Dakota State University
Beadle Scholar

Masters Theses & Doctoral Dissertations

Spring 3-1-2010

An Innovative Approach to Information Technology Risk Assessment for Small and Medium Sized Financial Institutions

Ashley L. Podhradsky
Dakota State University

Recommended Citation

Podhradsky, Ashley L., "An Innovative Approach to Information Technology Risk Assessment for Small and Medium Sized Financial Institutions" (2010). *Masters Theses & Doctoral Dissertations*. 277.
https://scholar.dsu.edu/theses/277

An Innovative Approach to Information Technology Risk Assessment for Small and Medium Sized Financial Institutions

A dissertation submitted to Dakota State University in partial fulfillment of the requirements for the degree of

Doctor of Science

In

Information Systems

March, 2010

By

Ashley L. Podhradsky

Dissertation Committee:

Dr. Kevin Streff

Dr. Josh Pauli

Dr. Pat Engebretson

Dr. Surendra Sarnikar

Dr. Mark Hawkes

DISSERTATION APPROVAL FORM

We certify that we have read this project and that, in our opinion, it is satisfactory in scope and quality as a project for the degree of Doctor of Science in Information Systems

Student Name: Ashley Leonora Podhradsky

Dissertation Title: An Innovative Approach to Information Technology Risk Assessment for Small and Medium Sized Financial Institution

Signature (committee chair) Date

Signature (chairperson) Date

Signature (chairperson) Date

Signature (chairperson) Date

Signature (chairperson) Date

ACKNOWLEDGEMENTS

I believe that people are who they are because of the support they have been given. I have been truly blessed for the amount of support I have been given throughout my life. I am very thankful my dissertation committee, family, friends, and above all my wonderful husband Nick.

I am forever indebted to my doctoral committee for all of the support you have given me. My committee consisted of some of DSU's finest faculty; Dr Streff, Dr. Pauli, Dr. Engebretson, Dr. Sarnikar and Dr. Hawkes. All of you helped me make become successful in this process. Dr Streff, thank you for assistance with the topic and to your company, SBS. A very special thank you is owed to Dr. Pauli for all of your revisions while writing my dissertation. You have helped me make my work something I can be proud of.

To my family and friends, those who are here, and those who have passed, you have served as a source of inspiration and encouragement during this process….

To Nick, my dedicated and patient husband. You have supported me in times when it was easy to give support. You have seen me through this process, and I am looking forward to our continued journey together.

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,

Ashley Leonora Podhradsky

ABSTRACT

Table of Contents

List of Figures

List of Tables

1. Introduction

1.1 Background

The world's financial system is constantly under attack by both outside forces and insider attacks. Over the past ten years the financial systems of the world has migrated from traditional brick and mortar buildings to online banking, bill pay and commerce (Benioff, 2005). This shift in transactions has prompted the world to take a serious look at the health of the infrastructure that supports the world's financial system.

Banking and finance has been named as two of the 11 critical infrastructures that are vital to the existence of Americans by the Department of Homeland Security (Lewis, 2006). Banking and finance has been increasingly dependent on the use of information technology and must be highly secure in order to maintain the confidentially, integrity, and availability of banking data and personal data (Streff, 2007).

Data breaches affect millions of people each year, and frequently result in identity theft and personal information being compromised. The Chronology of Data Breaches, published by PrivacyRights.org, list that there have been 262,582,926 data breaches that have involved sensitive information since January of 2005 (Chronology of Data Breaches, 2009). Data breaches can result in the loss of personal information that can lead to identity theft. Financial institutions, by nature, house personal information that can and does result in identity theft after a data breach (Streff, 2007).

Government regulations and legislation oversee the banking and financial sector. The Gramm-Leach-Bliley Act requires all financial institutions to conduct an information technology risk assessment (RA) to identify security risks to non-public customer information (The Gramm-Leach Bliley Act, 1999). Small and medium-sized financial institutions (SMFIs) struggle with this important exercise and often do not understand how to adequately integrate the important act into their banking practices. Therefore, community banks, credit unions and other SMFIs do not typically have a good understanding of what represents real information security risk to their financial institution, and what mitigating countermeasures should be deployed (Podhradsky, 2009).

The RA process identifies the risk associated with the information technology assets of the financial institution, and demonstrates the level of security of each asset, and for the financial institution as a whole. Banks also have a written information security policy, sound security policy guidelines, and well-designed system architecture, as well as provide for physical security, employee education, and testing, as part of an effective program (FDIC FIL 68-99 , 1999). The Federal Deposit Insurance Corporation (FDIC) issued this guidance in 1999 after the Gramm-Leach-Bliley Act (GLBA) was enacted and passed through Congress. Furthermore, the FDIC announced in June of 2003 that it was revising the compliance examination process to focus increased attention on an institution's compliance management system (FDIC FIL 81-05, 2005). Neither of these Financial Institution Letters (FIL’s) from the FDIC provides any direction on how to complete an information technology RA. Neither piece of guidance outlines a repeatable management process to follow to identify threats and make compensating control decisions. Therefore, financial institutions are left to their own devices in figuring out how to conduct a thorough and accurate information technology RA. This becomes very problematic at SMFIs as they typically do not have an information technology individual on staff, let alone an information security professional who is educated and current on information security threats, trends and countermeasures related to the banking industry

(Podhradsky, 2009).

1.2 Problem Definition

Financial institutions, of all sizes, are required to conduct a risk assessment (RA) every year by the FDIC. Large financial institutions, which are typically billions in financial assets, have different abilities and needs compared to smaller financial institutions which are typically millions in financial assets. However, according to the FDIC, both institution sizes have the same regulations and requirements for risk management. There are five specific problems this research aims to answer, which are the following.

1. Different size financial institutions have different resources available to protect IT assets in terms of financial, staffing and time.
2. Current RA practices are done to appease regulators, and not to add value to help make decisions.
3. Little guidance is given to financial institutions by the FDIC on how to conduct a RA.
4. Generic RA models require a high level of understanding that is usually not found in small to medium sized financial institutions.
5. Generic RA models available are mostly either asset or organizational based, not both. SMFIs need a RA that addresses both areas.

Large and small financial institutions have the same FDIC regulation but different resources available in terms of IT staffing, IT budgets, and overall security needs yet overall the FDIC regulations are written in a one-size-fits-all environment.

Small and Medium Sized Financial Institutions (SMFIs) understand they are required by the FDIC to conduct a RA, and they typically approach this process in a manner to appease regulators. The RA process that SMFIs take does not typically result in an accurate RA or add value to their organization (Streff, 2007). RAs for SMFIs need to identify assets and service providers, outline the risk with each asset, list the countermeasures applied to each asset and demonstrate how effective their current mitigating approach is in reducing the risk to the financial institution (Podhradsky, 2009). However, a majority of SMFIs handle the RA process in a completely different fashion where bankers pass around an Excel spreadsheet and various people throughout the bank list assets and the approach taken to secure the device (Streff, 2007). This process not only results in a grossly inaccurate RA, but it also adds no value to the organization. When organizations conduct RA's in this manner, they are only completing this assessment to conciliate government FDIC regulation, and not using it as a tool for their overall risk management process (Streff, 2007).

SMFIs cannot be held solely accountable for the understated RA process. With little guidance from the FDIC, they are approaching the RA process with the same regard as the FDIC. If the FDIC demanded tighter regulations and an accurate assessment, financial institutions would have no choice but to follow suit.

Generic RA models have been developed and deployed across several industries, including banking; however generic RA models assume a high level of understanding about banking assets, risks, threats, risk mitigation, and information security policy which is typically found in larger financial institutions. This type of advanced knowledge is usually not found in management (Gautam, 1989). SMFIs need a different approach to solving their information security RA process than their larger financial institutions counterparts. The generic models implemented by larger financial institutions are not applicable to smaller institutions, due to their IT staffing, IT budget, and IT security limitations. A RA model for a SMFI should also include both an asset and organizational assessment (Streff, 2007). Larger financial organizations have the financial and staffing resources to conduct both an asset and organizational based assessment, however SMFIs need to incorporate both assessments into one single assessment (Streff, 2007).

1.3 Objectives and Approach

The objectives for this research are to address the five challenges of facing SMFIs when conducting a RA outlined in secion1.2. An RA model for SMFIs needs to address FDIC regulations, IT staffing limitations, financial resource restrictions, knowledge limitations, assets and the organization, all while being tailored towards the banking industry. The new RA model, Small to Medium Entity Risk Assessment Model, SMERAM, works to address the unique needs of SMFIs.

The first problem SMERAM aims to address is problem 1, different size financial institutions have different resources available to protect IT assets. IT staffing limitations are met with SMERAM as financial institutions do not need a dedicated IT department or staff member on-site to complete the RA. Risk management is a management responsibility and a member of the management team can conduct the RA (Streff, 2007). SMERAM has been specifically created to be completed by both technical and non-technical personnel. Other Generic RA models require a certified consultant or full time

IT staff to complete the RA, while SMERAM does not. This unique characteristic of SMERAM reduces the cost of implementation and maintenance which is not typically seen in other generic RA models.

The smaller IT budgets associated with SMFIs are also factored into SMERAM. Most generic RA models such as ISO, NIST, or COBIT require a certified consultant or IT staff to complete the RA, while SMERAM does not, which results in reduced costs for completing a valid and value added RA. An ISO certification for example, costs upwards of $50,000 for a medium sized institution; this is well beyond the reach of most SMFIs (Martin, 2002). Also, SMERAM does not have any subscription costs associated with its implementation, which is unlike other generic RA models.

The second problem outlined in 1.2 that SMERAM addresses is the current practices of conducting a RA in SMFIs. Currently, the majority of SMFIs handle the FDIC regulated RA process in a manner that appeases regulators, not in a fashion that helps the financial institution add value to their organization. SMERAM is designed to show the financial institution what IT assets they have, what threats are associated with those assets, and how mitigating practices can reduce the risk their IT assets impose. From this information, the SMFI can determine what steps should be taken to further secure their organization.

The third problem as outlined in 1.2 that SMERAM aims to address is that little guidance is given to SMFIs by the FDIC. SMERAM meets FDIC FIL guidelines as it is designed for the RA to be completed every year, and reviewed on an ongoing basis. SMERAM encourages SMFIs to update their RA whenever there is a major change in their network or information technology infrastructure, which keeps the RA an adaptive and living part of the information security program. This approach not only adds value to the organization as it helps the financial institution identify and outline their current security posture and allows them make informed decisions regarding their information technology purchases and upgrades but also meets FDIC regulatory standards.

The fourth problem that SMERAM addresses is the knowledge limitations found in SMFIs when dealing with information technology security. The FDIC states that risk management is a management responsibility, as a result, the management teams in SMFIs need to conduct the annual RA. In order to do this properly, the SMFI management team will need assistance in assets, threats, and controls. Appendixes C, F, and E, respectively, have this information for typical SMFIs.

The fifth problem SMERAM aims to address is most generic RA models are either asset or organizational based, not both. SMERAM further adds value to the financial institution as it completes both an asset and organizational RA. Not all generic RA models evaluate security in both an asset and organizational level as SMERAM does. This approach saves time and money for SMFIs as only one RA has to be completed.

The unique needs of SMFIs are documented in Table 1, Generic Models vs SMERAM.

Table 1 Generic Models vs SMERAM

SMFI Needs	Generic Models	SMERAM
FDIC Federal Institution Letters	Not defined to financial organizations- applies to many	Meets FDIC guidelines as it is honed specifically to the financial industry

	industries	
IT Staff	Usually needed, added cost	Management Process- No additional staff required
Credential Consultant needed	Usually needed, added cost	Management Process- No additional staff required
Configured to banking industry	No	Assets/ Threats/ Countermeasures specific to banking industry
Asset or Organizational	Varies	Both asset and organizational based RA are completed with SMERAM

1.4 Methodology

This research will utilize the design science research methodology, as an IT artifact will be created. Hevner, et al. present the guidelines for design science research in the paper "Design Science in Information Systems Research" for validation and evaluation (Hevner, 2004). This research will employ each of the seven guidelines to provide a methodical evaluation of the research IT artifact.

The artifacts shaped from this research include a risk assessment model for SMFIs. This model will be created and evaluated with Design Science guidelines.

The seven guidelines outlined in the "Design Science in Information Systems Research" are listed in Table 2, along with the definition and the approach SMERAM takes to meet the guidelines (Hevner, 2004).

Table 2 Hevner Design Science Guidelines

Guideline	Description	SMERAM
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	The artifact, SMERAM, is created in accordance of Design Science guidelines
2- Problem Relevance	The objective of design-science research is to develop technology-based solutions to important, and relevant business problems	SMERAM was designed to address the staffing and financial limitations of SMFIs all while meeting and exceeding FDIC FIL regulation

3- Design Evaluation	The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods	SMERAM was effectively tested and deployed in a community bank
4- Research Contributions	Effective design-science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/ design methodologies	The SMERAM RA model for SMFIs is the contribution to the security and SMFI fields
5- Research Rigor	Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact	SMERAM was built on accepted generic RA models such as ISO, NIST, COBIT, and CORAS while being honed to the financial industry
6- Design as a Search Process	The search for an effective artifact requires utilization available means to reach	SMERAM was developed through a prototype environment

	desired ends while satisfying laws in the problem environment	after studying various established generic RA models
7- Communication of Research	Design-science research must be presented effectively both to technology-orientated as well as management-orientated audiences	SMERAM is designed to be used effectively by both technical and non-technical personnel; the intended audience is bank management

This research will also employ the qualitative research method approach of case study. A single case study was conducted to test the effectiveness of SMERAM in a financial institution while addressing the unique needs of staffing and financial limitations. Also, the overall quality of information technology assets along with the organization as a whole was evaluated.

2. Literature review

2.1 Background

Information technology is synonymous with responsibility in terms of daily processes, upkeep, and upgrading. However, none is more important than information security risk identification and mitigation. Although very little scientific research has been conducted in response to information system risk mitigation.

The goal of this research is to define what a risk assessment is, support the audience in developing an in-depth understanding of the risk assessment process while emphasizing several seminal works pertaining to information technology risk assessment. Also, several current generic RA for assessing risk in technology systems will be discussed. Ultimately, it is the intention of this research to demonstrate the importance of the information RA process and point out current gaps in the field in relation to generic RA models. The research also produces a generic RA model that has been honed for the use in SMFIs, the model is Small to Medium Entity Risk Assessment Model (SMERAM). Finally, this research will conclude with several suggestions for further research and development.

The study and analysis of risk is a customary practice throughout several key industries such as insurance, medical, finance, economics along with many others. The concept of studying, analyzing and scientifically outlining the risk assessment process explicitly for use in safeguarding information systems have traditionally been overshadowed in favor of more broadly applicable information security standards.

For the purpose of this research the definition of an information technology RA will be as follows: Risk assessments are the process of accurately and consistently measuring threats, or the potential of threats with an information system (Streff, 2007). Streff outlines that risk based management means that major decisions that are made regarding information security analyze the impact a change will have in either increasing or decreasing the amount of risk there is to informational assets in the bank (Streff, 2007).

Historically, when attempting to conduct an RA, organizations have been left to sort through several weighty generic standards such as OCTAVE, CORAS, ISO, NIST, or COBIT, among others. Attempting to apply these generic standards across all industries, in an identical fashion, can make for a time consuming and frustrating experience, especially for SMFIs. Many organizations, mostly smaller institutions, find that attempting to implement a generic standard fails to adequately implement the standard and as a result end up with throwing together parts of different standards, or worse, no standard at all. By not implementing a scientific standard the company is opening themselves up to failure with their information security program, which puts their customer's financial data in jeopardy (Streff, 2007).

As businesses continue to grow and become more dependent on large information systems, managers and organizations must learn to effectively identify, and assess risks to these systems. As pointed out in the article "Bayesian Probabilistic Risk Analysis" (Ali, 1985) the process of risk management includes identifying a system's weakness as well as effectively reducing the probability of the particular system from being impacted by the exposed weakness. Bayesian risk analyses were originally developed for use in the nuclear power industry.

A measurement of risk, according to Ali, can be determined by answering the following four fundamental questions (Ali, 1985);

- What can go wrong?
- How frequently can it be expected to happen?
- What would be it consequences?
- How certain are we about the answers to the first three questions (Ali, 1985).

Although the use of technology and the advancement of the RA process have drastically changed modern information system risk, the answers to these four questions can still provide a highly accurate and useful assessment of information system risk (Ali, 1985).

Network intruders work tirelessly to develop the newest attacks patterns and processes to exploit vulnerabilities and gain unauthorized access to networks. As a result, organizations need to vigilantly work to protect their information system assets by studying and learning the current attack processes (Myerson, 2002). It is not enough for an organization to simply have a risk assessment process in place; your risk assessment must be an active and adaptive part of the entire information security program (Podhradsky, 2008). This includes, but is not limited to, regularly updating the process to allow for flexibility in dealing with new threats and vulnerabilities (Myerson, 2002). If a risk assessment is completed only once a year it is merely a snapshot of that point in time, and it cannot be used as a valid and honest representation of the institutions security posture. Whereas an adaptive and updated risk assessment will change when your network or systems changes, this entails updating your risk assessment at least quarterly, or whenever there is significant changes made to the network. This method will result in an accurate information security risk assessment and current security posture for the institution.

The ability to safely and accurately defend an information system depends upon completely understanding the threats associated with that information system and applying controls and commensurate with the defined level of risk. This process of risk assessment helps organizations and managers appropriately spend time and money defending and protecting assets which need it most. Ultimately risk assessment can be seen as a productivity tool that saves the organization time, money along with their reputation.

RA’s examine the impact and probability that threats pose to an information system. A RA computes the probability of a specific threat taking place while also determining the impact of the specific threat. When organizations complete a risk assessment, they can begin to compute their risk level (Blakley, 2001).

There are several common fundamental themes within varying RA’s. For example, Woemer states that risk should be calculated as risk = impact x probability (Woerner, 2007). There are many different and widely used models to complete the actual risk assessment. Some models are built into an automated tool, and some are completed on paper. In the paper “Applications of Qualitative Modeling to Knowledge-Based Risk Assessment Studies”, Gautam, et al, the focus is on system failure to help identify risk (Gautam, 1989). The authors showcase a qualitative modeling technique to augment the RA process to assist in the design of an RA automated tool.

Gautam et al believe that the mutual use of a knowledge based system and qualitative problem solving can result in the development of a generic RA tool. They further state that by designing a generic tool, it can be widely implemented across several industries (Gautam, 1989). The issue with this approach within SMFIs is that by using a generic tool, the process is not unique to any one industry. In order to complete an accurate RA one would have to have all of the information about the information systems within the organization. Whereas with a tool or model that is designed for the specific audience there is a more user-friendly environment to complete the RA process. Depending on the industry there are very specific information systems; banking, ethanol, hospitals and education all have specific information systems tailored to their venue. A generic tool would require much more time and resources to complete than a model or tool that is tailored and designed for the industry. For SMFIs to use a generic tool they would have to first have the understanding of the information systems in within their organization and second have the manpower to use the tool, however they typically have limited resources on both fronts.

Organizations are continuing to lean on information systems for all aspect of their business, and they need to understand the risk associated with their business systems. Conducting a risk assessment will show the organization how to adequately protect their information and business assets.

One of the primary advantages of developing a knowledge based system using fault tree analysis is that it provides for an excellent tool to model “what-if” scenarios. By examining the potential system failures organizations and managers can get a broad and accurate picture of potential risk. The organization would then have a clear picture as to where to invest their information security dollars (Streff, 2008).

Bob Blakley, Ellen McDermott and Dan Geer discuss the process of measuring risk through the concept of Annualized Loss Expectation. (Blakley et al., 2001) Annualized Loss Expectation helps to quantify risk in terms of a financial definition where companies predict a specific value or cost associated with the occurrence of a particular risk. Using this model, an organization calculates risk by multiplying a specific dollar amount against the probability of the risk's occurrence. Cost is estimated by totaling both the direct and indirect dollar amounts, over the course of one year, which are related to the occurrence of the risk. Examples of direct and indirect dollar amounts include physical damage, equipment replacement, labor costs to repair, decreased employee productivity, lost sales, reputation damage, and legal costs.   Probability is determined by weighing the likelihood of a risk event on a 1 to "x" scale. This probability is then multiplied by the cost associated with the annual loss resulting in a final dollar value which is representative of risk for the particular system.

For example, the cost of a hacker defacing a company website is determined to be $2,000,000 while the probability of a hacker defacing the company's website is determined to be 1 in 15,000, the ALE measurement would be ($2,000,000 x 1/15,000 = $133)

Others have taken a different approach to defining the risk assessment process. Ye, et al, presented a six step approach to tackling risk assessment. (Ye, Barry, & Betsy, 2006) Their workflow begins with identifying a cost factor rating system. Once the rating system has been defined, risks are identified. Next the step is assigning risk probability, this is followed by analyzing risk impact, at this point an overall risk can be normalized on a scale from 1-100. The scale of 1-100 can then be disseminated into the following categories. Systems with an overall risk from:

- 0-5 are considered “low risk”,
- 5-15 are marked as “moderate risk”,
- 15-50 are said to be “high risk” while
- 50-100 should be labeled as “very high risk”. (Ye et al., 2006).

The final step is to offer ways of reducing the presented risk. While Ye et. al., offer a systematic approach for the RA process, SMEFI’s would find the approach daunting and un manageable for their IT RA. The result would be inaccurate RA results, which would result in the wrong protection profile be adapted for the SMEFI. This would put customers financial information in jeopardy.

Organizations often make the assumption that increased budgeting and spending on security investments will lead to a direct decrease in overall information system risk. This thinking is clearly demonstrated in the article “A model for evaluating IT Security Investments” (Cavusoglu, Mishra, & Raghunathan, 2004). The level of risk obtained from an organization’s completed RA often determines the organization’s willingness to invest in appropriate security controls. This type of organizational philosophy is another reason demonstrating the importance of an appropriate and accurate risk assessment, there are clear implications to an organizations financial health and bottom line.

Along this same line of thought, Hamdi and Boudriga (Hamdi & Boudriga, 2003) explain that the process of assessing risk is often too difficult to perform accurately without the use of automated software. Because of the complexity involved in accurate

RA, they argue there is a need for the creation of an automated system. According to Hamdi & Boudriga, the tool must ultimately assist in security decisions. Furthermore the authors point out that risk assessment can be sub-divided into two categories. Qualitative risk assessment expresses risk in subjective terminology while quantitative risk assessment attempts to assign values associated with the occurrence of a particular threat or risk.

2.2 Disastrous Results from Under-valuing the Risk Assessment Process

The result of undervaluing the RA process and not having proper documentation can lead to devastating results. Organizations, whether non-profit or for profit, that have a data breach face much more than monetary losses, a hit to their reputation also occurs. Table XX below is an overview of large data breaches that may have been avoided if proper controls were enacted to secure their data.

Table 3 Historic Data Breaches

Historic Data Breaches

Year	Company	Number of Accounts Compromised
2006	Veterans Administration	26.5 million plus
2007	TJX Enterprises	100 million
2008	Heartland Payment Systems / Hannaford Payment Systems	130 million

An example of this pressing issue is the Veterans Administrations who had a laptop stolen that contained confidential records of over 26.5 million retired veterans (Burger, 2006). The laptop was stolen from the home of a Veterans Affairs employee and resulted in the largest security breach in the history of the United States Government (Burger, 2006). It is important to note that this was not the result of a hacker or script kiddy but rather the result of simple human error and physical security issues (Burger, 2006). Proper documentation and a risk assessment process should have prevented the employee from leaving the government office with such a valuable asset. Further documentation should have mandated that storing that type of secure data on a portable device is prohibited (Burger, 2006). Information which is considered secure in nature, such as personal identifying information, belongs on a server, with proper credentials used to access the information.

For an organization to defend an information system they must have an understanding of the risk associated with the asset along with the knowledge for applying the appropriate controls to mitigate risk. This aspect of the RA process assists an organization in appropriately using resources to defend and protect organizational assets and data. Ultimately RA’s can be seen as a productivity tool that saves the organization time, money, and reputation, which would have served the department of Veteran Affairs a substantial amount of money, time, resources, and a hit to their reputation (Burger, 2006).

TJX Enterprises had one of the largest data breaches ever recorded. A TJX insider, requesting anonymity had the following to say about the infamous security breach that affected over 100 million accounts (Dawson, 2007):

> *"Poorly secured in-store computer kiosks are at least partly to blame for acting as gateways to the company's IT systems, the kiosks, located in many of TJX's retail stores, let people apply for jobs electronically but also allowed direct access to the company's network, as they weren't protected by firewalls. 'The people who started the breach opened up the back of those terminals and used USB drives to load software onto those terminals,' says the source. In a March filing with the Securities and Exchange Commission, TJX acknowledged finding 'suspicious software' on its computer systems.* (Dawson, 2007)*"*

The TJX data breach, which affected over 100 million credit card accounts, was discovered in 2007 (PrivacyRights, 2009).   TJX lost not only money, but also credibility due to their inadequate information security policies. Hackers gained access to the credit and debit card sever that house millions of card numbers. In addition to the credit card numbers, names, addresses, social security numbers and drivers license numbers were also stolen from TJX (Dawson, 2007). This type of personal information is what hackers look to steal when they are trying to steal an identity (Streff, 2006).

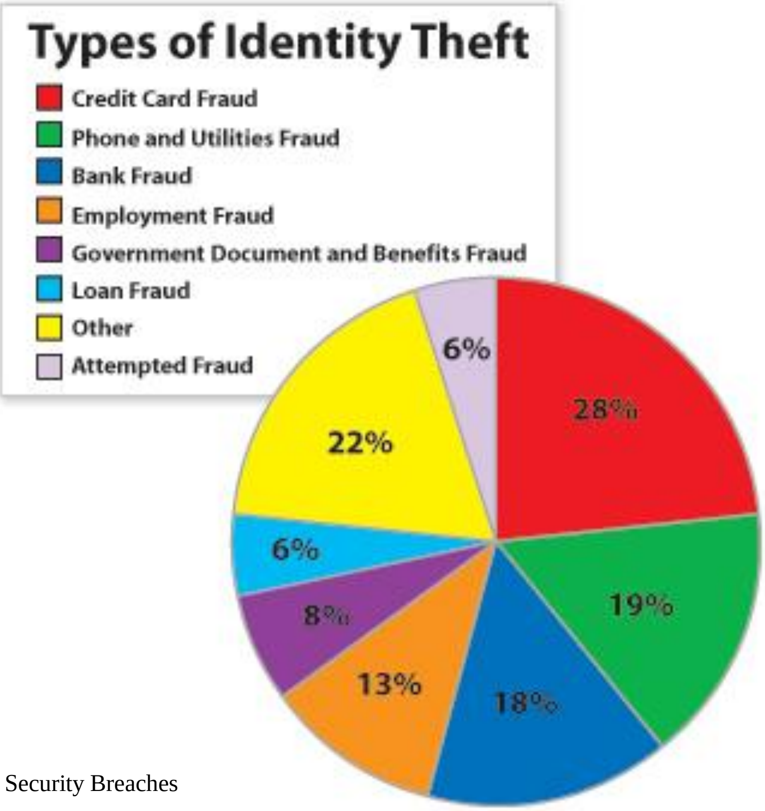


Figure 1- Types of Fraud / Security Breaches

Heartland, another example of a data breach involving credit / debit card fraud occurred in 2008. Heartland payment systems processes over 100 million transactions each month, as a result of that magnitude of data crossing their lines, it was very difficult to be able to identify the amount of data compromised due to inadequate security. At last count, the Heartland data breach affected over 130 million records when combined with the Hannaford breach (Chronology of Data Breaches, 2009).

According to Barnett Insurance agency, in 2008 credit card fraud accounts for over 28% of reported security breaches and fraud reports. The banking sector had 18% of reported security breaches, which means that overall the financial sector is accountable for over 56% of all security data breaches and fraud reports This is indicated in Figure 1, Types of Fraud / Security Breaches.

Data Breaches, which are a direct result of inadequate security, can be reduced when a proper RA is completed (Data Security Breach Statistics, 2009). The RA process identifies risk associated with information technology assets, which demonstrates the security level of each asset (Streff, 2007). When organizations fail to properly secure each information technology asset the results can be disastrous. Figures 2, 3, and 4 below depict the amount of records comprised in 2006, 2007, and 2008 respectively as a result of a data breach (Data Security Breach Statistics, 2009).

In 2006, theft was the overall leader in records compromised followed malicious insiders, carless/ untrained insider, hacking and 3rd party service providers followed (Data Security Breach Statistics, 2009). Theft accounted for over 35,000,000 breached records. Theft, which is part of physical security, should be a part of any RA process. Controls should also be in place for malicious insiders, hacking and 3rd party service providers which are all part of an overall RA process.

