and compliance.
4. Utilize existing research and methodologies.
5. Suggest improvements in the development of the holistic IT Audit framework.

The success of this study will be determined through case studies and focus groups, as discussed in the Methodology section.

This concludes the introduction to the research on the development of the holistic information technology audit framework. Chapter 2 will deal with the regulatory requirements of Information Assurance and also identifies existing frameworks and their shortcomings.

Key Terms/Glossary

FFIEC	The Federal Financial Institutions Examination Council
IT	Information Technology
IA	Information Assurance
NSA	National Security Agency
DiD	Defense-in-Depth
DOD	Department of Defense
IS	Information Security
CIA	Confidentiality, Integrity, and Availability
EDP	Electronic Data Processing
CIS	Computer Information Systems
ISACA	Information Systems Audit and Control Association
CISA	Certified Information Systems Auditor
ISO 27001	International Organization for Standardization
BFS	Banking and Financial Sector
FDIC	Federal Deposit and Insurance Corporation
FRB	Federal Reserve Board
NCAU	National Credit Union Administration
OCC	Office of the Comptroller of the Currency
OTS	Office of Thrift Supervision
Infosec Triangle	Information Security triangle is commonly accepted as the perception model for analyzing, managing, and auditing information security
RBA	Risk-Based Auditing
CSO	Chief Security Officer
COSO ERM	Committee of Sponsoring Organizations of the Treadway Commission Enterprise Risk Management-Integrated Framework, published in 2004
COBIT	Control Objectives for Information and related Technology
ISMS	Information Security Management System
SMEFI	Small- and Medium-Sized Financial Institution
SOX	Sarbanes-Oxley Act
GLBA	Gramm-Leach-Bliley Act
VA	Vulnerability Assessment
PT	Penetration Testing
ISP	Information Security Program
IDS	Intrusion Detection System
ISO	Information Security Officer
SE	Social Engineering

CHAPTER 2

Literature Review

Information Assurance

The term Information Assurance (IA) is often used interchangeably with the term Information Security (IS). IA actually dates back to World War II, when the first modern computers were created and utilized to develop code-breaking computations. The initial purpose of these machines was to crack the codes from the powerful Enigma machine, developed by the Germans. The computer equipment had to be protected from physical threats. Access controls such as facial recognition, badges, and keys were utilized for these areas, hence the term computer security. IA, on the other hand, was not quite as complex, and usually simply involved document classifications. Obviously, there were no application security requirements during this period, leading to the focus of physical security against sabotage, espionage, and the likes (Johnson, 2005).

IA has since then developed into a greater area and takes into consideration three levels of asset protection–Confidentiality, Integrity, and, finally, Availability (CIA). According to John McCumber, "the primary consideration for confidentiality is not simply keeping information secret from everyone else; it is making it available only to those who need it, when they need it, and under appropriate circumstances." Integrity is critical, ensuring that accurate information is always available. In other words, integrity provides the "accuracy and robustness of data." Finally, availability represents the timeliness of data. If data is unreachable when needed, it is simply not available. Availability is often seen by organizations as an afterthought, as a demand for redundancy and uptime requirements (McCumber, 2005).

Information Technology Auditing – Basics

As with Information Assurance, Information Technology Auditing is considered a relatively new discipline. However, much has changed as it relates to its importance of IT auditing from several key incidents in history. Because of financial fiascos such as Enron, WorldCom, and Global Crossing, as well as the events of September 11, 2001, every industry has come to realize that IT auditing has become crucial in ensuring the integrity of information systems. "The need to control and audit IT has never been greater." (Gallegos, Sneft, Manson, & Gonzales, 2004).

Electronic Data Processing (EDP), Computer Information Systems (CIS) auditing, and Information Systems (IS) auditing have all become parts of IT auditing. Furthermore, each is considered an extension of traditional auditing. The initial need for IT auditing comes from several areas, among them auditors' realization that computers and information systems are critical, and valuable to businesses. Furthermore, professional organizations and government agencies realized that there was a need for IT controls, as well as for auditing those controls (Gallegos, Sneft, Manson, & Gonzales, 2004).

Initially, auditing components were taken from internal controls and information systems management that provide methodologies necessary to implement and design information systems (Gallegos, Sneft, Manson, & Gonzales, 2004).

From these early stages, IT auditing has evolved into a profession with conduct, aims, and qualities that are characterized by worldwide standards, as well as ethical rules as defined by ISACA. Professionals can also seek certifications, such as Certified Information Systems Auditor (CISA) (Gallegos, Sneft, Manson, & Gonzales, 2004).

The breadth and extensive knowledge required to perform IT audits are various and many. A few examples may be:

- Implementing and conducting risk-oriented audit approaches
- Applications of standards, such as ISO 27002
- Business understanding
- Assessment of information security and privacy issues that can impose risk for an organization
- Legal and regulatory requirements
- Management reporting and follow-up (Sayana, 2002).

Information systems have significant meaning to every organization. In the past, computer systems were seen as merely a way to record business transactions. Today information systems drive key aspects of the organization. The main purpose of information systems auditing is to review and provide feedback, assurances, and suggestions to the organization regarding its information security posture. These topics can be grouped into the McCumber cube's CIA:

1. Confidentiality: Will critical information on systems only be disclosed to authorized personnel?
2. Availability: Will critical business systems be available at all times when they are required to be? How well are these systems protected against all types of threats, e.g., disasters and losses?
3. Integrity: Will information on critical systems always be accurate, reliable and timely? What controls are in place to prevent unauthorized modification to the software, information, or databases? (Sayana, 2002).

As mentioned, information systems are more than just simply computers. They are complex systems and include several components that make up the business solution. An auditor can only give assurance about an information system if all of the components are evaluated and secured by the organization. Within any IT audit, the weakest link during the audit process is the total strength of the overall audit process.

Industry-Specific Background Information (Banking and Financial Sector)

The events of September 11, 2001, have brought attention to several security issues that make the United States vulnerable to a host of attacks. Over 85% of the critical infrastructure and assets are not owned by the federal government, but rather by the private sector (Dan, 2003). Information assurance is a pivotal factor to secure critical infrastructures and assets, so much so that former President Clinton identified a national goal to secure these national private-sector information assets and infrastructures in *Presidential Decision Directive 63*. It identifies eight key sectors that are extremely vulnerable to attack, including Telecommunications, Electrical Power Systems, Gas and Oil Storage and Transportation, Banking and Finance, Water Supply Systems, Transportation, Emergency Services, and Continuity of Government (Clinton, 1998).

Another publication, *Homeland Security Presidential Directive 7,* outlines specific requirements to what each sector is responsible for. The Department of the Treasury is the government body that is responsible for protecting the critical banking and financial sector. The Banking and Financial Sector (BFS) accounts for nearly eight percent of the US annual gross domestic product and is considered a backbone for the world economy. As terrorism and malicious attacks become more common, the BFS sector is a high-value and symbolic target. Furthermore, protection is also needed for

power outages, natural disasters. With increasing concern, flu pandemics must also be taken into consideration when protecting such a critical asset to our nation. Protecting the BFS means cooperation between financial regulators and private sector owners and operators. The goal is to ensure the safety and soundness of this industry by developing programs that provide protection. Furthermore, this coalition continuously improves these programs to include current and new threats to the banking and financial sector (Banking and Finance - Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan, 2007).

The Federal Financial Institutions Examination Council (FFIEC) is a formal interagency body and is a part of the cooperation that is in charge of protecting the banking and financial sector. Its purpose is to develop and design standards, develop uniform principles, and report forms for federal examinations. The FFIEC is a body of regulators from the Federal Reserve Board (FDR), Federal Deposit and Insurance Cooperation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS). The FFIEC's main goal is to promote uniformity in the supervision of the banking and financial sector. In an effort to develop a standard, the FFIEC has published the *FFIEC InfoBase Handbook*. This handbook is used to provide financial institutions with guidelines on Information Technology and Information Security, and is the basis for any IT examination. The *Handbook* incorporates a broad area of topics, including: Audit, Business Continuity Planning, Development and Acquisition, Information Security, and E-Banking (Greene, 2006).

In the *Information Technology Audit Program Booklet*, the FFIEC states that a well-structured IT audit program is critical for the evaluation of management practices, internal control, and, finally, compliance with bank policy regarding IT. Furthermore, the audit program should be risk-based, promote critical controls, ensure that recommendations are addressed in a timely manner, and keep the Board of Directors current on its risk management efforts. Ensuring a sound risk-based IT audit program and audit function may reduce the time examiners spend on reviewing certain areas of the bank. Finally, depending on the size and complexity of the institution, the IT audit program should ideally be a continuous process of internal review, coupled with an annual well-structured external IT audit (FFIEC, 2008).

The FFIEC IT Handbook also 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 that management promptly and effectively implements the required actions. (FFIEC, 2008)

Banks and other 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 (FDIC, 2000). This audit can be conducted either internally or externally. Whether the institution is conducting an internal IT audit or is contracting for it externally, the question remains the same—how to complete the IT audit successfully.

Because regulators provide little or no guidance to financial institutions, it is difficult to prepare for IT audits. Of the IT audit models on the market today, none is customized to provide feedback for both, adequacy and compliance, and none includes 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. Through research, several general problems have emerged with any type of audit, not simply IT audits. The most common one is that the auditor is not gathering enough evidence to make adequate recommendations. Any organization should pay special attention to audit trails and, in particular, electronic records created by IT systems, such as system logs. These should be prioritized and stored appropriately as they become extremely important when conducting an IT audit (Burnelli, 2004).

The second most common audit issue is that the framework used has design errors, more specifically, that the auditors failed to accurately calculate the inherent risk and adjust the audit program accordingly (Beasley, Carcello, Hermanson, & Neal, Spring 2009).

The breath and extensive knowledge required to perform IT audits are various and many. A few examples may be:

- Implementing and conducting risk-oriented audit approaches
- Applications of standards such as ISO 27002
- Business understanding
- Assessment of information security and privacy issues that can impose risk on an organization
- Legal and regulatory requirements
- Management reporting and follow up (Sayana, 2002).

Several articles and papers have been written about information security, including management and IT audits. IT auditing is, generally speaking, similar to more conventional audits that are more nontechnical, and is based on a risk assessment model. Most information security management and IT audits are generally based on the Infosec Triangle (Singleton T. W., 2007)—confidentiality, integrity, and availability (CIA), considered to be the most commonly protected characteristics of information assets. Some models have additional terms added to these three. The Infosec model is commonly accepted as the perception model for analyzing, managing, and auditing information security (Singleton T. W., 2007).

ISACA has outlined some broad major components of the information systems auditing classification:

1. Physical and environmental review: This includes physical security, power supply, air conditioning, humidity control, and other environmental factors.

2. System administration review: This includes security review of the operating systems, database management systems, all system administration procedures and compliance.
3. Application software review: The business application could be payroll, invoicing, a web-based customer order processing system or an enterprise resource planning system that actually runs the business. Review of such application software includes access control and authorizations, validations, error and exception handling, business process flows within the application software and complementary manual controls and procedures. Additionally, a review of the system development life cycle should be completed.
4. Network security review: Some typical areas of coverage are review of internal and external connections to the system, perimeter security, firewall review, router access control lists, port scanning and intrusion detection.
5. Business continuity review: This includes the existence and maintenance of fault tolerant and redundant hardware, backup procedures and storage, and a documented and tested disaster recovery/business continuity plan.
6. Data integrity review: The purpose of this is scrutiny of live data to verify adequacy of controls and impact of weaknesses, as noticed in any of the above reviews. Such substantive testing can be done using generalized audit software, e.g., computer assisted audit techniques (Sayana, 2002).

According to Sayana, these six elements will need to be adequately addressed and presented to management to achieve a clear and complete assessment of the system.

> For example, application software may be well designed and implemented with all the security features, but the default super-user password in the operating system used on the server may not have been changed, thereby allowing someone to access the data files directly. Such a situation negates whatever security is built into the application. Likewise, firewalls and technical system security may have been implemented very well, but the role definitions and access controls within the application software may have been so poorly designed and implemented that by using their user IDs, employees may get to see critical and sensitive information far beyond their roles. (Sayana, 2002)

Furthermore, it is important to realize that different audits may involve all of these steps to some degree. Some audits may only analyze one of the elements outlined, while others will drop some of them. However, the fact remains that they all need to be addressed, though it is not mandatory to do all of them in one audit, as the skills required by the auditor in each step may be different. Though they may be performed at different times, it is also important to understand that the result of each step has to be looked at by management as a relationship, ensuring that a complete view of the issues and problems is adequately presented (Sayana, 2002).

As more traditional audit methods are usually regarded as a controls review, a new method has surfaced—Risk-Based Auditing (RBA). That means that regulators 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).

There is clearly a need for RBA, as most organizations utilize a number of different information systems. These may have different applications for various functions and activities. Furthermore, computer systems may be installed at different geographical locations. Usually, the auditor is left with questions on what, when, and how often to conduct an audit. The answers to these questions are to deploy an RBA approach (Griffiths, 2006).

Risk-based IT auditing is an approach that focuses on analyzing risk applicable to the business. More precisely,

> [It] is an approach that focuses on the response of the organization to the risks it faces in achieving its goals and objectives. Unlike other forms of audit, Risk Based Auditing starts with business objectives and their associated risks rather than the need for controls. It aims to give independent assurance that risks are being managed to an acceptable level and to facilitate improvements where necessary (Arun District Council, 2009)

Every information system has some form of inherent risks. These will have a different impact on the systems in various ways. There are four short steps in developing an RBA audit plan:

1. Take an inventory of the information systems in use by the organization and categorize them.
2. Determine which of the systems affects critical functions or assets, such as money, materials, customers, decision making, and how close to real time they operate.
3. Assess what risks affect these systems and the severity of impact on the business.

4. Rank the systems based on the above assessment and decide the audit priority, resources, schedule, and frequency. (Griffiths, 2006)

Based on these four steps, an auditor can develop an annual audit plan that outlines the audits to be performed during the calendar year, taking into consideration the schedule and resources required.

Risk-based internal auditing (RBIA) is considered the methodology utilized by the internal audit department to ensure that risks are being managed and that the residual risk falls within appropriate levels. 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, through a risk assessment process, identified all risks and implemented all controls for each asset. When controls have been applied and fall within the acceptable risk level as approved, the risk assessment process is complete. 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 (Griffiths, 2006).

As it relates to external auditing, a risk-based audit will also require that auditors completely understand their clients, their clients' industry, the nature of their business and the environment they operate in. "Without a thorough understanding, the auditor may

fail to correctly identify the critical business process and corresponding internal controls that he should evaluate" (Hunton, Bryant, & Bagranoff, 2004).

Risk-based auditing extends and improves the risk assessment process by looking at areas based on risk instead of focusing on controls (McNamee, 1997). By focusing on high risk areas, the auditor must also understand that "some activities might never be deemed important enough to receive internal audit attention" because they are considered low risk areas (Parkinson, 2004).

The risk-based audit methodology is relatively new, and it greatly differs from more traditional audit approaches. Table 1 outlines these differences (Lindow & Race, 2002).

Table 1: Traditional vs. Risk-Based Audit Approach

Traditional	**Risk-Based**
Audit focus	Business focus
Transaction-based	Process-based
Financial account focus	Customer focus
Compliance objective	Risk identification, process improvement objective
Policies and procedures focus	Risk management focus
Multi-year audit coverage	Continual risk-reassessment coverage
Policy adherence	Change facilitator
Budgeted cost center	Accountability for performance improvement results
Career auditors	Opportunities for other management positions
Methodology: Focus on policies, transactions and compliance	Methodology: Focus on goals, strategies, and risk management processes

Banks and financial institutions are required to conduct an annual RBA. If an institution is not compliant, the Federal Deposit and Insurance Corporation (FDIC) can shut the bank down (Rothman, 2007). The FFIEC has outlined the following requirements for an RBA audit:

- 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)

Defense-in-Depth

As stated previously, Information Assurance is so much more than simply computer systems. Reality is that IA is the sum of the total methods of the protection of people, process, and technology. As proven with research, there is no "silver bullet" for IA— no single method or technology will make a single asset or information safe from

internal or external threats. A layered defense approach is needed, better known as Defense-in-Depth (DiD). The National Security Agency (NSA) published the DiD framework that outlines the "best practices" for information assurance. It integrates people, operations, and technology capabilities to establish information assurance (IA) protection across multiple layers and dimensions (See Figure 2). Several layers of defense will cause a hacker who attempts to penetrate or break down one security barrier to encounter another layer of defense, called Defense-in-Depth (National Security Agency, n.d). DiD is considered by most experts as a "best practice" for information security, and has been incorporated into different information security fields, such as network protection (Kelly, 2006).

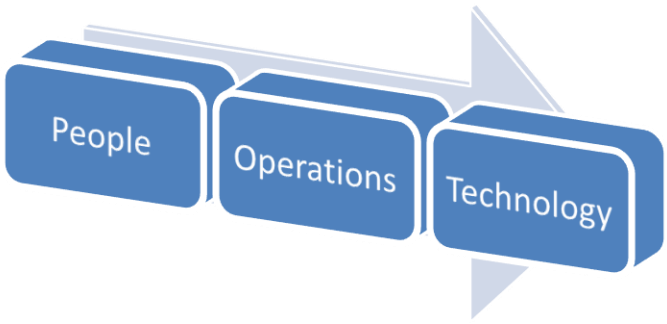

Figure 2: Defense-In-Depth

People are often considered the most critical asset of protection to any organization, and therefore play a crucial role in the DiD framework, as people are generally considered the "first line of defense." Protecting the information assets in any organization begins at the people aspect of the DiD framework, usually with the Chief Information Officer. The CIO must have a clear understanding of what is being protected against what threats. This knowledge must be clearly communicated in information security policies and procedures, as well as assignments of roles and responsibilities.

This includes training of personnel (National Security Agency, n.d.). Figure 3 gives an example of topics that would be included in the People aspect of the DiD theory.