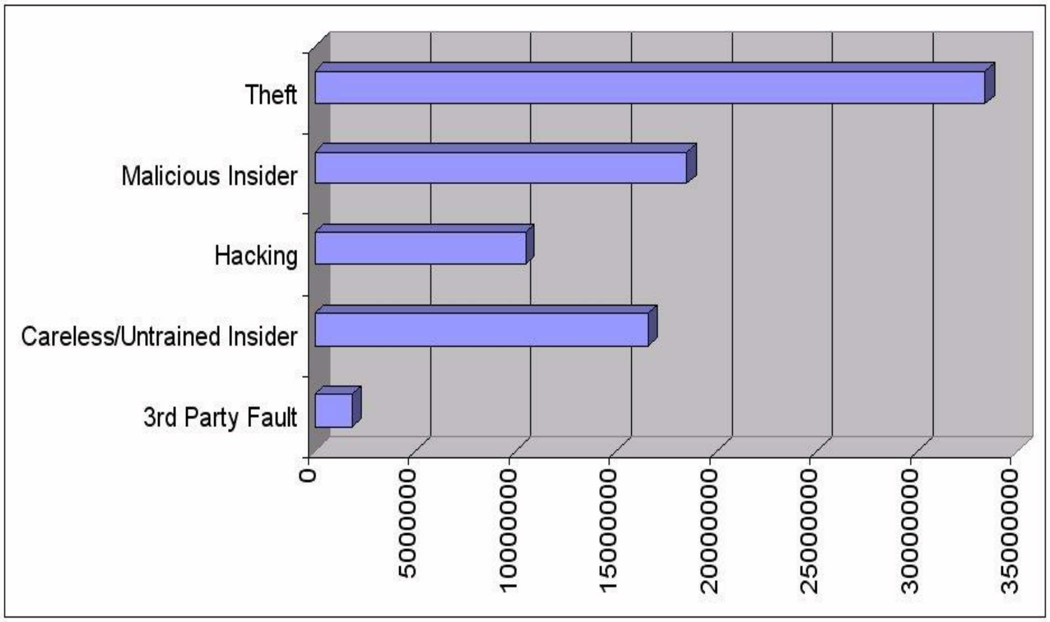


Figure 1 Records Compromised by Breach Source-2006

In 2007, hacking was the overall leader in records compromised followed by malicious insiders, theft, carless/ untrained insider, 3rd party service providers followed worms and viruses (Data Security Breach Statistics, 2009). Hacking accounted for over 100,000,000 breached records.

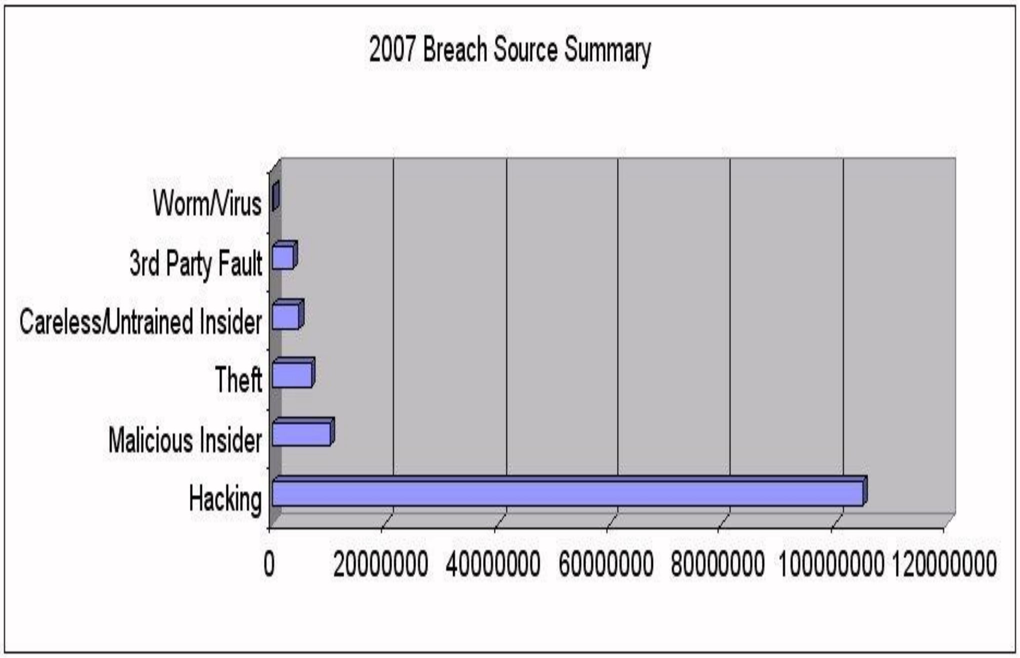


Figure 2 Records Compromised by Breach Source- 2007

In 2008, similar to 2007, hacking was the overall leader in records compromised followed by malicious insiders, theft, carless/ untrained insider, and 3rd party service providers (Data Security Breach Statistics, 2009). Hacking accounted for over 180,000,000 breached records.

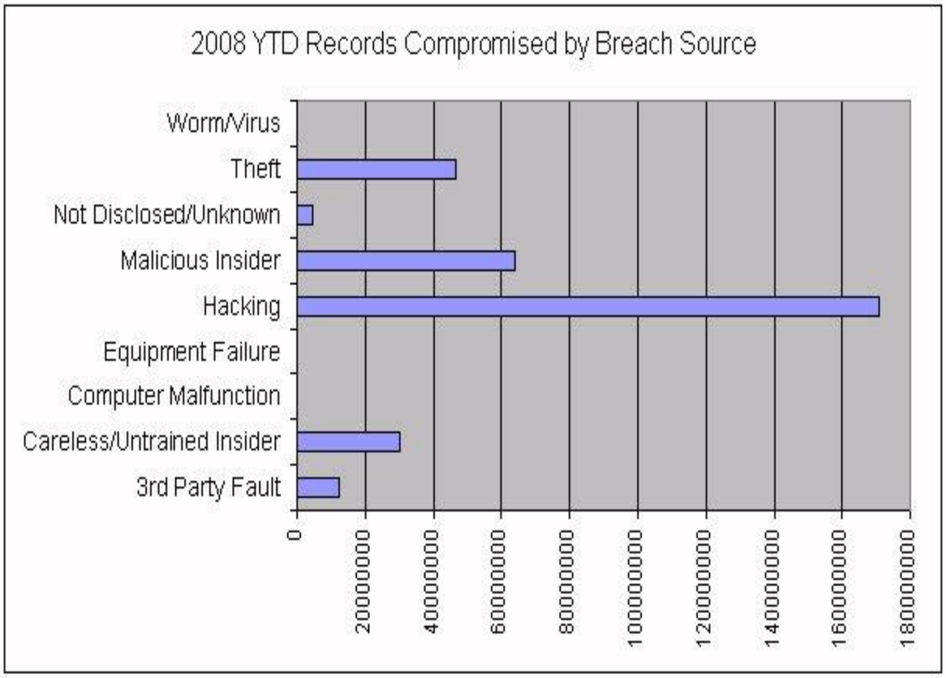


Figure 3 Records Compromised by Breach Source- 2008

Over 2006, 2007, and 2008 hacking, malicious insiders, theft, and careless or untrained insiders resulted in billions of compromised accounts (Data Security Breach Statistics, 2009). These compromised accounts can contain personal identifying information such as SSN's, names, addresses, date of birth that is used to steal identities (Podhradsky, 2008). By have a valid and defined RA in process, the number of compromised records will naturally decrease. RA assess the overall risk with an asset and demonstrate where security resources should be allocated (Streff, 2007).

2.3 Regulation

The financial industry is a highly regulated environment due to the financial and personal information that is stored at many financial institutions. This information has an inherent attraction to identity thieves. Table 4, Regulation for Financial Institutions, outlines the major regulation that governs financial institutions, whether small or large.

Table 4 Regulation for Financial Institutions

Regulation	Purpose or Intent
FDIC FIL 68-99	FDIC FIL 68-99 states banks should have a written information security policy, sounds security policy guidelines, and well-designed system architecture, as part of an overall security policy. However, it does not state how to conduct a RA, or with what methodology. Available in Appendix A.
Gramm-Leach-Bliley Act (GLBA)	Requires all financial institutions to conduct an information security RA to identify risk to non-public customer information. Available in Appendix C.
FDIC FIL 81-05	FDIC 81-05 was written to focus more attention on the RA process and information security program for information technology assets. However, there still isn't a repeatable management process listed for the RA

	process. Available in Appendix B.

The Gramm-Leach-Bliley Act (GLBA) of 1999 requires all financial institutions to conduct an information technology risk assessment to identify security risks to non-public customer information (The Gramm-Leach Bliley Act, 1999). Small and medium-sized financial institutions struggle with this important exercise and often do not understand how to adequately integrate the act into their banking practices. Therefore, community banks, credit unions and other small and medium-sized financial institutions do not have a good understanding of what represents real information security risk to their financial institution, and what mitigating countermeasures should be deployed.

The RA process provides a framework for establishing policy guidelines and identifying the risk assessment tools and practices that may be appropriate for an institution (Streff, 2007). According to the FDIC banks should have a written information security policy, sound security policy guidelines, and well-designed system architecture, as well as provide for physical security, employee education, and testing, as part of an effective program (FDIC FIL 68-99 , 1999). The FDIC issued this guidance in 1999 after the Gramm-Leach-Bliley ACT was passed. Further, The FDIC announced in June of 2003 that it was revising the compliance examination process to focus increased attention on an institution's compliance management system (FDIC FIL 81-05, 2005).

Together these two pieces of regulation are the sole guidelines from the FDIC and can be found in the appendix A and appendix B respectively of this paper. Neither of these two Financial Institution Letters from the FDIC provides any direction on how to complete an information technology RA. Nor does either piece of guidance outline a repeatable management process to follow to identify threats and make compensating control decisions. Therefore, small and medium sized financial institutions are left to their own devices in figuring out how to conduct a thorough, accurate information technology risk assessment. This becomes very problematic at small and medium sized financial institutions as they typically do not have an information technology individual on staff, let alone an information security professional who is educated and current on information security threats, trends and countermeasures.

In August of 2005, the FDIC updated the procedures and processes for member banks to include a risk-focused examination concentrating on the area of information technology for 3rd party entities. This was the first update to their Financial Institution Letters that dealt specifically with information security in nearly 8 years; to date, there have not been any other updates.

The highlights of the 2003 FIL focused on member banks implementing an information security program as well as asking financial institutions to define a process for securing information assets (FDIC FIL 81-05, 2005). The FDIC's new Information Technology Risk Management Program (IT-RMP) applied universally to all FDIC Insured banks despite their level of technology or the size of the financial institution. As outlined in the FIL-81-2005 (FDIC FIL 81-05, 2005). The process of conducting a technology focused risk assessment is specifically listed as a requirement for compliance with the IT-RMP FDIC FIL 81-05 can be found in Appendix A.

The FDIC stopped short of spelling out the specific details for "how to" conduct an information system risk assessment, rather they choose to let each institution follow its own path for assessing risk. There is also no guidance on the use of an automated tool to aid in their assessment process. This causes serious issues to SMFIs due to their limited knowledge and resources to conduct a viable risk assessment.

2.5 Generic Risk Assessment Models

National Institute of Standards and Technology

The National Institute of Standards and Technology, NIST, attempt's to promote guidance for development of technical standards and processes. In July of 2002, NIST introduced a special publication directed towards the development of risk management for information technology systems. In the publication, NIST outlines and defines the process of risk assessment as not only a key component to securing information systems but also clearly states that the process is a management responsibility (Stoneburner, 2002). This new framework suggests that technology risk assessments should be conducted by an organization's management team, and not necessarily its technical support staff.

Similar to the FDIC, NIST defines risk assessment as the first step of an overall risk management plan. NIST incorporates the RA process into the system development life cycle (SDLC). NIST defines risk assessment as "the likelihood of a given threat-source's exercising a particular potential vulnerability and the resulting impact of that adverse event on the organization" (Stoneburner, 2002). In order to accurately assign a risk rating, NIST states that an organization must measure both probability and impact (Stoneburner, 2002). Determining the probability measurement requires an organization to examine their unique vulnerabilities, particular threats, and individual controls for each system. In order to assign and produce an impact score, the organization must rate the criticality and sensitivity of each system. Specifically, NIST describes 9 primary steps in the risk assessment process which are outlined in Table 5, NIST Risk Assessment Model (Stoneburner, 2002).

Table 5 NIST

NIST Step	Description
1- System Characterization	Characterization of the IT system being analyzes along with the current security and system boundary
2- Threat Identification	A threat statement containing an overview of threat sources that could compromise system vulnerabilities
3- Vulnerability Identification	A overview of system vulnerabilities that be leveraged by potential threat sources listed in step 2
4- Control Analysis	A overview of current or future controls implemented on IT systems to mitigate potential vulnerabilities and reduce the impact of any successfully compromised vulnerabilities
5- Likelihood	Likelihood rating, such as high, medium and

	Determination	low
6-	**Impact Analysis**	A range of high, medium and low applied to an impact
7-	**Risk Determination**	The risk level in terms of high, medium or low
8-	**Control Recommendations**	Control recommendations and other alternative solutions to mitigate risk
9-	**Results Documentation**	The risk assessment report which includes threats, and counteracting vulnerabilities. Also risk measurements and recommendations for further control implementation

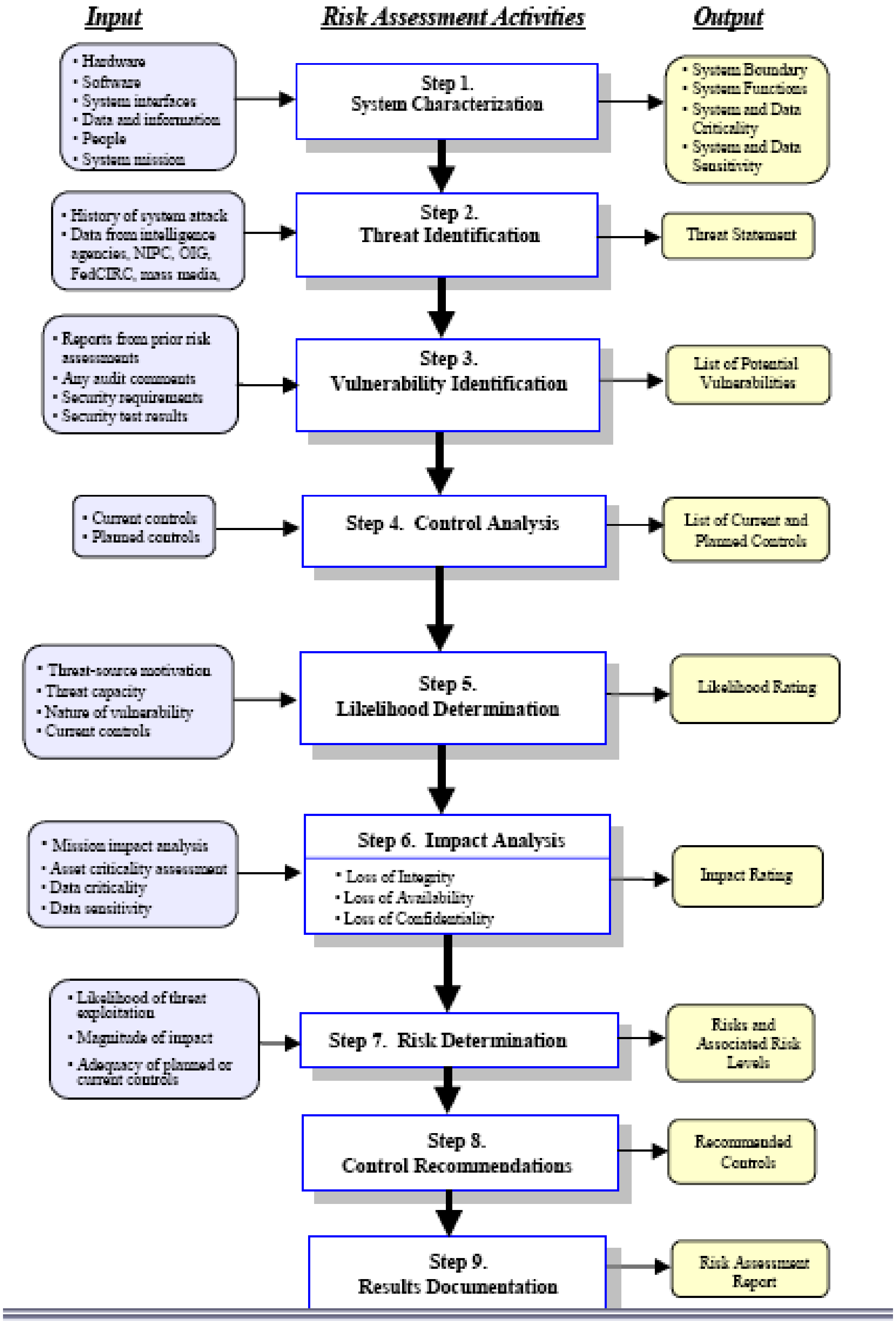


Figure 4 NIST RA STEPS

International Standards Organizations (ISO)

The International Standards Organization, ISO, has developed a risk assessment process that is outlined in Table 6, ISO Risk Assessment Model.

Table 6 ISO Risk Assessment Model

ISO Step	Description
Security Policy	The security policy of the organization is both created and evaluated. An example is the organizations password policy.
Organizational Security	Security at the organization level, not just the system or asset level. Examples are a business continuity plan and Information Security Programs.
Asset Classification and Control	Assets are classified depending on their security needs. An example is assigning ownership for business assets.
Personnel Security	The security risk from people is evaluated and calculated. An examples is non-disclosure agreements with new employees.

Physical and Environmental Security	The security of assets and the organization is evaluated at the physical level. An example is access control to a server room using keys or biometrics.
Communications and Operations Management	Used to ensure the correct and secure operation of information processing facilities. Examples are backup policies and documentation of business plans.
Access Control	Access control is established for assets based on personnel needs. An example is allowing only specific personnel access to information technology assets such as network shares or routers.
Systems Development	Software development creates and assigns ownership to information systems. An example is controlling software code during the software development lifecycle.
Business Continuity	The creation and validation of a practiced plan for how an

	organization will recover after a natural or man-made disruption. Developing, testing, and training on the Business Continuity plan is essential for reduced downtime. An example is the Y2K scare that occurred in the late 90’s; businesses worked to protect their information technology assets.

The ISO standard is often referred to as a “mile wide, and inch deep (Quality Management Cocktail: ISO, Lean, Six Sigma)”. The ISO standards cover many topics, but none in depth. This results in confusion on the best way to adequately protect information security assets by conducting a risk assessment.

The ISO standard is often referred to as “a mile wide and an inch deep (Westguard, 2005).” ISO lacks in the area of asset management; the standard tells you to inventory your assets but does not lay out a recommended process. The lack of concern of asset management is a valid concern of ISO. Many data breaches are a direct result to the lack proper asset management, the VA is a fantastic example of what the lack of asset management can result it. The VA had over 26.5 million records compromised due to inadequate asset management. (A Chronology of Data Breaches). With such a high rate of data breached related to the loss of assets, not having my information related to asset management within the ISO standard is a great concern.

The access control section of the ISO model includes a great section on including mobile technology. This is important because in addition to physical access to mobile technology, regular access is needed. Another area of concern would by cryptography. The ISO standard does not have any significant reference to cryptography, the CISSP standard has cryptography as its own domain which is outlined in over 100 pages (Peltier, 2005). Also there is little discussion on wireless access. With wireless access becoming more prevalent every day with lack of consideration on wireless standards is also a concern.

Cost of Risk Assessment Software (CORAS)

CORAS is a standard developed by a consortium of European Union members in an effort to improve and streamline the RA process. CORAS has a strong emphasis on maintaining the "confidentiality, integrity, availability and non-repudiation, accountability, authenticity, and reliability of IT systems (Siv-Hilde Houmb)". CORAS works toward considerations for both human operators and the information systems. The CORAS framework relies greatly on the use of modeling to provide the risk assessment. The methodology has implemented Unified Modeling Language (UML) along with diagrams to define associations. The CORAS framework is a 4 part series as demonstrated in Table 7, CORAS Risk Assessment Framework.

Table 7 CORAS

CORAS Steps	Description
System Risk Documentation	Risks that are associated with specific assets are documented and categorized.
Risk Management Process	Integrates risk management practices into the overall RA process. This includes confidentiality, integrity, availability and non-repudiation, accountability, authenticity, and reliability of IT systems.
Risk Integration and Developmental Process	Risk analysis is tightly integrated into a UML and RM-ODP setting
Tool Integration	The CORAS RA process involves integrating a predefined tool into the RA process. The tool has been developed by the CORAS development team.

One of the unique characteristics of this type of risk assessment is that it combines different aspects from several types of risk assessments (Siv-Hilde Houmb). (Eheo Dimitrakos)

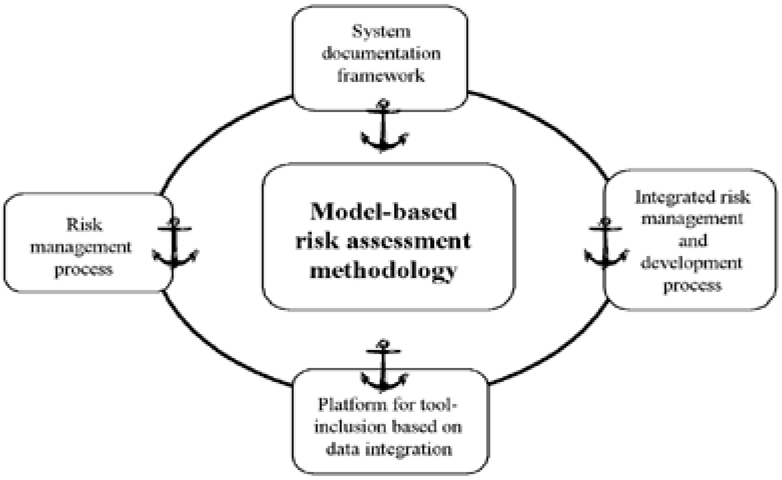

System documentation framework
Risk management process
Model-based risk assessment methodology
Integrated risk management and development process
Platform for tool-inclusion based on data integration

Figure 5 CORAS Methodology

Control Objectives for Information and related Technology

The Control Objectives for Information and related Technology (COBIT) is a risk assessment framework developed by the Information Systems Audit and Control Association (ISACA), and is outlined in Table 8, COBIT Risk Assessment Framework.

COBIT , an IT governance framework, is a supporting toolset that allows upper management to bridge the gap between technical issues, control requirements, and business risks. COBIT lays the foundation for clear policy development and good practice policy for information systems throughout the entire organizations. COBIT emphasizes the importance for regulatory compliance, regardless of industry, and assists the organization in increasing the value derived from information technology systems (ISACA).

Table 8 COBIT

COBIT Step	Description
Plan and Organize	Defines a strategic IT plan and direction which includes information architecture, technological direction, IT Processes, organization and relationships related to IT.
Acquire and Implement	This step involves identifying current IT requirements, acquiring the appropriate technology, and integrating it throughout the organizations business processes. This step also includes the creation of a maintenance plan that organizations should implement in order to extend the life of an IT system and its components.
Deliver and Support	This step focuses on the delivery aspects of the information system. Execution of applications and results of execution are included in this step. This step includes security

	issues and training.
Monitor & Evaluate	A company’s overall strategy in assessing the unique needs of the organization and effectiveness of the current IT system is evaluated. The organization needs to determine if the initial purpose for purchasing the IT asset has been meet and if it meets the objectives for which it was designed. The asset also needs to evaluate the controls necessary to comply with regulatory requirements

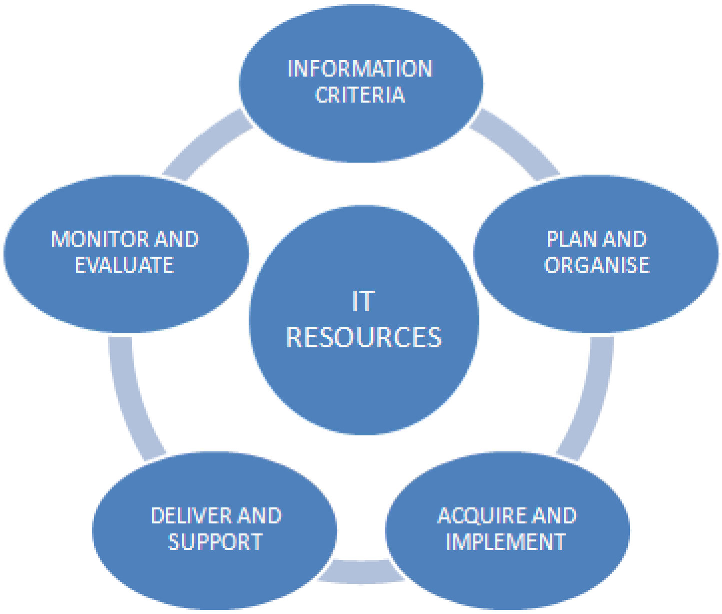


Figure 6 COBIT Framework

COBIT also attempts to account for some “human” risk by asking the assessment process to include questions about job satisfaction, potential lay-offs, and attitudes towards ethics. Including this part in the RA process is important, because human error accounts for the majority of data breaches (Chronology of Data Breaches, 2009).

Operationally Critical, Threat, Asset and Vulnerability Evaluation (OCTAVE)

Finally, OCTAVE is a risk analysis approach which attempts to define information system risk by evaluating the risk based on four elements; asset, threat, impact and vulnerability (Alberts, 2002). OCTAVE was created at Carnegie Mellon University in conjunction with the Software Engineering Institute. The OCTAVE Risk Assessment framework is outlined in Table X, OCTAVE Risk Assessment Framework.

Table 9 OCTAVE

OCTAVE Step	Description
Asset	The organization determines the information technology assets they have.
Threat	The organization determines the threats that are inherent to each information technology asset. Threats include man made or natural disasters.
Impact	The organization determines the chances each threat has of occurring. For example, if the organization is in the Midwest, there is a low chance of a typhoon hitting the organization.

Vulnerability Evaluation	The organization determines how vulnerable their information systems are and they rank them in the order controls should be applied.

With OCTAVE, the first step in managing risk is to understand what the risks are for the organization's key assets. The organization’s mission statement is also analyzed in relation to the risk assessment process, meaning that mission critical assets are protected more than non mission critical assets. Once assets are identified, organizational personnel can draft plans to mitigate the inherent risks that will have the highest impact on the organization's assets (Dorofee).

OCTAVE’S four steps; Threat, Asset, and Vulnerability Evaluation outline the essential steps in a systematic, comprehensive, context-driven information security risk assessment (Dorofee). When implementing the OCTAVE RA, an organization can make information-protection decisions based on risks to the confidentiality, integrity, and availability of critical information technology assets (OCTAVE Information).

Organizations that implement the OCTAVE RA model include the United States Department of Defense as well as the Computer Emergency Response Team (CERT) of the United Kingdome Ministry of Defense. In addition to these notable organizations others include those in health care as OCTAVE supports HIPPA compliance, insurance, and many others (OCTAVE Information).

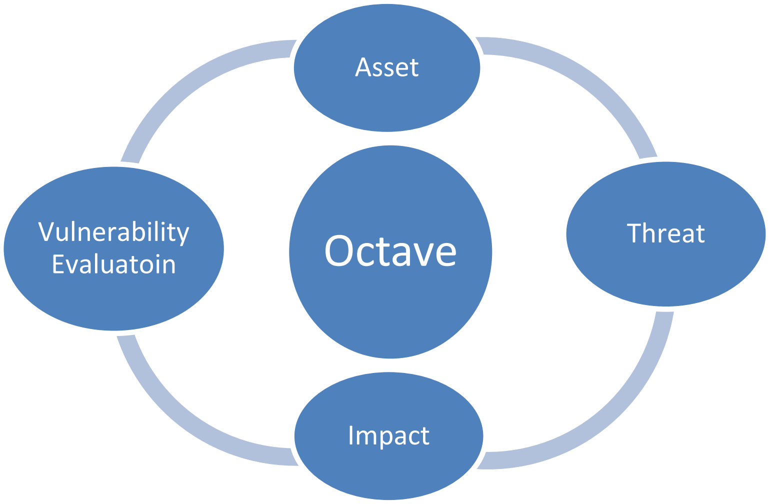


Figure 7 OCTAVE Framework

As demonstrated in the preceding section, completing an accurate risk assessment is both valuable and necessary for an organization and its ability to properly protect their information systems. Upon completion of the RA process the organization and management staff will be ready to make informed decisions with regard to budgeting, staffing and resource management. A well defined RA leads to a deeper and more complete understand of both the overall level of risk associated with the implemented technology as well as the risks associated with each individual system along with the organization.

Generic Risk Assessment Models available for deployment in financial institutions are many; the highlighted models are ISO, NIST, COBIT, OCTAVE, and CORAS. These models are heavily adopted into many large industries including large financial institutions. While these models provide a highly accurate RA model for these organizations, they are not as adaptable to smaller financial institutions. Small to medium sized financial institutions have unique needs in terms of financial resources, staffing resources, an overall ability to implement a large generic RA mode that is not honed to their institution (Podhradsky, 2009).

As demonstrated in the preceding sections, completing an accurate risk assessment is both valuable and necessary for an organization and its ability to properly protect their information system assets. Upon completion of the risk assessment process the organization and management staff will be ready to make precise and informed decisions with regard to budgeting, staffing and resource management. A well defined risk assessment leads to a deeper and more complete understand of both the overall level of risk associated with the implemented technology as well as the risks associated with each individual system.

Blakley, McDermott and Geer (2002) suggest that an organization has four options when addressing each risk. The first option for managing risk is “Liability Transfer”. This occurs when a business is able to convey the risk to another party outside of the organization, effectively removing the responsibility or accountability for the particular risk. Most often this is accomplished through use of a disclaimer or other type of binding agreement. A second option for addressing risk is through “Indemnification”. Indemnifying risks is effectively insuring the organization against the occurrence of a particular risk. The third option identified by Blakely et. al, is “Mitigation”. This is the process of reducing identified risks through procedure, processes, or controls. It is important to note that mitigation can be used to specifically reduced the impact, probability, or both impact and probability of a risk. The final option for addressing risk is “Retention”. This is essentially an organization’s acceptance of a given risk. The specific risk is acknowledged and documented during the risk assessment process but no further steps are taken to reduce the current level of risk. This path is typically chosen when the probability or impact of a risk occurring are very small. Retention is also a viable option when the "return on risk reduction spending" does not produce a meaningful return.

2. 5 Evaluation of Risk Assessment Models

The process of comparing and evaluating various generic RA models is outlined In the paper "A Framework for Comparing Different Information Security Risk Analysis Methodologies." This framework aims to provide organizations with guidance in selecting a suitable RA model. While the overall goal of identifying and classifying risk remains consistent across organizations, each may have different needs and requirements when it comes to assessing risk (Labuschagne, 2005).When attempting to choose a methodology Benoit recommends comparing the various approaches by answering five distinct questions, which are outlined in Table 10, Labuschagne Risk Assessment Evaluation.

Table 10 Labuschagne Risk Assessment Evaluation

Labuschagne Risk Assessment Evaluation
Will the risk assessment is completed by examining one asset at time or if several assets are grouped together to assess risk
Where in the methodology is risk analysis done? Due to various models requiring different degrees of information, the answer to this question will give an organization the ability to differentiate between preparation time and the overall accuracy of a risk assessment
Who will complete the risk assessment? Some risk assessments will be completed by internal personal while others rely extensively on experts who are external to the organization
What formulas are used to calculate risk
Is the output is relative or absolute? As an example of this is some RA's may have a value of "high" while others will compute a specific number

When attempting to choose a methodology Vorster and Labuschagne suggest comparing the various approaches by answering five distinct questions, which are the following:

1. "Does the risk assessment examine risk to each asset individually, or does it group assets?" The first question seeks to determine whether the RA is completed by examining one asset at time or if several assets are grouped together to assess risk. This is important for assessing the overall risk of the information system assets.

   To determine if the RA conducts the analysis on a single asset or group of asset the research can review the final results. If the result of the analysis if the results review each assets, then the RA is based on a single asset, however if the results group assets into systems or profiles the RA is based on a group of assets.

   If the organization employing the methodology prefers a quicker analysis, than the organization should adopt an RA model that completes the analysis on a group of assets.

   Scale of Criteria:

   1- Indicates that the risk analysis is completed on an individual asset

   2- Indicates that the risk analysis is completed on a group of assets

2. "Where in the methodology is risk analysis done?" Various RA models require different degrees of information, the answer to this question will

allow an organization to differentiate between preparation time and the overall accuracy of a risk assessment.

The time invested to complete the risk assessment is important for the institutions to consider.

The accuracy of the RA is also a very important consideration. Both the time it takes to complete the assessment and the overall accuracy are a trade-off according to Vorster and Labuschagne.

Scale of criteria:

Scale from 1-3- Trade-off from time and accuracy

If time is most important-

1- Risk analysis is conducted after extensive preparation

2- Risk analysis is conducted after some preparation

3- Risk analysis is conducted after little preparation

If accuracy is most important-

1- Risk analysis is conducted after little preparation

2- Risk analysis is conducted after some preparation

3- Risk analysis is conducted after extensive preparation

3. “Who will complete the risk assessment?” The framework calls for differentiating methodologies by classifying who will complete the risk assessment. Some risk assessments will be completed by internal personal while others rely extensively on experts who are external to the organization.

Depending on the risk assessment model, the assessment is either conducted by external experts or internal staff. Both the cost and expertise is conducted in one category due to the nature of the trade-off; if cost is most important, the analysis is most likely conducted by internal staff opposed to external experts.

Scale from 1-3- Trade-off from cost and expertise

If cost is most important-

1- Risk analysis is conducted by external experts

2- Risk analysis is conducted by both external and internal people

3- Risk analysis is conducted by internal people

If expertise is most important-

1- Risk analysis is conducted by internal people

2- Risk analysis is conducted by both external and internal people

3- Risk analysis is conducted by external experts

4. “What formulas will be used to calculate risk?” Once this previous question, question 3, has been answered an organization should compare the various types of risk assessment based on what specific formulas are used to calculate risk. This will allow the organization to determine how risk is calculated for their adopted RA model.

Organizations need to determine what type of formula is used to calculated risk, which indicates the complexity of the risk analysis.

If an organization only needs basic RA values from analysis than they need to adopt a model that uses an expected value matrix; an example is OCTAVE.

On the other hand, if an organization needs detailed results form the RA, then they should implement model that uses extensive formulas.

The organization needs to determine the trade-off of between accuracy and simplicity for their chosen RA.

Scale of criteria:

If simplicity is most important-

1- Risk analysis integrates extensive mathematical calculations

2- Risk analysis integrates a little simple mathematical calculations

3- Risk analysis integrates no mathematical calculations

If accuracy is most important-

1- Risk analysis integrates no mathematical calculations

2- Risk analysis integrates a little simple mathematical calculation

3- Risk analysis integrates extensive mathematical calculations

5. "Is the methodologies output is relative or absolute?" As an example, some risk assessments may result with a value of "high" while others will present the organization with a specific number risk number.

   Absolute ratings can be compared, for example, if asset A has a value of 35, and asset B has a value to 70, it is fair to say that asset B has twice the risk of asset A.

   Relative ratings have ratings that might indicated that asset A and asset B both have a rating of "high", but that is all that can be said about the two assets.

   The trade off between the ranking of risk and the indication of difference between the risk need to be evaluated and decided on by the organization adopting the model.

   Scale of criteria-

   If ranking the risks is most important-

   1- Analysis of results are able to be compared

   2- Analysis of results are not able to be compared

   If ranking the risks need to be comparable-

   1- Analysis of results are not able to be compared

   2- Analysis of results are able to be compared

Labuschagne's approach was used to evaluate the overall effectiveness of generic RA models such as ISO, NIST, COBIT, OCTAVE, and CORAS into SMFIs. Labuschagne's approach is identified in Table 11, Labuschangne's Risk below.

Table 11 Labuschagne Risk

Labuschagne Risk Assessment Evaluation	OCTAVE	CORAS	ISO	NIST	COBIT
Whether risk analysis is done on single assets or groups of assets: Scale (1 or 2) Weight= .2	1	1	2	1	2
Where in the methodology is risk analysis done? Scale (1-3) Weight = .2	1- Time 3- Accuracy	2- Time 2- Accuracy	1- Time 3-Accuracy	1- Time 3- Accuracy	1- Time 3- Accuracy

People involved in the risk assessment? Scale (1-3) **Weight = .2**	3- Cost 1- Expense	3- Cost 1- Expertise	3- Cost 1- Expertise	2- Cost 2- Expertise	2- Cost 2- Expertise
The main formulas used **Scale (1-3)** **Weight =.2**	3- Simplicity 1- Accuracy	3- Simplicity 1- Accuracy	1- Simplicity 3- Accuracy	2- Simplicity 2- Accuracy	2- Simplicity 2- Accuracy
Whether results are relative or absolute. **Scale (1 or 2)** **Weight = .2**	2- Not Comparable 1- Comparable	2- Not Comparable 1- Comparable	2- Not Comparable 1- Comparable	1- Not Comparable 2- Comparable	1- Not Comparable 2- Comparable

3. Research Methods

3.1 Design Science

This research will utilize the design science research methodology, as an IT artifact will be created. Hevner, et al. present the guidelines for design science research in the paper “Design Science in Information Systems Research” for validation and evaluation (Hevner, 2004). This research will employ each of the seven guidelines to provide a methodical evaluation of the research IT artifact as outlined in table x

The artifacts shaped from this research include a RA model for SMFIs, SMERAM, which has been tailored towards the financial sector. This model has been created and evaluated with design research, using Hevner, et al’s. design science approach (Hevner, 2004).

The seven guidelines outlined in the “Design Science in Information Systems Research” are listed in Table 12. SMERAM has been developed in accordance with Hevner, et al’s. guidelines and the SMERAM approach overview is also listed in Table 13.

Table 12 Hevner Design Science Guidelines

Guideline	Description	SMERAM
1- Design as an Artifact	Design-science research must produce a viable artifact in the form of a construct, a model, a	The artifact, SMERAM, is created in accordance of

	method, or an instantiation	Hevener, et al. design science guidelines
2- Problem Relevance	The objective of design-science research is to develop technology-based solutions to important, and relevant business problems	SMERAM was designed to address the staffing and financial limitations of SMFIs all while meeting and exceeding FDIC FIL regulation
3- Design Evaluation	The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods	SMERAM was effectively tested and deployed in a community bank
4- Research Contributions	Effective design-science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/	The SMERAM RA model for SMFIs is the contribution to the security and SMFI fields

	design methodologies	
5- Research Rigor	Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact	SMERAM was built on accepted generic RA models such as ISO, NIST, COBIT, and CORAS while being honed to the financial industry
6- Design as a Search Process	The search for an effective artifact requires utilization available means to reach desired ends while satisfying laws in the problem environment	SMERAM was developed through a prototype environment after studying various established generic RA models
7- Communication of Research	Design-science research must be presented effectively both to technology-orientated as	SMERAM is designed to be used effectively by both technical and

	well as management-orientated audiences	non-technical personnel; the intended audience is bank management

Design as an Artifact

In guideline one, Design as an Artifact, research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation **(**Hevner**,** 2004**)**. This research will produce a RA model, SMERAM, that is tailored towards the small to medium sized financial industry. SMERAM is intended for the use in small and medium size entities.

SMERAM has been tested and evaluated with the management team in a SMEFI. The SMFI was sought out due to their size and location and they agreed to allow the researchers complete a no cost RA using the SMERAM model in exchange for publishing data.

Problem Relevance

Guideline two, Problem Relevance, states that design-science research is to develop technology-based solutions important and relevant to business problems (Hevner, 2004). SMERAM does this by creating an RA model that addresses the FDIC regulations and other federal mandates imposed on the financial industry.

There are several generic IT RA models that organizations can adapt to protect their information security. ISO, NIST, COBIT, CORAS and OCTAVE are included in this research. However, none of these generic RA models are designed for the explicit use in SMFIs. In fact, all of the generic models discussed fall short when it comes to the unique needs of SMFIs which include financial limitations, staffing limitations, industry configuration, along with a RA that evaluats security in terms of assets and organizational security.

Most of these models are too large for SMFIs, as a result, SMFIs do not adequately implement an entire generic standard, rather they employ various sections of their chosen model, however not the entire standard. This makes benchmarking and future assessments difficult to assess the continued evaluation in the RA process. In addition to the extensive nature of the models, the generic models also usually require a certified consultant or account to perform the RA, which is a cost SMFIs can’t afford. If the generic model doesn’t require a certified consultant the IT department at the organization needs to have knowledgeable staff to complete the RA, which usually isn’t typical of a SMFI. The overall cost of these generic RA models is typically out of reach of SMFIs.

None of the generic models are honed for the use in SMFIs. The financial institution needs to be able to identify assets and threats along with identifying mitigating approaches for reducing risk to the financial institution. This task, with no guidance, is very difficult for SMFIs management team.

Not all of the generic, industry accepted RA models are both asset and organizational based models. Including both assets and the organization itself is important to the overall security of an institution.

Design Evaluation

Guideline three, Design Evaluation, states that the utility, quality, and efficiency of a design artifact must be rigorously demonstrated via well-executed evaluation methods (Hevner, 2004).

SMERAM was tested via case study research with a volunteer financial institution that is under $500 million in assets. A case study was conducted in Fall 2007 with the financial institution's management team. A year two follow up interview was conducted in Fall 2008 to determine the effectiveness of the initial RA conducted in Fall 2007.

During the initial visit the financial institution was interviewed to determine current RA practices. The financial institution stated they completed their yearly RA by simply passing around an excel spreadsheet that listed all the bank's assets, and then a separate column stating what activities they deploy on their system to mitigate risk.

A review of the document showed a highly inaccurate RA practice at this financial institution. The institution listed the following assets in their document:

- Person X Office Computer (name withheld)
- Person Y Office Computer (name withheld)
- Person X Office Computer (name withheld)
- Core Banking System

- FinCen
- Deposit Platform
- CU Serve Core System
- Teller Computer 1
- Teller Computer 2
- Teller Computer 3
- E mail
- Printers

After reviewing the list, and taking a guided tour around the bank, the researchers determined there were several assets that were not represented on their excel spreadsheet. The missing assets are the following:

- Checking Ordering Website
- Credit Bureau Website
- Email system
- Firewall
- Fund Transfer System
- Internet Banking System
- Internet Website Homepage
- Router
- Switch

The assets that were overlooked by the financial institution were mostly assets they outsourced such as their website, internet banking, E-mail system, and check ordering site. Examples of assets they overlooked because they didn't know they had them were their router, firewall, and switch. Organization can outsource an aspect of their business; however they cannot outsource their responsibility. If someone had hacked into their internet banking site, and accessed their customers information their customers would be looking at the financial institution for answers, not their 3rd party service provider.

Overlooking these core assets is a very serious concern that SMFIs face when they do not follow an appropriate RA model that is specific to their industry. RA's need to be completed by the management team, and they need a RA that is honed to their industry, with specific assets, threats, and countermeasures.

Research Contribution

Guideline four, Research Contributions, state that each artifact must provide a verifiable contribution to the area of the design artifact, which is in the areas of the design artifact, design foundations, and/ design methodologies (Hevner, 2004).

The model proposed by the authors, SMERAM, contributes to both the information technology security and SMFI fields. The information technology security field is benefiting from a generic RA model that can be adapted to other fields, similar to the fashion it was adapted to in SMFIs. The SMFI field is benefited from an RA model that is designed for their specific industry that is designed to aid in solving their unique information security concerns.

Research Rigor

Guideline five, Research Rigor, stats design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact (Hevner, 2004). SMERAM was built on industry accepted generic RA models such as ISO, NIST, COBIT, OCTAVE and CORAS while being honed to the financial industry, with is demonstrated in Figure 8.

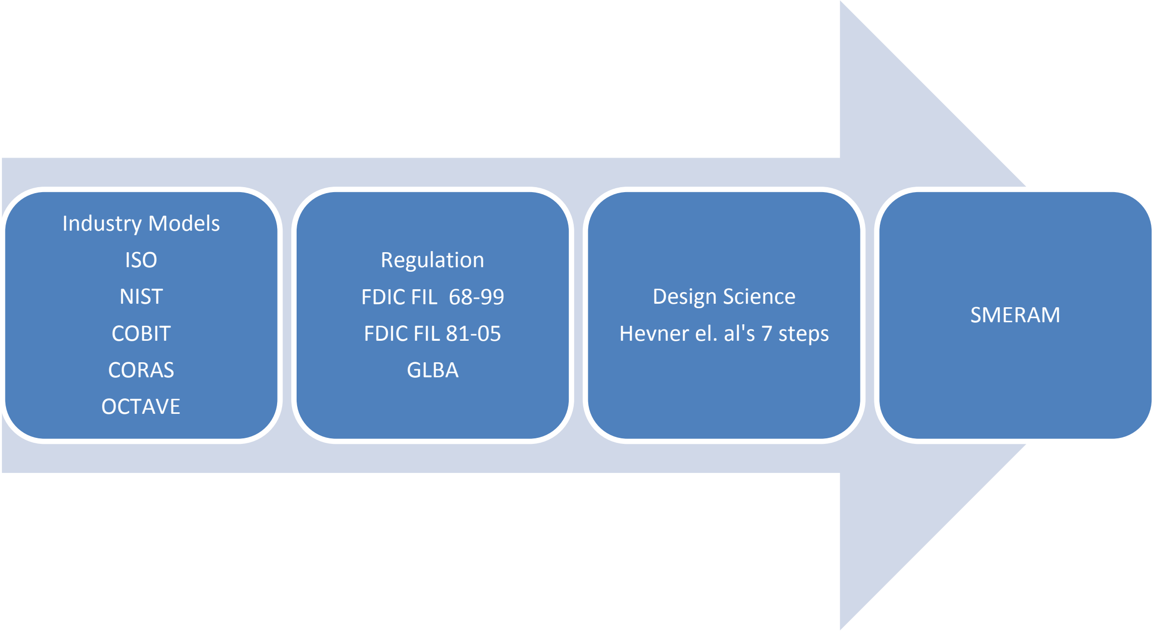


Figure 8 SMERAM Overview

Design as a Search Process

Guideline six, Design as a Search Process, the search for an effective artifact requires utilization available means to reach desired ends while satisfying laws in the problem environment (Hevner, 2004). SMERAM was developed through a prototype environment after studying various established generic RA models, such as ISO, NIST, COBIT, OCTAVE, and CORAS. Many different versions of SMERAM were developed and analyzed prior to the final version highlighted in this research.

Communication of Research

Guideline seven, Communication of Research, design science research must be presented effectively both to technology-orientated as well as management-orientated audiences (Hevner, 2004). SMERAM is designed to be used effectively by both technical and non-technical personnel.

The intended audience of SMERAM is the bank management team. One of the main concerns of SMFIs is the lack of technical personnel on staff, and SMERAM effectively addresses this concern as it is designed to be used by non-technical management staff.   This research will be allow SMFIs to conduct their annual RA as outlined by the FDIC, in a manner that produces a viable and value added RA.

3.2 Aspect of Generic Models used in SMERAM

The generic RA models NIST, ISO, COBIT, CORAS, and OCTAVE have many quality attributes that make implementation into large and robust industries an appropriate and efficient fit. However, these models are not an appropriate fit for smaller institutions due to financial and staffing limitations. There are steps within each model that has been integrated into SMERAM as introduced in Table 14.

Table 13 Generic Models Integrated into SMERAM

Generic RA Model	Steps Integrated into SMERAM
NIST	System Characterization
	Threat Identification
	Control Analysis
	Results Documentation
ISO	Organizational Security
	Personnel Security
CORAS	Asset, Threat, Vulnerability
COBIT	Monitor and Evaluate
OCTAVE	Vulnerability Evaluation

4. SMERAM

4.1 Introducing SMERAM

Through the use of design science and following Hevner's guidelines, a new RA model has been developed specifically for the use in smaller financial institutions. SMERAM works to provide a risk assessment model for small to medium sized financial that address their unique needs in a way larger generic RA models do not.

The first unique need is staffing limitations. Smaller financial institutions typically do not have the on-site technical staff. Larger generic RA models are not designed to be completed by management, and often require several onsite technical employees.

The second unique need is financial limitations. Smaller financial institutions typically do not have $50,000 or more to purchase the use of a generic RA model, which is the cost for a medium sized organization to conduct an ISO RA model (Martin, 2002). It is also important to note that the purchase price is an annual expense, not a onetime expense. SMERAM, a free model, is designed to be completed by bank management.

The third unique need works with the first and second need. Most generic RA models require not only a purchase price to use the model, but they also require certified consultants to complete the risk assessment (Podhradsky, 2009). The certified consultant is an addition expense on top of the cost of using the RA model.

The fourth unique need is addressing the information technology assets unique to financial institutions (Podhradsky, 2009). SMERAM helps small and medium sized financial institutions to complete a valid risk assessment that is both an adaptive and integrated part of the entire information security program. SMERAM has predefined assets, threats and countermeasures built into the RA model that are specific to the financial industry.

The fifth unique need that smaller financial institutions have is that they need an assessment that is both asset and organizational based (Streff, 2007). SMFIs need an all encompassing assessment that helps the organization determine the security risk with their IT assets along with the entire organization (Podhradsky, 2009).

Figure 9, SMERAM, is the model that has been developed for the use in SMFIs. The model addresses the six preceding unique needs of SMFIs.

SMERAM is designed to be completed in its entirety annually, and updated whenever there is a major change in IT assets or networking infrastructure. The model is designed to be conducted in a fashion where you progress to the next step after you complete the preceding step. Meaning, if you do not successfully inventory and audit assets and service providers in step one, step two will be incorrect and incomplete. The same concept applies to all proceeding steps. After the organization finishes the final step, they have successfully completed their annual RA with SMERAM. If there is any purchases, or infrastructure updates in that year, the SMFI will updated their RA starting with STEP one, finishing with step 7.

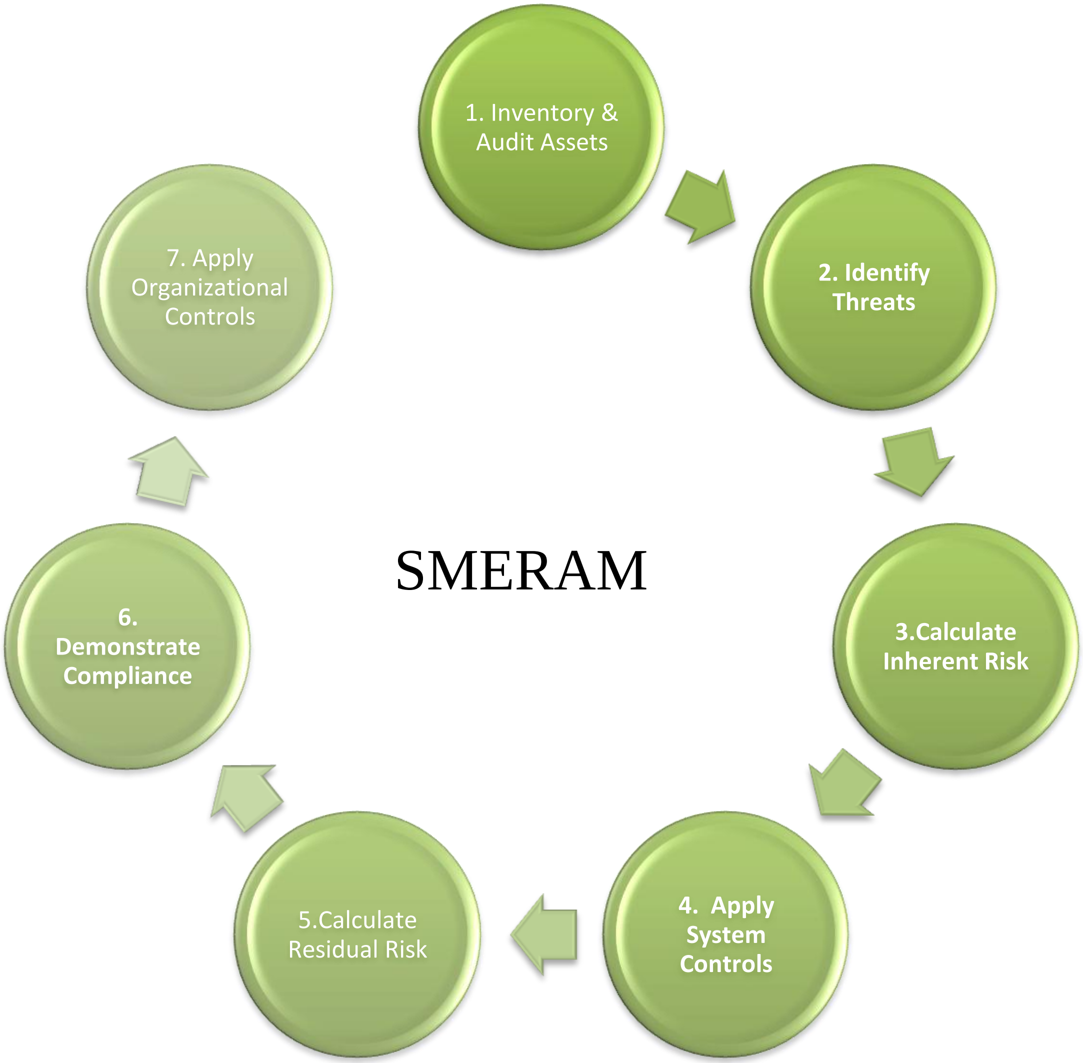

1. Inventory & Audit Assets
2. Identify Threats
3.Calculate Inherent Risk
4. Apply System Controls
5.Calculate Residual Risk
6. Demonstrate Compliance
7. Apply Organizational Controls
SMERAM

Figure 9 SMERAM Risk Assessment Model

4.1.1 Inventory & Audit Assets:

Step One, is modeled after both NIST and CORAS. In NIST, the step is called System Characterization, and in CORAS is called Asset. In this step, the financial institution works to determine the specific assets that are owned by the organization. Vendors and service providers are also reviewed and listed because even though an organization outsources some aspect of their business does not mean they are not responsible for the security of the process.

The inclusion of 3rd party service providers and vendors is a new concept for RAs. For example, if Bank of America's core server suffered a data breach, and customer's personal information was stolen, they could not tell their shareholders, board of directors, or customers that it wasn't their fault because they outsourced their information security with a Managed Security Service Provider (MSSP). The customer's, shareholders, and board of directors will look at Bank of America, and not the MSSP. As a result of the data breach their credibility will be damaged. It is extremely important to note that you can outsource your processes, but you cannot outsource your responsibility. Some other accepted models fail to include vendors and service providers, which the researchers feel is a serious oversight. There are certain levels of risk associated with certain service providers.

The protection profile in SMERAM is similar with other notable RA models: confidentiality, integrity, and availability. However, SMERAM also includes volume as part of the overall protection profile. Volume is not factored as high as confidentiality, integrity or availability, but it is included when needed.   The weight of each area is calculated in terms of high, medium and low, with high being 3, medium being 2 and low being represented by 1.

Confidentiality is defined as preserving authorized restrictions on information access and disclosure, including means for protection personal privacy and proprietary information (McCumber, 2005). Financial institutions have a responsibility to protect their customer's data from unauthorized access, they must make sure their information systems are protected and secure.

Integrity is defined as guarding against improper information modification or destruction and includes ensuing information non-repudiation and authenticity (McCumber, 2005). The data that is inherent to a financial institution involves personal identifying information that can be used to steal someone identity. This data needs to be secure and accurate. Inaccurate financial data can lead have serious consequences on someone's financial history. In SMERAM, the weight for data integrity is rated in terms of high, medium and low.

Availability is defined as ensuring timely and reliable access to and use of information (McCumber, 2005). The financial institution and the customers need to have near 24-7 access to the financial information. Customers need to know their balances and account data, and financial institutions need to be able to access all records to conduct their routine business.

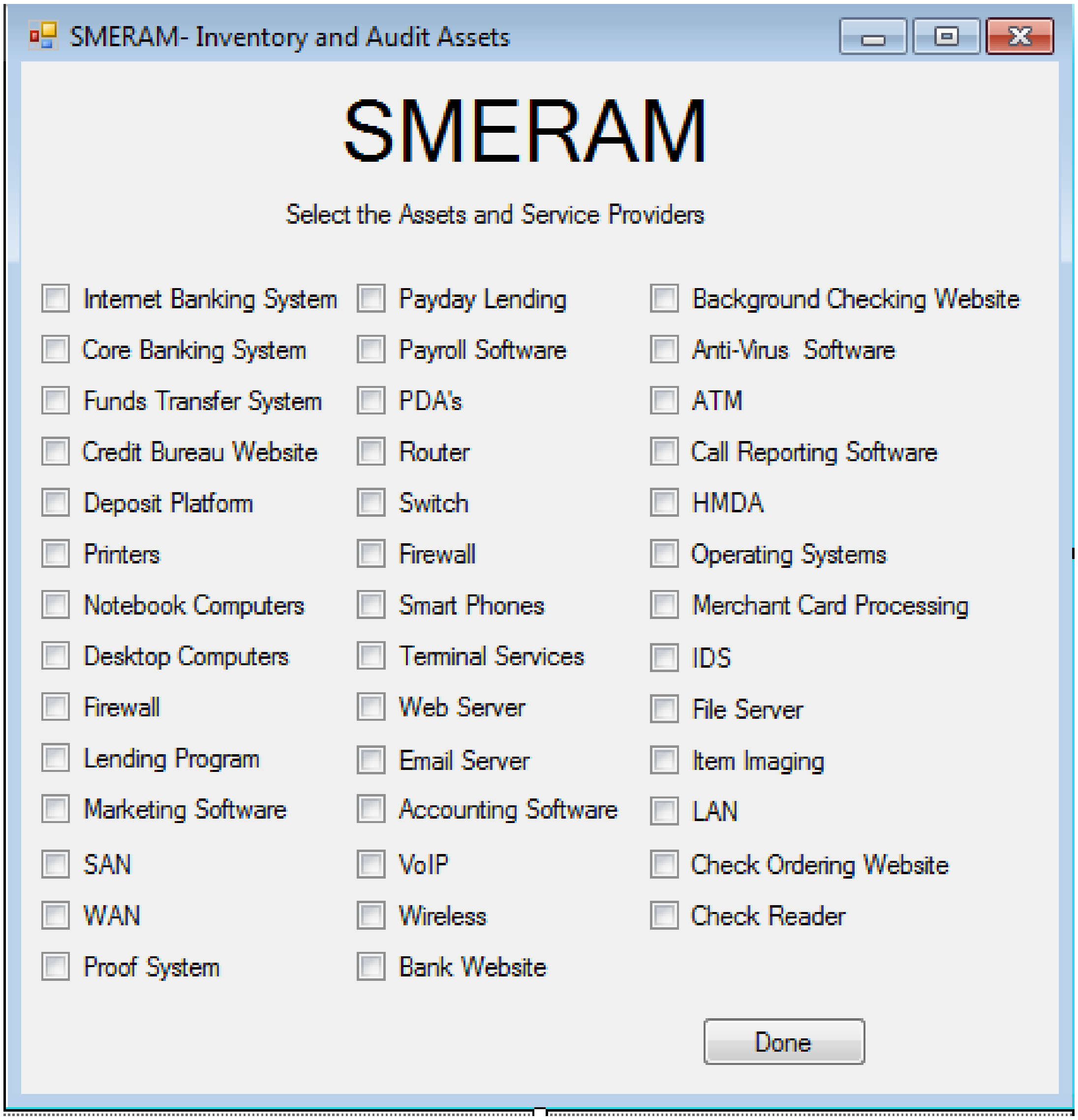
Availability goes well beyond the scope of data into services and information technology systems. A bank must have access to their core banking platform in order to conduct their business. Also, the connection to the FDIC must be secure and available when it is needed. If a bank cannot transfer deposits to the FDIC, they will lose money on their interest payments.