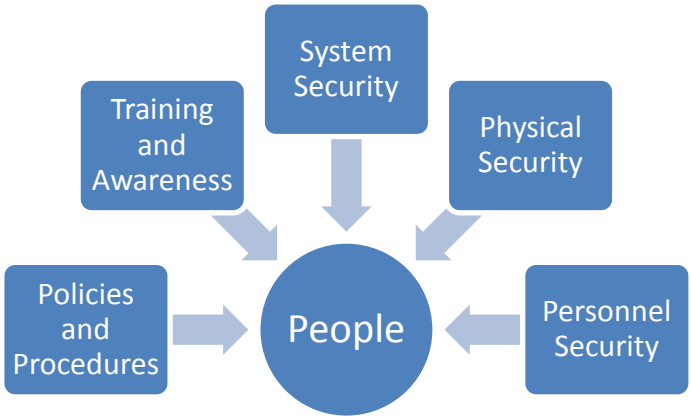

Figure 3: Defense-in-Depth (People)

In today's highly networked society, there is an abundance of technologies providing information assurance for detecting intrusions. Because there is a vast selection of potential products, it is important that the organization has the right methods for selecting and implementing these technologies. This can be done through policies and processes such as configuration (National Security Agency, n.d.). Figure 4 explains the Technology aspect of the DiD Theory.

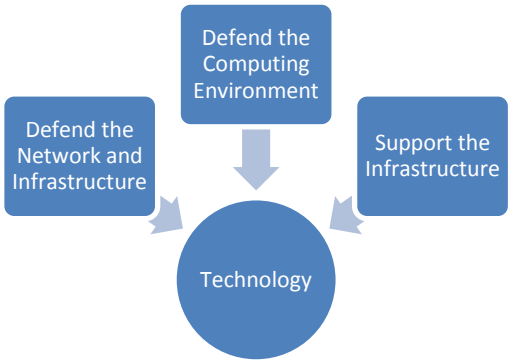

Figure 4: Defense-in-Depth (Technology)

Finally, the operations layer in the DiD model provides assurance on the organization's daily information security posture. This layer includes enforcement of the policies as well as ways of recovery from incidents as they happen. Emergency preparedness testing is one of the things an organization has to do to ensure readiness (National Security Agency, n.d.). Figure 5 outlines the Operations aspect of the DiD theory.

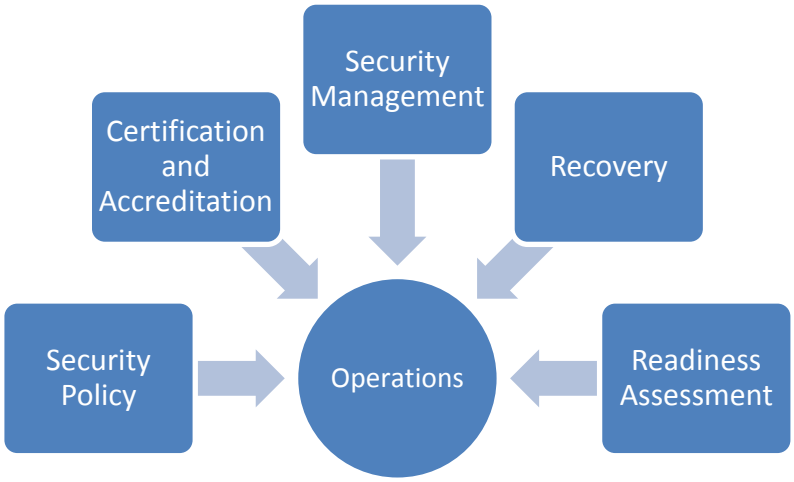

Figure 5: Defense-In-Depth (Operations)

Industry experts recognize DiD as one of the most acceptable and best frameworks to ensure Information Assurance. One expert is quoted as stating that

“enough emphasis cannot be applied to the importance of a defense-in-depth methodology to the overall security within an organization. This effort should be championed by the company’s CSO (or an equal role), and a series of steps should be defined to ensure that the methodology is carried out throughout all tiers within the organization” (National Security Agency, n.d.). Because of the acceptance of this framework in industry, the following audit models currently in place will be measured against this concept.

Current Frameworks

The financial sector has very specific regulatory guidelines for conducting an information technology audit (Beaumier, 2007). Several standards 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 ISO 27002, will help compliance with these regulations (Greene, 2006). Because guidance from regulators is scarce, audit frameworks can be utilized to conduct the IT audit. Some of the most accredited frameworks on the market are the COSO ERM framework, COBIT, and ISO 27002 Code of Practice. Although none of these frameworks is identical, some key areas that must be addressed, and are a part of all 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
- Customer complaint process
- Reporting and record keeping
- Board of directors and management reporting

ISO 27002, Code of Practice

The ISO 27002 is considered a widely recognized Information Security framework. It consists of eleven domain areas, 39 control objectives, and 133 controls. The ISO guidelines are considered to be an international standard for "best practices" for Information Security, and are the minimum baseline for controls that all information security programs should address in some way, depending on the size and complexity of the organization (Carlson, 2008).

It is important to note that the ISO 27002 is not a technical standard, nor is it product and technology driven. Finally, it is not considered an evaluation method for any equipment (Carlson, 2008). It has two stages of the audit process: Stage 1: Documentation Review; Stage 2: Implementation Audit.

ISO 27002 is based on the development of an Information Security Management System (ISMS)—on an organization's policies, procedures, plans, processes, practices, roles and responsibilities, resources, and, finally, structures used to protect and maintain confidentiality of information. An ISMS does further include all of the processes an organization uses to manage and control its information security risks, and is essentially a part of a larger management system (Praxiom, 2009).

The purpose of an ISO 27002 Audit is to check compliance as it relates to the following criteria:

- The organization's Security Policies and Procedures
- Customer and Contract Requirements
- Legal Requirements (regulatory requirements etc.)
- The documented Information Security Management System
- Organizational standards
- ISO 27002 Compliance (Zhu, 2007)

The SANS Institute has developed an IT Audit checklist for the ISO 27002 framework (SANS, 2006). This checklist can be used to perform a compliance audit for the ISO 27002 framework. In other words, an ISO 27002 audit is simply a compliance audit for documentation in place at the organization (SANS, 2006).

As it relates to SMEFIs, the ISO 27002 framework in general complies fully with the FFIEC documentation requirements. It is not risk-based, as it simply checks for policy controls, and does not rate the importance of each control. Furthermore, an ISO audit is simply done for certification purposes. As mentioned earlier, the ISO 27002 is not technology driven, and therefore leaves out a critical aspect of the Defense-In-Depth methodology.

COSO ERM Framework

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a nonprofit organization that in 1992 developed a definition for internal control. COSO created a framework that laid out methods for evaluating internal controls for organizations. After Congress passed the Sarbanes-Oxley Act (SOX) in 2002, requiring all public organizations to evaluate its internal controls, several organizations have adopted COSO to evaluate these internal controls.

Although SOX was intended for publicly traded companies, several privately owned organizations as well as nonprofit organizations have adopted the COSO framework. The way it is implemented in an organization depends on its size and complexity (Pullen, 2009).

According to COSO, there are three primary objectives of an internal control approach. The internal control system is to ensure: (1) efficient and effective operations, (2) accurate financial reporting, and (3) compliance with laws and regulations. The report also outlines five essential components of an effective internal control system:

- **Control Environment** contains the critical integrity and ethical values of the organization. The control environment includes the organization's code of ethics, as well as the Board of Directors' oversight and actions and how they affect the integrity and ethical values of the company, including its code of conduct, involvement of the Board of Directors and other actions that set the tone of the organization.
- **Risk Assessment**, the second component, is considered the process that management is utilizing to identify potential threats and how those risks are addressed by the organization. Not having a risk management process in place could potentially result in misstatements in the organization's financial statements.
- **Control Activities** are generally considered as internal controls, and include segregation of duties and information processing controls.
- **Information and Communication** is considered the internal and external reporting process, such as how information is presented to other vendors and

potential clients. This usually also includes an evaluation of the organization's technology environment, such as a vulnerability assessment and penetration test.

- Finally, **Monitoring** is essentially the auditing aspect of the COSO framework and includes a quality assessment of the organization's internal controls, as well as assurance that the organization continues to address new and upcoming risks associated to the organization. (Applegate & Willis, 1999)

These five components are usually utilized to integrate COSO into any auditing framework and by doing so, create a structure to the audit process. Dennis Applegate and Ted Wills (1999) state in an article published by the Institute of Internal Auditors that the idea of COSO auditing is to focus on one of the three COSO objectives at the time. By focusing on only compliance will allow the auditor to better determine the audit focus and ensure effectiveness of the implemented controls (Applegate & Willis, 1999).

Prior to the COSO framework, more traditional theories focused on financial controls. The COSO framework covers the financial aspect as well, but broadens this to include a more enterprise-wide view. COSO considers the evaluation of segregation of duties (hard controls) as well as soft controls, such as employee competence and professionalism (Simmons, 1997).

Implementing COSO in an organization is not a simple task. Utilizing the 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. 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 T. , 2008). Furthermore, there is no defined approach to auditing "soft" controls such as integrity and ethical values of employees and the approach management makes as it relates to the operation of the organization. In fact, experts have said that implementing COSO and customizing it to fit the organization have taken up to four years of hard work and research until a formal methodology was reached (Simmons, 1997).

Implementing the COSO framework can also have benefits to the organization, specifically in these five areas:

Effectiveness: Auditing all five components of COSO will ensure a baseline as it relates to the degree of assurance of the implemented controls.

Efficiency: Focusing on only one of the three COSO objectives at a time can ensure that the audit is not affected by the costly "scope creep".

Comparability: Because COSO is intended for large and complex organizations, and by utilizing its framework throughout the organization, it enables the organization to compare controls in different business segments.

Communication: By explaining and using the COSO during discussions with organizations, it increases the client's understanding and knowledge of the control objectives.

Audit Committee: Reports based on the COSO framework help the auditor to portray strengths and weaknesses in the internal control system to the organization. (Applegate & Willis, 1999)

COBIT

Control Objective for Information and Related Technology (COBIT) is a framework consisting of controls and standards published by the Information Systems Audit and Control Association (ISACA). The COBIT framework contains 34 processes as well as 220 low-level control objectives. It is intended as an IT Governance framework that establishes what an organization should do as it relates to IT governance (Meycor COBIT, n.d). Experts claim that one of the main reasons COBIT has been adopted by so many organizations internationally is that it deals with every aspect of IT (Financial Services 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). COBIT contains the following four core areas:

- Control Objectives: There very high-level generic statements of minimum good controls in an organization. A total of 220 of these control objectives split between 34 processes.
- Control Practices: This area contains explanations of why a certain control objective should be in place. Control practices also outline how the control objectives can be implemented.
- Audit Guidelines: They give guidance for each of the 34 processes on how the auditor can gain an understanding of the controls. The Audit guidelines also outline how the auditor can evaluate each control, as well as measure compliance and develop the residual risk if controls are not adequately implemented.

- Management Guidelines: These provide guidance on how to assess and improve IT process performance, using maturity models, metrics, and critical success factors. (Kowal, n.d)

The COBIT Framework is outlined in Figure **6**.

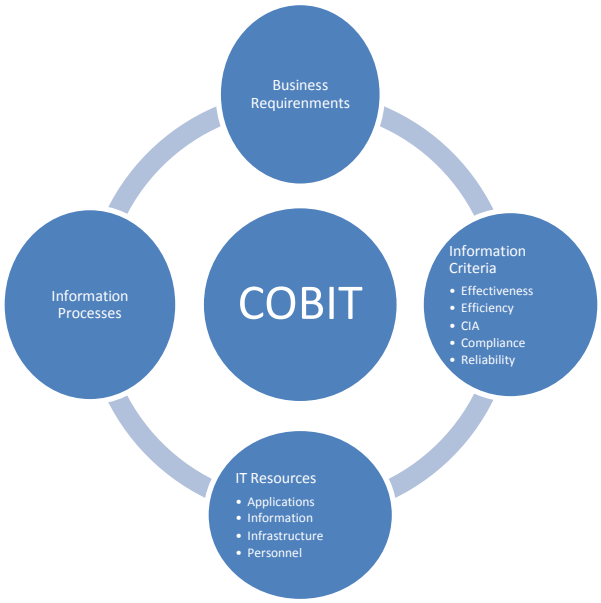

Figure 6: COBIT

Within COBIT, ISACA has published some general audit guidelines that generate a simple high-level structure, allowing for the review of the organization's processes and measuring them against COBIT. There are four goals of the COBIT Audit process:

- The auditor must gain an understanding of the organization's business requirements and associated risks and understand relevant controls.
- The second process contains the evaluation of the appropriate controls as well as the documented controls.

- The auditor must also assess the compliance of all controls to ensure that established controls are working as indicated.
- The final goal of the COBIT audit process is to compute the inherent and future risk if certain controls are not met, or if certain controls should be recommended to reduce the future risk score. (Turcato, 2006).

COBIT is in essence the closest to an IT Audit framework on the market today, and it has developed certain recommended steps of what an audit should include. COBIT suggests that any internal or external auditor or anyone with information security responsibilities should do the following to comply with the COBIT framework:

- Penetration Testing
- Vulnerability Assessment
- Physical Access Controls
    - Social Engineering
- Reporting (Turcato, 2006).

Included are specific guidelines on how to conduct each of these services.

The literature review has identified prominent models and investigated them to identify their shortcomings as they relate to the requirements for a holistic information technology audit framework. Based on these shortcomings and regulations, the holistic IT audit framework can be developed. Chapter 3 will discuss the design science research methodology utilized for this research.

CHAPTER 3

Research Methodology

This research is based on Design Science research. The importance of design science for the information systems design has been well documented in literature (Hevner, March, Park, & Ram, 2004). Hevner argues that the relevance of information systems directly relates to the applicability and design. Design science research and artifacts can be quite complex and need to contribute creative advances to current theories. As Design Science is increasingly applied to new areas, technical knowledge within design science is needed, as IT is increasingly applied to new areas. Usually, the result of the IT artifact relates closely to problem solving and the limitations of people. Ultimately, theories of the application of the IT artifact will follow the development and the use of Design Science research in the IT area. They must address the relationship among business strategy, IT strategy, organizational infrastructure, and IS infrastructure. This relationship is becoming more crucial as information technologies are seen as enablers of business strategy and organizational infrastructure (Hevner, March, Park, & Ram, 2004).

Design science is considered a problem solving process. Hevner et al. (2004) have developed seven guidelines based on the fact that the researcher must have knowledge and understanding of the design problem as well as its solution, required to build and develop an artifact. This research will follow these guidelines as outlined in Table 2.

Table 2: Research Methodology

Guidelines	Research Description	Dissertation Requirements
Guideline 1: Design as an Artifact	Design-science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation.	• Design a Holistic Information Technology Audit Framework for Small- and Medium-Sized Financial Institutions. • The framework will be based on the Defense-in-Depth theory.

Guideline 2: Problem Relevance	The objective of design-science research is to develop technology-based solutions to important and relevant business problems.	• Regulators require banks and financial institutions to conduct annual IT Audits to ensure safety of customer information
		• Frameworks today are:
		  o Not based on Defense-in-Depth
		  o Large and complex
		  o Resource intensive
		  o Not based on regulatory requirements
		• Scarce information from regulators:
		  o FFIEC IT Handbook
		  o Regulatory Requirements

Guideline 3: Design Evaluation	The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods.	• Artifact Design:
		  o See the Artifact Design section.
		• Artifact Evaluation:
		  o See the Artifact Evaluation section.

Guideline 4: Research Contributions	Effective design-science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies.	• Propose a new IT Audit Framework based on:
		  o Defense-in-Depth Theory
		  o Current Frameworks
		  o Current Regulatory Requirements

Guideline 5: Research Rigor	Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact.	• Based on the Defense-in-Depth Theory • Results from the evaluation before and after implementation in two financial institutions using multiple case study • Analysis using Cross-Case Synthesis

Guideline 6: Design as a Search Process	The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment.	• Generalizability may not be feasible as the framework is designed for small- and medium-sized financial institutions.
		• Developed the framework over time
		• Feedback from:
		  o Business implementation
		  o Research

Guideline 7: Communication of Research	Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences.	• Information for both IT practitioners and managers will be provided through:
		  o Publications in management journals/conferences
		  o Publications in technical journals/conferences

Design Validation

Hevner et al. provide five guidelines for design evaluation. The evaluation process is critical to design science research as it is regarded as an essential component of the validation of the research. The evaluation of the model is achieved through rigorous Artifact Design and Artifact Evaluation.

Artifact Design

There are several IT Audit frameworks organizations can use in today's information society. However, none of these frameworks is built on what is regarded as the basis for Information Assurance and Information Security, the Defense-in-Depth theory. This theory includes three simple, yet critical steps—people, operations, and technology. The frameworks in this research have proven to fall short of one or more of the DiD steps, designed to ensure a layered defense architecture. In fact, all of these frameworks fall short in the people aspect of the DiD theory. People are often considered the most critical asset and method of protection to any organization, and therefore play a crucial role in the DiD framework. Most security professionals regard people as the "first line of defense" in an organization. Furthermore, as discussed in the literature review section, there is a substantial mismatch in regulatory requirements and the IT audits that are done with current frameworks. Most of these frameworks are too large for small- and medium-sized financial institutions that are left to analyze and determine what exactly pertains to them. Not only are these frameworks large in size, but they also require special certified consultants at a relatively high cost, therefore difficult for smaller organizations to justify.

This research and its IT artifact, a "Holistic Information Technology Audit Framework," is based on the Defense-in-Depth theory, as it is regarded the "best practice" for Information Security. Furthermore, existing frameworks will be used to develop the details of the new holistic approach. The process of this research is explained and outlined in Figure 7.