There is a predefined amount of acceptable downtime for all services and information technology assets. Financial institutions need to be able to rate which assets have to have the highest amount of uptime. In SMERAM, the weight for availability is rated in terms of high, medium and low.

Volume is defined in relative terms. Volume is a new consideration in the information technology security area, and it is integrated into SMERAM. Confidentiality, integrity and availability have been constant and including volume is something the researchers believe valid and necessary inclusion. For example, if a financial institution has a two servers holding customer data, each that require high confidentiality, high integrity, and need high availability, but one server has 1 file, and the other has over 1,000,000 files, volume will tell the financial institution more weight should be placed on the server with more records. A data breach is serious regardless of where it occurs, however, the researchers believe a data breach that effects millions of people versus one that affects a few hundred has different considerations. In SMERAM, the weight for volume is rated in terms of high, medium and low.

Appendix C lists all of the assets that are typical to financial institution. This guideline helps to ensure that the financial institution doesn’t overlook any of their IT assets or service providers, which will result in a more accurate RA.

Figure 10 outlines the interface where the customers select the assets and service providers that are typical to SMFIs. After this they progress to step 2, Identify Threats, which is threats per each asset they outlined.



SMERAM- Inventory and Audit Assets

SMERAM

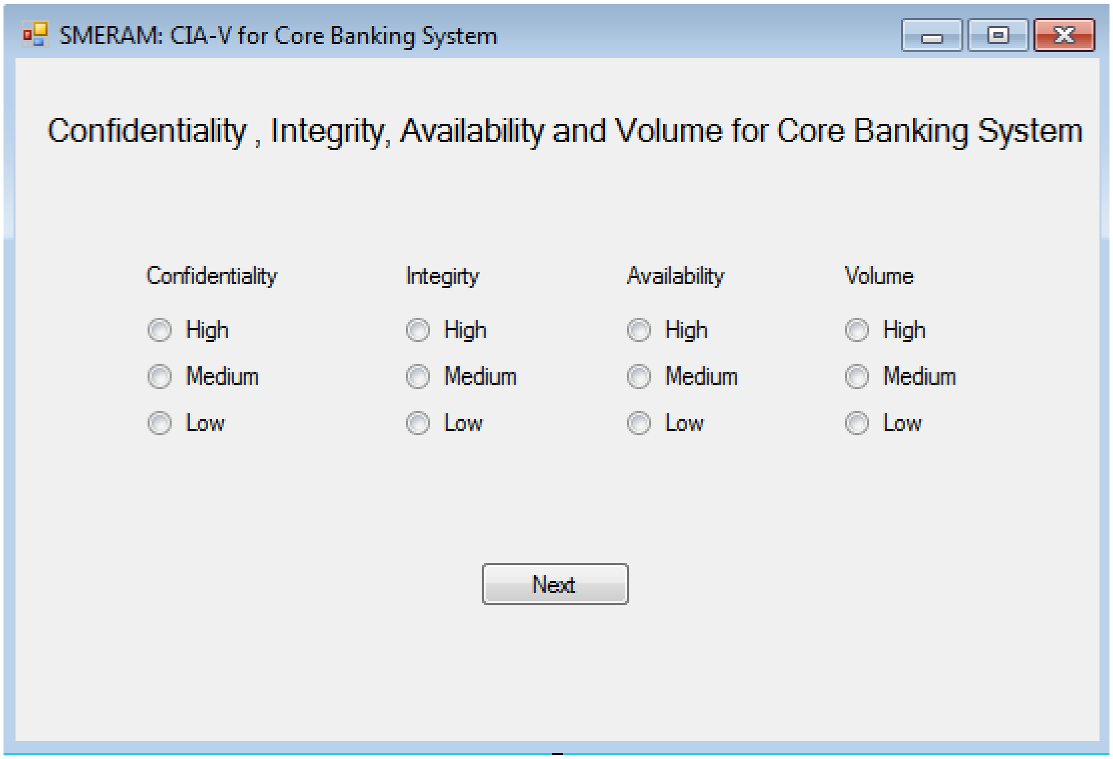
Select the Assets and Service Providers

- □ Internet Banking System
- □ Core Banking System
- □ Funds Transfer System
- □ Credit Bureau Website
- □ Deposit Platform
- □ Printers
- □ Notebook Computers
- □ Desktop Computers
- □ Firewall
- □ Lending Program
- □ Marketing Software
- □ SAN
- □ WAN
- □ Proof System
- □ Payday Lending
- □ Payroll Software
- □ PDA's
- □ Router
- □ Switch
- □ Firewall
- □ Smart Phones
- □ Terminal Services
- □ Web Server
- □ Email Server
- □ Accounting Software
- □ VoIP
- □ Wireless
- □ Bank Website
- □ Background Checking Website
- □ Anti-Virus Software
- □ ATM
- □ Call Reporting Software
- □ HMDA
- □ Operating Systems
- □ Merchant Card Processing
- □ IDS
- □ File Server
- □ Item Imaging
- □ LAN
- □ Check Ordering Website
- □ Check Reader

Figure 10 SMERAM Interface

The financial institution ranks each of the assets and service providers in terms of high, medium and low. After each asset is ranked, volume is included in the evaluation in a means that is relative to the financial institution. The screen the SMFI sees on each of the assets they outlined they have in their organization.

This step demonstrates how SMERAM is honed towards SMFIs. Some of the assets are typical to any institution, but SMERAM also lays out all FDIC assets.



SMERAM: CIA-V for Core Banking System

Confidentiality , Integrity, Availability and Volume for Core Banking System

Confidentiality	Integrity	Availability	Volume
○ High	○ High	○ High	○ High
○ Medium	○ Medium	○ Medium	○ Medium
○ Low	○ Low	○ Low	○ Low

Figure 11 SMERAM: CIA-V

4.1.2 Identify Threats:

The second step is modeled after NIST and CORAS. In NIST the step is Threat Identification, and in CORAS the step is Threat. In this step of SMERAM, the financial institution is assessing the threats inherent to each asset. Identifying threats is something that most organizations tend to confuse with vulnerabilities; a definition of a threat is "any circumstance with the potential to intentionally or unintentionally exploit a specific vulnerability in an information system resulting in a loss of confidentiality, integrity or availability (McCumber, 2005)."

A threat library is a valuable piece of literature for any organization, and that holds true for financial information. Threat libraries determine what threats are specific to specific assets. Financial institutions traditionally obtain a threat library in one of two ways, they could spend the time to research threats and build out their own library, or they could purchase a readymade library and apply the threats to their specific asses. In the case of SMERAM, the threat library that is specific to banking assets is already included with the RA model.

The financial institution determined the assets, service providers and venders in step one, and in step two, SMERAM assigns the threats that are unique to the assets, according to ISO (ISO 27002 Standard , 2005). All assets that are predefined for the financial industry are located in Appendix C. Tables 15, 16, 17 & 18 are examples of banking assets and threats associated with those assets. The full threat library that is associated with typical financial institution assets and 3rd party service providers is also located in the appendix in Appendix F (ISO 27002 Standard , 2005).

Table 14 Internet Banking System Threats

Internet Banking System				
Data Leakage	Pharming	Phishing	Defacement	Intentional Misuse
Unauthorized Remote Access	Degraded / Unavailable	Malicious Software	Outsourced	Unauthorized Physical Access
Unauthorized Viewing	User Error	Environmental Incident	Man-made / Natural Disaster	

Table 15 Core Banking System Threats

Core Banking System				
Data Loss	Unauthorized System Access	Intentional Misuse	Outsourced	Unauthorized Remote Access
Degraded / Unavailable	Hardware Failure	Unauthorized Physical Access	Eavesdropping / Sniffing	Malicious Software
Unauthorized Viewing	Social Engineering	Software Acquisition	Man-made / Natural	Environmental Incident
User Error				

Table 16 Funds Transfer System Threats

Funds Transfer System				
Unauthorized System Access	Eavesdropping / Sniffing	Degraded / Unavailable	Malicious Software	Unauthorized Viewing
Intentional Misuse	Unauthorized Remote Access	User Error	Outsourced	Social Engineering
Man-made / Natural	Unauthorized Physical Access			

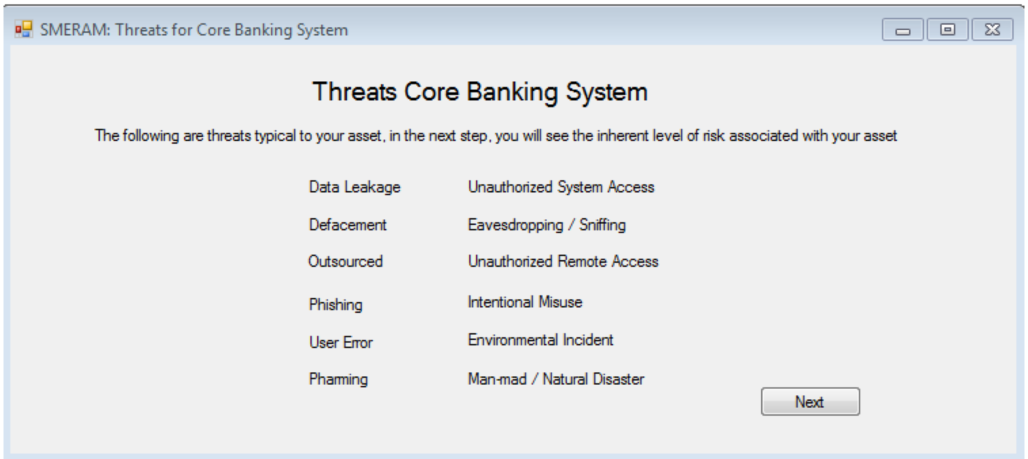
Table 17 Credit Bureau Website

Credit Bureau Website				
User Error	Data Loss	Social Engineering	Defacement	Intentional Misuse
Unauthorized Viewing	Eavesdropping / Sniffing	Unauthorized System Access	Outsourced	

Table 18 Deposit Platform Threats

Deposit Platform				
User Error	Data Loss	Social Engineering	Defacement	Intentional Misuse
Unauthorized Viewing	Eavesdropping / Sniffing	Unauthorized System Access	Outsourced	Software Acquisition
Man-made / Natural Disaster				

Figure 12 depicts a screen shot form SMERAM showing the threats associated with a Core Banking System. In the next step, SMERAM shows the inherent level of risk associated with each asset.



Threats Core Banking System

The following are threats typical to your asset, in the next step, you will see the inherent level of risk associated with your asset

Data Leakage
Defacement
Outsourced
Phishing
User Error
Pharming

Unauthorized System Access
Eavesdropping / Sniffing
Unauthorized Remote Access
Intentional Misuse
Environmental Incident
Man-mad / Natural Disaster

Figure 12 SMERAM: Threats to Core Banking System

4.1.3 Calculate Inherent Risk:

Step three is modeled after the CORAS step Vulnerability. In this step, Determining the Inherent Risk, the financial institution will be able to see which assets represent the greatest risk to the bank. The inherent risk of each asset is the asset with no security controls applied to mitigate risk (McCumber, 2005). For example, what would be the risk of having a domain controller with absolutely no controls for security enabled?

The current accepted industry standard uses the equation risk =asset*value*threat. The researchers believe this formula is inherently flawed due to the consideration of the monetary value. If you ask 10 different people to place a value on an asset, you will more than likely get 10 different answers. Is it the purchase cost, the replacement cost, or the depreciated cost? There is no standard for this issue.

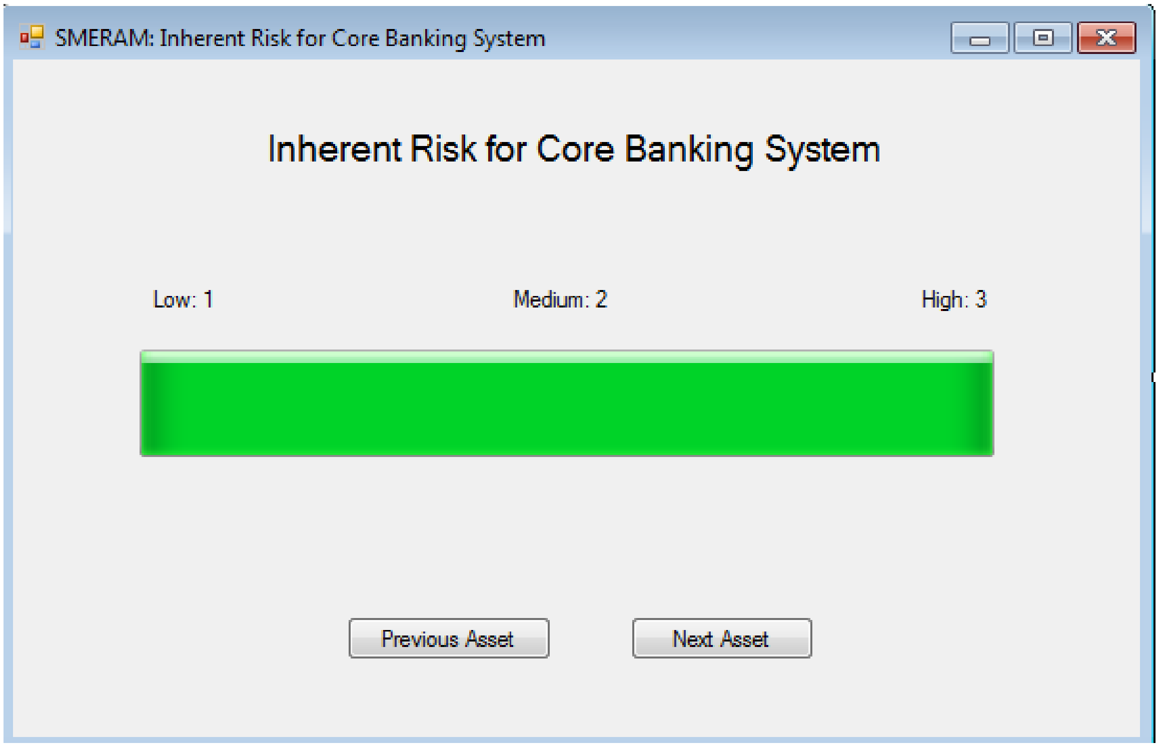
The formula the researchers would like the audience to consider is risk = confidentiality *integrity*availability, with the consideration of volume when CIA is equal.

With the introduced scale of 1-3 for high, medium, and low; a high confidentiality, high integrity, and high availability would equate to 3*3*3 times by a volume decimal multiplier if confidentiality, integrity, and availability are equal.

If there are two servers equal in CIA, and Server A has 1,000 records, and Server B has 1,000,000 records, and if both servers were compromised, Server B would result in a higher loss for the institution. In this new approach of including volume, the servers with higher volume should be protected more, as a breach could result in more harm, when CIA is equal. Figure 12 shows the inherent risk level for a Core Banking System, while Figure 13 shows the inherent risk a printer introduces to the organization. This comparison allows the SMFI to have a visual depiction of the different inherent risk levels of their assets and service providers.

The calculation that SMERAM employs to determine the inherent risk involves analyzing the threats associated with the asset. Each threat is given a weight of high, medium or low; whereas high equals 3, medium is 2, and low is 1. The assets are then compared against each other, and ranked in sequential order. Figures 13 and 14 depict the asset with the highest risk and the asset with the lowest inherent risk to the financial institution.

This step is a demonstration of how SMERAM helps in the decision making process at SMFIs, and is honed towards the financial sector.



SMERAM: Inherent Risk for Core Banking System

Inherent Risk for Core Banking System

Low: 1

Medium: 2

High: 3

Figure 13 SMERAM: Inherent risks for Core Banking System

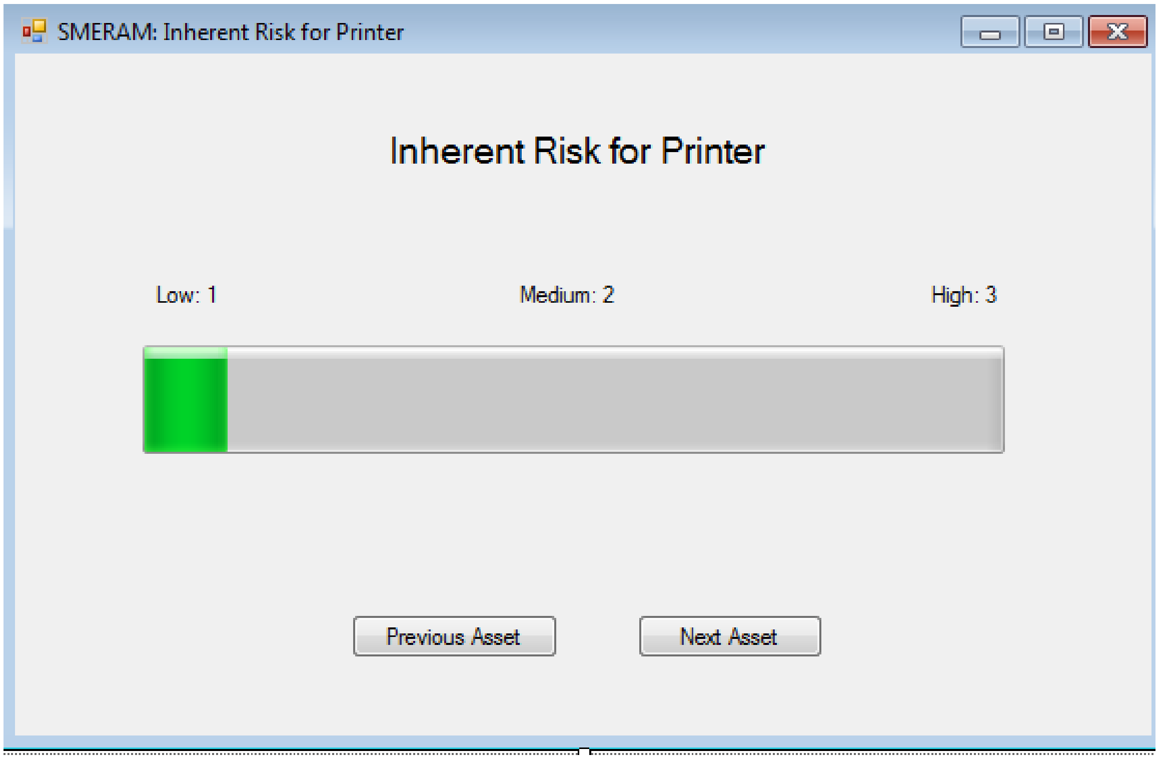


Figure 14 SMERAM: Inherent risks for a Printer

4.1.4 Apply System Controls:

The next step is modeled after the NIST Controls phase. System controls are the system safeguards the bank wants to implement to protect their information technology assets. The system controls that are available for implementation are included with the treat library, and are listed in Appendix F. The organization needs to determine what controls they apply to their information systems to mitigate risk.

In this step, the financial institution keeps building on the previous steps of inventory their assets and 3rd party service providers, indentifying steps, and determining the inherent risk to the IT assets. During step 4, Apply System Controls, the SMFI reviews the predefined list of system safeguards that they currently deploy on their IT assets.

This step allows the financial institution to determine what type of controls they are currently applying and what type of controls are available to apply towards their IT assets. This step is also crucial for developing a baseline in which all other RA’s can be evaluated against.

Table 19 outlines the typical controls that are implemented in SMFIs, which is also outlined in Appendix D (ISO 27002 Standard , 2005). Appendix E lists controls mapped to assets (ISO 27002 Standard , 2005).

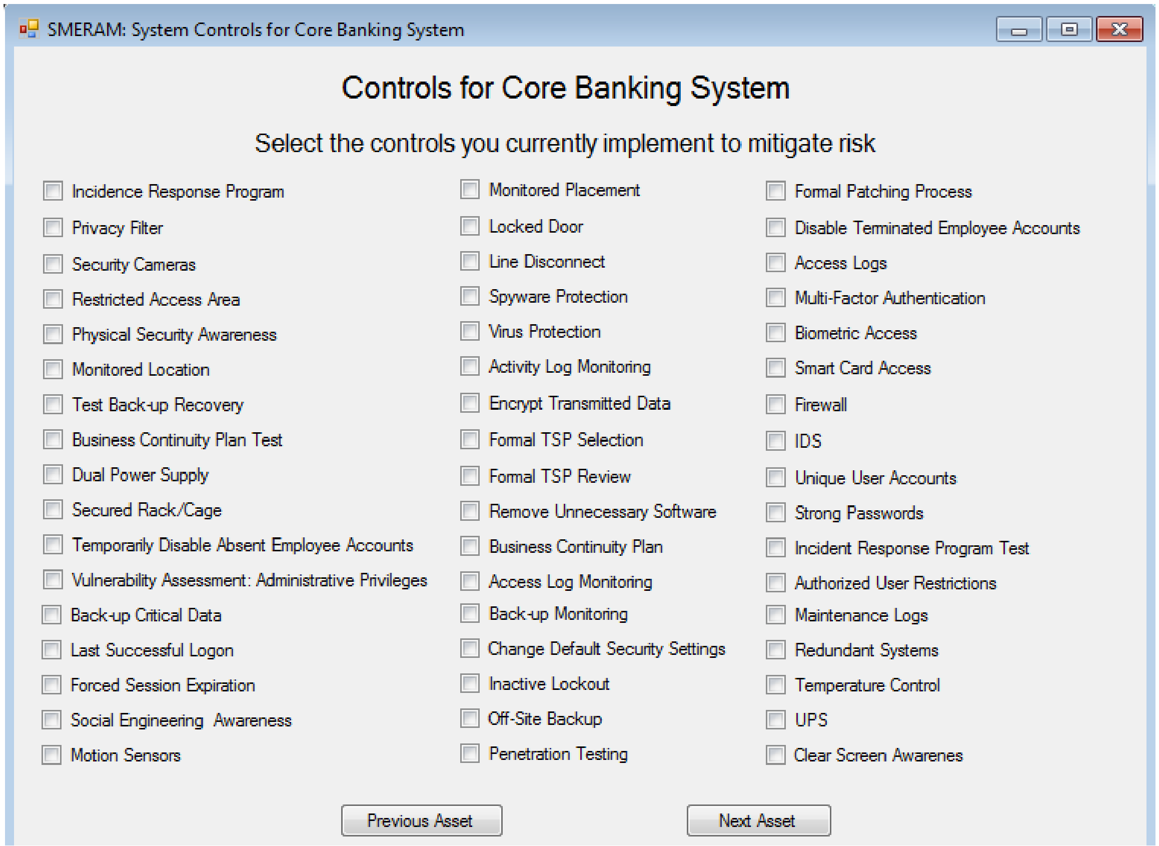
Table 19 Controls Typical to Small and Medium Sized Financial Institutions

Controls Typical to SMFIs				
Authorized User Restrictions	Access Logs	Formal TSP Review	Formal TSP Selection	Access Log Monitoring
Invalid Attempt Lockout	Strong Passwords	Unique User Accounts	Encrypt Stored Data	Formal Patching Process
Intrusion Detection/ Prevention	Back-up Critical Data	Change Default Security Settings	Incident Response Program	Incident Response Program Test
Clear Screen Awareness	Forced Session Expiration	Maintenance Logs	Multi-Factor Authentication	System Access Warning
Activity Logs	Change Default Account Settings	Maintenance Log Review	Temporarily Disable Absent Employee Accounts	Vulnerability Assessment: Administrative Privileges
Activity Log Monitoring	Last Successful Logon	Business Continuity Plan Test	Network Diagram	Test Back-up Recovery
Formal TSP Selection	Penetration Testing	Social Engineering Security Awareness	Spyware Protection	Virus Protection
Security Cameras	Physical Security Awareness	Motion Sensors	Restricted Access Area	Formal Patching Process
Monitor Placements	Dual Power Supply	Firewall	Alert Reporting	Back-up Critical Data

Activity Log Monitoring	Remove Unnecessary Software	Maintenance Logs	Uninterruptible Power Supply	Off-Site Backup
Power Conditioning	Disable / Remove Hardware	Dust Filtering	Humidity Control	Temperature Control
Locked Door	Biometrics	Content Filtering	Disable Terminated Employee Accounts	Inactive Lockout
Business Continuity Plan	Vulnerability Assessment	Off-Site Backup	Formal TSP Review	Monitored Location
Network Diagram	Line Disconnect	Backup Generator	Redundant Systems	

Figure 15 shows the screen the bank management uses to select the controls for each of the assets they outlined in step 1. This screen is displayed for each asset they own.

SMERAM assigns a ranking of high, medium, or low to each of the controls to determine the impact they have on mitigating risk to the assets. Appendix D shows the rating that has been applied to each control.



Controls for Core Banking System

Select the controls you currently implement to mitigate risk

□ Incidence Response Program
□ Privacy Filter
□ Security Cameras
□ Restricted Access Area
□ Physical Security Awareness
□ Monitored Location
□ Test Back-up Recovery
□ Business Continuity Plan Test
□ Dual Power Supply
□ Secured Rack/Cage
□ Temporarily Disable Absent Employee Accounts
□ Vulnerability Assessment: Administrative Privileges
□ Back-up Critical Data
□ Last Successful Logon
□ Forced Session Expiration
□ Social Engineering Awareness
□ Motion Sensors

□ Monitored Placement
□ Locked Door
□ Line Disconnect
□ Spyware Protection
□ Virus Protection
□ Activity Log Monitoring
□ Encrypt Transmitted Data
□ Formal TSP Selection
□ Formal TSP Review
□ Remove Unnecessary Software
□ Business Continuity Plan
□ Access Log Monitoring
□ Back-up Monitoring
□ Change Default Security Settings
□ Inactive Lockout
□ Off-Site Backup
□ Penetration Testing

□ Formal Patching Process
□ Disable Terminated Employee Accounts
□ Access Logs
□ Multi-Factor Authentication
□ Biometric Access
□ Smart Card Access
□ Firewall
□ IDS
□ Unique User Accounts
□ Strong Passwords
□ Incident Response Program Test
□ Authorized User Restrictions
□ Maintenance Logs
□ Redundant Systems
□ Temperature Control
□ UPS
□ Clear Screen Awarenes

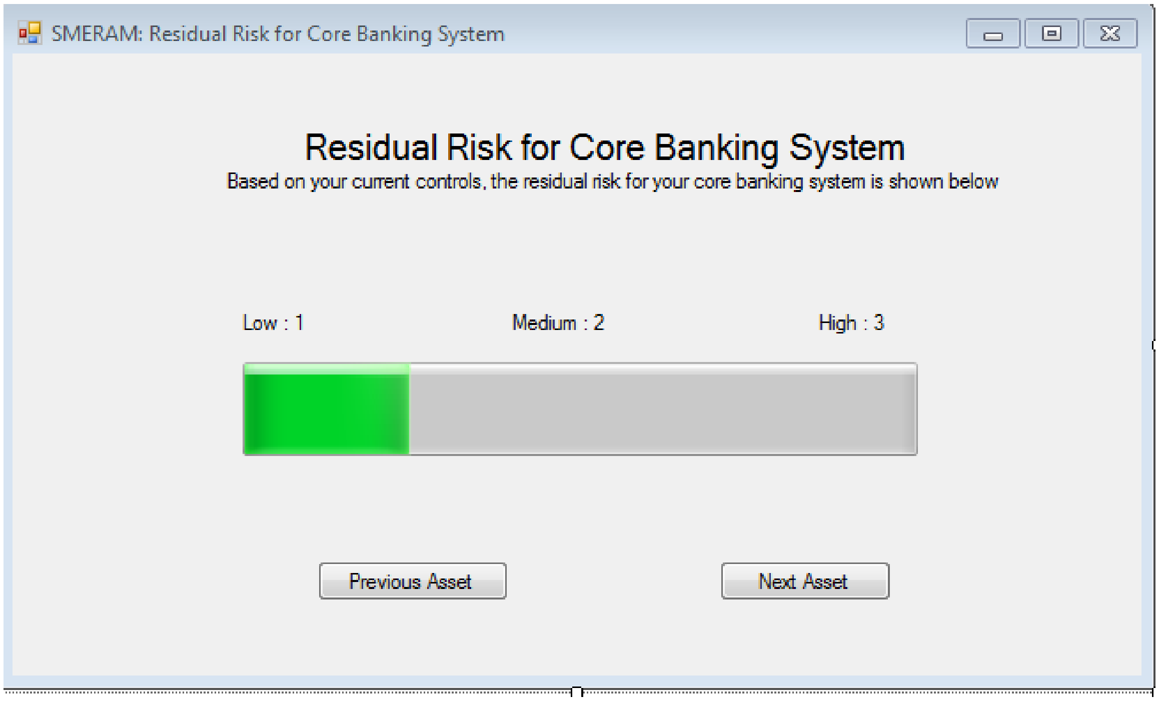
Figure 15 SMERAM: System Controls for Core Banking System

4.1.5 Calculate Residual Risk:

The fifth step is modeled after OCTAVE's Vulnerability step. In this step the financial institution determines the residual risk that is associated with IT assets after the controls are applied. The residual risk is the risk the asset imposes after having controls applied to it. Ideally, the controls will reduce your assets risk. It is extremely important to note that applying controls to IT assets does not completely eliminate the risk the asset imposes to the institution. Risk can only be at an acceptable level, not a "zero" level.