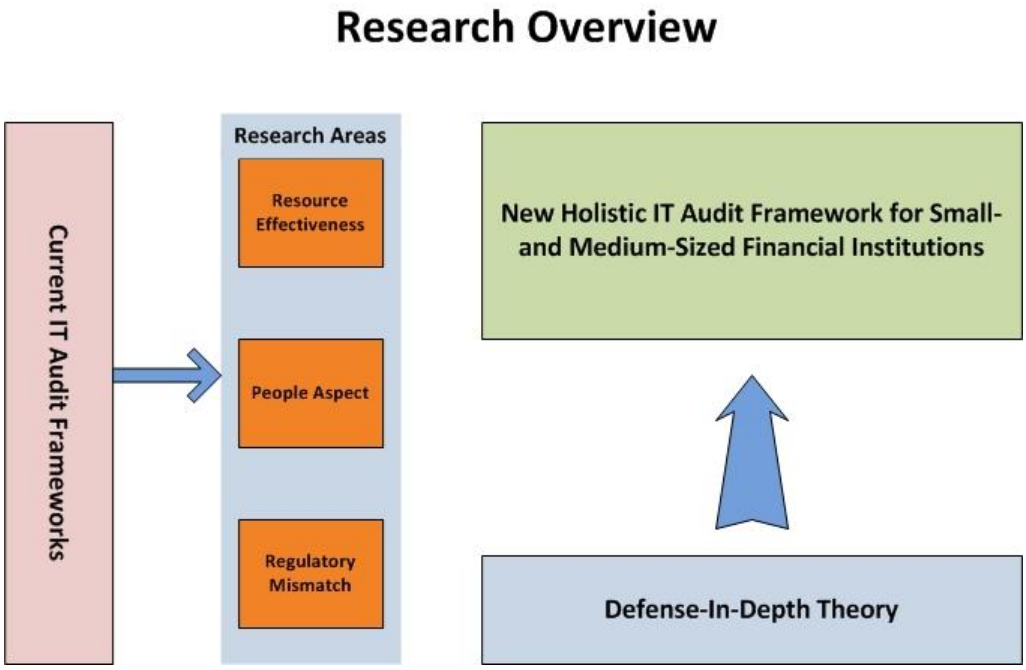

Figure 7: Research Overview

Artifact Evaluation

To validate the field study and answer the three areas outlined above, this research will be validated through two implementations of the artifact (model) in financial institutions. Furthermore, evaluation will be conducted through a set of measurable questions before and after implementation of the model. Four simple questions will be asked prior to implementation:

1. What IT audit framework did you previously use to complete your IT audit requirements?

2. What were some of the concerns you had with this framework?
3. Did regulators make any comments about adequacy of this framework?
4. Did regulators indicate that they would like more auditing for:
    a. People (social engineering)
    b. Process (compliance with regulatory requirements/current framework)
    c. Technology (Vulnerability Assessment, Penetration Testing).

Two question sets will be asked after artifact implementation. The first set corresponds to the pre-implementation questions, comparing these results.

1. How did this framework compare to your previous IT audit?
2. If you had any concerns prior to this audit, did this process take care of these issues?
3. Did you feel that this IT audit covered all of the following areas:
    a. People
    b. Operations
    c. Technology?
4. Since this IT audit, have you had a regulatory exam?
    a. If so, what were the examiner's comments?

The second question set asked will answer the three research goals, outlined above:

1. Does this new Holistic IT Audit Framework (artifact) cover and solve issues in the following areas:
    a. Regulatory Mismatch
    b. People aspect of auditing
    c. More resource effectiveness?

Validation of this post-assessment will be completed according to the metrics in Table 3.

Table 3: Evaluation Metrics

Resource Effectiveness	**Cost**	**Manpower**	**Time**
	Interview	Interview	Interview
Value of Social Engineering (People Aspect)	**Measure Training level**	**Identify Areas of Risk**	**Training Suggestions**
	Test Results	Test Results	Test Results
Regulatory Mismatch	**Framework too large for organization size**	**Organization Awareness Lacking**	**Not part of scoping**
	Interview/Regulatory Reports	Interview/Regulatory Reports	Interview

From the Evaluation Metrics this research intends to collect data from three separate sources to ensure validity. Interviews will be done with a pre- and post-assessment questionnaire. The question set is outlined in the Artifact Evaluation section to evaluate the resource effectiveness of the Holistic IT Audit Framework and potential regulatory mismatches.

The Value of the Social Engineering Assessment will be evaluated through the actual IT Audit results. Based on this assessment, the researcher intends to measure the training level of the institution, such as awareness of internal controls and procedures, as it relates to Social Engineering. This assessment will also identify any risks the institution has. For example, awareness is lacking, appropriate recommendations are made in the IT Audit report.

Finally, regulatory mismatches will be measured through feedback and from the pre- and post-assessment questionnaire.

This entire process will be done through the utilization of a multiple-case study. The results will be analyzed using Yin's recommendations for smaller multiple-case

studies, Cross-Case Analysis (Yin, 2003). Refer to the Case Study Section for further details.

Limitations

1. This research is based on a multiple-case study and has a relatively small sample. The conclusion of this research will therefore have an inherent limitation of generalizeability that stems from using a case study approach.
2. The IT Audit Framework is being developed and tested for small- and medium-sized financial institutions, but may also be applicable to other industries. Future research may include possibilities for this framework to be more general and adaptable to other areas.

This chapter outlined the seven guidelines to design science research and how this research intends to follow these guidelines. In addition, a multiple-case study was utilized for validation purposes. Chapter 4 will discuss the development and requirements of the holistic IT audit model, how it was implemented in the multiple-case study, and the qualitative analysis on the data to develop conclusions to this research.

CHAPTER 4

Artifact Design

Existing Models

The literature review section of this research has discussed ISO 27002, COBIT, and finally, COSO. These three models are generally considered the IT audit models to follow. When comparing these frameworks with the Defense-in-Depth theory, there are significant shortcomings, in relationship to the theory itself and to regulatory requirements set forth by banking regulators. This section will examine these shortcomings and suggest a new innovative holistic framework to close the gap.

Experts claim that no single enterprise risk management (ERM) framework is comprehensive enough to cover the entire organization, and that some reinforcements are needed. In today's world, organizations are faced with compliance, governance, and risk management (Briggs, 2007). Combining some of these frameworks may be the best solution. Briggs (2007) suggests that COBIT plays well with both, COSO and ISO 27002.

One of the biggest advantages of COBIT is that the framework has become so popular within the industry. Therefore, the COBIT community has developed official maps to complement other frameworks, such as COSO and ISO 27002. The essential downfall of COBIT is that it is not an Information Security standard. As described in the literature review, COBIT has 34 processes, and only one of them relates to information security. Therefore, it may be a good idea to team COBIT with an Information Security standard, such as ISO 27002 (Briggs, 2007). Perhaps the biggest strength of the 27002

standard is that the COBIT framework has been mapped to it, which can help make external audits more efficient.

If you combine COBIT and ISO 27002, though they complement each other to create a very complete framework, COBIT by itself with its 34 processes is too complex for SMEFIs (Small- and Medium- Sized Financial Institutions) (Albayrak, Gadatsch, & Olufs, 2009), and adding thirteen domains of ISO 27002 will just make the framework larger. Combining COBIT with COSO will also create a strong framework, with COSO focusing on the business side, and COBIT focusing on the IT side. However, again, the framework simply gets too large and complex for a SMEFI to implement.

COSO has also been regarded as one method of implementing internal controls and complying with SOX section 404. One of the problems with the COSO framework is that it provides little or no guidance on how to implement the controls. In fact, a study suggests that only a few percent of the respondents felt that COSO was of value to the organization (Gupta & Thomson, 2007).

Implementation of these frameworks also brings up another issue—cost. COBIT and COSO both can be extremely expensive for SMEFIs to implement, and will usually involve hiring expensive consultants to map the processes to the frameworks.

When examining these frameworks, one can see some definite faults just as standalone models. When you add requirements, such as the DiD theory, the flaws become even more significant. ISO strictly covers information security from a management prospective, meaning policies and procedures. ISO 27002 reflects a more holistic and managerial approach to IT. By itself, ISO 27002 covers the process section of the DiD theory. ISO also briefly discusses people, again as it relates to polices, but

talks little about how to conduct an audit if management conveys these important policies and procedures to employees of the organization.

Finally, since ISO is not a technical standard, it does not explain or guide organizations through the implementation process.

COBIT, on the other hand, discusses the process and technology aspect of the DiD theory. COBIT is strictly technology driven, and provides guidance on how to implement its controls. Finally, when looking at the people aspect of the DiD theory, as discussed in the literature review, the audit section does discuss social engineering as a type of audit.

COSO, on the other hand, covers only one of the three core areas of DiD—operations. As mentioned, COSO is involving strictly internal controls and affects on the organization. It is an organizational framework, and provides no specific guidance for information security or information technology.

None of these frameworks is inherently considered risk-based. Risk-Based Auditing is simply a method of auditing, and essentially means that the focus of the audit resources is on critical assets and areas of the organization. This does not mean that you completely ignore the less important assets, but you focus less on them, or an auditor would audit fewer controls for these assets. The foundation of any risk-based IT audit is a solid risk management process. This process will help ensure that a rating is given to each asset. COBIT, ISO 27002, and COSO all deal with the importance of a risk management process, but their audits do not build on this process.

Finally, regulatory requirements are another important factor for SMEFI. Complying with all laws and regulations that regulators set forth is critical to a successful

IT regulator examination. For decades, SMEFIs have been able to respond to regulations pertaining only to their state and market. SOX, GLBA, and data and privacy protection laws have changed that. Today, SMEFIs and most other organizations find themselves having to answer to regulators, stockholders, and Board of Directors regarding the status of these requirements pertaining to their industry.

These new regulatory requirements impose new hurdles for organizations as they relate to compliance. The regulations focus mainly on confidentiality, integrity, and availability of electronically-held information. Many of these new laws appear to overlap one another in one way or another. On top of that, very little guidance exists regarding compliance with these regulations. In fact, in most cases the regulations are technology-neutral and simply describe what needs to get done, but leave out how. Organizations are therefore left to establish how to meet these requirements (Calder, 2006).

Another issue with these new regulations is that there are no significant case laws and proven compliance methodologies that the organization can turn to for guidance. No single technology product can ensure compliance with any of the data security regulations. Instead, it is composed of technology, procedure, and human behavior, or DiD (Calder, 2006).

ISO 27002 will, by itself, generally cover most of these regulatory requirements, and can therefore help organizations with compliance. However, since ISO is geared towards information security only, it should be combined with another model, such as COBIT and COSO.

Based on this research, a conclusion can be drawn from the frameworks currently on the market. A summary of the findings, based on this literature review and the

requirements of this research can be found in Table **4**. If an item is marked with a "C", it indicates that the model includes that aspect of the research requirements. If an item is marked"P", it indicates partial fulfillment of the requirement, and finally, if no marks are outlined, it indicates that there is no fulfillment of the requirements based on the research questions and requirements.

Table 4: Current Frameworks and Shortcomings

Requirements	**ISO 27002**	**COBIT**	**COSO ERM**	
Defense-in-Depth				
People	P	P	P	
Operations	C	C	C	
Technology	C	C		**Legends:**
Risk-Based Auditing		P	C	C = Compliant
Information Security	C	P		
Designed for Small- and Medium-Sized Financial Institutions				P = Partially Compliant

Holistic IT Audit Framework for Small- and Medium-Sized Financial Institutions

Based on earlier discussions in this research, it can be determined that current IT audit frameworks have significant shortcomings in relationship to SMEFIs. First of all, when comparing each model to the DiD theory, the research showed that all of them have a lot to be desired when it comes to the people aspect of this theory. The frameworks does have some discussions about people—ISO 27002 has a personnel security section of its framework—but the IT Audit section does not discuss the importance of conducting annual assessments that test the effectiveness of controls. COSO strictly focuses on the internal processes of an organization and will therefore inherently focus on people in the organization. However, COSO is not IT or Information Security based, and therefore leaves out assessments relating to that.

Furthermore, none of these frameworks is particularly designed for SMEFIs, though, as discussed, they do comply with regulatory requirements. Additionally, these frameworks can be very costly to implement, as they will require specialized consultants. Since these frameworks are comprehensive in their own way, ISO for Information Security, COBIT for IT governance, and COSO for its internal controls, ultimately, they are simply too large for most SMIFEs.

Finally, none of these current frameworks is considered risk-based. The FFIEC requires all financial institutions to conduct a risk-based IT audits on an annual basis. These frameworks can all be made risk-based, but the process will be lengthy.

Based on this research, the researcher is suggesting the following framework as outlined in Figure 8.

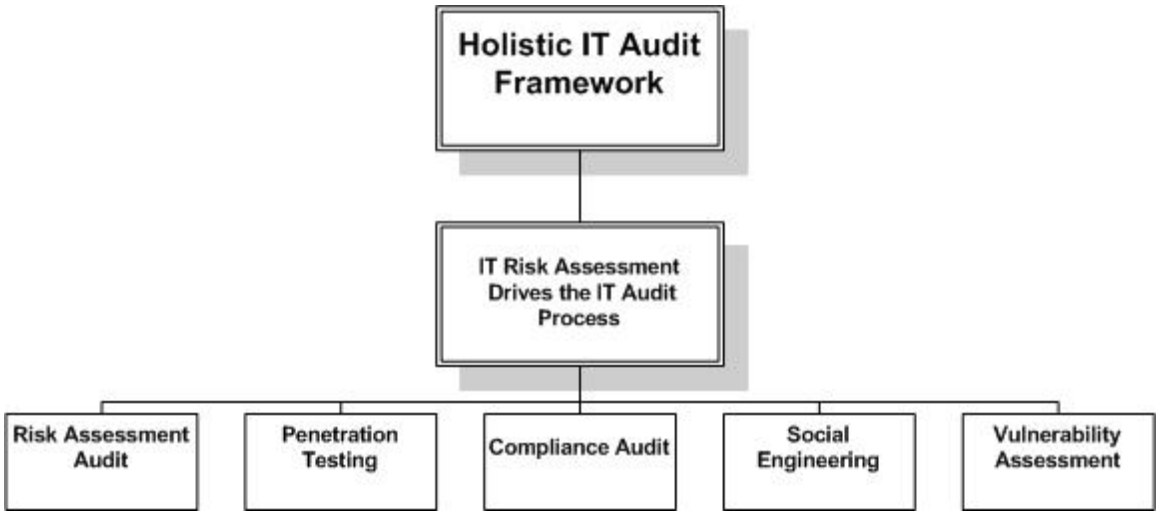

Figure 8: Holistic IT Audit Framework for SMEFIs

IT Risk Assessment

A thorough IT risk assessment is the initial step to a sound Information Security Program, and a risk-based IT audit program (Accounting Web, 2008). The risk assessment is an ongoing process of evaluating threats and vulnerabilities and applying

mitigation strategies to each asset (FDIC, 1999). There are several ways of conducting a risk assessment, and several methodologies have been developed. Among them are OCTAVE, CORAS, ISO, NIST, and COBIT, and the institution may implement any of these methodologies. It is up to the auditor to determine whether the risk assessment process is adequate. This step of the risk-based audit will ensure that focus is given to critical assets rather than simply focusing on every single control for each asset. Are your printers equally critical to a core banking system? Obviously, the answer is "no." Ensuring a sound risk assessment will ensure that assets are rated appropriately, and that focus during the IT audit process is given to critical assets.

Regulatory Compliance

The main focus of regulatory compliance in this context is a verification of what the organization has in place, and how well it is in place. The auditor can use ISO 27002, combined with COBIT, to get a general understanding of the organization's information technology and security controls. Usually, a questionnaire can be utilized to gain the basic understanding of this. As an auditor is generally not too familiar with all regulatory requirements, it may be useful to utilize ISO and COBIT, as they will cover all of the regulatory requirements.

Social Engineering

Security is a difficult culture, and is mainly based on trust in protection and authenticity. As discussed earlier, people are generally considered the weakest link in any security chain. The willingness of humans to accept someone's word leaves so many organizations open to attacks from potential social engineers. It really does not matter how many articles are published about network vulnerabilities, patches, and firewalls—

the threat can only be partially reduced. Then it is up to the employees of the organization to keep the corporate network secure (Granger, 2001). Exploiting this weak link to acquire unauthorized information is referred to as Social Engineering. It is the art of deceiving people into acting in a manner that may result in unauthorized disclosure of information or unauthorized access to systems. Social Engineering preys on qualities of human nature, such as the desire to be helpful, the tendency to trust people, and the fear of getting into trouble. The purpose of the Social Engineering Assessment is to protect the institution's information by identifying weaknesses through the testing of employees and business processes against common social engineering attacks.

COBIT suggests that Social Engineering Assessments should be a part of the IT Audit process. This process will test the controls, such as policies and procedures, as well as training to ensure that employees are aware of and able to identify attempts of social engineering. COBIT suggests the following assessments:

- Telephone Access: The more the intruder knows about the organization, the easier it will be to get access to critical information.
- Dumpster Diving: Going through the dumpster verifies that confidential data is shredded appropriately.
- Desktop Review: This ensures that computers are locked and screen savers are turned on, and that no critical information is on the desk (COBIT, 2004).

Other critical tests may include:

- Physical Impersonation: Impersonating one of the organization's service providers to attempt to gain access to critical areas of the bank.

- Phishing Scam: Deploying an email phishing scam to ensure that employees are not providing sensitive information.
- Physical Security Assessment: checking the institution's physical areas, such as cameras, monitor viewing angles, and general physical security issues.

From my experience with social engineering assessments, institutions have a hard time passing these tests, although with training, awareness, and with management support in the enforcement of policies, it becomes increasingly difficult to get critical information. However, this shows the importance of conducting annual Social Engineering assessments.

Vulnerability Assessment and Penetration Testing

The FDIC suggests that a Vulnerability Assessment (VA) and a Penetration Test (PT) can be an integral part of an institution's Information Security Program (ISP). All financial institutions are required to implement an ISP. This program is designed to make the Board of Directors as well as senior management aware of information security issues in the development of this critical ISP. This program should outline a proactive and ongoing concept that incorporates the following three components:

- Prevention includes security policies, well-designed system architecture, properly configured firewalls, and strong authentication programs.
- Detection is the method of reviewing and analyzing information that helps determine if data has been compromised, misused, or accessed by unauthorized individuals. An Intrusion Detection System (IDSs) device can help an institution monitor exactly that. It acts as a burglar alarm, alerting the institution to potential external break-ins or internal misuse of systems being monitored. A VA and PT

are, according to the FDIC, excellent detection methods that an institution should utilize.

- Response is another key area of the ISP. It involves the preparation of a response program that assists the institution with handling intrusion incidents once they are detected. All financial institutions should have a comprehensive Emergency Preparedness Plan in place. Such a plan should include Business Continuity, Disaster Recovery, and an Incident Response Plan. These plans should document and discuss responses to incidents as well as establish reporting requirements. (FDIC, 1999)

Vulnerability Assessment

A Vulnerability Assessment tool, also called security scanning tool, is used for an assessment of a particular network or a host system. It scans everything on a network, such as servers, firewalls, routers, and applications for vulnerabilities, and detects known flaws and bugs in software and hardware. A database within the tool maintains a list of these known issues. On a regular basis, these are updated to add new vulnerabilities. VA scans can also determine if settings on the network, such as passwords, are set according to security policies the bank has documented.

When utilizing any of these VA tools, it is critical to consider how often they are updated to include new vulnerabilities. A VA is not generally done on a real-time basis, but rather conducted periodically, and SMEFIs are generally expected to conduct an assessment at least annually or when the network changes significantly.

No matter the tool or provider that the organization selects, VA tools can generate both, technical and management reports, including text, charts, and graphs. The report

will lay out the vulnerabilities and weaknesses that exist on the network and explain how to fix these issues (FDIC, 1999).

Penetration Testing

Penetration Testing (PT) is another important aspect of a comprehensive IT Audit. It is an analysis of a bank's external network connections (Internet, FedLine, Internet Banking, etc.), usually conducted by experts and designed to measure if connections and ports are vulnerable to a series of attacks. Similar to the VA, it is designed to identify the weaknesses and propose corrective actions.

A PT is critical to an organization, but, as mentioned earlier, becomes even more critical if the institution has any external access points. According to the FDIC, the PT should be done by an independent, usually external, organization. For SMEFIs in particular, this should be conducted on an annual basis, or when significant network changes occurs.

After the initial risk assessment is completed, management may determine if a penetration analysis (test) should be conducted. For the purpose of this paper, "penetration analysis" is broadly defined. Bank management should determine the scope and objectives of the analysis. The scope can range from a specific test of a particular information system's security or a review of multiple information security processes in an institution.

Though a PT is extremely critical, it does not provide a guarantee that the systems being tested are secure, because they are snapshots of the institution's security measures

at a certain point in time. That is why conducting a PT on a regular basis is important as new vulnerabilities become known.

The PT itself can sometimes impose new risks to an institution. Therefore it is important to consider some of the following items before conducting a test:

- The reputation of the external entity hired to conduct the evaluation should be checked. The same type of precautions for hiring a new employee should be considered (background checks, etc.). This is important, because the consultant or organization will have access to confidential data when conducting these tests. This is critical, because the entity may exploit the vulnerabilities.
- Some managers want to keep a PT secret to the Information Security Officer (ISO) and other IT personnel. This is not always a good thing, and it is important to keep in mind the consequences of this, such as unwanted results, including law enforcement notifications. To prevent this, it may be good practice to at least inform certain people, such as the ISO, of a PT being conducted to ensure appropriate responses.
- The final aspect to be considered is the importance of the systems being tested. The bank may have determined from its Risk Management results that certain systems are simply too critical to be exposed to some of the methods utilized by a PT (FDIC, 1999).

COBIT also notes the importance of integrating PT and VA into the IT Audit (COBIT, 2004).

Research Findings

Figure 9 outlines and compares the Holistic IT Audit Framework to the DiD theory, and maps each area of the framework with the theory.

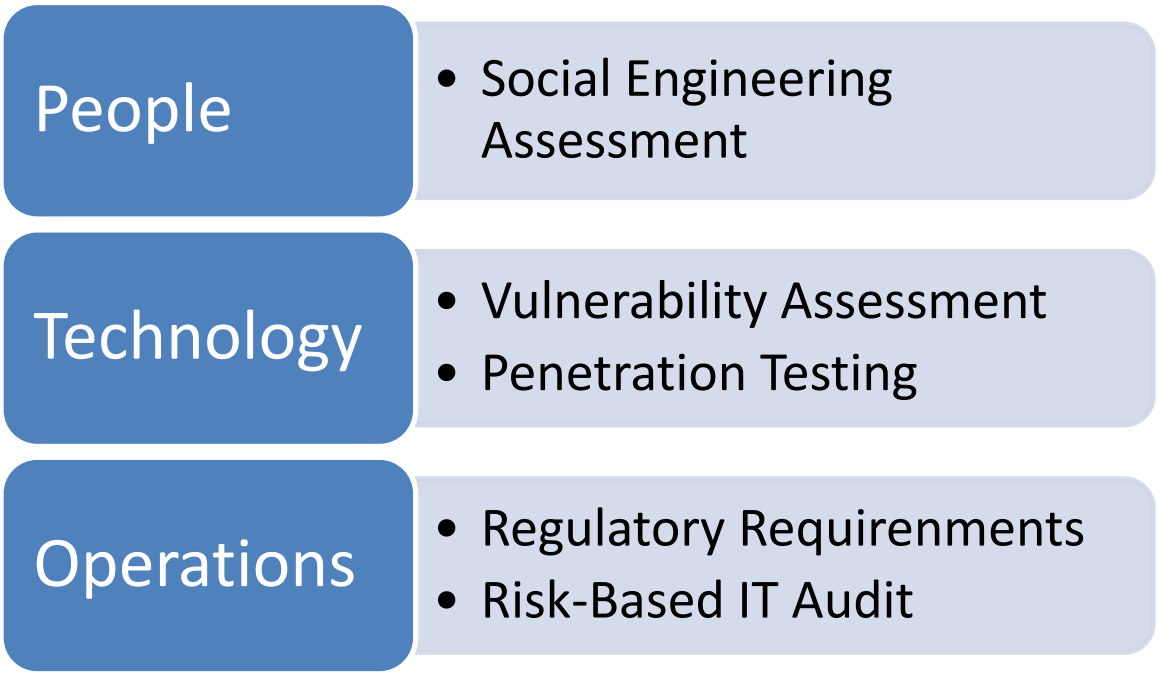

Figure 9: Framework vs. Theory

According to the DiD theory, People include policies and procedures, physical security, training and awareness, and personnel security. Conducting a Social Engineering Assessment will ensure that policies and procedures are communicated to the organization's employees. Furthermore, based on the assessment results, the auditor is able to recommend training improvements after reviewing the institution's current program. Conducting a Physical Security Assessment will ensure that the organization has taken appropriate measures to protect sensitive information. Items to look for in a physical security assessment are alarms, fire extinguishers, privacy screens for monitors, and locked doors.

The technology aspect of the DiD theory is covered mainly by conducting a VA and a PT. However, ensuring that appropriate controls are in place, based on the institution's size and complexity, is also measured through the IT risk assessment.

Since ISO 27002 and COBIT include many of the processes that are critical to IT and Information Security, utilizing these frameworks is critical in the audit process and ensures regulatory compliance. Both frameworks are updated regularly to include new requirements.

Finally, the cost of implementing this holistic IT Audit Framework is considerably less. With this framework, the organization is able to determine what should be included in an annual IT Audit to meet regulatory requirements. The model is comprehensive, thus covers a variety of areas, and will ultimately provide the institution with assurance that the framework is successful. Implementing this framework will also ensure that the institution stays ahead of regulatory requirements because of the industry standard that both COBIT and ISO provide.

Case Study

Feagin et. al. (1991) have stated a case study methodology can be ideal when the researcher is investigating a holistic artifact. Case studies in the past have been widely used in sociological studies and increasingly in instruction (Feagin, Orum, & Sjoberg, 1991). Yin (2003) as well as others have developed sound procedures on how to conduct case studies. When following these procedures, the researcher is able to utilize well tested and documented procedures. Case study analysis and data collection are designed to investigate the viewpoint of the actual participants by utilizing multiple sources of data (Yin, 2003).

Yin (2003) outlines five components for case study research:

1. Outlining the study's questions, forming the question in terms of "what", "who", "where", "how", and finally "why". Yin suggests that "how" and "why" questions will lean towards a case study. This research is intended to answer the following questions:
    a. How does the Holistic IT Audit Framework impact the overall quality of an IT audit for small- and medium- sized financial institutions?
    b. How does the People aspect impact the comprehensiveness of the IT audit process?
    c. How does implementing the Holistic IT Audit framework impact resources needed to complete the audit compared to other frameworks?

    These questions were developed to further validate the IT Audit model in addition to the design science methodology. Beyond the literature review and the development of the artifact, these case study questions will be used to determine the success of this case study. When investigating the literature review, it becomes evident that a clear validation is not present, which is why a case study is essential (Yin, 2003).
2. Studying Propositions. This research does not have any specific propositions because it is based on a survey of two institutions. However, there is still a significant purpose to the study. It is based on the three research questions identified and is meant to measure:

a. If the successful implementation of the Holistic IT Audit Framework increases the quality of the IT audit, not only as it relates to current models, but in general to what the institution is currently doing.
b. Secondly, this case study and its questions are designed to determine if the people aspect of IT auditing has any impact of the comprehensiveness of the IT audit.
c. Finally, this case study intends to determine if implementing the holistic IT audit framework will decrease resources needed from the financial institution, both in terms of cost, as well as the institution's own resources.

The collection of the data used for this analysis will be done through the following methods:

- Interviews, a pre- and post-assessment will be conducted with the Information Security Officer (ISO). The Methodology section lists the questions asked prior to any IT audit work, as well as upon completion of the IT audit.
- IT audit reports, evidence, and recommendations will be collected through work papers during the IT audit, the actual audit reports, and notes.
- Finally, any regulatory reports will be utilized. The researcher has access to these reports onsite. However, no examiner reports were taken off site and kept as part of this research. Furthermore, any specific comments and behavior of the examiners were reported to the researcher by the ISO.

3. The Unit of analysis for this case study is based on the two financial institutions where the Holistic IT Audit Framework was implemented. Specifically, the

"cases" for the study or the subject will be the Information Security Officers at the institutions. Furthermore, results from regulatory exams will be utilized to further validate the results. It is critical to note that this framework will only be tested and implemented for financial institutions.

4. The logical proposition of this research is the investigation of the research questions outlined in step 1 through implementation in two cases. The linking of propositions or the coding and analysis of the data will be collected from pre- and post-assessment interviews with the ISO, IT audit reports, and, finally, regulatory exams and comments.
5. The criteria for interpreting the findings. After collecting all the data, qualitative analysis will be performed. The analysis of the data collected will be coded based on nine separate areas, outlined in the methodology section above. The coding and category system involves stringent review of the data collected, line by line. The researcher will analyze the data and extract information from the sources outlined and put them into their respective category to further examine the results. Since this is a multiple-case study, further validation will be performed using Cross-Case Synthesis analysis, a comparison of the results in both institutions. Based on this, results can be extracted and conclusions to the research questions developed. Because only two case studies were conducted, no statistical calculations are possible, but Yin (2003) states that as long as two rival propositions are studied, and conclusions can be drawn, it satisfies this criteria.

Yin (2003) further outlines that validity plays an important role in any case study research. Four tests have been commonly used to establish quality in empirical social

research. Yin suggests that these four tests are also relevant to case studies. The four validity tests are: construct validity, internal validity, external validity, and reliability. This research will comply with these guidelines as described in Table 5.

Table 5: Case Study Validity Tests

Tests	Case Study Tactic	Compliance	Phase of Research
Construct Validity	1. Use multiple sources of evidence 2. Establish Chain of Evidence 3. Informants review	1. DiD Theory, regulatory requirements, ISO assessments 2. Evidence of the case study will be collected in form of interviews, examiners reports. 3. Informants will review their responses.	1. Data collection 2. Data collection 3. Composition
Internal Validity	1. Address rival explanations	1. Thorough literature review that will investigate current models 2. Based on current models and examining the cases and effects of these models	Data collection
External Validity	1. Replication Logic	1. The model will be tested in two institutions to determine if the results are the same	Research design
Reliability	1. Use case study protocol	1. Ensuring a repeatable process through documentation of research	Data collection

A SMEFI is considered small to medium when its assets are below 500 million dollars. Through this study, the researcher has designed and implemented the Holistic IT Audit Framework in two financial institutions. One has assets of 250 million dollars with six locations throughout Nebraska and Kansas, the second institution with two branches in South Dakota is a 50-million-dollar bank.

The process that was followed consisted of the following:

1. Pre-Assessment Questionnaire (Refer to the Methodology section.)
2. Audit Model Implementation (conducting the VA, PT, Social Engineering, Risk Assessment, and Compliance)
3. Deliver Reports

4. Post-Assessment Questionnaire (Refer to the Methodology section.)
5. Examination Results
6. Regulatory Feedback (if any)

The initial step in both institutions was to develop an adequate risk assessment methodology. For the purpose of this research, Figure 10 outlines the method utilized.

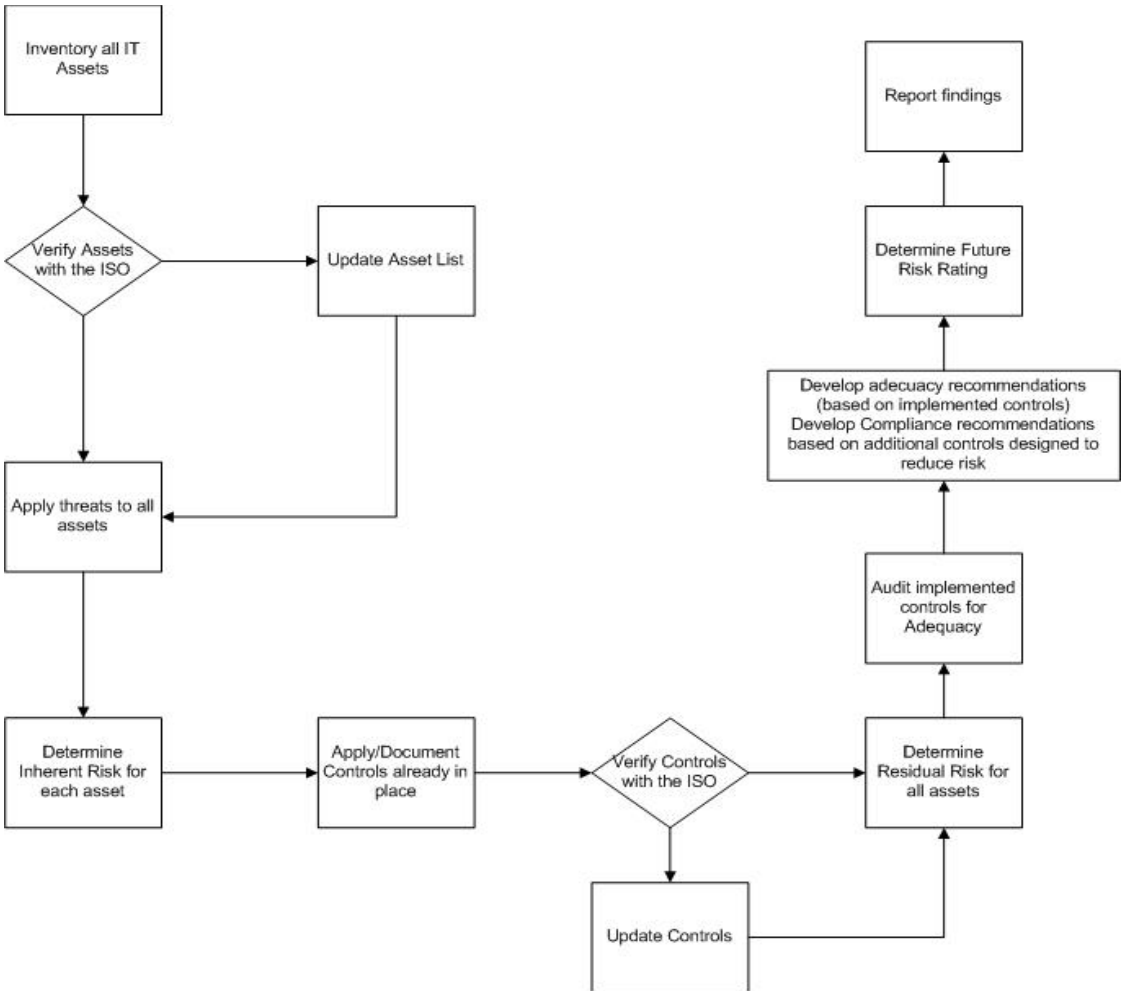

Figure 10: IT Risk Assessment Process

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, Engebretson, & Lovaas, 2009). SMERAM helps determine if institutions are compliant with regulatory requirements and if each asset falls

within the acceptable risk level that is dependent 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). For more details on the Risk Assessment Process and for a detailed example on how this method was audited risk-based, refer to Appendix A.

The second aspect of the Holistic IT Audit Framework is regulatory compliance. The researcher developed a questionnaire that will make the auditor more familiar with the organization as it relates to regulatory compliance. The questions are based on ISO, COBIT, and other regulations that financial institutions must comply with. The entire questionnaire can be found in Appendix C. It is the basis for adequacy and compliance recommendations upon completion of the IT audit. The auditors asked the ISO of the institution all of the questions and, based on the answers, were able to create a work plan. These questions ask for yes and no answers. Further documentation will need to be investigated onsite. The process utilized for the compliance section is outlined in Figure 11.