The financial institution has already inputted their assets and service providers, as outlined in step 1. In step 2, they were given the threats that are associated with their assets. Next, the financial institution outlined the controls they apply from the given control list. Next, the system displays the residual risk associated with their information technology assets. SMERAM calculates residual risk by determining the available controls, and dividing the applied controls, by remaining, unapplied controls. Figure 16 depicts the residual risk calculation of a core banking system.

To calculate the residual risk SMERAM references the inherent risk value, which is the initial value placed on the asset. The inherent risk, which is the treats associated with the asset, has an equal amount of controls. Meaning, if there is 100 points of threats, there is 100 points of available controls. SMERAM then analyzes the controls that are actually implemented to mitigate risk. SMERAM then compares the initial value with no controls implemented, and the value with controls implemented. The initial value, is then compared to the implement controls value, to see what percentage of controls available are being implements. For example, if the available controls have a total sum of 100 (high is 3, medium is 2, low is 1), and they are implementing a host of controls that total 80, the SMFI is implementing 80% of what is available. The final value on the High (3), Medium (2), and Low (1) scale would be 2.42, which was calculated by taking .8 divided by .33; .8 is the percentage of controls implemented, and .33 is used because of the scales ratio.



Residual Risk for Core Banking System

Based on your current controls, the residual risk for your core banking system is shown below

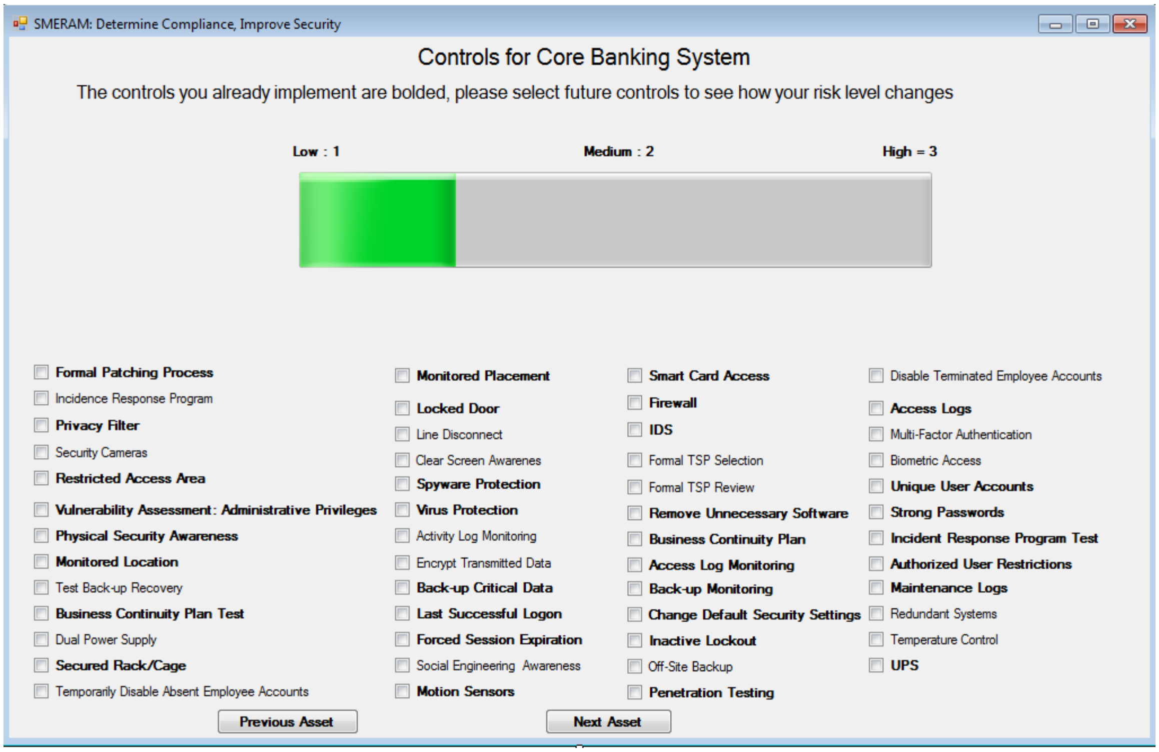
Figure 16 SMERAM: Residual Risk for Core Banking System

4.1.6 Preliminary Results and Reporting

The sixth step is modeled after both NIST and COBIT. The NIST step Results, and the COBIT step Monitor and Evaluate are combined for this step. This step revolves around reporting preliminary results of the RA and improving the process. In this step, the organization learns if they are incompliance with the laws that govern the industry. They also get a firsthand look at what they are currently doing and what they can do to improve their security.

In terms of regulatory compliance, conducting an annual RA by the management team earns the compliance approval.

In this step the financial institution has a screen that is a combination to the screen in the previous step. On the screen the institution views a particular asset, the current controls implemented, and the progress bar which indicates their residual risk. The financial institution can then select future controls they would like to implement to see how their risk level for their asset will be reduced; this is demonstrated in Figure 15. This is a demonstration of how SMERAM is helps in the decision making process. The SMFI can use the results of their RA to determine how to spend their limited information security budget.



Controls for Core Banking System

The controls you already implement are bolded, please select future controls to see how your risk level changes

- □ **Formal Patching Process**
- □ Incidence Response Program
- □ **Privacy Filter**
- □ Security Cameras
- □ **Restricted Access Area**
- □ **Vulnerability Assessment: Administrative Privileges**
- □ **Physical Security Awareness**
- □ **Monitored Location**
- □ Test Back-up Recovery
- □ **Business Continuity Plan Test**
- □ Dual Power Supply
- □ **Secured Rack/Cage**
- □ Temporarily Disable Absent Employee Accounts
- □ **Monitored Placement**
- □ **Locked Door**
- □ Line Disconnect
- □ Clear Screen Awarenes
- □ **Spyware Protection**
- □ **Virus Protection**
- □ Activity Log Monitoring
- □ Encrypt Transmitted Data
- □ **Back-up Critical Data**
- □ **Last Successful Logon**
- □ **Forced Session Expiration**
- □ Social Engineering Awareness
- □ **Motion Sensors**
- □ **Smart Card Access**
- □ **Firewall**
- □ **IDS**
- □ Formal TSP Selection
- □ Formal TSP Review
- □ **Remove Unnecessary Software**
- □ **Business Continuity Plan**
- □ **Access Log Monitoring**
- □ **Back-up Monitoring**
- □ **Change Default Security Settings**
- □ **Inactive Lockout**
- □ Off-Site Backup
- □ **Penetration Testing**
- □ Disable Terminated Employee Accounts
- □ **Access Logs**
- □ Multi-Factor Authentication
- □ Biometric Access
- □ **Unique User Accounts**
- □ **Strong Passwords**
- □ **Incident Response Program Test**
- □ **Authorized User Restrictions**
- □ **Maintenance Logs**
- □ Redundant Systems
- □ Temperature Control
- □ **UPS**

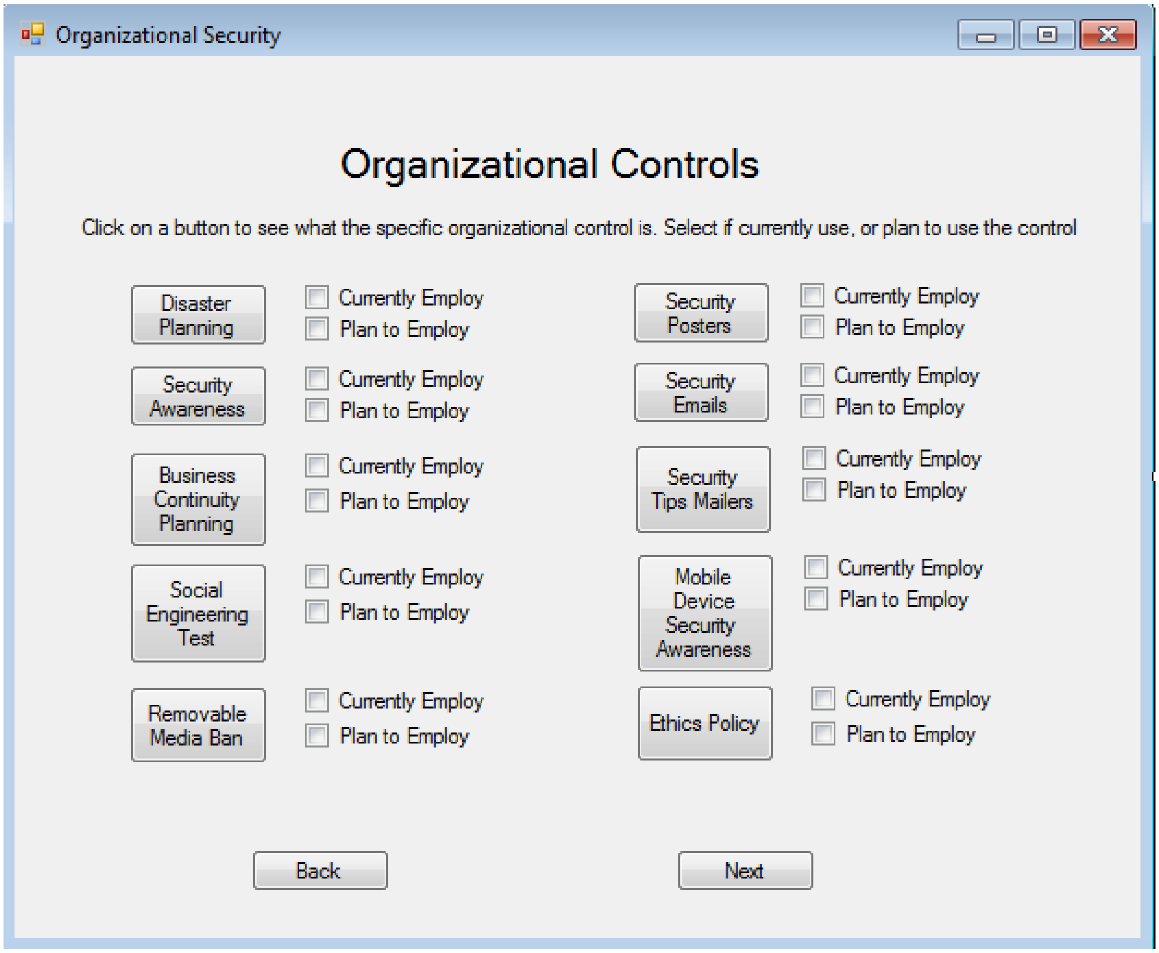
Figure 17 SMERAM: Determine Compliance, Improve Security

4.1.7 Apply Organizational Controls:

The final step, which is designed after ISOs Organizational Security step, allows the financial organization determines safeguards the bank want to implement on an organizational level, not system level as outlined in the previous steps above. Organizational security allows the SMFI to determine what security practices should be implemented to establish sound information security practices to support the entire organization, opposed to just a single asset.

In the previous steps, the SMFI determined their asset based RA, in this step the SMFI works to address the security for the entire organization.

A security awareness program would be an excellent example. Getting all employees' familiar with information security is a great way to make people feel involved. There are different things you can do, such as posters, fliers, email reminders, among other activities. As indicated in Figure 16, the SMFI can select an organizational control, learn about what it is, and then determine if they currently or plan to employ the control.



Organizational Security

Organizational Controls

Click on a button to see what the specific organizational control is. Select if currently use, or plan to use the control

Figure 18 SMERAM: Organizational Security & Controls

5.0 Single Case Study, Anonymous SMFI

5.1 Case Study Research

For validation and evaluation of SMERAM a single case study was completed. There are five rationales for selecting a single case study opposed to a multiple case study (Yin, 2003):

1. The first rationale for adopting a single case study is when the case represents the critical case in evaluating and testing a well-formed theory. The theory that is being evaluated needs to be clean with the propositions and the circumstances within the propositions that are being perceived as true. A single case study is used to confirm, challenge, or extend the given theory. A single case study can be adopted to determine whether a theory's propositions are accurate or whether some alternative set of explanations could prove to be more relevant.
2. The second rationale for a single case study is when the study represents a unique or extreme case. These two situations commonly occur in clinical psychology, when a diagnosis is so rate, it would be important to document all findings when analyzing the data.
3. The third rationale for a single case study is when the single case is the representative or typical case for the environment. The lessons learned from this type of study have proved to be indicative of the lesions learned had the case study been a multiple case study.

4. The fourth rationale for a single case study is when the study is considered a revelatory case. This situation is used when a research has an opportunity to observe a phenomenon that was previously inaccessible to scientific investigations.
5. The fifth rationale for implementing a single case study is longitudinal studies. This situation is used when a study is compromised of two or more points of time. For example you conduct your experiment one year, and do a follow-up the next year.

A single case study was selected for testing SMERAM due to the third and fifth rationales. First, the third rationale, because it indicates if a single case is the representative or typical case for the environment then one single case study is sufficient. The SMFI that was selected for deployment doesn't have any impact of the outcome of the research. Regardless of what SMFI was used, the results from deployment would have been the same. Second, the firth rational is used because the study will be conducted over two years. The first year will be the initial interview and risk assessment. The second year will be compromised of a follow-up and interview.

One downfall of single case studies is that they might prove to be different from the initial case design. As a result, single-case design requires very careful thought and investigation of the potential case to minimize the occurrence of misrepresentation (Yin, 2003).

The case study allowed the researchers to work close with the financial institution to get a firsthand look at the strengths and weaknesses of SMERAM implemented in the SMFI.

5.2 Single Case Study

The researchers piloted the generic SMERAM model to understand its strengths and limitations in SMFIs. Specifically, the SMERAM risk assessment model was tested through a case study in a SMFI in South Dakota. The SMFI was sought out by the researchers to perform a voluntary RA in return for publishing data and testing purposes. The SMFI met with the researchers on five separate occasions, four times in the fall of 2007 to complete the SMERAM RA process, and once again during the fall of 2008 to hold a follow-up meeting. Table 20 introduces a step by step account for the four week process during fall of 2007.

Table 20 SMERAM integration into Financial Institution- Overview

Week	What was done
Week 1	The first week involved determining all of the assets that the credit union had. The SMFI had two of their management employees working with the authors to complete the RA. The two management employees were

	not technologically advanced employees. The SMFI employees were given a list of the traditional assets that banks have and had to determine which of the assets that they had.
Week 2	The second week the researchers came bank onsite to review the list of assets, vendors and services providers. After the asset, vendor and service providers were complete, the SMFI needed to determine, what controls they currently apply to mitigate risk. The authors then outlined the threats that applied to each asset which is available from a predefined list. As demonstrated in Figure 11.
Week 3	The third week involved reviewing the controls the SMFI determined were in place, and determining residual risk. Residual risk, as demonstrated in Figure 14 is the risk associated with the asset after controls have been applied. Next the SMFI can review how implementing further controls can further reduce their security risk, as

	demonstrated in Figure 15.
Week 4	The fourth week, the SMFI reviewed the available organizational controls that were available, and selected whether they currently implement, or plan to implement the control. If they do not implement a control, they simply leave it blank; this is indicated in Figure 16. If the SMFI is not certain what the specific control is, they click on the controls button, and there is a description of what the control is, and what it is useful.

5.1.1 Case Study Questionnaire

The case study questions were developed to determine current RA practices and concerns, while also addressing the 5 research problems indicated in section 1.2. The answers to these questions were used to help determine the effectiveness of implementing SMERAM into a SMFI.

1. What are your current risk assessment practices?
2. Are you following a defined model?
3. Who conducts the risk assessment?
4. How often do you complete your assessment?
5. Do you upgrade your assessment throughout the year?
6. What security concerns do you have with your organization?
7. What are you assets?
8. What threats are associated with your assets?
9. What controls do you apply to mitigate risk?
10. Do you feel you have a good handle on your information security?
11. What areas would you like to improve?
12. What type of annual budget do you have for information security?
13. How do you decide to spend your funds?
14. Do you outsource any of your information technology?
15. Are you concerned about your 3rd party service providers security?

Year One Answers: The answers were gathered through an interview during the fall of 2007, answers are paraphrased.

1. What are your current risk assessment practices?

   We have an Excel spreadsheet that the management staff passes around and lists our assets and the acts taken to secure them

2. Are you following a defined model?

   No

3. Who conducts the risk assessment?

   Employee listed 2 personnel in the management team

4. How often do you complete your assessment?

   Whenever we are about to be audited

5. Do you upgrade your assessment throughout the year?

   No

6. What security concerns do you have with your organization?

   None

7. What are you assets?

   The SMFI listed person x computer, person y computer, teller computers, core banking sever, check ordering computer, printer, payroll software, funds transfer system, proof system and lending program

8. What threats are associated with your assets?

   I'm not sure

9. What controls do you apply to mitigate risk?

   Anti-Virus, user accounts and passwords

10. Do you feel you have a good handle on your information security?

    Not really, I'm a loan specialists

11. What areas would you like to improve?

    Not sure what needs to be improved

12. What type of annual budget do you have for information security?

Very limited

13. How do you decide to spend your funds?

Whatever the board of directors says to improve, we improve

14. Do you outsource any of your information technology?

Website, online banking, ATM, credit card processing, and email

15. Are you concerned about your 3rd party service providers security?

No

Year Two Answers: The answers were gathered through an interview during the fall of 2008, answers are paraphrased.

1. What are your current risk assessment practices?

We follow the RA process that you introduced last year [SMERAM]

2. Are you following a defined model?

Yes [SMERAM]

3. Who conducts the risk assessment?

The bank employee listed 2 of the managers

4. How often do you complete your assessment?

Annually

5. Do you upgrade your assessment throughout the year?

Yes, we just had a new Proof System installed, and we updated our assets, and *knew what controls were on the previous system, and what to implement on this system*

6. What security concerns do you have with your organization?

Increased security concerns with 3rd party service providers.

7. What are you assets?

The organization showed the researcher a list of assets from their RA- Researcher reviewed and determined their work was highly accurate

8. What threats are associated with your assets?

The organization showed the researcher a list of threats associated with their assets- Researcher reviewed and determined their work was highly accurate

9. What controls do you apply to mitigate risk?

The organization showed the researcher a list of controls associated with their assets- Researcher reviewed and determined their work was highly accurate

10. Do you feel you have a good handle on your information security?

Yes, we feel that know we have a model to follow, and even though we don't fully understand the details of all the technology, we feel we can adequately protect our assets

11. What areas would you like to improve?

More automation of the process

12. What type of annual budget do you have for information security?

Very minimal

13. How do you decide to spend your funds?

The assets with the highest inherent and residual risk

14. Do you outsource any of your information technology?

Yes, quite a bit; website, online banking, card processing and ATM

15. Are you concerned about your 3rd party service providers security?

Yes, we have heard there have been a few breaches at different, service providers, however, none of ours have been hit

To further evaluate the effectiveness of SMERAM, an evaluation matrix was created to triangulate the model with the objectives of the research along with the case study. Table 21 outlines the matrix and the research objectives. Each area of the matrix was aided by the interview questions, which are listed after the matrix.

Table 21 Evaluation Matrix

Evaluation Matrix			
Resource Effectiveness	**Financial Limitations**	**Staffing Limitations**	**Time Limitations**
	Interview	Interview	Interview
Value added / Decision Making	**Measure current knowledge**	**Identify Areas of Risk**	**Decision Making**
	Interview / Observation	Assessment Results	Assessment Results
Organizational Acceptance	**Appropriate of Model Size**	**Organization Awareness Lacking**	**Not part of scoping**
	Interview/RA Report	Interview	Interview

1. Resource Effectiveness: Financial Limitations

Questions Asked

- What type of annual budget do you have for information security?
- How do you decide to spend your funds?
- Do you outsource any of your information technology?
  - Year One Answers
    - Very limited
    - Whatever the BOD says to improve, we improve
    - Website, online banking, ATM, credit card processing, and email
  - Year Two Answers
    - Very minimal
    - The assets with the highest inherent and residual risk
    - Quite a bit; website, online banking, card processing, and email

The second question asked, “How do you decided to spend your funds,” proved to be very informative on how SMERAM helps SMFIs make decisions. In year one, the SMFI relied on the board of directors to initiate the spending of IT dollars. In year two, the SMFI used SMERAM to determine which assets impose the greatest amount of risk to the institution, which is where they spent their IT dollars. This is one of the objectives of this research.

2. Resource Effectiveness: Staffing Limitations

Questions Asked

- Who conducts the risk assessment?
- How often do you complete your assessment?
- Do you upgrade your assessment throughout the year?
- Do you outsource any of your information technology?
    - Year One Answers
        - Two Personnel
        - Whenever we are about to be audited
        - No
        - Website, online banking, ATM, credit card processing, and email
    - Year Two Answers
        - Two members of the management team
        - Annually
        - Yes, whenever there is a major change to the organization
        - Quite a bit; website, online banking, card processing, and email

The second question, “How often do you complete your assessment,” demonstrated that SMERAM is effective in bringing the institution into compliance with the regulation that governs their industry. In year one, the SMFI only complete the RA when they were about to be audited; which is every 18 months. With SMERAM the SMFI conducted the RA annually, which bring the institution from out of compliance to in compliance. This is one of the objectives of this research.

3. Resource Effectiveness: Time Limitations

Questions Asked

- What are your current risk assessment practices?
- Are you following a defined model?
- How often do you complete your assessment?
- Do you upgrade your assessment throughout the year?

  - Year One Answers

    - Excel Spreadsheet
    - No
    - Whenever we are about to get audited
    - No
    - Website, online banking, ATM, credit card processing, and email

  - Year Two Answers

    - Model introduced last year; SMEREAM
    - Yes, SMERAM
    - Annually
    - Yes, whenever there is a change: New proof system
    - Quite a bit; website, online banking, card processing, and email

The first question asks the SMFI, "What are your current risk assessment practices," this question showed the researchers that the SMFI went from not gaining any value from their RA to a RA that is value added to the SMFI.

4. Value Added/ Decision Making: Measure Current Knowledge

Questions Asked

- What security concerns do you have with your organization?
- What are you assets?
- What threats are associated with your assets?

    - Year One Answers

        - None
        - SMFI listed Person Xs computer, Person Ys computer, teller computers, core banking server, check ordering computer, printer, payroll software, funds transfer system, proof system and lending program
        - I'm not sure

    - Year Two Answers

        - Increased security concerns with TSP
        - The organization showed the researcher a list of assets that were found with their use of SMERAM, this was checked by the researchers and proved to be correct
        - The organization showed the researchers a list of threats associated with their assets form SMERAM

The three questions demonstrate that the SMFI went from merely appeasing regulators to conducting a RA that adds values to the institution. This is one of the objectives of the research.

5. Value Added/ Decision Making: Identify Areas of Risk

Questions Asked

- What controls do you apply to mitigate risk?
- Do you feel you have a good handle on your information security?
- What areas would you like to improve?
- Are you concerned about your 3rd party service providers security?

- Year One Answers
    - Anti-Virus, ser accounts and passwords
    - Not really, I'm a loan specialists
    - Not sure what needs to be improved
    - No
- Year Two Answers
    - The organization showed the researchers a list of controls associated with their assets. The researchers reviewed the list, and it proved to be accurate
    - Yes, we feel we know we have a model to follow, and even though we don't fully understand the details, we feel we can adequately protect our assets
    - More automation of the process
    - Yes, we have heard there have been a few breaches at different service providers, however none of ours have been compromised.

The second question asks the SMFI, "Do you feel you have a good handle on your information security ," this question showed the researchers that the SMFI went from not feeling they couldn't conduct a value added RA to feeling they could conduct a reliable RA for the institution.

7. Value Added/ Decision Making: Decision Making

Questions Asked

- Do you upgrade your assessment throughout the year?
- What security concerns do you have with your organization?
- What areas would you like to improve?

  - Year One Answers

    - No
    - None
    - Note sure what needs to be improved

  - Year Two Answers

    - Yes, whenever there is a major change
    - Increase security concerns with TSP
    - More automation

The second question asked the institution, “What security concerns do you have with your organization.” In year one, the SMFI did have any concerns, in year two the SMFI was aware of security concerns with TSP, and that was their focus.

8. Organizational Acceptance: Appropriateness of Model Size

Questions Asked

- What are your current risk assessment practices?
- Are you following a defined model?
- Do you feel you have a good handle on your information security?
- What areas would you like to improve?

  - Year One Answers

    - Excel spreadsheet passed around
    - No

    - Not really, I'm a loan specialist
    - Not sure what needs to be improved

  - Year Two Answers

    - We follow the RA process introduced last year
    - Yes, SMERAM
    - Yes, we feel that know we have a model to follow, and even though we don't fully understand the details of all the technology, we feel we can adequately protect our assets
    - More automation

8. Organizational Acceptance: Organization Awareness Lacking

Questions Asked

- What security concerns do you have with your organization?
- Do you feel you have a good handle on your information security?
- What areas would you like to improve?
- Are you concerned about your 3rd party service providers security?

  - Year One Answers

    - None
    - Not really, I'm a loan specialist
    - Not sure what needs to be improved
    - No

  - Year Two Answers

    - Increased concerns with TSP
    - Yes, we feel that know we have a model to follow, and even though we don't fully understand the details of all the technology, we feel we can adequately protect our assets
    - More Automation

        - Yes, we have heard there have been a few breaches at different service providers, however non of ours have been hit

9. Organizational Acceptance: Not part of scoping

Questions Asked

- What are your current risk assessment practices?
- Are you following a defined model?
- Who conducts the risk assessment?

    - Year One Answers

        - Excel Spreadsheet passed around management
        - No
        - 2 personnel

    - Year Two Answers

        - RA model introduced last year, SMERAM
        - Yes
        - 2 members of the management team

The overall message the researchers received from the two interviewers is that the information security posture at the SMFI increased from year one to year two. The SMFI stated that while they are still unsure of their abilities to handle information technology on the technical side, they believe they can manage the security of the systems.

The SMFIs managers stated that they feel they have a better grasp on their assets and countermeasures needed to protect the organization and their customer's personal data. The SMFI also was using the data provided by SMERAM to decide how to spend their information security budget.

The interview process helped the researches identify whether or not SMERAM helped the SMFI handle the core objectives of this research, which was financial limitations, staffing limitations, aid in the decision making process, all while being honed to the financial sector.

The overall message the researchers received from the anonymous SMFI is that they were surprised how easy the RA process could be, along with the added value it gave to their institution. The two management employees indicated were impressed with their ability to conduct a viable RA involving their information technology, given their nontechnical background.

The SMFI found that determining their assets and service providers was easier than expected, and when compared to previous RA's they found they had more assets than they were reporting before. This means, they were not only under reporting their assets, they were giving zero consideration to their unreported assets security. This incident is a serious concern.

5.2.1 Step One: Inventory and Audit Assets

In this step, the financial institution outlined having the following assets. The assets with an "*" indicate the asset management has been outsourced.

1- Deposit Platform*

2- FinCen

3- Advantage ATM*

4- Anti-Virus Software

5- Check Ordering Website*

6- Credit Bureau Website*

7- CU Serve Core System*

8- Desktop Computers

9- E-Mail*

10- Firewall*

11- Funds Transfer System*

12- Internet Banking System*

13- Printers

14- Router

15- Switch

Table 22, outlines typical assets that are located in SMFIs, the SMFI had some of the assets as indicated in the list above, but not all of the assets.

Table 22- Common SMFI Assets & Service Providers

Common SMFI Assets and Service Providers				
Internet Banking System	Core Banking system	Fund Transfer System	Credit Bureau Website	Deposit Platform
Printers	Notebook Computers	Desktop Computers	Firewall	Lending Program
Marketing Software	Payday Lending	Payroll Software	PDA’s	Router
Switch	Firewall	Smart Phones	Terminal Services	Web Server
Email Server	Accounting Software	Background Checking Website	Anti-Virus Software	ATM
Call Reporting Software	HMDA	Operating Systems	Merchant Card Processing System	Intrusion Detection System
File Server	Item Imaging	Local Area Network	Check Ordering Website	Check Reader / Sorter
VoIP	Deb/Credit Cards	Bank Website	Application Server	Remote Capture Systems
Storage Area Network	Wide Area Network	Proof System		

5.2.2 Step Two: Identify Threats

In this step, the financial institution has already selected their assets and SMERAM determines their corresponding threats. Considering that SMERAM is honed to the SMFI industry, the financial institution did not have to research the threats associated with the asset as it is already pre-defined. The threats associated with typical SMFI assets include environment threats, natural threats, and human threats.