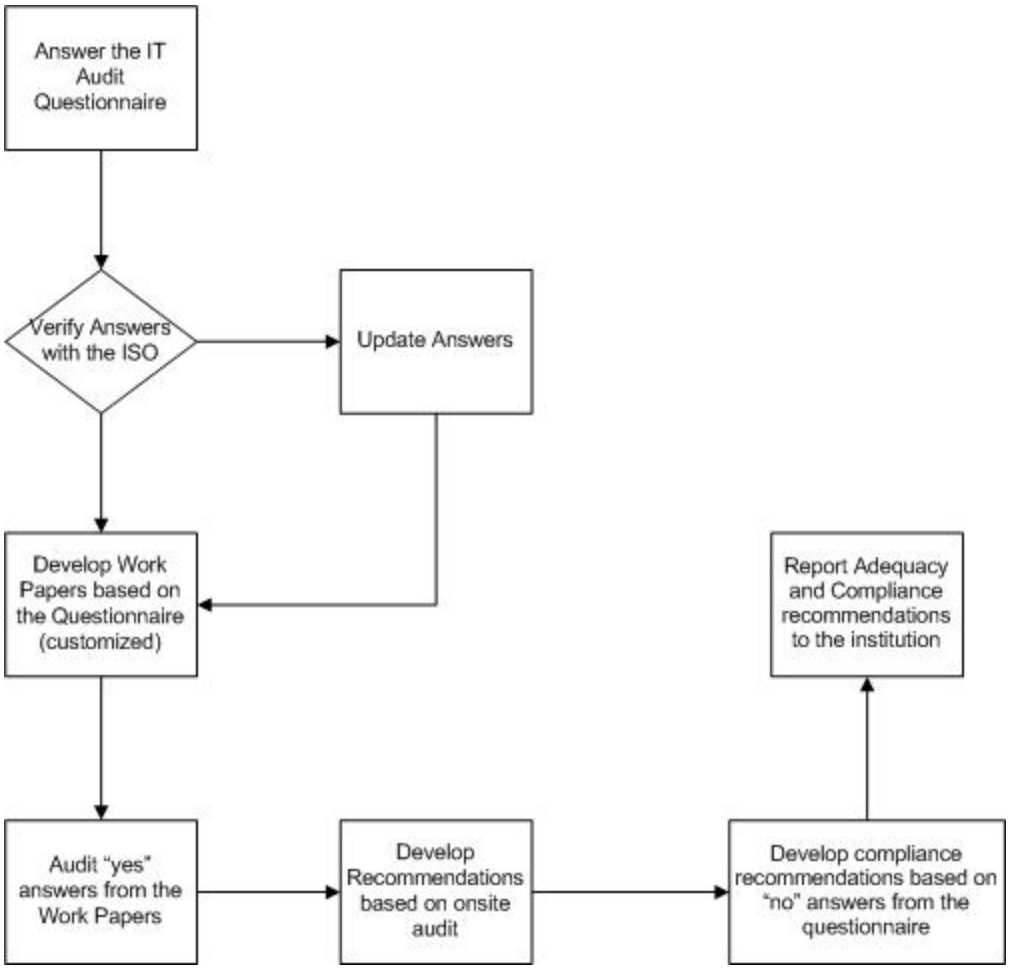

Figure 11: IT Audit Compliance Process

Two methods of social engineering were performed at both locations and at all of their branches. The institutions were able to pick between the following methods:

- Dumpster Diving
- Physical Security Assessment
- Phishing Scam
- Phone

Both institutions chose physical security assessment. For work papers, please refer to Appendix D. Figure 12 outlines the Social Engineering Assessment process utilized for this study.

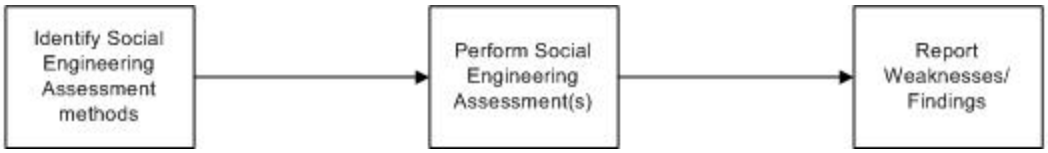

Figure 12: Social Engineering Assessment Process

Finally, the Vulnerability Assessment and Penetration Tests were performed at both institutions utilizing Nessus software. The Vulnerability Assessment was based on the IP address range that was given to the auditor at the time of the audit. The assessment took place onsite. Figure 13 outlines the VA process utilized. The Penetration Test conducted was completed offsite, and again was based on the scoping the institutions had already done. Figure 14 outlines the process utilized.

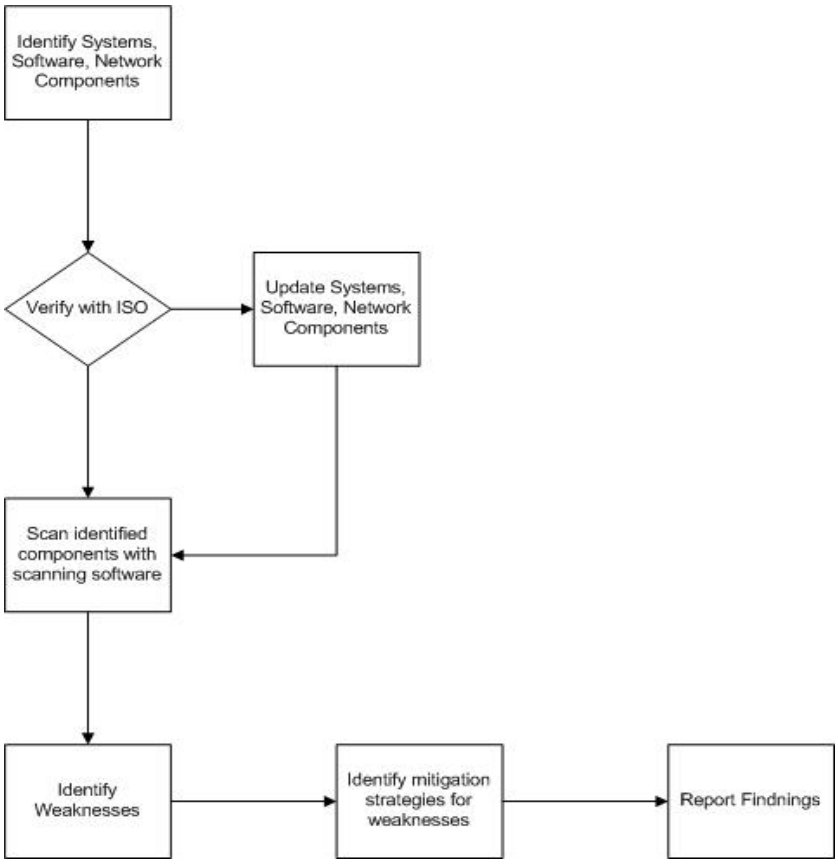

Figure 13: Vulnerability Assessment Process

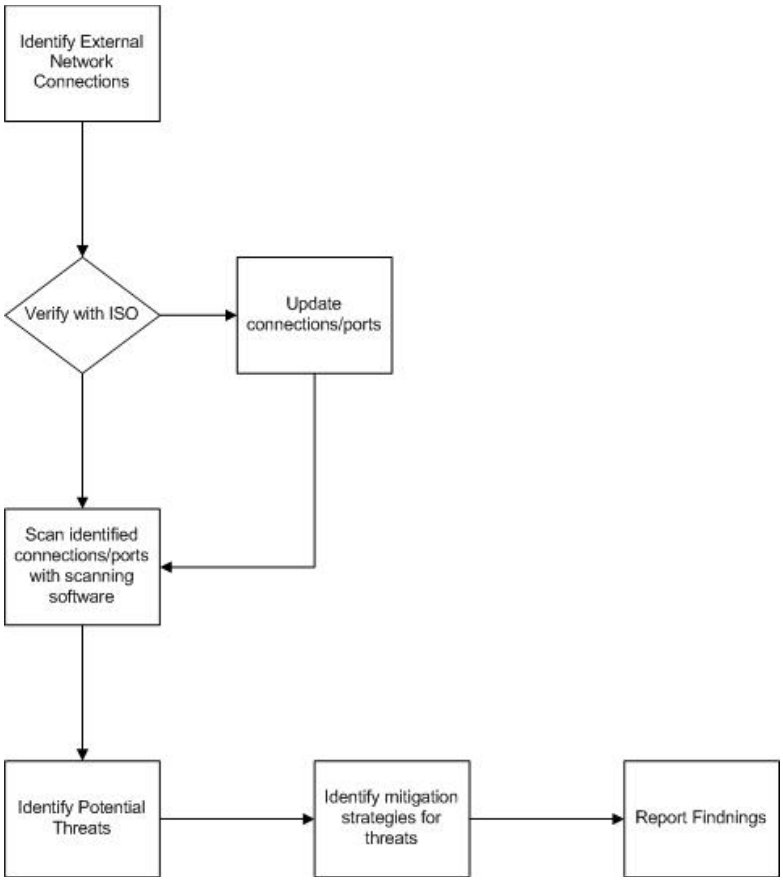

Figure 14: Penetration Testing Process

The VA and PT conclude the Holistic IT Audit framework.

Pre-Assessment Questionnaire Results

When this research was conducted, the researcher was employed as a consultant by an information security consulting organization specializing in bank and financial security. This organization had created an IT audit contract with two financial institutions, one with an asset size of 250 million, hereafter named Bank X, and an institution with an asset size of 50 million, hereafter named Bank Y. Both institutions were asked by the researcher to take part in the development of the holistic IT Audit framework specially designed for small- and medium-sized financial institutions. Both agreed to go through pre- and post-assessment questionnaire to determine if the research

questions for this research had been satisfied. Prior to agreeing to take part, the process of the IT audit framework was explained in detail to the institutions, and any questions were answered. Because the consulting company is known for its security expertise, no additional liabilities were required from the institutions. Furthermore, since the framework is built on proven theory, current frameworks, and regulatory requirements, the process was very smooth. Following the consent of each institution, prior to the IT Audit work, the pre-assessment questionnaire had to be filled out, in this case by the institution's Information Security Officer (ISO).

Table 6: Pre-Assessment Questions

Pre-Assessment Questions	**Bank X**	**Bank Y**
1. What IT Audit Framework did you previously use to complete your IT Audit requirements?	The bank previously only completed some internal auditing. No framework was utilized.	Did not have a framework in place. Did some policy compliance audits, but it did not satisfy regulators.
2. What were some of the concerns you had with this framework?	Examiners wanted more details, covering additional areas.	Not covering IT, system controls, and not based on a framework for SMEFIs.
3. Did regulators make any comments about adequacy of this framework?	The OCC specifically asked the bank to conduct annual penetration tests, vulnerability assessments, and external IT auditing. The OCC also required the IT audit to be risk-based.	Prior to this IT Audit, regulators required the institution to expand its IT audit program to cover IT assets, policy, VA, PT, SE, regulatory compliance. The audit should also be done by an external entity and be risk-based.
4. Did regulators indicate that they would like more auditing for:		
a. People (social engineering)	Examiners have not specifically asked for a social engineering assessment.	Examiners suggested the institution complete a social engineering assessment.
b. Process (compliance with regulatory requirements/ current framework)	Examiners wanted the institution to improve its overall information security posture, including risk management.	Regulators suggested the institution expand its compliance efforts with its own policy to include more regulatory requirements, as well as be based on the institution's risk assessment.
c. Technology (Vulnerability Assessment, Penetration Testing)?	Examiners suggested that in addition to the IT audit the institution conduct annual vulnerability assessments and Penetration Testing on its IT system.	Last exam suggested that the institution complete annual Penetration Testing and Vulnerability Assessments on its IT systems.

Upon completion of the pre-assessment, a compliance questionnaire was distributed to the ISO. The ISO and the organization had five business days to respond to the questions. The questions were based on federal regulation, and in particular the FFIEC IT Handbook (FFIEC, n.d), the Information Technology Examination Officer's Questionnaire (FDIC, 2005), as well as ISO 27002, COBIT, and other good security practices that institutions have in place and should implement. (For a specific list of questions, please refer to Appendix C.) At the same time, the researcher asked for evaluation of the most current IT risk assessment. He evaluated the risk assessment methods utilized. Based on the results, he utilized the risk assessment methodology mentioned above to develop his own methodology and threats and controls. For an example of controls for one asset/threat combination, refer to Appendix A.

Once the risk assessment and IT audit questionnaire was completed, the auditor (researcher in this case) spent time on getting the work papers documented. The initial step in this risk-based IT audit framework is to determine what controls from the risk assessment process should be audited. This process is usually completed with the institution to ensure that ratings are correctly assigned. The rating for each asset is determined on the basis of what is most critical to the institution. Based on this, each asset will get a high, medium, or low rating. The inherent risk rating is based on how the organization and auditor rate the Confidentiality, Integrity, and Availability of each asset. An example of what the inherent risk table could look like can be found in Table 7.

Table 7: Risk Assessment Table

Asset	Confidentiality	Integrity	Availability	Inherent Risk
Core Banking System	**H**	**H**	**H**	**H**
Check Imaging Server	**M**	**H**	**L**	**M**
Terminal Server	**H**	**H**	**M**	**H**
Web Server	**H**	**H**	**H**	**H**
Lending	**H**	**M**	**L**	**M**
Deposit	**H**	**M**	**L**	**M**
Firewall	**M**	**M**	**H**	**M**
ATM	**M**	**M**	**M**	**M**
Thin Clients	**H**	**H**	**H**	**H**
Laptops	**L**	**M**	**L**	**L**
Backup Tapes	**H**	**H**	**H**	**H**
Phone Banking	**M**	**H**	**L**	**M**
Printers	**L**	**L**	**M**	**L**

To make the risk assessment process risk-based, the researcher suggests the following as outlined in Table 8:

Table 8: Risk-Based Risk Assessment IT Audit

Asset Rating	Required Controls (Adequacy and Compliance)	Optional Controls (Adequacy and Compliance)
High	• All controls must be audited for both compliance and adequacy.	NA
Medium – High	• All high and medium rated controls must be audited for compliance and adequacy.	• A collection of low rated controls should also be audited for compliance and adequacy.
Medium	• 75 percent of the high rated controls, • 25 percent of medium rated controls, • and 25 percent of low rated controls	
Low – Medium	• 50 percent of high rated controls, • and no more than 25 percent of medium rated controls • 10 percent of the low rated controls	• The auditor may decide that for certain assets, more controls must be audited.
Low	• 25 percent of high rated controls • 10 percent of medium rated controls	• The auditor may decide that for certain assets, more controls must be audited.

Following this process ensures that the process is risk-based, and that audit resources are focused on the institution's critical assets.

The second step, prior to the onsite visit, is the IT Audit questionnaire. The auditor went through this questionnaire, not only to determine what to look for, but also to learn all about the institution, to develop an understanding of what is being done, and to determine if there are areas the institutions needs to improve. The analysis of the questionnaire is fairly straightforward. The auditor will go through the answers, one by one, and, based on the institutions' responses, will determine how to further investigate a specific topic or control. Usually, there are three ways to determine this—by interview, further documentation, or physical checks. With experience and knowledge, this process can be completed fairly quickly. If the auditor wishes to make this process risk-based as well, he/she can rate the various areas, and even drill down to each question to determine its criticality. These ratings may change, based on the size and complexity of the institution.

Once these two tasks are done and the work papers for the risk assessment, compliance, and physical checks have been completed, the auditor will schedule the onsite visit. (For an example work paper, see Appendices B and C.) The onsite portion of the IT Audit may be quite time consuming, again depending on the size and complexity of the institution.

During the onsite visit, the Vulnerability Assessment utilizing Nessus must also be completed. This process scans all the devices on the bank's network for vulnerabilities. The Penetration Test may also be done at the same time, but it is not necessary to conduct this assessment onsite.

Based on the results of the onsite visit, the auditor will document recommendations in two ways, adequacy and compliance. The adequacy piece will allow the auditor to investigate the controls that the institution has documented, and how the bank meets these requirements. If a control is not satisfactory, the auditor will make an adequacy recommendation. If certain controls are not in place, but the auditor determines that they should be, a compliance recommendation is prepared.

Once the findings are documented in an IT Audit report, delivered, and explained to the Board of Directors and to the ISO, the IT Audit is considered to be completed.

Post-Assessment Questionnaire Results

After the report was delivered to the institution, the researcher asked the following questions (See Table 9) to verify that the Holistic IT Audit Framework fulfilled the requirements of this research. The subjects for this post assessment included the ISO. The Board of Directors was present in the event that they should have any comments about the process.

Table 9: Post-Assessment Questions

Post-Assessment Questions	Bank X	Bank Y
1. How did this framework compare to your previous IT Audit?	The bank previously conducted a policy audit, not risk-based. This is the bank's second IT audit and covers additional areas, including policy and regulatory compliance. Most importantly, it was risk-based.	The bank felt comfortable that a framework was in place that covered regulatory requirements.
2. If you had any concerns prior to this audit, did this process take care of these issues?	The main concern before conducting external audit was staff knowledge, and as time went on, IT audits and examiners' requirements simply got too complicated.	The previous audit was not based on theory, and it was not risk-based according to regulators. This framework was risk-based and covered a broad range of issues and was based on DiD.
3. Did you feel that this IT Audit covered all of the following areas?		
a. People	Because of the physical review/social engineering assessment, this framework covered the people aspect of DiD.	The social engineering assessment was an eye opener to the entire organization, a great addition to the bank's IT audit requirements and a great lesion to all of the employees.
b. Process	Policies and overall information security posture were checked and improvements were suggested.	Processes were covered through policy compliance as well as recommendations for other issues the bank should consider implementing to improve its Information Security Posture.
c. Technology	The vulnerability assessment and penetration test satisfied regulatory requirements, as well as the technology aspect of the DiD.	The VA and PT covered the technology aspects of the IT Audit framework nicely. All machines and external access points were scanned.
4. Since this IT Audit, have you had a regulatory exam?	Yes, October 2009 (State)	Yes, in December 2009 (Federal).
a. If so, what were the examiners' comments?	Examiners did not particularly talk about the audit process, and had no suggestions of improvements.	Head examiner made specific comments on the IT audit framework and its holistic approach, being risk-based, covering regulatory requirements, appropriate for the institution's size and complexity.

Table 10: Post-Exam Questions

Post-Regulatory Exam Questions	Bank X	Bank Y
1. Does this new Holistic IT Audit Framework (artifact) cover and solve issues in the following areas:		
a. Regulatory Mismatch	Regulators utilized the IT audit report to make recommendations and areas of improvements.	No recommendation from the lead examiner was made in regards to the IT Audit framework. Regulators were excited about the IT audit efforts being done at the bank.
b. People aspect of auditing	Social Engineering was not specifically recommended, but the bank wants to conduct annual assessments.	The institution will keep doing social engineering assessments on an annual basis as part of their IT Audit.
c. More resource effective?	The bank freed up internal resources, and feels confident in the process. Great learning experience that will make the bank look at improvements and move forward as it relates to information security.	NA. The bank did not previously conduct external audits.

Data Analysis, Pre- and Post-Assessment Results

Coding and Developing Categories

The case study results from interviews, examiners comments and reports, and IT audit reports gave significant results to be examined. The researcher developed nine categories based on the research metrics outlined in the Research Methodology. All the data collected was examined and put into these categories to determine if significant results could be developed. The coding and categories will be used to examine the case study purpose and questions.

Appendix E outlines the results of the qualitative data analysis. Tables 11, 12 and 13 outline a summary of the results based on each research question and its categories.

The initial case study research question was set to answer the following question: How does the Holistic IT Audit Framework impact the overall quality of an IT audit for

small- and medium- sized financial institutions? The categories to measure this question are outlined in Table 11.

Table 11: Case Study Question 1 Result Summary

Category	Summary
Effectiveness	ISO states that external auditing with such broad topics creates a complete and effective IT audit. Another consideration when discussing effectiveness is that these institutions would not have to have any awareness of the technology, theory, and methods of the IT audit framework. That means that staffing is less of an issue. Furthermore, instead of addressing IT audit recommendations from the past and conducting IT audits, critical personnel can be used to address issues and focus on one area.
Identify Areas of Risk	Several areas of risk were discovered throughout the IT Audit process. When examining the IT Audit reports for both institutions, an average of 30 recommendations per institution was identified.
Organization Awareness Lacking	Through the IT audit process it was discovered that both institutions were lacking awareness of both internal processes of the institutions as well as regulatory requirements. As mentioned earlier, on an average 30 recommendations were made per institution. The IT Audit Questionnaire developed in Appendix D has 124 questions and is based on regulatory requirements. That in essence indicates that each institution is 24% incompliant with regulations.
Framework too large for size of organization	Because neither institution utilized any framework previously, it is difficult to determine from the interviews and observations if the framework fits SMEFIs. However, through the literature review, conclusions can be drawn that existing frameworks are simply too large and bulky for these types of organizations. Additionally, the expense for hiring such consultants is significant and difficult for these institutions to justify. Finally, implementing any of these frameworks will require specialized consultants for extended periods of time.

The second case study research question to be investigated was: How does the People aspect impact the comprehensiveness of the IT audit process? Table 12 outlines the categories used to measure this question.

Table 12: Case Study Question 2 Result Summary

Category	Summary
Measure Training Level	Based on the IT Audit reports for both institutions, it can clearly be identified that several recommendations were made relating to training. The physical assessment developed for the process measured the level of training for each institution. Not only was physical security measured, but social engineering schemes such as shoulder surfing were investigated as well. Furthermore, through interviews it was determined that the physical assessment results were extremely important recommendations to the Banks. For example, Bank Y has several branches and is often not able to check the different sites for physical security. This type of assessment creates overall value to the audit, as more traditional audits simply focus on the main branch location where most of the IT assets are located.
Training Suggestions	During the IT audit it was recommended that both institutions implement better security awareness programs. Little or no training existed. Furthermore, it was discovered that Bank Y did not have a security awareness program at all. Regulators require institutions to develop a training program. Social engineering is a great source for discovering areas where the institution could use more training and awareness. Furthermore, both institutions felt that this was a great assessment and discovered several vulnerabilities in their organization.

Table 13 outlines the answers to the third and final case study research question: How does implementing the Holistic IT Audit framework impact resources needed to complete the audit compared to other frameworks?

Table 13: Case Study Question 3 Result Summary

Category	Summary
Cost	As neither institution conducted any IT auditing functions prior to implementing the Holistic IT Audit framework, the cost perspective is difficult to determine. However, from comments made, both institutions felt the value of conducting external IT auditing, not necessarily because of cost savings, but for the safety of having one done. Furthermore, as other research and experts have stated, security cannot be measured in dollars and cents because it is extremely difficult to put a value on customer information (Davidson, 2009).
Manpower	Manpower needed to complete the IT Audit is considered to be more than what the institutions used previously. The main reason for this is that neither institution really completed any form of auditing. In addition, from the data collected, it can also be determined that the institutions simply did not have enough time, manpower, and knowledge to conduct IT Audits that covered all of the regulatory requirements and recommendations from previous exams. The main reason both institutions contracted to conduct external IT auditing was on the requests of regulators. The internal auditing completed previously was simply not sufficient according to regulators.
Time	The ISO stated that the external IT audit did not take as long as that of the internal auditor. Specialized auditors know what they are looking for and therefore, time spent onsite is considerably less. The second time factor that should be taken into consideration is the fact that for these institutions to conduct their own IT Audits, it would most likely require several training seminars that can be very expensive. In addition, when considering the software utilized for the Vulnerability Assessment and Penetration Tests, conducting a Holistic IT Audit can become extremely costly for these relatively small organizations.
Not part of scoping	Because neither institution had previously conducted IT Audits, any results drawn from the data analysis is deemed inconclusive.

Another important aspect of case study research is the data analysis. However, according to Yin, it is one of the least developed aspects of completing a case study (Yin, 2003). Yin outlines three general strategies, and in particular "relying on theoretical propositions", which is considered the most preferred strategy. Because this study considered a multiple-case study, Yin suggests utilizing the Cross-Case Synthesis as a specific analytical tool for multiple case studies such as this. A Cross-Case Synthesis treats each of the cases as an individual study, utilizing the results from each individual case and incorporating them into a multiple case study. Yin also suggests that if there are large numbers of cases, quantitative analysis can be performed. Because of the small number of cases in this research, Yin suggests using word tables to display the individual cases in a uniform framework (Yin, 2003). One important aspect to remember when using this type of analysis is that it relies strictly on argumentative interpretation, and not quantitative methods (Yin, 2003).

Based on Yin's recommendations, and Table 3, the evaluation framework will be split into three categories: Resource Effectiveness, Value of Social Engineering, and less Regulatory Mismatch. The results of the Cross-Synthesis Analysis can be found in Appendix F. From this analysis it can be concluded that both institutions were located in rural areas and independently owned and operated. Furthermore, based on the categories, both institutions have similar results, such as not previously having conducted any form of external IT audit. Both institutions also reported positively on regulatory feedback on the Holistic IT Audit Model. Both institutions also found great value of implementing the model, because of its holistic approach and coverage of all critical areas. The people aspect of auditing became crucial to both institutions, and recommendations were made

based on these results that gave the institutions both training suggestions and general awareness. Finally, neither of the institutions received any IT audit recommendations from regulators. In fact, in both cases examiners utilized the reports to conduct their own IT exams.

Case Study Result Summary

The experience of this research was extremely positive. Feedback from both regulators as well as the institutions indicates that the framework for this research meets requirements set forth. One of the issues with this research is that very little knowledge of security and IT existed in the banks. Neither of the institution really conducted any formal IT auditing previously, making it difficult to compare previous frameworks with the new Holistic IT Audit approach. The case study had three critical questions to answer. These answers and this conclusion are drawn from the implementation in the two institutions. Furthermore, the results were qualitatively analyzed by developing categories and labels from the pre-assessment, post-assessment, regulatory feedback, interviews, and literature review. A summary of the category results, based on the nine labels taken from the Evaluation Metrics outlined in Chapter 2 can be found in Table 11 to Table 13. Because this case study was based on two individual cases, a Cross-Synthesis analysis was performed to compare the results from the two institutions. The Cross-Synthesis analysis results can be found in Appendix F. For a complete list of the data analysis and results, refer to Appendix E.

This case study intended to have the following three questions answered:

a. How does the Holistic IT Audit Framework impact the overall quality of an IT audit for small- and medium-sized financial institutions?

When discussing and determining the overall impact on quality of the Holistic IT Audit framework, it is safe to conclude that the quality of the audit was high. First of all, neither institution conducted IT audits previously. Secondly, regulators actually utilized the results of these audits to determine what they were examining and recommending. Additionally, when looking at the literature review, having a framework specifically designed for SMEFIs will also improve the overall quality of the IT audit.

In addition, examiners had previously recommended the institutions conduct external IT auditing and further explained that this process should be risk-based and include Penetration Testing, Vulnerability Assessments, Compliance with regulatory requirements. These requirements were the very criteria that this research is based on.

b. How does the People aspect impact the comprehensiveness of the IT audit process?

From the evidence provided in the data analysis, the impact of the comprehensiveness of the IT audit is also significant. Through the onsite visitation, several areas were identified as potential training and awareness issues with each institution. From the very basics of creating a security awareness program to expanding the current program to include business continuity training and creating red flag/identity theft procedures the people aspect of the Holistic IT audit program proved to be very efficient. Other areas identified through the analysis were actually protecting the IT assets from potential malicious attacks such as shoulder surfing and simple acceptable use banners. All of these provide better and improved overall security posture for the institutions, both from a physical and training perspective.

c. How does implementing the Holistic IT Audit framework impact resources needed to complete the audit compared to other frameworks?

Investigating the resources needed for conducting the IT audit, assuming the institution already has a framework in place, is significant. From the data analysis, it can be seen that conducting this audit requires minimal resources from the organization. However, cost is higher than conducting a short term internal IT audit. When an institution is conducting internal audits, very little cost is imposed on the organization, as no specialized consultants need to be on staff. However, when performing the same IT audit internally, cost of software, training, and education needs must be taken into consideration. Because SMEFI are generally located in rural areas, another factor of costs includes travel expenses when internal auditors need to get training to perform these audits. In addition, employees will not be able to perform regular duties while attending training. In the long run, both resources and costs may decrease, but further investigation is needed to determine this. Perhaps the greatest benefit to the institution is that the framework is based on proven theory, and that all areas of the organization (People, Operations, Technology) are audited and will ensure a sense of safety, in particular as it relates to regulatory examinations.

Furthermore, the resources needed for this audit are fewer than those of current frameworks designed for large organizations. The Holistic IT Audit Framework is specifically designed for SMEFIs and will improve the overall information security posture.

This concludes the artifact design portion of this research. A holistic IT audit framework has been developed based on current frameworks, regulatory requirements,

and the Defense-in-Depth theory. The artifact has been implemented and validated through a multiple-case study analysis and these results have been analyzed to verify the artifacts integrity. Chapter 5 summarizes the research and describes future research opportunities.

CHAPTER 5

Conclusion

This research had the following goals:

1. Identify shortcomings of existing IT audit frameworks, in particular how they relate to small- and medium-sized financial institutions;
2. Develop a holistic comprehensive risk-based IT audit framework, incorporating Defense-in-Depth, specifically designed for small- and medium-sized financial institution, based on current research and methods;
3. Test and evaluate the model.

A thorough literature review discovered several issues with current IT audit frameworks, including the fact that none of them are designed especially for SMEFIs. All are large frameworks, making an implementation extremely costly and time-consuming. In addition, it is generally left for banks to decipher what should be audited and implemented regarding the size and complexity of the organization. Furthermore, none of the frameworks is considered risk-based, as none is focused on the IT risk assessment. A sound risk-based IT audit should always be based on a comprehensive risk assessment methodology. This will ensure that audit resources are focused on the institution's critical assets.

Based on a hybrid between current frameworks, regulatory requirements, and the Defense-in-Depth theory, the researcher developed a Holistic IT Audit Framework specifically designed for small- and medium-sized financial institutions. The research suggests that the IT audit has five core areas/steps that need to be included to comply

with the requirements—Risk-Assessment, Compliance, Vulnerability Assessment, Penetration Testing, and Social Engineering. The initial step is to base the IT audit on an IT risk assessment, checking controls for IT assets. The second step is to conduct research about the institution, learn about the processes the organization has in place, and to determine where they need to go. This step is strictly focusing on policies and procedures. The Social Engineering assessment audits the employees of the organization and also provides good training.

Testing and evaluating the model was completed in two financial institutions. Both implementations were successful, although it was somewhat difficult to satisfy the three goals of the implementation. This was the institutions' first external IT audit that utilized a framework. However, feedback from regulators was quite positive.

Future Research

Though most of this research is successful, certain improvements can be made. To further show the success of this research, more case studies should be conducted. This will enable the researcher to make some generalizability statements. Critical questions are: Can the IT audit framework be successfully implemented in ANY SMEFI? Does it work for other industries?

The researcher would also like to make the risk management process more available and more scientific. Since the risk management process utilized in this research is proprietary, it is necessary to look at other solutions to actually build the entire framework for any institution to implement. The purpose of such a study is to incorporate and map threats and controls based on the Common Attack Pattern Enumeration and Classification (CAPEC) and the National Institute of Standards and

Technology (NIST) Special Publication 800-53. Dr. Engebretson, an Information Security specialist, has researched NIST 800-53 (National Institute of Standards) controls and CAPEC (Common Attack Pattern Enumeration and Classification) threats and mapped these controls to each other. This could be valuable information to include in the risk assessment process to make it more scientific. The researcher would like to investigate Engebretson's results further to see if this could be incorporated into the Holistic IT Audit Framework. The mappings done by Engebretson are extremely important for a future study to enable the researcher to develop threats and controls specific to IT systems utilized by financial institutions. The outcome of these mappings will determine if the data can be utilized for a Risk-Based IT Auditing Standard for all small- and medium-sized financial institutions.

The second goal of this research is to develop a standard questionnaire set that outlines all the requirements for banks and financial institutions, ensuring that all areas will be audited, not simply controls based on the Risk Management process. To ensure that these questions are risk-based as well, a rating scheme will be developed, ensuring that areas considered more important are audited more often and more rigorously than less critical areas. This question set will be based on the FFIEC IT Handbook and Financial Institutions Letters (FILs) required to be in place at small- and medium-sized financial institutions.

References

Hevner, A., March, S., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. MIS Quarterly , 75-105.

Hunton, J., Bryant, S., & Bagranoff, N. (2004). *Core Concepts of Information Technology Auditing*. New Jersey: Wiley.

Johnson, D. J. (2005). *Best Practices in Information Assurance and Information Technology Networking in Organizations That Have Two Departments.* Retrieved November 13, 2009 from http://faculty.ed.umuc.edu/~meinkej/inss690/johnson.pdf

Kelly, W. (2006). *Defense In-Depth, Exercise Best Practices & a Tiered Security Defense To Protect Your Internal Network*. Retrieved November 21, 2009, from http://www.processor.com/editorial/article.asp?article=articles/P2840/30p40/30p40.asp

Kowal, L. (n.d). *COBIT for Internal Auditors.* Retrieved December 13, 2009 from www.nysscpa.org/committees/emergingtech/cobit.ppt

Lindow, P. E., & Race, J. D. (2002). *Beyond Traditional Audit Techniques.* Retrieved April 9, 2009 from http://www.journalofaccountancy.com/Issues/2002/Jul/BeyondTraditionalAuditTechniques.htm

Martin, A. G. (2008). *Assess Your IT Controls.* Retrieved January 30, 2009 from http://www.creditunionmagazine.com/Assess_Your_IT_Controls_823.html

McCumber, J. (2005). *Assessing and Managing Security Risk in IT Systems*. Boca Raton: Auerbach.

McGladrey & Pullen. (2009). *What is COSO?* Retrieved December 13, 2009 from http://www.mcgladrey.com/Resource_Center/Audit/Articles/WhatIsCOSO.html

McNamee, D. (1997). *Risk-based Auditing*. The Internal Auditor, 22-27.

Meycor COBIT. (n.d). *Information Assurance Using COBIT.* Retrieved December 12, 2009 from www.datasec-soft.com/.../Aseguramiento_de_la_Informacio_CSA_AG_EN.ppt

National Security Agency. (n.d.). *Defense-In-Depth*. Retrieved March 5, 2008 from www.nsa.gov/ia/_files/support/defenseindepth.pdf

Parkinson, M. (2004). *A Strategy for Providing Assurance*. The Internal Auditor, 63-68.

Patel, R. (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

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. Honolulu: Hawaii International Conference on Business.

Praxiom. (2009). *ISO 27002*. Retrieved November 13, 2009 from http://www.praxiom.com/iso-27001-definitions.htm#Information%20security%20management%20system%20%28ISMS%29

Rothman, M. (2007). *Audit: Five Fearless Strategies for Survival*. Retrieved March 7, 2007 from http://searchcio-midmarket.techtarget.com/tip/0,289483,sid183_gci1273981,00.html

SANS. (2006). *ISO 17779 Checklist.* Retrieved December 13, 2009 from http://www.sans.org/score/checklists/ISO_17799_2005.doc

Sayana, S. A. (2002). *IT Audit Basics.* Retrieved July 7, 2007 from http://www.isaca.org/Template.cfm?Section=IT_Audit_Basics&Template=/ContentManagement/ContentDisplay.cfm&ContentID=11223

Simmons, M. R. (1997). *COSO Based Auditing.* Retrieved July 1, 2007 from http://www.cwu.edu/~atkinsom/coso.htm

Singleton, T. W. (2008). *The COSO Model: How IT Auditors can use it to Measure the Effectiveness on Internal Controls (Part 2)*. Retrieved January 28, 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

Singleton, T. W. (2007). *What Every IT Auditor Should Know About Auditing Information Security*. Retrieved October 3 2008, from http://www.isaca.org/Content/NavigationMenu/Students_and_Educators/IT_Audit_Basics/What_Every_IT_Auditor_Should_Know_About_Auditing_Information_Security.htm

Turcato, L. M. (2006). *Integrating COBIT into the IT Audit Process.* Retrieved December 13, 2009 from http://www.sfisaca.org/download/Integrating%20CobiT%20Domains%20into%20the%20IT%20Audit%20Process.pdf

Yin, R. K. (2003). *Case Study Research*. Thousand Oaks: Sage Publications.