Environment threats include long-term power failure, liquid damage, chemical damage, among others. Natural threats include floods, tornadoes, earthquakes, electrical storms, among others. Human threats include intentional and unintentional acts such as viruses, Trojans and data deletion, and unauthorized access among others.

5.2.3 Step Three: Determine Inherent Risk

The inherent risk is viewed by the financial institution after the assets and threats that are associated with their assets are determined, as indicated in Figure 12 in section 4.1.3. The SMFI views the risk associated with each of their assets with no controls applied. This helps visually demonstrate the importance of controls and mitigating activities. The SMFI can visually determine which assets introduce more risk to the organization. This also gives the SMFI the opportunity to determine which assets needed the greatest protection. In the anonymous SMFI, they found that the assets they outlined introduced risk into the organization in the following order.

1- Core Banking System
2- Deposit Platform*
3- Funds Transfer System*
4- Internet Banking System*
5- FinCen
6- Advantage ATM*
7- Check Ordering Website*
8- Credit Bureau Website*
9- Anti-Virus Software
10- Desktop Computers
11- Firewall*
12- E-Mail*
13- Router
14- Switch
15- Printers

5.2.4 Step Four: Identify Controls

In this step, the SMFI reviewed the controls that are specific to their assets they outlined in step one. Figure 13 outlines a single asset, the Core Banking System, and the controls available to implement on that system. The SMFI see's a screen similar to Figure

13 for each of the assets they outlined in Figure 11 in section 4.1.3. The SMFI has to go through this process for each of the assets they own.

Common controls found in SMFIs are listed in Table 22, Common Controls; this list is not asset specific rather in general terms. A list of assets associated with controls can be found in Appendix D.

Table 23 Common Controls

Common Controls Applied to Assets				
Authorized User Restrictions	Access Logs	Formal TSP Review	Formal TSP Selection	Access Log Monitoring
Invalid Attempt Lockout	Strong Passwords	Unique User Accounts	Encrypt Stored Data	Formal Patching Process
Intrusion Detection/ Prevention	Back-up Critical Data	Change Default Security Settings	Incident Response Program	Incident Response Program Test
Clear Screen Awareness	Forced Session Expiration	Maintenance Logs	Multi-Factor Authentication	System Access Warning
Activity Logs	Change Default Account Settings	Maintenance Log Review	Temporarily Disable Absent Employee Accounts	Vulnerability Assessment: Administrative Privileges
Activity Log Monitoring	Last Successful Logon	Business Continuity Plan Test	Network Diagram	Test Back-up Recovery
Formal TSP Selection	Penetration Testing	Social Engineering Security Awareness	Spyware Protection	Virus Protection
Security Cameras	Physical Security Awareness	Motion Sensors	Restricted Access Area	Formal Patching Process
Monitor Placements	Dual Power Supply	Firewall	Alert Reporting	Back-up Critical Data

Activity Log Monitoring	Remove Unnecessary Software	Maintenance Logs	Uninterruptible Power Supply	Off-Site Backup
Power Conditioning	Disable / Remove Hardware	Dust Filtering	Humidity Control	Temperature Control
Locked Door	Biometrics	Content Filtering	Disable Terminated Employee Accounts	Inactive Lockout
Business Continuity Plan	Vulnerability Assessment	Off-Site Backup	Formal TSP Review	Monitored Location
Network Diagram	Line Disconnect	Backup Generator	Redundant Systems	

5.2.5 Step Five Residual Risk

In this step, the SMFI built on their previous four steps to determine what the residual risk is for their institution technology assets. The SMFI can see what residual risk is left after they apply their controls. In this specific SMFI, they were able to see that they have been doing a good job protecting their assets, however, they could do more to protect their router, switch, desktop computers, and core banking system. The order of volatility, which indicates the assets that have the highest need for further protection for the anonymous SMFI, is listed below.

1- Router

2- Switch

3- Desktop Computers

4- Core Banking System

5- Deposit Platform

6- Firewall

7- FinCen

8- Advantage ATM

9- Anti-Virus Software

10- Check Ordering Website

11- Credit Bureau Website

12- E-Mail

13- Funds Transfer System

14- Internet Banking System

15- Printers

This part of the RA process allows the SMFI to see what order they should consider applying future controls to protect their information systems. This helps the SMFI determine where they should apply their IT security budget.

Further, the SMFI viewed what more controls would mean to their overall security. This step naturally leads to step six, Demonstrate Compliance.

5.2.6 Step Six Demonstrate Compliance

By this step, the SMFI has viewed their assets, threats, controls, and residual risk, and they can see if they are at an adequate protection level for their governing board, which is the FDIC. FDIC mandates an annual RA conducted by the management team, if the RA is at this step in the process they are indeed in compliance.

In this specific case study, the SMFI found that their actions were acceptable to their industry. However, they saw improvements that could be made to their institution that would further protect their institution. The main improvements, as indicated by SMERAM, should be on the router, switch, desktops and core banking system. The SMFI also determine that future controls for each of those assets should include an Incidence Response Program, UPS, Physical Security Awareness, Penetration Testing, and Log File Reviews. These controls, some of which don’t have a monetary price tag, would significantly improve their assets security.

5.2.7 Step Seven Apply Organizational Controls

In the final step, the SMFI looked at available organization security controls that they could implement. Admittedly, the SMFI stated they didn’t do much in terms of organization security awareness. The SMFI reviewed available security controls available at the organizational level. Examples include security awareness posters, emails, and informational sessions.

For this specific SMFI, they determined implementing monthly security awareness emails, and a security awareness program was a great way to start increasing the overall security level of the financial institution.

5.4 Year Two Follow Up Meeting (Fall 2008)

The year two follow up meeting, which was held during the Fall of 2008, gave the researchers the ability to see the model integrated into the SMFI over the course of the year. The researchers were focused on seeing how the SMFI felt SMERAM helped them address their information security needs, while also being user friendly to the management team conducting the RA.

The management team stated they were successful in getting most of their proposal approved by the board of directors; which included the Incidence Response Program, Physical Security Awareness, and UPS's. The management team further stated that they will continue conducting RA's and will use the initial RA as a baseline to view how their IT security is improving.

The management team continued to state they updated their RA during the year and could see a graphical depiction of how their information security improved over the course of the year in SMERAM. For example, the SMFI could see how conducting a vulnerability assessment, and moving backups offsite increased their security level on their assets. The management team also stated that within the month, they would begin their year two RA.

6.0 Conclusion

6.1 Conclusion

Financial Institutions by nature house data that is susceptible to attacks and other malicious actions. The data that is housed in financial institutions can result in identity theft if compromised by a data breach. Due to the inherent risks associated with the financial industry there are regulation requirements that are specific to the financial industry.

Financial institutions, of all sizes, are required to conduct a risk assessment (RA) every year by the FDIC. Large financial institutions, which are typically billions in financial assets, have different abilities and needs compared to smaller financial institutions which are typically millions in financial assets. However, according to the FDIC, both institution sizes have the same regulations and requirements for risk management. Large and small financial institutions have the same FDIC regulation but different resources available in terms of IT staffing, IT budgets, and overall security needs yet overall the FDIC regulations are written in a one-size-fits-all environment.

Small and Medium Sized Financial Institutions (SMFIs) understand they are required by the FDIC to conduct a RA, and they typically approach this process in a manner to appease regulators. The RA process that SMFIs take does not typically result in an accurate RA or add value to their organization (Streff, 2007). RA’s for SMFIs need to identify assets and service providers, outline the risk with each asset, list the countermeasures applied to each asset and demonstrate how effective their current mitigating approach is in reducing the risk to the financial institution (Podhradsky, 2009).

However, a majority of SMFIs handle the RA process in a completely different fashion where bankers pass around an excel spreadsheet and various people throughout the bank list assets and the approach taken to secure the device (Streff, 2007). This process not only results in a grossly inaccurate RA, but it also adds no value to the organization. When organizations conduct RA's in this manner, they are only completing this assessment to conciliate government FDIC regulation, and not using it as a tool for their overall risk management process (Streff, 2007).

Generic RA models have been developed and deployed across several industries, including banking; however generic RA models assume a high level of understanding about banking assets, risks, threats, risk mitigation, and information security policy which is typically found in larger financial institutions. This type of advanced knowledge is usually not found in management (Gautam, 1989). SMFIs need a different approach to solving their information security RA process than their larger financial institutions counterparts. The generic models implemented by larger financial institutions are not applicable to smaller institutions, due to their IT staffing, IT budget, and IT security limitations. A RA model for a SMFI should also include both an asset and organizational assessment (Streff, 2007). Larger financial organizations have the financial and staffing resources to conduct both an asset and organizational based assessment, however SMFIs need to incorporate both assessments into one single assessment (Streff, 2007).

The generic model, SMERAM, which is honed for the specific use in small and medium sized financial institutions, was developed after studying the generic risk assessment models ISO, NIST, OCTAVE, COBIT and CORAS. SMERAM was built on these specific generic RA models.

SMFIs have unique needs that are not adequately addressed with most generic RA models. An RA model for SMFIs needs to address FDIC regulations, IT staffing limitations, financial resource restrictions, all while being tailored towards the banking industry. SMERAM works to address the unique needs of SMFIs.

SMERAM meets FDIC FIL guidelines as it is designed for the RA to be completed every year, and reviewed on an ongoing basis. Furthermore, SMERAM also encourages SMFIs to update their RA whenever there is a major change in their network or information technology infrastructure, which keeps the RA an adaptive and living part of the information security program. This approach adds value to the organization as it helps the financial institution identify and outline their current security posture and allows them make informed decisions regarding their information technology purchases and upgrades.

IT staffing limitations are met with SMERAM as financial institutions do not need a dedicated IT department or staff member on-site to complete the RA. Risk management is a management responsibility and a member of the management team can conduct the RA (Streff, 2007). SMERAM has been specifically created to be completed by both technical and non-technical personnel. Other Generic RA models require a certified consultant or full time IT staff to complete the RA, while SMERAM does not. This unique characteristic of SMERAM reduces the cost of implementation and maintenance which is not typically seen in other generic RA models.

The smaller IT budgets associated with SMFIs are also factored into SMERAM. Most generic RA models such as ISO, NIST, or COBIT require a certified consultant or IT staff to complete the RA, while SMERAM does not, which results in reduced costs for completing a valid and value added RA. Also, SMERAM does not have any subscription costs associated with its implementation, which is unlike other generic RA models.

SMERAM further adds value to the financial institution as it completes both an asset and organizational RA. Not all generic RA models evaluate security in both an asset and organizational level as SMERAM does. This approach saves time and money for SMFIs as only one RA has to be completed.

6. 2 Future Work

The researchers theorize that one way to overcome such diversity and complexity of RA's is to create cohorts of similar businesses. The creation of these "risk assessment realms" will allow for the application and development of tighter standards which can then be applied to each realm. This will also help to overcome the immense diversity among businesses, organizations, and industries, and allow for a relative comparison of threats, probabilities, impacts, and assets to similar organizations. A key value to creating risk realms based on organization size, industry type, or business unit would be the creation of accurate, comparable risk assessments to other organizations in the same realm. Data mining for historical purposes and future trends would then be possible.

The goal of future research would be to identify key "realms" and related fields, then provide a common framework for accurately and consistently measuring risk for the identified realms. The author proposes defining systems and risks as associated with a particular industry for the creation of these realms. While many of the pre-defined threats and their corresponding impacts, probability and volume will apply across several industries, the author feels it is important to compile these lists individually.

Upon completion of identifying a particular realm, the author feels there is need for future research and the creation of a "risk assessment artifact". This would allow for the uniform, standardized risk assessment process which is specifically aimed at particular cohort. The researchers also feel that by introducing network discovery protocols integrating SMERAM into these other realms.

6.3 Limitations of SMEREAM

SMERAM has known limitations, which includes implementation outside of the financial sector. SMERAM, has been tailored towards specific implementation in SMFI's, and in its current form, it isn't appropriate for implementation outside of the financial sector.

SMEREAM was also tested in a single SMFI, according to Yin a single case study is sufficient, and there was only one full implementation of the model.

BIBLIOGRAPHY

(n.d.). Retrieved October 2007, from A Chronology of Data Breaches: http://www.privacyrights.org/ar/ChronDataBreaches.htm

A Chronology of Data Breaches. (2009). Retrieved 2009, from PrivacyRights.Org: http://www.privacyrights.org/ar/chrondatabreaches.htm

Alberts, C. (2002). *Managing information security risks: the OCTAVE approach.* Wesley.

Ali, M. H. (1985). Bayesian Probabilistic Risk Analysis. *ACM* , Vol. 13 pp 5-12.
Benioff, M. R. (2005). Cyber Security: A Crisis of Prioritization. . *President's Information Technolgoy Advisory Committee.*

Benoit, A. A. (2006). A Framework for Information Technology Outsourcing Risk Managment. *ACM Press* , 9-28.

Blakley, B. M. (2001). Information Security in Information Risk Management. *New Secutiy Raradigms.*

Burger, A. K. (2006). US Mobile Security, Part 1L How Great is the Risk?

Cavusoglu, H. M. (2004). A Model for Evaluating IT security Investments. *ACM Press* , 87-92.

Chronology of Data Breaches. (2009, July). Retrieved July 2009, from PrivacyRights: http://www.privacyrights.org/ar/ChronDataBreaches.htm

Data Security Breach Statistics. (2009). Retrieved 2009, from Information Security Analysis: http://www.infosecurityanalysis.com/

Dawson. (2007). *TJX Security Breach Described*. Retrieved 2009, from Slashdot: http://it.slashdot.org/article.pl?sid=07/08/16/207215

Dorofee, C. A. (n.d.). *OCTAVE*. Retrieved 2009, from Software Engineering Institute-Carnegie Mellon University: http://www.cert.org/octave/methodintro.html

Eheo Dimitrakos, J. B. (n.d.). *CORAS- A Framework for Risk Analysis of Security Critical Systems*. Retrieved 2009, from ERCIM News: http://www.ercim.org/publication/Ercim_News/enw49/dimitrakos.html

FDIC FIL 68-99 . (1999, July 7). Retrieved 2009, from FDIC: http://www.fdic.gov/news/news/financial/1999/fil9968.html

FDIC FIL 81-05. (2005, August 18). Retrieved 2009, from FDIC: http://www.fdic.gov/news/news/financial/2005/fil8105.html

Fung, P. &. (2003). Electronic Information Security Documentation. *Australian Computer Society, Inc.* , (pp. 22-31). Darlinghurst, Australia.

Gautam, B. H. (1989). Applications of Qualitative Modeling to Knowlege-based Risk Assessment Studies. *International Congerence on Industrial and Engineering Applications of Artificial Intelligence and Expert Systems.*

Hevner, M. P. (2004). Design Science in Information System Research. *Journal of* .
ISACA. (n.d.). Retrieved 2009, from COBIT: http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981

Lewis, T. G. (2006). Critical Infrasturcure Protection in Homeland Security: Defending a Networkd Nation. Wiley-Interscience.

Martin, C. &. (2002). *ISO Certification*. Retrieved from QP Management Group: http://www.qpmanagementgroup.com/iso2.htm

McCumber, J. (2005). *Assessing and Managing Security Risk in IT Systems: A Structured Methodology.* New York: Auerbach.

Messmer, E. (2009, February). *Data-breach cost rising, study finds*. Retrieved 2009, from NetworkWorld: http://www.networkworld.com/news/2009/020209-data-breach.html

Myerson, J. M. (2002). *Identifying Enterprise Network Vulnerabilities.* New York, NY USA: John Wiley & Sons, Inc.

OCTAVE Information. (n.d.). Retrieved December 2009, from Security Risk Solutions: http://www.securityrisksolutions.com/OCTAVE.htm

Peltier. (2005). *CISSP Prep Book.* New York.

Podhradsky, S. L. (2009). An Innovative Information Technology Risk Assessment Model for Small and Medium-Sized Financial Instituti. *Hawaii International Conference on Business.* Honolulu.

Population- Google- Public Information. (2008, July). Retrieved July 2009, from Google:http://www.google.com/publicdata?ds=uspopulation&met=population&tdim=true&q=what+is+the+population+of+the+united+states

Quality Management Cocktail: ISO, Lean, Six Sigma. (n.d.). Retrieved 2008, from Westgard: http://www.westgard.com/guest30.htm#ISO
Siv-Hilde Houmb, F. d. (n.d.). Towards a UML Profile for Model-Based Risk Assessment . *Sintef Telecom & Informatics* .

Stoneburner, G. G. (2002). *Risk Management Gude for Information Technolgoy*. NIST Special Publication 800-30.

Streff, K. (2007). *Informatin Security in Banking.* IGI Publishing.

The Gramm-Leach Bliley Act. (1999). Retrieved 2009, from FDIC: http://www.ftc.gov/privacy/privacyinitiatives/glbact.html

Westguard. (2005). *Quality Management Cocktail* . Retrieved from Quality Management Cocktail: http://www.westgard.com/guest30.htm

Woerner, R. (2007). Security Friday Fast Fact: Risky Business (without Tom Cruise).
Yin. (2003). *Case Study Research- Third Edition.* Thousand Oaks: Sage .

Appendix A:

FDIC FIL 68-99

Risk Assessment Tools and Practices
for Information System Security

INTRODUCTION

The purpose of this paper is to provide financial institutions and examiners with background information and guidance on various risk assessment tools and practices related to information security. Institutions using the Internet or other computer networks are exposed to various categories of risk that could result in the possibility of financial loss and reputational harm. Given the rapid growth of the Internet and networking technology, the available risk assessment tools and practices are becoming more important for information security.

This paper provides a summary of critical points, discusses components of a sound information security program, and describes the risk assessment and risk management processes for information security. The appendix provides specific information on certain risk assessment tools and practices that may be part of an institution's information security program. The paper and appendix are intended to provide useful information and guidance, not to create new examination standards, impose new regulatory requirements, or represent an exclusive description of the various ways financial institutions can implement effective information security programs.

Whether financial institutions contract with third-party providers[1] for computer services such as Internet banking, or maintain computer services in-house, bank management is responsible for ensuring that systems and data are protected against risks associated with emerging technologies and computer networks. If a bank is relying on a third-party provider, management must generally understand the provider's information security program to effectively evaluate the security system's ability to protect bank and customer data.

The FDIC has previously issued guidance on information security concerns such as data privacy and confidentiality, data integrity, authentication, non-repudiation, and access control/system design. This paper is designed to supplement Financial Institution Letter 131-97, "Security Risks Associated With the Internet," dated December 18, 1997, and to complement the FDIC's safety and soundness electronic banking examination procedures. Related guidance can be found in the FFIEC Information Systems Examination Handbook.

SUMMARY OF CRITICAL POINTS

To ensure the security of information systems and data, financial institutions should have a sound information security program that identifies, measures, monitors, and manages potential risk exposure. Fundamental to an effective information security program is ongoing risk assessment of threats and vulnerabilities surrounding networked and/or Internet systems. Institutions should consider the various measures available to support and enhance information security programs. The appendix to this paper describes certain vulnerability assessment tools and intrusion detection methods that can be useful in preventing and identifying attempted external break-ins or internal misuse of information systems. Institutions should also consider plans for responding to an information security incident.

INFORMATION SECURITY PROGRAM

A financial institution's board of directors and senior management should be aware of information security issues and be involved in developing an appropriate information security program. A comprehensive information security policy should outline a proactive and ongoing program incorporating three components:

- Prevention
- Detection
- Response

Prevention measures include sound security policies, well-designed system architecture, properly configured firewalls, and strong authentication programs. This paper discusses two additional prevention measures: vulnerability assessment tools and penetration analyses. Vulnerability assessment tools generally involve running scans on a system to proactively detect known vulnerabilities such as security flaws and bugs in software and hardware. These tools can also detect holes allowing unauthorized access to a network, or insiders to misuse the system. Penetration analysis involves an independent party (internal or external) testing an institution's information system security to identify (and possibly exploit) vulnerabilities in the system and surrounding processes. Using vulnerability assessment tools and performing regular penetration analyses will assist an institution in determining what security weaknesses exist in its information systems.

Detection measures involve analyzing available information to determine if an information system has been compromised, misused, or accessed by unauthorized individuals. Detection measures may be enhanced by the use of intrusion detection systems (IDSs) that act as a burglar alarm, alerting the bank or service provider to potential external break-ins or internal misuse of the system(s) being monitored.

Another key area involves preparing a response program to handle suspected intrusions and system misuse once they are detected. Institutions should have an effective incident response program outlined in a security policy that prioritizes incidents, discusses appropriate responses to incidents, and establishes reporting requirements.

The appendix provides a detailed discussion on prevention (vulnerability assessment tools and penetration analyses), detection (IDS tools), and response measures. Before implementing some or all of these measures, an institution should perform an information security risk assessment. Depending on the risk assessment, certain risk assessment tools and practices discussed in this paper may be appropriate. However, use of these measures should not result in decreased emphasis on information security or the need for human expertise.

RISK ASSESSMENT/MANAGEMENT

A thorough and proactive risk assessment is the first step in establishing a sound security program. This is the ongoing process of evaluating threats and vulnerabilities, and establishing an appropriate risk management program to mitigate potential monetary losses and harm to an institution's reputation. Threats have the potential to harm an institution, while vulnerabilities are weaknesses that can be exploited.

The extent of the information security program should be commensurate with the degree of risk associated with the institution's systems, networks, and information assets. For example, compared to an information-only Web site, institutions offering transactional Internet banking activities are exposed to greater risks. Further, real-time funds transfers generally pose greater risks than delayed or batch-processed transactions because the items are processed immediately. The extent to which an institution contracts with third-party vendors will also affect the nature of the risk assessment program.

Performing the Risk Assessment and Determining Vulnerabilities

Performing a sound risk assessment is critical to establishing an effective information security program. The risk assessment provides a framework for establishing policy guidelines and identifying the risk assessment tools and practices that may be appropriate for an institution. Banks still should have a written information security policy, sound security policy guidelines, and well-designed system architecture, as well as provide for physical security, employee education, and testing, as part of an effective program.

When institutions contract with third-party providers for information system services, they should have a sound oversight program. At a minimum, the security-related clauses of a written contract should define the responsibilities of both parties with respect to data confidentiality, system security, and notification procedures in the event of data or system compromise. The institution needs to conduct a sufficient analysis of the provider's security program, including how the provider uses available risk assessment tools and practices. Institutions also should obtain copies of independent penetration tests run against the provider's system.

When assessing information security products, management should be aware that many products offer a combination of risk assessment features, and can cover single or multiple operating systems. Several organizations provide independent assessments and certifications of the adequacy of computer security products (e.g., firewalls). While the underlying product may be certified, banks should realize that the manner in which the products are configured and ultimately used is an integral part of the products' effectiveness. If relying on the certification, banks should understand the certification process used by the organization certifying the security product. Other examples of items to consider in the risk assessment process include:

- Identifying mission-critical information systems, and determining the effectiveness of current information security programs. For example, a vulnerability might involve critical systems that are not reasonably isolated from the Internet and external access via modem. Having up-to-date inventory listings of hardware and software, as well as system topologies, is important in this process.
- Assessing the importance and sensitivity of information, and the likelihood of outside break-ins (e.g., by hackers) and insider misuse of information. For example, if a large depositor list were made public, that disclosure could expose the bank to reputational risk and the potential loss of deposits. Further, the institution could be harmed if human resource data (e.g., salaries and personnel FILes) were made public. The assessment should identify systems that allow the transfer of funds, other assets, or sensitive data/confidential information, and review the appropriateness of access controls and other security policy settings.
- Assessing the risks posed by electronic connections with business partners. The other entity may have poor access controls that could potentially lead to an indirect compromise of the bank's system. Another example involves vendors that may be allowed to access the bank's system without proper security safeguards, such as firewalls. This could result in open access to critical information that the vendor may have "no need to know."
- Determining legal implications and contingent liability concerns associated with any of the above. For example, if hackers successfully access a bank's system and use it to subsequently attack others, the bank may be liable for damages incurred by the party

that is attacked.

Potential Threats To Consider

Serious hackers, interested computer novices, dishonest vendors or competitors, disgruntled current or former employees, organized crime, or even agents of espionage pose a potential threat to an institution's computer security. The Internet provides a wealth of information to banks and hackers alike on known security flaws in hardware and software. Using almost any search engine, average Internet users can quickly find information describing how to break into various systems by exploiting known security flaws and software bugs. Hackers also may breach security by misusing vulnerability assessment tools to probe network systems, then exploiting any identified weaknesses to gain unauthorized access to a system. Internal misuse of information systems remains an ever-present security threat.

Many break-ins or insider misuses of information occur due to poor security programs. Hackers often exploit well-known weaknesses and security defects in operating systems that have not been appropriately addressed by the institution. Inadequate maintenance and improper system design may also allow hackers to exploit a security system. New security risks arise from evolving attack methods or newly detected holes and bugs in existing software and hardware. Also, new risks may be introduced as systems are altered or upgraded, or through the improper setup of available security-related tools. An institution needs to stay abreast of new security threats and vulnerabilities. It is equally important to keep up to date on the latest security patches and version upgrades that are available to fix security flaws and bugs. Information security and relevant vendor Web sites contain much of this information.

Systems can be vulnerable to a variety of threats, including the misuse or theft of passwords. Hackers may use password cracking programs to figure out poorly selected passwords. The passwords may then be used to access other parts of the system. By monitoring network traffic, unauthorized users can easily steal unencrypted passwords. The theft of passwords is more difficult if they are encrypted. Employees or hackers may also attempt to compromise system administrator access (root access), tamper with critical FILes, read confidential e-mail, or initiate unauthorized e-mails or transactions.

Hackers may use "social engineering," a scheme using social techniques to obtain technical information required to access a system. A hacker may claim to be someone authorized to access the system such as an employee or a certain vendor or contractor. The hacker may then attempt to get a real employee to reveal user names or passwords, or even set up new computer accounts. Another threat involves the practice of "war dialing," in which hackers use a program that automatically dials telephone numbers and searches for modem lines that bypass network firewalls and other security measures. A few other common forms of system attack include:

- Denial of service (system failure), which is any action preventing a system from operating as intended. It may be the unauthorized destruction, modification, or delay of service. For example, in a "SYN Flood" attack, a system can be flooded with requests to establish a connection, leaving the system with more open connections than it can support. Then, legitimate users of the system being attacked are not allowed to connect until the open connections are closed or can time out.
- Internet Protocol (IP) spoofing, which allows an intruder via the Internet to effectively impersonate a local system's IP address in an attempt to gain access to that system. If other local systems perform session authentication based on a connection's IP address, those systems may misinterpret incoming connections from the intruder as originating from a local trusted host and not require a password.
- Trojan horses, which are programs that contain additional (hidden) functions that usually allow malicious or unintended activities. A Trojan horse program generally performs unintended functions that may include replacing programs, or collecting, falsifying, or destroying data. Trojan horses can be attached to e-mails and may create a "back door" that allows unrestricted access to a system. The programs may automatically exclude logging and other information that would allow the intruder to be traced.
- Viruses, which are computer programs that may be embedded in other code and can self-replicate. Once active, they may take unwanted and unexpected actions that can result in either nondestructive or destructive outcomes in the host computer programs. The virus program may also move into multiple platforms, data files, or devices on a system and spread through multiple systems in a network. Virus programs may be contained in an e-mail attachment and become active when the attachment is opened.

CONCLUSION

It is important for financial institutions to develop and implement appropriate information security programs. Whether systems are maintained in-house or by third-party vendors, appropriate security controls and risk management techniques must be employed. A security program includes effective security policies and system architecture, which may be supported by the risk assessment tools and practices discussed in this guidance paper and appendix. Information security threats and vulnerabilities, as well as their countermeasures, will continue to evolve. As such, institutions should have a proactive risk assessment process that identifies emerging threats and vulnerabilities to information systems.

A sound information security policy identifies prevention, detection, and response measures. The appendix provides more details on risk assessment tools and practices that may be used to improve information security programs. Preventive measures may include regularly using vulnerability assessment tools and conducting periodic penetration analyses. Intrusion detection tools can be effective in detecting potential intrusions or system misuse. Institutions should also develop a response program to effectively handle any information security breaches that may occur.

[1] For the purposes of this paper, "third-party provider" is broadly defined. Third-party providers include entities that may provide the following services or products to institutions: system design, development, administration, and maintenance services; data processing services; and hardware and/or software solutions.

APPENDIX

PART ONE – PREVENTION: Discusses the use of vulnerability assessment tools and penetration analyses. When used regularly, both techniques can be integral components of an institution's information security program.

VULNERABILITY ASSESSMENT TOOLS

Vulnerability assessment tools, also called security scanning tools, assess the security of network or host systems and report system vulnerabilities. These tools can scan networks, servers, firewalls, routers, and applications for vulnerabilities. Generally, the tools can detect known security flaws or bugs in software and hardware, determine if the systems are susceptible to known attacks and exploits, and search for system vulnerabilities such as settings contrary to established security policies.

In evaluating a vulnerability assessment tool, management should consider how frequently the tool is updated to include the detection of any new weaknesses such as security flaws and bugs. If there is a time delay before a system patch is made available to correct an identified weakness, mitigating controls may be needed until the system patch is issued.