Zhu, A. (2007). *ISMS and Audit Methodology.* Retrieved December 3, 2009 from http://www.docstoc.com/docs/13575720/ISO-27001---ISMS-and-Audit-Methodology

Appendix A: SMERAM Risk Assessment Example

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

SMERAM Controls for Data Loss Threat

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

Appendix B: IT Audit Work Paper Example

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 and documentation exist to support the bank's 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					

Appendix C: IT Audit Questionnaire

IT Audit Compliance Questionnaire and Work Papers					
Identifier	**Question**	**Section**	**Sub-Section**	**Compliance**	**Adequacy**
1.0.1	Has an Information Security Program (ISP) been implemented?	01) Management	00) Management		
1.0.2	Are employee and management roles and responsibilities documented?	01) Management	00) Management		
1.0.3	Does the Board of Directors oversee information security activities and maintenance?	01) Management	00) Management		
1.1.1	Is there an Information Technology (IT) Committee?	01) Management	01) IT Management		
1.1.2	Does the IT Committee review all reports generated through the ISP?	01) Management	01) IT Management		
1.1.3	Does the bank have an Information Security Officer?	01) Management	01) IT Management		
1.1.4	Is the ISO responsible for the day-to-day implementation and management of the ISP?	01) Management	01) IT Management		
1.1.5	Does the ISO hold a management position?	01) Management	01) IT Management		
1.1.6	Does the ISO have sufficient knowledge, background, and training to perform job requirements?	01) Management	01) IT Management		
1.2.1	Does an accurate and up-to-date organizational chart exist?	01) Management	02) Organizational Chart		
1.2.2	Does the organizational chart include the Board of Directors and a management hierarchy?	01) Management	02) Organizational Chart		
1.2.3	Does the organizational chart include the employee roles / titles?	01) Management	02) Organizational Chart		
1.3.1	Does the bank have insurance to mitigate the residual risk of threats to information and IT systems that the bank does not have the ability to control or that could result in significant financial loss to the bank?	01) Management	03) IT Insurance		
1.4.1	Does the bank maintain an Information Technology (IT) Strategic Plan?	01) Management	04) IT Planning		
2.0.1	Does the bank identify and assess risks to information and IT systems?	02) Risk Management Program	00) Risk Management Program		
2.1.1	Are risk assessments conducted on a reoccurring basis? Please enter the date of the last risk assessment in the comments box.	02) Risk Management Program	01) Risk Assessment		

2.1.2	Does the risk assessment identify and prioritize risk exposure?	02) Risk Management Program	01) Risk Assessment		
2.2.1	Does management prioritize the findings of the risk assessment and determine which recommendations will be implemented and which risks will be accepted?	02) Risk Management Program	02) Risk Assessment Reports		
3.0.1	Does the bank require the completion of a risk-based IT audit (internal and/or outsourced)?	03) IT Audit Program	00) IT Audit Program		
3.1.1	Are IT audits required at least annually?	03) IT Audit Program	01) Scope and Schedule		
3.1.2	Have the scope and schedule of IT audits been defined?	03) IT Audit Program	01) Scope and Schedule		
3.1.3	Are the risk assessment results used to formulate the IT audit scope and schedule?	03) IT Audit Program	01) Scope and Schedule		
3.2.1	Does the bank have an IT audit committee?	03) IT Audit Program	02) IT Audit Committee		
3.3.1	Has an internal IT auditor been designated?	03) IT Audit Program	03) Internal IT Audit		
3.3.2	Is the internal IT auditor experienced in the IT functions audited?	03) IT Audit Program	03) Internal IT Audit		
3.3.3	Is the internal IT auditor independent from the IT functions audited?	03) IT Audit Program	03) Internal IT Audit		
3.3.4	Does the internal IT auditor receive training in the IT functions audited?	03) IT Audit Program	03) Internal IT Audit		
3.4.1	Does the bank outsource the IT audit function? This outsourced IT audit function may complement or fully replace the internal IT audit function.	03) IT Audit Program	04) Outsourced IT Audit		
3.4.2	Does the bank require outsourced IT audit engagement letters to include scope, timeframe, and cost of services?	03) IT Audit Program	04) Outsourced IT Audit		
3.5.1	Are minimum requirements set for IT audit coverage?	03) IT Audit Program	05) Audit Coverage		
3.5.2	Did the most recent IT audit include an assessment of the IT organizational structure including separation of duties?	03) IT Audit Program	05) Audit Coverage		
3.5.3	Did the most recent IT audit verify compliance with policy and procedure controls?	03) IT Audit Program	05) Audit Coverage		
3.5.4	Did the most recent IT audit include adequacy recommendations to improve IT policies?	03) IT Audit Program	05) Audit Coverage		
3.5.5	Did the most recent IT audit verify compliance with GLBA section 501(b)?	03) IT Audit Program	05) Audit Coverage		
3.6.1	Do IT audit reports contain recommendations for corrective actions to be taken?	03) IT Audit Program	06) Audit Reports		

3.6.2	Are IT audit conclusions based on the findings of the auditor(s) with no intervention from other bank employees?	03) IT Audit Program	06) Audit Reports		
3.6.3	Does management prioritize the IT audit recommendations and determine the actions to be taken to correct the deficiencies?	03) IT Audit Program	06) Audit Reports		
4.1.1	Are vulnerability assessments conducted on a reoccurring basis? Please enter the date of the last vulnerability assessment in the comments box.	04) Network Security Assessment Program	01) Vulnerability Assessment		
4.2.1	Are penetration tests conducted on a reoccurring basis? Please enter the date of the last penetration test in the comments box.	04) Network Security Assessment Program	02) Penetration Testing		
4.3.1	Do network security assessment reports (e.g., vulnerability assessment report, penetration testing report, etc.) include a description of the scope and systems assessed?	04) Network Security Assessment Program	03) Network Security Assessment Reports		
4.3.2	Do network security assessment reports include recommendations for corrective actions?	04) Network Security Assessment Program	03) Network Security Assessment Reports		
4.3.3	Does management prioritize the findings of the network security assessments and determine which recommendations will be implemented and which risks will be accepted?	04) Network Security Assessment Program	03) Network Security Assessment Reports		
5.0.1	In general, does the bank take steps to protect IT systems and processes?	05) Internal Control Program	00) Internal Control Program		
5.1.1	Does the bank have a program to provide management direction and support in the area of personnel security?	05) Internal Control Program	01) Personnel Security Program		
5.1.2	Does the bank verify job application information for all new employees (e.g., character references, experience, education, qualifications, identity, and background)?	05) Internal Control Program	01) Personnel Security Program		
5.1.3	Does the bank conduct screening of all personnel, both potential and current employees, according to the level of risk associated with their positions?	05) Internal Control Program	01) Personnel Security Program		
5.1.4	Does the bank document job responsibilities for all positions that clearly outline the expectations of both the employee and the bank?	05) Internal Control Program	01) Personnel Security Program		

5.1.5	Does the bank have employees sign a confidentiality and non-disclosure agreements to prohibit information sharing or disclosure beyond the scope of the employees' job responsibilities?	05) Internal Control Program	01) Personnel Security Program		
5.10.1	Is there a program/schedule in place for regularly identifying and applying vendor-supplied updates or patches to systems?	05) Internal Control Program	10) Patch Management Program		
5.10.2	Are patches and updates tested on non-production systems before the patch or update is installed institution-wide?	05) Internal Control Program	10) Patch Management Program		
5.11.1	Is encryption utilized on high-risk systems that process, store, and transmit restricted information?	05) Internal Control Program	11) Encryption		
5.12.1	Is there a program in place to provide management direction and support in the area of physical security?	05) Internal Control Program	12) Physical Security Program		
5.12.2	Are there security controls for the building and its secure areas that provide physical security to confidential information and to critical IT functions?	05) Internal Control Program	12) Physical Security Program		
5.12.3	Is physical security provided for equipment within the bank by evaluating the placement, power supply, cabling, maintenance, and disposal needs?	05) Internal Control Program	12) Physical Security Program		
5.13.1	Is there a program in place to manage assets and information within the bank?	05) Internal Control Program	13) Asset Management Program		
5.13.2	Is an inventory of IT assets maintained?	05) Internal Control Program	13) Asset Management Program		
5.13.3	Is the asset inventory up-to-date?	05) Internal Control Program	13) Asset Management Program		
5.13.4	Are physical assets labeled with an identifying label?	05) Internal Control Program	13) Asset Management Program		
5.13.5	Does the bank have asset acquisition procedures?	05) Internal Control Program	13) Asset Management Program		
5.13.6	Does the bank have asset tracking procedures?	05) Internal Control Program	13) Asset Management Program		
5.13.7	Does the bank have a network diagram?	05) Internal Control Program	13) Asset Management Program		
5.13.8	Is the network diagram up-to-date?	05) Internal Control Program	13) Asset Management Program		
5.13.9	Is information classified in terms of value, sensitivity, and/or criticality?	05) Internal Control Program	13) Asset Management Program		

5.14.1	Are maintenance logs that track changes made to information system assets documented and maintained?	05) Internal Control Program	14) Maintenance Logging Program		
5.2.1	Does the bank have processing controls over preparation, input, and processing of sensitive information?	05) Internal Control Program	02) Processing Control Program		
5.3.1	Are all employees required to read and sign an Acceptable Use policy (AUP)?	05) Internal Control Program	03) Acceptable Use		
5.3.2	Does the AUP define clear desk and clear screen requirements?	05) Internal Control Program	03) Acceptable Use		
5.3.3	Does the AUP define procedures for enforcement and disciplinary actions?	05) Internal Control Program	03) Acceptable Use		
5.4.1	Does the bank conduct security awareness training of security weaknesses and emerging issues reoccurring basis? Please enter the date of the last training event in the comments box.	05) Internal Control Program	04) Security Awareness Education Program		
5.4.4	Are information security policies reviewed and discussed with all employees on a reoccurring basis?	05) Internal Control Program	04) Security Awareness Education Program		
5.5.1	Does the bank conduct social engineering testing on a reoccurring basis? Please enter the date of the last social engineering assessment in the comments box.	05) Internal Control Program	05) Social Engineering Assessments		
5.5.2	Do your social engineering tests include at least one of the following: physical impersonation, pretext calling, dumpster diving, shoulder surfing, phishing and pharming attacks, and handling of unidentified removable media?	05) Internal Control Program	05) Social Engineering Assessments		
5.5.3	Does the bank review social engineering test results with employees?	05) Internal Control Program	05) Social Engineering Assessments		
5.6.1	Is all sensitive information sanitized or destroyed after its useful life has expired?	05) Internal Control Program	06) Information Sanitation and Disposal Program		
5.7.1	Does the bank have a program for controlling logical access to IT systems? Logical access refers to user based authenticated access to systems and the data that is processed.	05) Internal Control Program	07) Access Control Program		
5.7.10	Is system access temporarily disabled when a user is absent for an extended period of time?	05) Internal Control Program	07) Access Control Program		
5.7.11	Is all system access removed immediately when a user permanently leaves employment?	05) Internal Control Program	07) Access Control Program		

5.7.2	Does the bank have an enrollment process in place to add new users to system resources?	05) Internal Control Program	07) Access Control Program		
5.7.3	Are account access levels restricted to minimal resources necessary? Meaning, are employees limited only to resources and information that they need to perform their job functions?	05) Internal Control Program	07) Access Control Program		
5.7.4	Are all accounts and permissions reviewed on a reoccurring basis to ensure proper access levels?	05) Internal Control Program	07) Access Control Program		
5.7.5	Does the bank have a process for updating access rights based on personnel or system changes?	05) Internal Control Program	07) Access Control Program		
5.7.6	Are usernames and passwords composed in a secure and consistent manner that minimizes risk to the bank's systems?	05) Internal Control Program	07) Access Control Program		
5.7.7	Are accounts disabled after a consecutive number of failed login attempts?	05) Internal Control Program	07) Access Control Program		
5.7.8	Are session controls used to terminate and/or lock accounts according to specified periods of time?	05) Internal Control Program	07) Access Control Program		
5.7.9	Are appropriate controls in place for external connectivity (remote access) if third parties or out-of-office employees are allowed to connect to the bank?	05) Internal Control Program	07) Access Control Program		
5.8.1	Does the bank maintain and monitor system logs for IT and security events. For example, system logs, access logs, activity logs, and firewall logs?	05) Internal Control Program	08) System Logging and Monitoring Program		
5.9.1	Is there an anti-malware program (software, employee education, etc.) in place to protect the bank from malicious software like spyware, viruses, trojans, worms, etc?	05) Internal Control Program	09) Malicious Software Protection Program		
5.9.2	Does the anti-malware program include software on all workstations, portable computers, servers, and applicable network devices?	05) Internal Control Program	09) Malicious Software Protection Program		
5.9.3	Are all applicable systems scheduled for periodic malware scans?	05) Internal Control Program	09) Malicious Software Protection Program		
5.9.4	Are the software definition files updated on a regular basis for the bank's anti-malware software?	05) Internal Control Program	09) Malicious Software Protection Program		
6.0.1	Is there a program in place to manage service providers, purchasing of hardware and software from vendors, outsourcing, and internal development of systems?	06) Development, Acquisition, and Oversight Program	00) Development, Acquisition, and Oversight Program		

6.1.1	Is there a program in place to oversee the internal development of systems/applications?	06) Development, Acquisition, and Oversight Program	01) Systems Development		
6.2.1	Is proper due diligence performed when selecting service providers?	06) Development, Acquisition, and Oversight Program	02) Vendor and Service Provider Selection		
6.3.1	Does the bank analyze contracts with third parties to ensure they define the rights and responsibilities of both the bank and the service provider?	06) Development, Acquisition, and Oversight Program	03) Vendor and Service Provider Contract Requirements		
6.4.1	Does the bank perform the necessary service provider oversight to ensure that ongoing relationships remain viable?	06) Development, Acquisition, and Oversight Program	04) Vendor and Service Provider Management		
6.5.1	Does the bank outsource management and control of some or all IT systems, networks, and/or desktop environments?	06) Development, Acquisition, and Oversight Program	05) Outsourced Services		
6.5.2	Does the bank have contracts in place that address the risks, security controls, and procedures for the outsourced systems?	06) Development, Acquisition, and Oversight Program	05) Outsourced Services		
7.1.1	Does the bank have an identity theft prevention program to detect, prevent, and mitigate identity theft of covered accounts (FDIC FIL-100-2007) which are used for personal, family, or household purposes that permit multiple payments or transactions.	07) Emergency Preparedness Program	01) Identity Theft Prevention Program		
7.1.2	Does the identity theft prevention program include processes for identifying, detecting, and responding to red flags?	07) Emergency Preparedness Program	01) Identity Theft Prevention Program		
7.1.3	In the identity theft prevention program, are suspicious address change requests verified by notifying the customer at their former address or through other forms of communication?	07) Emergency Preparedness Program	01) Identity Theft Prevention Program		
7.2.1	Does the bank have an incident response plan (IRP)?	07) Emergency Preparedness Program	02) Incident Response Program		
7.2.2	Does the IRP include appropriate escalation procedures to address varying alerts or incidents?	07) Emergency Preparedness Program	02) Incident Response Program		
7.2.3	Has an incident response team (IRT) been established to address incidents?	07) Emergency Preparedness Program	02) Incident Response Program		
7.2.4	Are there procedures in place for reporting suspected crimes and computer intrusions on Suspicious Activity Reports (SARs)?	07) Emergency Preparedness Program	02) Incident Response Program		

7.3.1	Does the bank have a disaster recovery plan that will protect the safety of people and limit damage to the bank?	07) Emergency Preparedness Program	03) Business Continuity Management Program		
7.3.2	Is a business continuity plan in place for resuming the bank's essential business functions?	07) Emergency Preparedness Program	03) Business Continuity Management Program		
7.3.3	Has a business impact analysis been performed to prioritize the bank's business functions?	07) Emergency Preparedness Program	03) Business Continuity Management Program		
7.3.4	Is a list of non-IT items needed for normal business functions maintained in case of a disaster?	07) Emergency Preparedness Program	03) Business Continuity Management Program		
7.3.5	Is the business continuity plan and/or disaster recovery plan kept up-to-date and are employees trained and aware of their role in implementation?	07) Emergency Preparedness Program	03) Business Continuity Management Program		
7.3.6	Is the business continuity plan and/or disaster recovery plan tested? Please enter the date of the most recent test in the comments box.	07) Emergency Preparedness Program	03) Business Continuity Management Program		
7.4.1	Does the bank have a documented Pandemic Influenza Plan?	07) Emergency Preparedness Program	04) Pandemic Influenza Program		
7.4.2	Are procedures included in the Pandemic Influenza Plan to reduce the likelihood that the bank’s operations will be significantly affected by a pandemic event?	07) Emergency Preparedness Program	04) Pandemic Influenza Program		
7.4.3	Does the Pandemic Influenza Plan provide scaling of the bank’s pandemic efforts as conditions of the pandemic vary?	07) Emergency Preparedness Program	04) Pandemic Influenza Program		
7.4.4	Does the Pandemic Influenza Plan include countermeasures (additional systems, policies, and procedures) for addressing reductions in available workforce? Such items could include social distancing to reduce human contact, telecommuting; promote use of drive-up window and Internet Banking, or conducting operations from alternative sites.	07) Emergency Preparedness Program	04) Pandemic Influenza Program		
7.4.5	Is the Pandemic Influenza Plan tested? Please enter the date of the most recent test in the comments box.	07) Emergency Preparedness Program	04) Pandemic Influenza Program		
7.4.6	Is the Pandemic Influenza Plan, including supporting policies, standards, and procedures, kept up-to-date?	07) Emergency Preparedness Program	04) Pandemic Influenza Program		

7.5.1	Is mission critical information backed up on a regular basis. Mission critical information can include: master files of customer information; critical business databases, files, and programs; operating systems; and customized security settings files.	07) Emergency Preparedness Program	05) Data Backup Program		
7.5.2	Are backups rotated off-site at the end of each processing day to ensure the most recent data is stored off-site at all times?	07) Emergency Preparedness Program	05) Data Backup Program		
7.5.3	Are backups, both on-site and off-site, stored in a secure location providing protection from unauthorized access and environmental hazards such as fire, water, etc?	07) Emergency Preparedness Program	05) Data Backup Program		
7.5.4	Does the alternative backup site have the hardware and software necessary to support the restoration of critical information and system program files?	07) Emergency Preparedness Program	05) Data Backup Program		
7.5.5	Is backup media encrypted during transit and storage?	07) Emergency Preparedness Program	05) Data Backup Program		
7.5.6	Are backup systems and procedures tested on a reoccurring basis? This includes testing the backup data and media for integrity.	07) Emergency Preparedness Program	05) Data Backup Program		
8.0.1	Does management report the status of the ISP and compliance with GLBA 501(b) guidelines to the Board of Directors?	08) Reviews and Evaluations	00) Reviews and Evaluations		

Appendix D: Physical IT Audit Assessment

Social Engineering / Physical Assessment

Physical Impersonation

Approach the Bank with no name tag or identifier; ask to take a look around. Verify what vendors are required to do as well as if the work is authorized by the ISO.