Generally, vulnerability assessment tools are not run in real-time, but they are commonly run on a periodic basis. When using the tools, it is important to ensure that the results from the scan are secure and only provided to authorized parties. The tools can generate both technical and management reports, including text, charts, and graphs. The vulnerability assessment reports can tell a user what weaknesses exist and how to fix them. Some tools can automatically fix vulnerabilities after detection.

Host- Versus Network-Based Vulnerability Assessment Tools

As in intrusion detection systems, which are discussed later in this appendix, there are generally two types of vulnerability assessment tools: host-based and network-based. Another category is sometimes used for products that assess vulnerabilities of specific applications (application-based) on a host. A host is generally a single computer or workstation that can be connected to a computer network. Host-based tools assess the vulnerabilities of specific hosts. They usually reside on servers, but can be placed on specific desktop computers, routers, or even firewalls. Network-based vulnerability assessment tools generally reside on the network, specifically analyzing the network to determine if it is vulnerable to known attacks. Both host- and network-based products offer valuable features, and the risk assessment process should help an institution determine which is best for its needs. Information systems personnel should understand the types of tools available, how they operate, where they are located, and the output generated from the tools.

Host-based vulnerability assessment tools are effective at identifying security risks that result from internal misuse or hackers using a compromised system. They can detect

holes that would allow access to a system such as unauthorized modems, easily guessed passwords, and unchanged vendor default passwords. The tools can detect system vulnerabilities such as poor virus protection capabilities; identify hosts that are configured improperly; and provide basic information such as user log-on hours, password/account expiration settings, and users with dial-in access. The tools may also provide a periodic check to confirm that various security policies are being followed. For instance, they can check user permissions to access FILes and directories, and identify FILes and directories without ownership.

Network-based vulnerability assessment tools are more effective than host-based at detecting network attacks such as denial of service and Internet Protocol (IP) spoofing. Network tools can detect unauthorized systems on a network or insecure connections to business partners. Running a host-based scan does not consume network overhead, but can consume processing time and available storage on the host. Conversely, frequently running a network-based scan as part of daily operations increases network traffic during the scan. This may cause inadvertent network problems such as router crashes.

PENETRATION ANALYSIS

After the initial risk assessment is completed, management may determine that 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.

A penetration analysis usually involves a team of experts who identify an information system's vulnerability to a series of attacks. The evaluators may attempt to circumvent the security features of a system by exploiting the identified vulnerabilities. Similar to running vulnerability scanning tools, the objective of a penetration analysis is to locate system vulnerabilities so that appropriate corrective steps can be taken.

The analysis can apply to any institution with a network, but becomes more important if system access is allowed via an external connection such as the Internet. The analysis should be independent and may be conducted by a trusted third party, qualified internal audit team, or a combination of both. The information security policy should address the frequency and scope of the analysis. In determining the scope of the analysis, items to consider include internal vs. external threats, systems to include in the test, testing methods, and system architectures.

A penetration analysis is a snapshot of the security at a point in time and does not provide a complete guaranty that the system(s) being tested is secure. It can test the effectiveness of security controls and preparedness measures. Depending on the scope of the analysis, the evaluators may work under the same constraints applied to ordinary internal or external users. Conversely, the evaluators may use all system design and implementation documentation. It is common for the evaluators to be given just the IP address of the

institution and any other public information, such as a listing of officers that is normally available to outside hackers. The evaluators may use vulnerability assessment tools, and employ some of the attack methods discussed in this paper such as social engineering and war dialing. After completing the agreed-upon analysis, the evaluators should provide the institution a detailed written report. The report should identify vulnerabilities, prioritize weaknesses, and provide recommendations for corrective action.

A penetration analysis itself can introduce new risks to an institution; therefore, several items should be considered before having an analysis completed, including the following:

- If using outside testers, the reputation of the firm or consultants hired. The evaluators will assess the weaknesses in the bank's information security system. As such, the confidentiality of results and bank data is crucial. Just like screening potential employees prior to their hire, banks should carefully screen firms, consultants, and subcontractors who are entrusted with access to sensitive data. A bank may want to require security clearance checks on the evaluators. An institution should ask if the evaluators have liability insurance in case something goes wrong during the test. The bank should enter into a written contact with the evaluators, which at a minimum should address the above items.
- If using internal testers, the independence of the testers from system administrators.
- The secrecy of the test. Some senior executives may order an analysis without the knowledge of information systems personnel. This can create unwanted results,

including the notification of law enforcement personnel and wasted resources responding to an attack. To prevent excessive responses to the attacks, bank management may consider informing certain individuals in the organization of the penetration analysis.

- The importance of the systems to be tested. Some systems may be too critical to be exposed to some of the methods used by the evaluators such as a critical database that could be damaged during the test.

PART TWO – DETECTION: Discusses intrusion detection systems, and using these tools as the detection component of an institution's information security program.

INTRUSION DETECTION SYSTEMS

Vulnerability assessments and penetration analyses help ensure that appropriate security precautions have been implemented and that system security configurations are appropriate. The next step is to monitor the system for intrusions and unusual activities. Intrusion detection systems (IDSs) may be useful because they act as a burglar alarm, reporting potential intrusions to appropriate personnel. By analyzing the information generated by the systems being guarded, IDSs help determine if necessary safeguards are in place and are protecting the system as intended. In addition, they can be configured to automatically respond to intrusions.

Computer system components or applications can generate detailed, lengthy logs or audit trails that system administrators can manually review for unusual events. IDSs automate the review of logs and audit data, which increases the review's overall efficiency by reducing costs and the time and level of skill necessary to review the logs.

Typically, there are three components to an IDS. First is an agent, which is the component that actually collects the information. Second is a manager, which processes the information collected by the agents. Third is a console, which allows authorized information systems personnel to remotely install and upgrade agents, define intrusion detection scenarios across agents, and track intrusions as they occur. Depending on the complexity of the IDS, there can be multiple agent and manager components.

Generally, IDS products use three different methods to detect intrusions. First, they can look for identified attack signatures, which are streams or patterns of data previously identified as an attack. Second, they can look for system misuse such as unauthorized attempts to access FILes or disallowed traffic inside the firewall. Third, they can look for activities that are different from the user's or system's normal pattern. These "anomaly-based" products (which use artificial intelligence) are designed to detect subtle changes or new attack patterns, and then notify appropriate personnel that an intrusion may be occurring. Some anomaly-based products are created to update normal use patterns on a regular basis. Poorly designed anomaly-based products can trigger frequent false-positive responses.

Although IDSs may be an integral part of an institution's overall system security, they will not protect a system from previously unknown threats or vulnerabilities. They are not self-sufficient and do not compensate for weak authentication procedures (e.g., when an intruder already knows a password to access the system). Also, IDSs often have overlapping features with other security products, such as firewalls. IDSs provide additional protections by helping to determine if the firewall programs are working properly and by helping to detect internal abuses. Both firewalls and IDSs need to be properly configured and updated to combat new types of attacks. In addition, management should be aware that the state of these products is highly dynamic and IDS capabilities are evolving.

IDS tools can generate both technical and management reports, including text, charts, and graphs. The IDS reports can provide background information on the type of attack and recommend courses of action. When an intrusion is detected, the IDS can automatically begin to collect additional information on the attacker, which may be needed later for documentation purposes.

Host- Versus Network-Based IDS Tools

As with vulnerability assessment tools, there are generally two types of IDS products: host-based and network-based. A third product category is sometimes used for IDSs that look for unusual application events (application-based) on a host. Both network- and host-based tools offer valuable features, and the risk assessment process should help institutions determine if either, or a combination of both, is best for their needs.

Host-Based IDSs

Host-based IDSs are also known as audit trail analysis tools or server-based IDSs (often placed on servers). A host-based IDS will look for potential intrusions or patterns of misuse by monitoring host event activities, audit logs, and other security-related activities. The tools will track audit trails from operating systems, applications, Web servers, routers, and firewalls, as well as monitor critical FILes for Trojan horses and unauthorized changes. This can provide valuable evidence of a break-in and can assist in assessing damage because the intruder's actions are logged on the specific hosts. If done in real-time, the IDS can promptly notify the bank of unauthorized attempts to gain system administrator (root) controls, access or change critical files, or replace log-in programs.

An important benefit of host-based IDSs is that they are effective in detecting insider misuse because they monitor activities on the specific hosts. For example, they can monitor a user's attempt to access a restricted file, or an attempt to execute a system administrator's command. In addition, they can monitor encrypted transmissions as the data is generally decrypted before it is logged at the host.

A problem with host-based systems is that notification of the attack is delayed if an agent does not examine the audit trail in real-time. This problem relates to the relatively large consumption of computer processing speed and disk space that is required to run these programs in real-time. If not run in real-time, they still allow a bank to identify larger trends and problems with system security.

Network-Based IDSs

With network-based IDSs, software or sniffers are placed on one or multiple points

across the network. The sniffer agent analyzes packets of information moving across the network for potential intrusions. Network packets contain data, including the message and headers that identify the sending and receiving parties. Network-based IDSs look for patterns of misuse, specific types of attacks, and unusual activity such as unexpected volume and types of network traffic. Compared to host-based IDSs, certain types of network-orientated attacks such as IP spoofing, packet floods, and denial of service, are best detected through packet examination.

Network-based IDSs can detect potential intrusions in real-time, and offer concurrent notification and response capabilities to potential intrusions. The software does not need to be put on the various hosts throughout the network, thus it is generally easier to monitor and may be less expensive than host-based IDSs.

Network-based IDSs sometimes mistakenly identify normal traffic as an intrusion ("false positives") and vice versa ("false negatives"). They can have difficulties detecting slow attacks and experience problems with busy networks. Network-based IDSs cannot monitor encrypted transmissions (only detect that data is being transferred across the network), and are less effective at detecting insider misuse because network packet analysis does not monitor the activities on specific hosts.

Factors to Consider in Evaluating IDSs

Once it is determined that an IDS is necessary to detect possible security breaches, several factors should be considered in evaluating IDSs, including:

- The comprehensiveness of the attack signature database, including the frequency of updates that incorporate newly identified concerns. Most products rely on vendor updates, so banks need to assess the timeliness of the IDS vendor's updates. Products can be updated through Internet downloads, CD-ROM or floppy disk updates, or even manually if the user has a sufficient degree of technical knowledge.

- The effectiveness of the IDS in protecting an institution from both internal and external threats to a computer system. The IDS should limit the number of false positives (incorrectly identifying an attack when none has occurred) and false negatives (not identifying an attack when one has occurred).
- The impact on performance of the network and/or host(s). Generally, IDSs work on a real-time basis. Real-time analysis provides quicker notification of potential intrusions; however, it can reduce system performance due to the additional memory and processing requirements. Non-real-time analysis generally consumes fewer resources, but has the disadvantage that the potential intrusion has already occurred. Knowledgeable intruders, moreover, can manipulate audit trails, making the after-the-fact analysis useless in detecting these particular intruders.
- The security of the IDS itself and how secure the update process is, especially if updated remotely.
- The reporting and automated response capabilities. IDSs will sometimes generate more information than can be reviewed by present qualified staff. Also, for privacy reasons, management should consider informing all affected system users about the scope and type of monitoring being conducted.

Other things to consider include training and support from the vendor, cost of hardware, software, and maintenance agreements, integration with vulnerability assessment tools, and configuration capabilities.

Determining Which is Best for an Institution

An institution's risk assessment process should first determine whether an IDS is necessary. Next, the type or placement of an IDS depends on the priority of identified threats or vulnerabilities. If one or a few hosts contain information that management views as critical, a host-based IDS may be warranted. If the information is less essential, other controls such as a firewall and/or filtering routers may be sufficient to protect the information. If an institution is primarily concerned with attacks from the outside or views the entire network system as critical, a network-based product may be appropriate. A combination of host- and network-based IDSs may also be appropriate for effective system security. Management should be aware that even after an IDS is in place, there may be other access points to the bank's systems that are not being monitored. Management should determine what types of security precautions are needed for the other access points.

The placement of the IDS within the institution's system architecture should be carefully considered. The primary benefit of placing an IDS inside a firewall is the detection of attacks that penetrate the firewall as well as insider abuses. The primary benefit of placing an IDS outside of a firewall is the ability to detect such activities as sweeping, which can be the first sign of attack; repeated failed log-in attempts; and attempted denial of service and spoofing attacks. Placing an IDS outside the firewall will also allow the monitoring of traffic that the firewall stops.

PART THREE – RESPONSE: Discusses implementing an incident response strategy for the response component of an institution's information security program.

INCIDENT RESPONSE

After implementing a defense strategy and monitoring for new attacks, hacker activities, and unauthorized insider access, management should develop a response strategy. The sophistication of an incident response plan will vary depending on the risks inherent in each system deployed and the resources available to an institution. In developing a response strategy or plan, management should consider the following:

- The plan should provide a platform from which an institution can prepare for, address, and respond to intrusions or unauthorized activity. The beginning point is to assess the systems at risk, as identified in the overall risk assessment, and consider the potential types of security incidents.
- The plan should identify what constitutes a break-in or system misuse, and incidents should be prioritized by the seriousness of the attack or system misuse.
- Individuals should be appointed and empowered with the latitude and authority to respond to an incident. The plan should include what the appropriate responses may be for potential intrusions or system misuses.
- A recovery plan should be established, and in some cases, an incident response team should be identified.
- The plan should include procedures to officially report the incidents to senior management, the board of directors, legal counsel, and law enforcement agents as appropriate.

Today's products not only can detect intrusions in real-time, but can automatically respond to intrusions. Depending on the software, information systems personnel can be notified on a real-time basis during an attack, rather than detect the attack afterward during a manual log review. Methods of notification can include e-mail, pager, fax, audio alarm, or message displays on a computer monitor. Responses can include shutting down the system, logging additional information, and disabling a user's account (e.g., by disallowing a particular user account or Internet address). Access can be disabled for a period sufficient for information systems personnel to review the attack information or verify the user. Also, an institution can add warning banners to protected systems, notifying users that they are accessing a protected computer system.

When determining an appropriate response, a distinction should be made between incidents in which actual changes to a system are suspected (e.g., changing audit logs) versus incidents in which system misuse is suspected (e.g., unauthorized system access). Attempts to actually change the system or data may warrant notifying a security officer, who could reconfigure the identified weaknesses and/or communication paths. An appropriate response to system misuse may include automatic log-off, warning messages, or notifying the appropriate personnel.

Not only are attacks often undetected, in many cases identified attacks are not reported. Institutions should develop a plan to respond to unauthorized activities and involve law enforcement when appropriate. Institutions should report suspected computer crimes and computer intrusions on Suspicious Activity Reports (SARs) in accordance with the guidelines outlined in Financial Institution Letter 124-97, "Suspicious Activity Reporting," dated December 5, 1997.

Appendix B:

FDIC FIL 81-05

Instructions for Completing the Information Technology Examination Officer's Questionnaire

Please answer the following information security program questions as of the examination
date pre-determined by the FDIC. The majority of the questions require only a "Yes" or "No" response; however, you are encouraged to expand or clarify any response as needed directly below each question, or at the end of this document under the heading "Clarifying or Additional Comments". For any question deemed non-applicable to your institution or if the answer is "None", please respond accordingly ("NA" or "None"). Please do not leave responses blank. At the bottom of this document is a signature block, which must be signed by an executive officer attesting to the accuracy and completeness of all provided information.

I hereby certify that the following statements are true and correct to the best of my knowledge and belief.		
Officer’s Name and Title	**Institution’s Name and Location**	
Officer’s Signature	**Date Signed**	**As of Date**
This is an official document. Any false information contained in it may be grounds for prosecution and may be punishable by fine or imprisonment.		

PART 1 – RISK ASSESSMENT

An IT risk assessment is a multi-step process of identifying and quantifying threats to information assets in an effort to determine cost effective risk management solutions. To help us assess your risk management practices and the actions taken as a result of your risk assessment, please answer the following questions:

a. Name and title of individual(s) responsible for managing the IT risk assessment process:

b. Names and titles of individuals, committees, departments or others participating in the risk assessment process. If third-party assistance was utilized during this process, please provide the name and address of the firm providing the assistance and a brief description of the services provided:

c. Completion date of your most recent risk assessment:

d. Is your risk assessment process governed by a formal framework/policy (Y/N)?

e. Does the scope of your risk assessment include an analysis of internal and external threats to confidential customer and consumer information as described in Part 364, Appendix B, of the FDIC's Rules and Regulations (Y/N)?

f. Do you have procedures for maintaining asset inventories (Y/N)?

g. Do risk assessment findings clearly identify the assets requiring risk reduction strategies (Y/N)?

h. Do written information security policies and procedures reflect risk reduction strategies identified in "g" above (Y/N)?

i. Is your risk assessment *program* formally approved by the Board of Directors at least annually (Y/N)?

   If yes, please provide the date that the risk assessment program was last approved by the Board of Directors:

j. Are risk assessment *findings* presented to the Board of Directors for review and acceptance (Y/N)?
   If yes, please provide the date that the risk assessment findings were last approved by the Board of Directors:

PART 2 – OPERATIONS SECURITY AND RISK MANAGEMENT

To help us assess how you manage risk through your information security program, please answer the following questions for your environment. If any of the following questions are not applicable to your environment, simply answer "N/A."

a. Please provide the name and title of your formally designated IT security officer:

b. Please provide the name and title of personnel in charge of operations:

c. Do you maintain topologies, diagrams, or schematics depicting your physical and logical operating environment(s) (Y/N)?

d. Does your information security program contain written policies, procedures, and guidelines for securing, maintaining, and monitoring the following systems or platforms:

1. Core banking system (Y/N)?
2. Imaging (Y/N)?
3. Fed Line and/or wire transfer (Y/N)?
4. Local area networking (Y/N)?
5. Wide-area networking (Y/N)?
6. Wireless networking – LAN or WAN (Y/N)?
7. Virtual private networking (Y/N)?
8. Voice over IP telephony (Y/N)?
9. Instant messaging (Y/N)?
10. Portable devices such as PDAs, laptops, cell phones, etc. (Y/N)?
11. Routers (Y/N)?
12. Modems or modem pools (Y/N)?
13. Security devices such as firewall(s) and proxy devices. (Y/N)?
14. Other remote access connectivity such as GoToMyPC, PcAnyWhere, etc. (Y/N)?
15. Other – please list:

e. Do you have formal logging/monitoring requirements for 1-15 above (Y/N)?

f. Do you have formal configuration, change management, and patch management procedures for all applicable platforms identified in "d." above (Y/N)?

g. Do you have an antivirus management program to protect systems from malicious content (Y/N)?

h. Do you have an anti-spyware management program to protect end-user systems (Y/N)?

i. Do you have a formal intrusion detection program, other than basic logging, for monitoring host and/or network activity (Y/N)?

<u>Instructions for Completing the Information Technology Examination Officer's Questionnaire</u>

Please answer the following information security program questions as of the examination date pre-determined by the FDIC. The majority of the questions require only a "Yes" or "No" response; however, you are encouraged to expand or clarify any response as needed directly below each question, or at the end of this document under the heading "Clarifying or Additional Comments". For any question deemed non-applicable to your institution or if the answer is "None", please respond accordingly ("NA" or "None"). Please do not leave responses blank. At the bottom of this document is a signature block, which must be signed by an executive officer attesting to the accuracy and completeness of all provided information.

I hereby certify that the following statements are true and correct to the best of my knowledge and belief.		
Officer's Name and Title	**Institution's Name and Location**	
Officer's Signature	**Date Signed**	**As of Date**
This is an official document. Any false information contained in it may be grounds for prosecution and may be punishable by fine or imprisonment.		

PART 1 – RISK ASSESSMENT

An IT risk assessment is a multi-step process of identifying and quantifying threats to information assets in an effort to determine cost effective risk management solutions. To help us assess your risk management practices and the actions taken as a result of your risk assessment, please answer the following questions:

a. Name and title of individual(s) responsible for managing the IT risk assessment process:

k. Names and titles of individuals, committees, departments or others participating in the risk assessment process. If third-party assistance was utilized during this process, please provide the name and address of the firm providing the assistance and a brief description of the services provided:

l. Completion date of your most recent risk assessment:

m. Is your risk assessment process governed by a formal framework/policy (Y/N)?

n. Does the scope of your risk assessment include an analysis of internal and external threats to confidential customer and consumer information as described in Part 364, Appendix B, of the FDIC's Rules and Regulations (Y/N)?

o. Do you have procedures for maintaining asset inventories (Y/N)?

p. Do risk assessment findings clearly identify the assets requiring risk reduction strategies (Y/N)?

q. Do written information security policies and procedures reflect risk reduction strategies identified in "g" above (Y/N)?

r. Is your risk assessment *program* formally approved by the Board of Directors at least annually (Y/N)?

If yes, please provide the date that the risk assessment program was last approved by the Board of Directors:

s. Are risk assessment *findings* presented to the Board of Directors for review and acceptance (Y/N)?
If yes, please provide the date that the risk assessment findings were last approved by the Board of Directors:

PART 2 – OPERATIONS SECURITY AND RISK MANAGEMENT

To help us assess how you manage risk through your information security program, please answer the following questions for your environment. If any of the following questions are not applicable to your environment, simply answer "N/A."

e. Please provide the name and title of your formally designated IT security officer:

f. Please provide the name and title of personnel in charge of operations:

g. Do you maintain topologies, diagrams, or schematics depicting your physical and logical operating environment(s) (Y/N)?

h. Does your information security program contain written policies, procedures, and guidelines for securing, maintaining, and monitoring the following systems or platforms:

1. Core banking system (Y/N)?
2. Imaging (Y/N)?
3. Fed Line and/or wire transfer (Y/N)?
4. Local area networking (Y/N)?
5. Wide-area networking (Y/N)?
6. Wireless networking – LAN or WAN (Y/N)?
7. Virtual private networking (Y/N)?
8. Voice over IP telephony (Y/N)?
9. Instant messaging (Y/N)?
10. Portable devices such as PDAs, laptops, cell phones, etc. (Y/N)?
11. Routers (Y/N)?
12. Modems or modem pools (Y/N)?
13. Security devices such as firewall(s) and proxy devices. (Y/N)?
14. Other remote access connectivity such as GoToMyPC, PcAnyWhere, etc. (Y/N)?
15. Other – please list:

e. Do you have formal logging/monitoring requirements for 1-15 above (Y/N)?

f. Do you have formal configuration, change management, and patch management procedures for all applicable platforms identified in "d." above (Y/N)?

g. Do you have an antivirus management program to protect systems from malicious content (Y/N)?

h. Do you have an anti-spyware management program to protect end-user systems (Y/N)?

i. Do you have a formal intrusion detection program, other than basic logging, for monitoring host and/or network activity (Y/N)?

j. Has vulnerability testing been performed on internal systems (Y/N)?

If yes, please provide date performed and by whom:

k. Has penetration testing of your public or Internet-facing connection(s) been performed (Y/N)?

If yes, please provide date performed and by whom:

l. Do you have an incident response plan defining responsibilities and duties for containing damage and minimizing risks to the institution (Y/N)?

If yes, does the plan include customer notification procedures (Y/N)?

m. Do you have a physical security program defining and restricting access to information assets (Y/N)?

n. Do you have a vendor management program (Y/N)?

o. Are all of your service providers located within the United States (Y/N)?

p. Do you have an employee acceptable use policy (Y/N)?

If yes, please provide how often employees must attest to the policy contents:

q. Do you have an employee security awareness training program (Y/N)?

If yes, please indicate the last date training was provided:

r. Are you planning to deploy new technology within the next 12 months (Y/N)?

If you answered “Yes”, were the risks associated with this new technology reviewed during your most recent risk assessment (Y/N)?

s. Have you deployed new technology since the last FDIC examination that was not included in your last risk assessment (Y/N)?

t. Is security incorporated into your overall strategic planning process (Y/N)?

u. Do you have policies/procedures for the proper disposal of information assets (Y/N)?

PART 3 – AUDIT/INDEPENDENT REVIEW PROGRAM

To help us assess how you monitor operations and compliance with your written information security program, please answer the following questions:

a. Please provide the name and title of your IT auditor or employee performing internal IT audit functions. Include who this person reports to, and a brief description of their education and experience conducting IT audits.

b. Do you have a written IT audit/independent review program (Y/N)?

c. Please provide the following information regarding your most recent IT audit/independent review:

1. Audit Date:
2. Firm name (if external):
3. Was an audit report produced (Y/N)?
4. Date audit report was reviewed and approved by the Board:
5. Audit scope and objectives:

d. Does audit coverage include a comparison of actual system configurations to documented/baseline configuration standards (Y/N)?

e. Does audit coverage include assessing compliance with the information security program requirements (Y/N)?

f. Does audit coverage include assessing users and system services access rights (Y/N)?

g Is audit involved in your risk assessment process (Y/N)?

h. Briefly describe any security incidents (internal or external) affecting the bank or

bank customers occurring since the last FDIC IT examination.

i. Briefly describe any known conflicts or concentrations of duties.

PART 4 - DISASTER RECOVERY AND BUSINESS CONTINUITY

To help us assess your preparedness for responding to and recovering from an unexpected event, please answer the following:

a. Do you have an organization-wide disaster recovery and business continuity program (Y/N)?

If yes, please provide the name of your coordinator:

b. Are disaster recovery and business continuity plans based upon a business impact analyses (Y/N)?

If yes, do the plans identify recovery and processing priorities (Y/N)?

c. Is disaster recovery and business continuity included in your risk assessment (Y/N)?

d. Do you have formal agreements for an alternate processing site and equipment should the need arise to relocate operations (Y/N)?

e. Do business continuity plans address procedures and priorities for returning to permanent and normal operations (Y/N)?

f. Do you maintain offsite backups of critical information (Y/N)?

If "Yes," is the process formally documented and audited (Y/N)?

g. Do you have procedures for testing backup media at an offsite location (Y/N)?

h. Have disaster recovery/business continuity plans been tested (Y/N)?

If "Yes", please identify the system(s) tested, the corresponding test date, and the date reported to the Board:

PART 5 – Gramm-Leach-Bliley Act/FDIC Rules and Regulations – 12 CFR Part 364 Appendix B

The Interagency Guidelines Establishing Information Security Standards require each bank to have a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the bank and the nature and scope of its activities. Please answer the following questions pertaining to your written information security program:

a. Has management developed a written information security program meeting the information security standards of Part 364, Appendix B (Y/N)?

If you answered "Yes" to question "a" above, please provide the date that the Board of Directors last approved the written information security program:

b. Please provide the names and titles and/or committee members charged with formally overseeing and implementing Part 364, Appendix B, requirements:

c. Are compliance audits of your Part 364 standards periodically performed and formally reported to the Board of Directors (Y/N)?

If you answered "Yes" to question "c", please provide the date of your last Part 364 compliance audit or review:

d. Have employees received Part 364 related security awareness training (Y/N)?

e. Please describe the bank's reporting process for communicating Part 364 program and compliance status to the Board of Directors:

j. Has vulnerability testing been performed on internal systems (Y/N)?

   If yes, please provide date performed and by whom:

k. Has penetration testing of your public or Internet-facing connection(s) been performed (Y/N)?

   If yes, please provide date performed and by whom:

l. Do you have an incident response plan defining responsibilities and duties for containing damage and minimizing risks to the institution (Y/N)?

   If yes, does the plan include customer notification procedures (Y/N)?

m. Do you have a physical security program defining and restricting access to information assets (Y/N)?

n. Do you have a vendor management program (Y/N)?

o. Are all of your service providers located within the United States (Y/N)?

p. Do you have an employee acceptable use policy (Y/N)?

   If yes, please provide how often employees must attest to the policy contents:

q. Do you have an employee security awareness training program (Y/N)?

   If yes, please indicate the last date training was provided:

r. Are you planning to deploy new technology within the next 12 months (Y/N)?

   If you answered “Yes”, were the risks associated with this new technology reviewed during your most recent risk assessment (Y/N)?

s. Have you deployed new technology since the last FDIC examination that was not included in your last risk assessment (Y/N)?

v. Is security incorporated into your overall strategic planning process (Y/N)?

w. Do you have policies/procedures for the proper disposal of information assets (Y/N)?

PART 3 – AUDIT/INDEPENDENT REVIEW PROGRAM

To help us assess how you monitor operations and compliance with your written information security program, please answer the following questions:

a. Please provide the name and title of your IT auditor or employee performing internal IT audit functions. Include who this person reports to, and a brief description of their education and experience conducting IT audits.

b. Do you have a written IT audit/independent review program (Y/N)?

c. Please provide the following information regarding your most recent IT audit/independent review:

1. Audit Date:
2. Firm name (if external):
3. Was an audit report produced (Y/N)?
4. Date audit report was reviewed and approved by the Board:
5. Audit scope and objectives:

d. Does audit coverage include a comparison of actual system configurations to documented/baseline configuration standards (Y/N)?

e. Does audit coverage include assessing compliance with the information security program requirements (Y/N)?

f. Does audit coverage include assessing users and system services access rights (Y/N)?

g Is audit involved in your risk assessment process (Y/N)?

h. Briefly describe any security incidents (internal or external) affecting the bank or bank customers occurring since the last FDIC IT examination.

j. Briefly describe any known conflicts or concentrations of duties.

PART 4 - DISASTER RECOVERY AND BUSINESS CONTINUITY

To help us assess your preparedness for responding to and recovering from an unexpected event, please answer the following:

a. Do you have an organization-wide disaster recovery and business continuity program (Y/N)?