Perimeter

Are employee monitors visible from windows and doors?

Are employee documents visible from windows and doors?

Are non-customer entrances secured?

Is the building structure secure and sound?

Are external windows locked?

Is critical IT equipment visible from windows and doors?

Are there unsecured access points between other buildings?

Main Entrance

Is there a visitor/vendor sign-in sheet?

Are visitor/vendors required to wear badges?

Are there physical barrier between customer and bank areas?

Are all entrances monitored by employees?

Data Center / Network Areas

Are important assets consolidated into data centers for easier protection?

Are drop ceilings or raised floors in the data center or other areas that house critical IT equipment secured against access?

Do environmental controls (heating, cooling, humidity) exist which can maintain consistent IT equipment operating temperature?

Are there signs denoting secured areas?

Are there signs restricting food and beverage?

Are unattended secure areas locked?

Is critical IT equipment located a safe distance from water?

Are areas that house critical IT equipment equipped with fire detection and suppression?

Is critical IT equipment located on stable platform?

Is critical IT equipment located in locked area/rack/cage?

Is critical IT equipment run through UPSs and/or a backup generator?

Are network and power cables located in secure locations?

Are unused ports on switches/routers or on walls disabled or secured?

General Areas

Is there video surveillance?

Is there a motion detection alert system?

Do unattended offices have clear desks?

Do unattended computers have clear screens?

Are computer monitors securely positioned?

Are easily removable storage devices and media anchored down?

Is critical IT information located in trash cans?

Is there any wireless network technology implemented?

Are delivered materials handled in a secure manner?

Is general equipment safe from theft?

Are locked covers or plugs used to protect media access ports (USB, CD drives, etc)?

Are media ports easily accessible to the public?

Are any customer areas located in obscure areas?

Are office printers located near customer areas?

Are wiring closets securely locked?

Other Checks

Talk with customer to determine if there are any additional physical checks they would like performed.

Offer to take a sampling of the asset inventory and compare it against the actual assets at each location.

Perform a general assessment of physical storage used to house paper documents and electronic media

Appendix E: Qualitative Data Analysis

Category	Comments	Institution	Method of Evidence
Measure Training Level	The Bank should develop a Security Awareness Program that requires the Bank to hold annual training for employees. The training should include social engineering, malware awareness, acceptable use, the Information Security Program, and other current information security topics.	Bank Y	IT Audit Report
	The Bank should consider adding dates for when organizational charts are updated and changes are made. This will ensure that only the most recent copy is utilized.	Bank Y	IT Audit Report
	The Bank should consider adding Pandemic Preparedness scenarios to its annual Emergency Preparedness Testing efforts. This will ensure that the plan is accurate and current.	Bank X	IT Audit Report
	Great learning experience conducting the audit; many interesting findings and discoveries about the organization as well as suggestions to improve overall security	Bank X	Post-Assessment
Identify Areas of Risk	The Bank should document a personnel security program that ensures the following for new hires to comply with its ISP:	Bank Y	IT Audit Report
	The Bank should consider updating its Risk Assessment process to include specific threats and controls to each asset. Applying threats and controls to each asset will ensure that more critical assets have adequate controls in place.	Bank Y	IT Audit Report
	The Bank should consider implementing procedures on how to remove terminated employee access. Ensuring that access is removed will prevent unauthorized access for personnel no longer employed at the Bank.	Bank X	IT Audit Report

	The Bank should consider documenting what supplies should be on hand, such as surgical masks, hand sanitizer, and sneeze guards etc. In addition, the Bank should consider updating its plan to include planning for workforce reduction and rotation schedules.	Bank Y	IT Audit Report
	The Bank should consider implementing a formal third-party vendor management process on all of its critical vendors	Bank X	IT Audit Report
	The Bank should consider updating its Incident Response Program to include specific threats such as Internet Banking, Robbery, and Viruses, etc. Furthermore, procedures for these incidents should be developed.	Bank Y	IT Audit Report
	The Bank should consider implementing unique and separate authentication methods to its Proof Machine. Ensuring unique usernames and passwords will ensure that access to systems is only granted to authorized personnel.	Bank Y	IT Audit Report
	The Bank should review all monitor positions to ensure that they cannot be seen from any angle, including windows. If screens can be seen from different angles, the Bank should consider privacy screens, or decide if possible monitors should be rearranged to eliminate this issue.	Bank Y	IT Audit Report
	Great learning experience conducting the audit. Many interesting findings and discoveries about the organization as well as suggestions to improve overall security	Bank X	Post-Assessment
	The Bank should consider implementing unique and separate authentication methods to its Proof Machine. Ensuring unique usernames and passwords will ensure that access to systems is only granted to authorized personnel.	Bank Y	IT Audit Report

	The Bank should consider developing an Emergency Preparedness Test Plan. The objective of an Emergency Preparedness Test Plan is to ensure that the emergency preparedness plans remain accurate, relevant, and operable under adverse conditions. Testing should include applications and business functions that were identified during the IT Risk Assessment process.	Ban X	IT Audit Report
	Inactive Lockout Policy on the domain controller: Inactive lockout is when users are locked out of the system after a set period of time. The Bank should set this policy on the domain controller, not on individual systems.	Bank Y	IT Audit Report
	The Bank should consider adding procedures that help identify information systems and what type of information has been compromised, such as physical theft.	Bank Y	IT Audit Report
Training Suggestions	The Bank should consider on an annual basis to review its Security Awareness Training Program to determine its adequacy and if further training is necessary. Furthermore, a report of the findings, topics covered, and a list of who attended should be given to the Board for review on an annual basis.	Bank Y	IT Audit Report
	The Bank should consider adding Pandemic Preparedness scenarios to its annual Emergency Preparedness Testing efforts. This will ensure that the plan is accurate and current.	Bank X	IT Audit Report
	Because the Physical Assessment was such an eye opener for the institution, they will keep conducting the same type of assessment on an annual basis	Bank X	Post-Assessment

	The Bank should consider documenting what supplies should be on hand, such as surgical masks, hand sanitizer, and sneeze guards etc. In addition, the Bank should consider updating its plan to include planning for workforce reduction and rotation schedules.	Bank Y	IT Audit Report
	The institution has put Social Engineering in their strategic planning for 2010. As long as the Board approves the assessment, it will continue doing such assessments	Bank Y	Post-Assessment
	The Bank should consider updating its Incident Response Program to include specific threats such as Internet Banking, Robbery, and Viruses etc. Furthermore, procedures for these incidents should be developed.	Bank Y	IT Audit Report
	The Bank should consider implementing a formal third party vendor management process on all of its critical vendors	Bank X	IT Audit Report
	Great learning experience conducting the audit. Many interesting findings and discoveries about the organization as well as suggestions to improve overall security.	Bank X	Post-Assessment
Framework too large for Organization size	The Bank should consider addressing recommendations from previous audits on a timely manner. Furthermore, these recommendations should be tracked, utilizing the Bank's exceptions tracking process. This process should include timeframes for when these exceptions should be implemented.	Bank Y	IT Audit Report
	Did not have a framework in place. Did some policy compliance audits, but it did not satisfy regulators.	Bank Y	Pre-Assessment
	The bank previously only completed some internal auditing. No framework was utilized.	Bank X	Pre-Assessment
	Examiners wanted more details, covering additional areas.	Bank X	Examiners

	Not covering IT, system controls, and not based on a framework for SMEFIs.	Bank Y	Examiners
	The OCC specifically asked the bank to conduct annual penetration tests, vulnerability assessments, and external IT auditing. The OCC also required the IT audit to be risk-based.	Bank X	Examiners
	Prior to this IT Audit, regulators required the institution to expand its IT audit program to cover IT assets, policy, VA, PT, SE, regulatory compliance. The audit should also be done by an external entity and be risk-based.	Bank Y	Examiners
	Furthermore, the Bank should consider expanding its IT Audit Program to include details on what should be audited and how frequently.	Bank Y	IT Audit Report
Organization Awareness Lacking	The organization should consider implementing formal discussions and formal documentation of any reports generated out of the Information Security Program. These reports may include: Risk Assessment, IT Audit Program and Reports, Internal Control Programs, Emergency Preparedness, etc.	Bank Y	IT Audit Report
	The Bank should consider creating a Risk Assessment specifically designed for its Red Flag Identity Theft Program. Such an assessment should apply threats and controls to the different methods of opening accounts. This will ensure that procedures are created, appropriate controls are applied.	Bank Y	IT Audit Report
	The Bank should consider documenting what supplies should be on hand, such as surgical masks, hand sanitizer, and sneeze guards etc. In addition, the Bank should consider updating its plan to include planning for workforce reduction and rotation schedules.	Bank Y	IT Audit Report

	The Bank should consider reviewing and monitoring domain logs. To assist in this effort, the Bank should consider implementing a Security and Event Management (SIEM) solution (software).	Bank Y	IT Audit Report
	The Bank should consider implementing procedures on how to remove terminated employee access. Ensuring that access is removed will prevent unauthorized access for personnel no longer employed at the Bank.	Bank X	IT Audit Report
	Inactive Lockout Policy on the domain controller: Inactive lockout is when users are locked out of the system after a set period of time. The Bank should set this policy on the domain controller, not on individual systems.	Bank Y	IT Audit Report
	An Acceptable Use Notification is a screen that appears before you log into the domain notifying the user on the acceptable use of the Bank's systems. Before continuing, the user must click "OK".	Bank X and Bank Y	IT Audit Report
Not part of scoping	Bank X did some internal IT auditing prior to implementing the holistic IT Audit Framework. However, simple compliance with documented policy was verified. No compliance with regulatory requirements was considered.	Bank X	Pre-Assessment
	Bank Y did not do any type of IT auditing prior to implementing the Holistic IT Audit Framework. Therefore this fell outside of the scope of the post-assessment	Bank Y	Pre-Assessment
Cost	Bank X and Bank Y were both required to complete external IT audits. Included in these recommendations were penetration testing and vulnerability assessments.	Bank X and Bank Y	Interview
	Cost was not an issue, as the bank was forced by regulators to conduct external IT Audits.	Bank X and Bank Y	Post-Assessment/Previous Regulatory Report

	Fewer internal resources needed;	Bank X	Post-Assessment
	overall increase in cost to conduct external IT auditing	Bank X	Post-Assessment
	ISO stated that the external IT audit may be more costly than internal auditing. However, ensuring that regulators are comfortable with the audit work is priceless.	Bank X	Post-Assessment/Interview
Manpower	Because Bank X was previously conducting internal IT audits, but still was recommended to conduct an external audit, manpower and knowledge were the main reasons for this recommendation. The researcher concluded that examiners deemed the organization not capable of doing its own IT auditing as a result of this.	Bank X	Interview/Previous Regulatory Report
	The institution freed up critical resources that can now be used elsewhere.	Bank X	Interview
	The Bank should consider a risk-rating system for all of its tracking reports. The rating system for each finding could be based on High-Medium-Low ratings. Such ratings will assist the Bank in determining how critical these findings are, and how quickly they will need to be addressed.	Bank X	IT Audit Report
	No additional training needed for the internal auditor	Bank X	Interview
	The institution did not conduct any type of audits prior to this audit. The resources needed from the institution were minimal.	Bank Y	Interview
	The main concern before conducting an external audit was staff knowledge, and as time went on, IT audits and examiners' requirements simply got too complicated.	Bank X	Post-Assessment
	Not based on theory, and it was not risk-based according to regulators. This framework was risk-based and covered a broad range of issues and was based on DiD.	Bank Y	Post-Assessment

	The Bank should consider implementing unique and separate authentication methods to its Proof Machine. Ensuring unique usernames and passwords will ensure that access to systems is only granted to authorized personnel.	Bank Y	IT Audit Report
	The Bank should consider creating a Risk Assessment specifically designed for its Red Flag Identity Theft Program. Such an assessment should apply threats and controls to the different methods of opening accounts. This will ensure that procedures are created, appropriate controls are applied.	Bank Y	IT Audit Report
	The Bank should consider documenting what supplies should be on hand, such as surgical masks, hand sanitizer, and sneeze guards etc. In addition, the Bank should consider updating its plan to include planning for workforce reduction and rotation schedules.	Bank Y	IT Audit Report
	The Bank should consider implementing an Acceptable Use Notification on its systems. An Acceptable Use Notification is a message that appears before logging into the domain notifying the user on the acceptable use of the Bank's systems. Before continuing, the user must click "OK".	Bank X	IT Audit Report
	Inactive Lockout Policy on the domain controller: Inactive lockout is when users are locked out of the system after a set period of time. The Bank should set this policy on the domain controller, not on individual systems.	Bank Y	IT Audit Report
Time	ISO stated that the external IT audit did not take as long as that of the internal auditor. Specialized auditors know what they are looking for and therefore, time spent onsite is considerably less.	Bank X	Interview

	Not based on theory, and it was not risk-based according to regulators. This framework was risk-based and covered a broad range of issues and was based on DiD.	Bank X	Post-Assessment
Effectiveness	ISO states that conducting external auditing including such broad topics creates a complete IT audit.	Bank Y	Interview
	Inactive Lockout Policy on the domain controller: Inactive lockout is when users are locked out of the system after a set period of time. The Bank should set this policy on the domain controller, not on individual systems.	Bank Y	IT Audit Report
	The Bank should consider creating a Risk Assessment specifically designed for its Red Flag Identity Theft Program. Such an assessment should apply threats and controls to the different methods of opening accounts. This will ensure that procedures are created, appropriate controls are applied.	Bank Y	IT Audit Report
	The bank previously conducted a policy audit, not risk-based. This is the second IT audit the bank has conducted, and it covers additional areas, but also includes policy and regulatory compliance. Most importantly, it was risk-based.	Bank X	Post-Assessment
	The main concern before conducting external audit was staff knowledge, and as time went on, IT audits and examiners' requirements simply got too complicated.	Bank X	Post-Assessment
	Not based on theory, and it was not risk-based according to regulators. This framework was risk-based and covered a broad range of issues and was based on DiD.	Bank X	Post-Assessment

Appendix F: Cross-Case Synthesis

Institution	Characteristics		
1	Both institutions are considered small- and medium-sized. One institution has $50 million in is assets while the other has $250 million.		
2	Both institutions are rural and independently owned and operated.		
3	Both institution are regulated by the same regulatory body.		
Comparison	**Characteristics**	**Method**	**Results**
4	The new Holistic IT Audit model is more resource effective:	Interview (post-assessment)	
	a) Cost		Conducting internal IT audits to the extent these organizations did (compliance) did not impose additional costs for the banks.
	b) Manpower		Less manpower is needed than that of specialized consultants used to implement current frameworks such as ISO 27002. When comparing it to utilizing current employees, the manpower used for the external audit is also less. No single individual had to devote time to interview, report and check.
	c) Time		Because the audit was conducted externally, time was not an issue. Ensuring that employees did not have to attend specialized training impacted the effectiveness and the time the institutions spent on internal audits.
5	The value of the Social Engineering assessment to the institution:	Audit results and post-assessment	Both Bank X and Bank Y will continue doing Social Engineering Assessments as part of their IT Audit efforts because of the experience with this assessment as well as the value of such results.
	a) Measure Training level		Doing a physical assessment (Appendix D) measures the level of training in the organization. It assesses the employees as well as internal policy understanding
	b) Identify Areas of Risk		The physical assessment (Appendix D) identified several areas of risk; shoulder surfing,

			additional internal policies such as shredding of documents
	c) Training Suggestions		Based on the assessment results, a series of training recommendations were made. Both institutions must ensure that employees are properly trained
6	The Holistic IT Audit Framework has less regulatory mismatch than previous model utilized.	Post-assessment and regulatory responses	Because neither Bank previously utilized any framework it is difficult to determine the validity of less regulatory mismatches. However, in both cases, the regulators utilized the IT Audit Results as their assessment. No recommendations were made in the examiner's report of the IT Audit, generally a good sign.
	a) Framework too large for organization size.		Since neither organization utilized any framework previously, this cannot be determined by the case study. However, looking at the cost and time of implementing current frameworks, it can be concluded that these frameworks are simply not appropriate for SMEFIs.
	b) Organization Awareness Lacking.		Regulators recommended that both institutions complete external IT audits, meaning that the institutions did not have adequately trained staff to conduct internal audits. Furthermore, through the IT audit report, several areas of improvements were identified.
	c) Not part of scoping.		Because simple compliance audits were conducted internally, DiD was not a part of scoping for either organization. Encompassing DiD was only done after regulatory exams where it was recommended that the institutions conduct audits that included PT, VA, and compliance.