If yes, please provide the name of your coordinator:

b. Are disaster recovery and business continuity plans based upon a business impact analyses (Y/N)?

If yes, do the plans identify recovery and processing priorities (Y/N)?

c. Is disaster recovery and business continuity included in your risk assessment (Y/N)?

d. Do you have formal agreements for an alternate processing site and equipment should the need arise to relocate operations (Y/N)?

e. Do business continuity plans address procedures and priorities for returning to permanent and normal operations (Y/N)?

f. Do you maintain offsite backups of critical information (Y/N)?

If “Yes,” is the process formally documented and audited (Y/N)?

g. Do you have procedures for testing backup media at an offsite location (Y/N)?

h. Have disaster recovery/business continuity plans been tested (Y/N)?

If “Yes”, please identify the system(s) tested, the corresponding test date, and the date reported to the Board:

PART 5 – Gramm-Leach-Bliley Act/FDIC Rules and Regulations – 12 CFR Part 364 Appendix B

The Interagency Guidelines Establishing Information Security Standards require each bank to have a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the bank and the nature and scope of its activities. Please answer the following questions pertaining to your written information security program:

a. Has management developed a written information security program meeting the information security standards of Part 364, Appendix B (Y/N)?

   If you answered "Yes" to question "a" above, please provide the date that the Board of Directors last approved the written information security program:

b. Please provide the names and titles and/or committee members charged with formally overseeing and implementing Part 364, Appendix B, requirements:

c. Are compliance audits of your Part 364 standards periodically performed and formally reported to the Board of Directors (Y/N)?

   If you answered "Yes" to question "c", please provide the date of your last Part 364 compliance audit or review:

d. Have employees received Part 364 related security awareness training (Y/N)?

e. Please describe the bank's reporting process for communicating Part 364 program and compliance status to the Board of Directors:

Appendix C

Assets Typical to Small and Medium Sized Financial Institutions

Internet Banking System	Core Banking system	Fund Transfer System	Credit Bureau Website	Deposit Platform
Printers	Notebook Computers	Desktop Computers	Firewall	Lending Program
Marketing Software	Payday Lending	Payroll Software	PDA’s	Router
Switch	Firewall	Smart Phones	Terminal Services	Web Server
Email Server	Accounting Software	Background Checking Website	Anti-Virus Software	ATM
Call Reporting Software	HMDA	Operating Systems	Merchant Card Processing System	Intrusion Detection System
File Server	Item Imaging	Local Area Network	Check Ordering Website	Check Reader / Sorter
VoIP	Deb/Credit Cards	Bank Website	Application Server	Remote Capture Systems
Storage Area Network	Wide Area Network	Proof System		

Appendix D

Controls Typical to Small and Medium Sized Financial Institutions

Authorized User Restrictions	Access Logs	Formal TSP Review	Formal TSP Selection
Disable Terminated Employee Account	Access Log Monitoring	Invalid Attempt Lockout	Strong Passwords
Unique User Accounts	Encrypt Stored Data	Formal Patching Process	Inactive Lockout
Intrusion Detection / Prevention Systems	Back-up Critical Da	Change Default Security Settings	Incident Response Program
Incident Response Program Test	Business Continuity Plan	Clear Screen Awareness	Forced Session Expiration
Maintenance Logs	Multi-factor Authentication	System Access Warning	Vulnerability Assessment
Activity Logs	Change Default Account Settings	Maintenance Log Review	Temporarily Disable Absents Employee Accounts
Vulnerability Assessment Administrative Privileges	Off-Site Backup	Activity Log Monitoring	Last Successful Logon
Business Continuity Pl Test	Network Diagram	Test Back-up Recove	Virus Protection
Spyware Protection	Penetration Testing	Social Engineering an Security Awareness	Security Cameras
Monitored Locations	Physical Security Awareness	Motion Sensors	Restricted Access Area
Maintenance Log Review	Network Diagram	Privacy Filer	Dual Power Supply
Disable/Remove Hardware	Redundant Systems	Temperature Control	Humidity Control

Dust Filtering	Power Conditioning	Backup Generator	Uninterruptible Power Supply
Test Back-up Recovery	Line Disconnect	Locked Door	Monitor Placement
Encryption	Secured Rack or Ca for IT assets	Alert Reporting	Internet History
Internet History Monitoring	Removable Media Ban- Personal	Offsite Removal of fil	File storage on portable device ban

Appendix E

Controls specific to assets

Deposit Platform:

Test Back-up Recovery

Network Diagram

Business Continuity Plan Test

Last Successful Logon

Activity Log Monitoring

Off-Site Backup

Vulnerability Assessment: Administrative Privileges

Temporarily Disable Absent Employee

Accounts

Maintenance Log Review

Change Default Account Settings

Activity Logs

Vulnerability Assessment

System Access Warning

Multi-Factor Authentication

Maintenance Logs

Forced Session Expiration

Clear Screen Awareness

Business Continuity Plan

Incident Response Program Test

Incident Response Program

Change Default Security Settings

Back-up Critical Data

Intrusion Detection / Prevention

Inactive Lockout

Formal Patching Process

Encrypt Stored Data

Unique User Accounts

Strong Passwords

Invalid Attempt Lockout

Disable Terminated Employee Accounts

Access Log Monitoring

Formal TSP Selection

Formal TSP Review

Access Logs

Unauthorized Access Restrictions

FinCen:

Strong Passwords

Virus Protection

Spyware Protection

Business Continuity Plan

Encrypt Stored Data

Activity Log Monitoring

Social Engineering Security Awareness

Penetration Testing

Clear Screen Awareness

Forced Session Expiration

Encrypt Transmitted Data

Change Default Security Settings

Change Default Account Settings

Activity Logs

Temporarily Disable Absent Employee Accounts

Last Successful Logon

Inactive Lockout

Formal TSP Selection

Formal TSP Review

Disable Terminated Employee Accounts

Incident Response Program Test

Incident Response Program

System Access Warning

Authorized User Restrictions

Access Log Monitoring

Multi-Factor Authentication

Invalid Attempt Lockout

Access Logs

Unique User Accounts

ATM:

Monitored Location

Incident Response Program Test

Incident Response Program

Business Continuity Plan Test

Business Continuity Plan

Restricted Access Area

Motion Sensors

Formal TSP Selection

Formal TSP Review

Physical Security Awareness

Security Cameras

Anti-Virus Software:

Inactive Lockout

Clear Screen Awareness

Network Diagram

Maintenance Log Review

Vulnerability Assessment: Administrative Privileges

Temporarily Disable Absent Employee Accounts

Intrusion Detection / Prevention

Change Default Account Settings

Business Continuity Plan Test

Vulnerability Assessment

Maintenance Logs

Last Successful Logon

Social Engineering Security Awareness

Incident Response Program Test

Incident Response Program

Change Default Security Settings

Formal Patching Process

Multi-Factor Authentication

Disable Terminated Employee Accounts

Business Continuity Plan

Invalid Attempt Lockout

Access Logs

Unique User Accounts

Strong Passwords

Formal TSP Selection

Formal TSP Review

Check Ordering Website:

Strong Passwords

Business Continuity Plan

Social Engineering Security Awareness

Virus Protection

Spyware Protection

Formal TSP Selection

Formal TSP Review

Privacy Filter

Penetration Testing

Encrypt Stored Data

Clear Screen Awareness

Temporarily Disable Absent Employee Accounts

Monitor Placement

Encrypt Transmitted Data

Forced Session Expiration

Change Default Account Settings

Change Default Security Settings

Authorized User Restrictions

System Access Warning

Inactive Lockout

Multi-Factor Authentication

Invalid Attempt Lockout

Disable Terminated Employee Accounts

Unique User Accounts

Website:

Strong Passwords

Temporarily Disable Absent Employee Accounts

Forced Session Expiration

Social Engineering Security Awareness

Last Successful Logon

Change Default Security Settings

Clear Screen Awareness

Encrypt Transmitted Data

Incident Response Program Test

Incident Response Program

Monitor Placement

Disable Terminated Employee Accounts

Inactive Lockout

Multi-Factor Authentication

Invalid Attempt Lockout

Authorized User Restrictions

Unique User Accounts

Core System

Incidence Response Program

Privacy Filter

Security Cameras

Restricted Access Area

Physical Security Awareness

Monitored Location

Test Back-up Recovery

Business Continuity Plan Test

Dual Power Supply

Temporarily Disable Absent Employee Accounts

Secured Rack/Cage

Monitor Placement

Locked Door

Line Disconnect

Spyware Protection

Activity Log Monitoring

Vulnerability Assessment: Administrative Privileges

Encrypt Transmitted Data

Formal TSP Selection

Formal TSP Review

Virus Protection

Remove Unnecessary Software

Business Continuity Plan

Access Log Monitoring

Back-up Critical Data

Last Successful Logon

Forced Session Expiration

Change Default Security Settings

Activity Logs

Alert Reporting

Change Default Account Settings

Inactive Lockout

Encrypt Stored Data

Vulnerability Assessment

Formal Patching Process

Disable Terminated Employee Accounts

Access Logs

Multi-Factor Authentication

Invalid Attempt Lockout

Firewall

Intrusion Detection / Prevention

Unique User Accounts

Strong Passwords

Incident Response Program Test

Authorized User Restrictions

Maintenance Logs

Redundant Systems

Temperature Control

Humidity Control

Dust Filtering

Disable / Remove Hardware

Power Conditioning

Network Diagram

Backup Generator

Social Engineering Security Awareness

Off-Site Backup

Uninterruptible Power Supply

Motion Sensors

Maintenance Log Review

Penetration Testing

Clear Screen Awareness

Desktop Computers

Intrusion Protection / Prevention

Off-Site Backup

Disable / Remove Hardware

Business Continuity Plan Test

Dual Power Supply

Network Diagram

Maintenance Logs

Maintenance Log Review

Inactive Lockout

Clear Screen Awareness

Monitor Placement

Encrypt Transmitted Data

Temporarily Disable Absent Employee Accounts

Access Log Monitoring

Restricted Access Area

Malware Awareness

Power Conditioning

Back-up Critical Data

Authorized User Restrictions

Spyware Protection

Uninterruptible Power Supply

Motion Sensors

Vulnerability Assessment: Administrative Privileges

Multi-Factor Authentication

Virus Protection

Physical Security Awareness

Access Logs

Remove Unnecessary Software

Security Cameras

Monitored Location

Incident Response Program Test

Last Successful Logon

Forced Session Expiration

Change Default Security Settings

Disable Unnecessary Services

Encrypt Stored Data

Incident Response Program

Disable Terminated Employee Accounts

Invalid Attempt Lockout

Unique User Accounts

Strong Passwords

Change Default Account Settings

Vulnerability Assessment

Formal Patching Process

Penetration Testing

Test Back-up Plan

Business Continuity Plan

Email:

Invalid Attempt Lockout

Physical Security Awareness

Temperature Control

Off-Site Backup

Activity Log Monitoring

Penetration Testing

Redundant Systems

Test Back-up Recovery

Formal TSP Selection

Formal TSP Review

Business Continuity Plan Test

Business Continuity Plan

Internet History Monitoring

Internet History

Activity Logs

Maintenance Log Review

Uninterruptible Power Supply

Encrypt Transmitted Data

Temporarily Disable Absent Employee Accounts

Maintenance Logs

Line Disconnect

Access Log Monitoring

Spyware Protection

Virus Protection

Vulnerability Assessment: Administrative Privileges

Authorized User Restrictions

Last Successful Logon

Forced Session Expiration

Change Default Security Settings

System Access Warning

Back-up Critical Data

Remove Unnecessary Software

Disable Unnecessary Services

Disable Terminated Employee Accounts

Access Logs

Formal Patching Process

Vulnerability Assessment

Encrypt Stored Data

Unique User Accounts

Strong Passwords

Intrusion Detection / Prevention

Multi-Factor Authentication

Content Filtering

Incident Response Program Test

Firewall

Incident Response Program

Firewall:

Intrusion /Detection Prevention

Business Continuity Plan

Backup Generator

Temperature Control

Redundant Systems

Dual Power Supply

Network Diagram

Maintenance Logs

Maintenance Log Review

Activity Log Monitoring

Power Conditioning

Restricted Access Area

Encrypt Transmitted Data

Temporarily Disable Absent Employee Accounts

Access Log Monitoring

Uninterruptible Power Supply

Motion Sensors

Locked Door

Line Disconnect

Alert Reporting

Activity Logs

Physical Security Awareness

Security Cameras

Monitored Location

Penetration Testing

Secured Rack/Cage

Authorized User Restrictions

Back-up Critical Data

Vulnerability Assessment: Administrative Privileges

Spyware Protection

Last Successful Logon

Forced Session Expiration

Change Default Security Settings

Incident Response Program Test

Access Logs

Virus Protection

Disable Terminated Employee Accounts

Incident Response Program

Unique User Accounts

Strong Passwords

Invalid Attempt Lockout

Disable Unnecessary Services

Vulnerability Assessment

Change Default Account Settings

Formal Patching Process

Dust Filtering

Vulnerability Assessment

Change Default Account Settings

Formal Patching Process

Intrusion Detection / Prevention

Disable / Remove Hardware

Test Back-up Recovery

Off-Site Backup

Business Continuity Plan Test

Humidity Control

Funds Transfer System

Dual Power Supply

Business Continuity Plan Test

Business Continuity Plan

Penetration Testing

Maintenance Logs

Maintenance Log Review

Formal TSP Selection

Formal TSP Review

Clear Screen Awareness

Monitor Placement

Inactive Lockout

Line Disconnect

Vulnerability Assessment: Administrative Privileges

Temporarily Disable Absent Employee Accounts

Encrypt Transmitted Data

Access Log Monitoring

Change Default Security Settings

Change Default Account Settings

Alert Reporting

Disable Unnecessary Services

Vulnerability Assessment

Last Successful Logon

Forced Session Expiration

Activity Log Monitoring

Encrypt Stored Data

System Access Warning

Firewall

Intrusion Detection / Prevention

Multi-Factor Authentication

Activity Logs

Incident Response Program Test

Disable Terminated Employee Accounts

Unique User Accounts

Strong Passwords

Invalid Attempt Lockout

Incident Response Program

Authorized User Restrictions

Internet Banking Systems

Incidence Response Program

Monitored Location

Clear Screen Awareness

Uninterruptible Power Supply

Social Engineering Security Awareness

Physical Security Awareness

Penetration Testing

Maintenance Log Review

Maintenance Logs

Dual Power Supply

Line Disconnect

Test Back-up Recovery

Business Continuity Plan Test

Monitor Placement

Temporarily Disable Absent Employee Accounts

Encrypt Transmitted Data

Business Continuity Plan

Spyware Protection

Activity Log Monitoring

Access Log Monitoring

Virus Protection

Back-up Critical Data

Vulnerability Assessment: Administrative Privileges

Activity Logs

Last Successful Logon

Forced Session Expiration

Change Default Security Settings

Encrypt Stored Data

Alert Reporting

Change Default Account Settings

Inactive Lockout

Disable Terminated Employee Accounts

Formal TSP Selection

Formal TSP Review

Formal Patching Process

Authorized User Restrictions

Access Logs

Unique User Accounts

Firewall

Vulnerability Assessment

Strong Passwords

Incident Response Program Test

Intrusion Detection / Prevention

Multi-Factor Authentication

Invalid Attempt Lockout

Redundant Systems

No

Motion Sensors

Backup Generator

Temperature Control

Power Conditioning

Off-Site Backup

Network Diagram

Security Cameras

Restricted Access Area

Internet Website

Incidence Response

Maintenance Logs

Maintenance Log Review

Forced Session Expiration

Encrypt Stored Data

Content Filtering

Clear Screen Awareness

Change Default Security Settings

Change Default Account Settings

Business Continuity Plan

Authorized User Restrictions

Unique User Accounts

Internet History Monitoring

Internet History

Encrypt Transmitted Data

System Access Warning

Virus Protection

Spyware Protection

Incident Response Program Test

Incident Response Program

Secured Rack/Cage

Dual Power Supply

Multi-Factor Authentication

Firewall

Vulnerability Assessment: Administrative Privileges

Invalid Attempt Lockout

Intrusion Detection / Prevention

Strong Passwords

Vulnerability Assessment

Formal Patching Process

Formal TSP Selection

Formal TSP Review

Printer

Monitored Location

Restricted Access Area

Locked Door

Physical Security Awareness

Motion Sensors

Security Cameras

Router

Intrusion Detection & Prevention

Multi-Factor Authentication

Business Continuity Plan Test

Business Continuity Plan

Backup Generator

Temperature Control

Humidity Control

Dust Filtering

Disable / Remove Hardware

Restricted Access Area

Redundant Systems

Network Diagram

Maintenance Logs

Maintenance Log Review

Line Disconnect

Invalid Attempt Lockout

Power Conditioning

Temporarily Disable Absent Employee Accounts

Motion Sensors

Locked Door

Access Log Monitoring

Uninterruptible Power Supply

Security Cameras

Monitored Location

Physical Security Awareness

Encrypt Transmitted Data

Secured Rack/Cage

Penetration Testing

Dual Power Supply

Spyware Protection

Alert Reporting

Authorized User Restrictions

Back-up Critical Data

Virus Protection

Vulnerability Assessment: Administrative

Privileges

Disable Terminated Employee Accounts

Firewall

Unique User Accounts

Strong Passwords

Incident Response Program Test

Incident Response Program

Change Default Account Settings

Change Default Security Settings

Disable Unnecessary Services

Vulnerability Assessment

Switch

Intrusion Detection & Prevention

Multi-Factor Authentication

Business Continuity Plan Test

Business Continuity Plan

Backup Generator

Temperature Control

Humidity Control

Dust Filtering

Disable / Remove Hardware

Restricted Access Area

Redundant Systems

Network Diagram

Maintenance Logs

Maintenance Log Review

Line Disconnect

Invalid Attempt Lockout

Power Conditioning

Temporarily Disable Absent Employee Accounts

Motion Sensors

Locked Door

Access Log Monitoring

Uninterruptible Power Supply

Security Cameras

Monitored Location

Physical Security Awareness

Encrypt Transmitted Data

Secured Rack/Cage

Penetration Testing

Dual Power Supply

Spyware Protection

Alert Reporting

Authorized User Restrictions

Back-up Critical Data

Virus Protection

Vulnerability Assessment: Administrative

Privileges

Disable Terminated Employee Accounts

Firewall

Unique User Accounts

Strong Passwords

Incident Response Program Test

Incident Response Program

Change Default Account Settings

Change Default Security Settings

Disable Unnecessary Services

Vulnerability Assessment

Appendix F

Threats Specific to Assets

Internet Banking System

Data Leakage

Unauthorized System Access

Phishing

Defacement

Pharming

Eavesdropping / Sniffing

Intentional Misuse

Unauthorized Remote Access

Degraded / Unavailable

Malicious Software

Outsourced

Unauthorized Physical Access

Unauthorized Viewing

User Error

Environmental Incident

Man-made / Natural Disaster

Core Banking System

Data Loss

Unauthorized System Access

Intentional Misuse

Outsourced

Unauthorized Remote Access

Degraded / Unavailable

Hardware Failure

Unauthorized Physical Access

Eavesdropping / Sniffing

Malicious Software

Unauthorized Viewing

Social Engineering

Software Acquisition

Man-made / Natural Disaster

Environmental Incident

User Error

Funds Transfer System

Unauthorized System Access

Eavesdropping / Sniffing

Degraded / Unavailable

Malicious Software

Unauthorized Viewing

Intentional Misuse

Unauthorized Remote Access

User Error

Outsourced

Social Engineering

Man-made / Natural Disaster

Unauthorized Physical Access

Credit Bureau Website

User Error

Data Loss

Social Engineering

Defacement

Intentional Misuse

Unauthorized Viewing

Eavesdropping / Sniffing

Unauthorized System Access

Outsourced

Degraded / Unavailable

Deposit Platform

Data Loss

Software Acquisition

Social Engineering

Intentional Misuse

Unauthorized System Access

Unauthorized Viewing

User Error

Man-made / Natural Disaster

Printers

Theft

Unauthorized physical access

Notebook Computers

Data Loss

Theft

Intentional Misuse

Unauthorized Physical Access

Malicious Software

Connection Of Unauthorized Equipment

Social Engineering

Unauthorized Remote Access

Unauthorized Viewing

Hardware Failure

Environmental Incident

User Error

Unauthorized System Access

Degraded / Unavailable

Eavesdropping / Sniffing

Man-made / Natural Disaster

Firewall

Data Loss

Theft

Intentional Misuse

Unauthorized Physical Access

Malicious Software

Connection Of Unauthorized Equipment

Social Engineering

Unauthorized Remote Access

Unauthorized Viewing

Hardware Failure

Environmental Incident

User Error

Unauthorized System Access

Degraded / Unavailable

Eavesdropping / Sniffing

Man-made / Natural Disaster

Lending Program

Social Engineering

Software Acquisition

User Error

Intentional Misuse

Unauthorized System Access

Unauthorized Viewing

Man-made / Natural Disaster

Data Loss

Marketing Software

Data Loss

Software Acquisition

Social Engineering

Unauthorized System Access

Unauthorized Viewing

User Error

Man-made / Natural Disaster

Intentional Misuse

Payday Lending

Unauthorized System Access

Data Loss

Eavesdropping / Sniffing

Defacement

Degraded / Unavailable

Unauthorized Viewing

Intentional Misuse

Social Engineering

User Error

Outsourced

Payroll

Data Loss

Intentional Misuse

Social Engineering

Software Acquisition

Unauthorized System Access

User Error

Man-made / Natural Disaster

Unauthorized Viewing

PDA

Theft

Data Loss

Unauthorized System Access

Environmental Incident

Unauthorized Viewing

Malicious Software

Eavesdropping / Sniffing

Router

Unauthorized Physical Access

Eavesdropping / Sniffing

Unauthorized Remote Access

Degraded / Unavailable

Hardware Failure

Connection Of Unauthorized Equipment

Unauthorized System Access

Environmental Incident

Man-made / Natural Disaster

Switch

Unauthorized Physical Access

Eavesdropping / Sniffing

Unauthorized Remote Access

Degraded / Unavailable

Hardware Failure

Connection Of Unauthorized Equipment

Unauthorized System Access

Environmental Incident

Man-made / Natural Disaster

Firewall

Unauthorized Remote Access

Degraded / Unavailable

Hardware Failure

Connection Of Unauthorized Equipment

Unauthorized Physical Access

Environmental Incident

Theft

Man-made / Natural Disaster

Smart Phones

Theft

Data Loss

Unauthorized System Access

Environmental Incident

Unauthorized Viewing

Malicious Software

Eavesdropping / Sniffing

Terminal Services

Hardware Failure

Unauthorized Remote Access

Unauthorized System Access

Malicious Software

User Error

Degraded / Unavailable

Theft

Man-made / Natural Disaster

Unauthorized Physical Access

Connection Of Unauthorized Equipment

Eavesdropping / Sniffing

Environmental Incident

Web Server

Hardware Failure

Social Engineering

Intentional Misuse

Malicious Software

Outsourced

Unauthorized System Access

Degraded / Unavailable

Unauthorized Physical Access

Unauthorized Remote Access

User Error

Theft

Environmental Incident

Man-made / Natural Disaster

Connection Of Unauthorized Equipment

Eavesdropping / Sniffing

Email Server

Data Loss

Eavesdropping / Sniffing

Hardware Failure

Intentional Misuse

Social Engineering

Unauthorized System Access

Malicious Software

Outsourced

Theft

Unauthorized Physical Access

Unauthorized Remote Access

User Error

Man-made / Natural Disaster

Connection Of Unauthorized Equipment

Degraded / Unavailable

Environmental Incident

Accounting Software

Data Loss

Social Engineering

Software Acquisition

Man-made / Natural Disaster

Intentional Misuse

Unauthorized System Access

User Error

Unauthorized Viewing

Background Checking

Data Loss

Defacement

Eavesdropping / Sniffing

Unauthorized System Access

User Error

Intentional Misuse

Social Engineering

Unauthorized Viewing

Outsourced

Degraded / Unavailable

Anti Virus Software

Software Acquisition

Intentional Misuse

Man-made / Natural Disaster

Unauthorized System Access

User Error

Social Engineering

ATM

Connection Of Unauthorized Equipment

Skimming

Man-made / Natural Disaster

Theft

Call Reporting

Social Engineering

Software Acquisition

Intentional Misuse

Man-made / Natural Disaster

Unauthorized System Access

User Error

Unauthorized Viewing

HMDA

Data Loss

Social Engineering

User Error

Software Acquisition

Intentional Misuse

Man-made / Natural Disaster

Unauthorized System Access

Unauthorized Viewing

Operating System

Malicious Software

Unauthorized System Access

Unauthorized Remote Access

Merchant Card Processing

Unauthorized System Access

Eavesdropping / Sniffing

Degraded / Unavailable

Malicious Software

Unauthorized Viewing

Intentional Misuse

Unauthorized Remote Access

User Error

Outsourced

Social Engineering

Man-made / Natural Disaster

Unauthorized Physical Access

Intrusion Detection

Unauthorized System Access

Eavesdropping / Sniffing

Degraded / Unavailable

Malicious Software

Unauthorized Viewing

Intentional Misuse

Unauthorized Remote Access

User Error

Outsourced

Social Engineering

Man-made / Natural Disaster

Unauthorized Physical Access

File Server

Data Loss

Hardware Failure

Unauthorized System Access

Social Engineering

Theft

Degraded / Unavailable

Intentional Misuse

Malicious Software

Eavesdropping / Sniffing

Unauthorized Physical Access

Unauthorized Remote Access

User Error

Connection Of Unauthorized Equipment

Environmental Incident

Man-made / Natural Disaster

Item Imaging

Data Loss

Unauthorized System Access

Hardware Failure

Degraded / Unavailable

Intentional Misuse

Outsourced

Unauthorized Remote Access

Social Engineering

Software Acquisition

Unauthorized Physical Access

Unauthorized Viewing

Eavesdropping / Sniffing

Environmental Incident

Malicious Software

Man-made / Natural Disaster

User Error

Local Area Network

Unauthorized Physical Access

Eavesdropping / Sniffing

Unauthorized Remote Access

Degraded / Unavailable

Hardware Failure

Connection Of Unauthorized Equipment

Unauthorized System Access

Environmental Incident 1

Man-made / Natural Disaster

Check Ordering website

Unauthorized System Access

Intentional Misuse

Data Loss

Defacement

Degraded / Unavailable

Eavesdropping / Sniffing

Unauthorized Viewing

User Error

Outsourced

Social Engineering

Check Reader/Sorter

Data Loss

Intentional Misuse

Theft

Unauthorized Viewing

User Error

Hardware Failure

Social Engineering

Environmental Incident

Unauthorized System Access

Malicious Software

Man-made / Natural Disaster

Unauthorized Physical Access

Unauthorized Remote Access

Connection Of Unauthorized Equipment

Degraded / Unavailable

Eavesdropping / Sniffing

VOIP

Connection Of Unauthorized Equipment

Unauthorized Physical Access

Unauthorized Remote Access

Eavesdropping / Sniffing

Unauthorized System Access

Degraded / Unavailable

Outsourced

Hardware Failure

Man-made / Natural Disaster

Debit/Credit Cards

Unauthorized System Access

Eavesdropping / Sniffing

Degraded / Unavailable

Malicious Software

Unauthorized Viewing

Intentional Misuse

Unauthorized Remote Access

User Error

Outsourced

Social Engineering

Man-made / Natural Disaster

Unauthorized Physical Access

Bank Website

Unauthorized System Access

Data Loss

Defacement

Eavesdropping / Sniffing

Unauthorized Viewing

Intentional Misuse

Social Engineering

Degraded / Unavailable

User Error

Outsourced

Application Server

Malicious Software

Unauthorized System Access

Theft

Degraded / Unavailable

Hardware Failure

User Error

Data Loss

Social Engineering

Unauthorized Physical Access

Unauthorized Remote Access

Intentional Misuse

Connection Of Unauthorized Equipment

Eavesdropping / Sniffing

Man-made / Natural Disaster

Environmental Incident

Remote Capture

Data Loss

Unauthorized System Access

Hardware Failure

Eavesdropping / Sniffing

Degraded / Unavailable

Intentional Misuse

Outsourced

Unauthorized Remote Access

Social Engineering

Software Acquisition

Unauthorized Physical Access

Environmental Incident

Malicious Software

Unauthorized Viewing

Man-made / Natural Disaster

User Error

Storage Area Network

Unauthorized Physical Access

Eavesdropping / Sniffing

Unauthorized Remote Access

Degraded / Unavailable

Hardware Failure

Connection Of Unauthorized Equipment

Unauthorized System Access

Environmental Incident

Man-made / Natural Disaster

Wide Area Network

Eavesdropping / Sniffing

Unauthorized Physical Access

Connection Of Unauthorized Equipment

Unauthorized Remote Access

Degraded / Unavailable

Environmental Incident

Hardware Failure

Unauthorized System Access

Man-made / Natural Disaster

Proof System

Unauthorized System Access

Hardware Failure

Eavesdropping / Sniffing

Degraded / Unavailable

Data Loss

Outsourced

Unauthorized Remote Access

Social Engineering

Software Acquisition

Unauthorized Physical Access

Environmental Incident

Malicious Software

Unauthorized Viewing

Intentional Misuse

Man-made / Natural Disaster

User Error