Global Information Assurance Certification Paper

A Simple & Practical Approach to Risk Analysis

GIAC Security Essentials Certification (GSEC)

Chris Donlon
February 23, 2004

Abstract:
Risk has become a buzzword in many areas of business; however, many people fail to see the relevance of a risk analysis beyond its primary security function. This paper will provide non-risk professionals the knowledge needed to understand the broad ranging impact a thorough risk analysis can have on a business unit. Real world examples will describe a simple, practical process that can be used to understand or perform a risk analysis of any business unit.

Numerous papers have been written and studies done on performing risk analysis and identifying the necessary controls needed to mitigate these risks. United States regulatory requirements such as the Gramm-Leach-Bliley Act and the more recent Sarbanes-Oxley Act have only added to the myriad of information available on the topic. A recent Google search on "Risk Assessment" returned over 3 million hits.

While large companies and/or publicly traded firms may have the financial ability and/or the regulatory impetus to have a professional performed risk analysis many smaller businesses do not. These businesses may not see the value in performing a risk analysis and without any regulatory requirements never will. In addition, individuals within both large and small business may not understand the benefit a risk analysis provides and in the case of small businesses may find the thought of doing the task themselves extremely daunting. This paper will answer many of the questions concerning the risk analysis process and provide a basic framework to understand and develop one.

This paper will consist of three parts:

1. Justification for the use of a Risk analysis in any business environment.

2. Real world examples of applying basic risk analysis techniques in an E-Banking environment. The techniques used in this example, while specific to the Information Technology risks in an E-Banking environment, can be used to formulate a risk analysis in any business environment.

3. An Appendix that includes a risk analysis of an E-Banking business unit.

The first thing we need to understand before we can continue is: What is a Risk Analysis?

A "classical definition"[1] of Risk Analysis provided by COBRA, a well-known Risk Analysis product, "describes it as a process to ensure that security controls for a system are fully commensurate with its risks."[2]

A family owned business with little concern for internal security may respond, "What do I need security controls for?" Another small company with little or no inventory and physical assets may respond, "We only have one computer not a system. What good is a risk analysis to me?"

The way the Risk Analysis Process is normally defined and presented, it is easy to see how its value can be underestimated. Another definition of Risk Analysis could be: Risk Analysis is the process of identifying events that effect business processes and formulating procedures and policies to ensure that the effect of negative events are minimized and positive events are fully realized. A more abbreviated description of the Risk Analysis could be described as "What If?"

Now that we have defined what a Risk Analysis is we can see what the process can do for a small business.

Business Communication
Understanding how one business process affects another is crucial to effective communication between company components. Procedures developed because of a thorough risk analysis provide a great tool for lower end managers to use when a problem develops. It allows them to notify other units directly affected by the problem. Sometimes the areas affected by a problem are not always apparent. A well thought out risk analysis ensures that no one is forgotten.

Disaster Recovery.
Using the "What if" mindset when doing a risk analysis of your company allows you to better prepare your company in the event of a natural or manmade disaster.

> Disasters often cause small businesses to relocate or cease operation temporarily, which may lead to substantial economic and personal hardship. Many businesses that are forced to close after

[1] COBRA. "Security Risk Analysis & Assessment, and ISO 1799/B57799 Compliance." URL: http://www.riskworld.net/benefits.htm (7 Feb. 2004)

[2] COBRA. "Security Risk Analysis & Assessment, and ISO 1799/B57799 Compliance." URL: http://www.riskworld.net/benefits.htm (7 Feb. 2004)

> a disaster never reopen at all. Thorough planning… is essential to maximize the chances for recovery.[3]

As previously stated, while the processes identified in this paper are no substitute for a professional risk analysis of your company it will provide a framework to use in order to ensure that your decisions at this crucial time are well thought out and not just a reaction to the current circumstance.

> Too often, loss prevention measures, if they exist at all, are implemented as a hurried reaction to a bad experience. These are frequently emotional rather than logical decisions. Little or no research is done. Little effort is made to distinguish between real and perceived problems. No consideration is given to alternatives. The end result is a collection of independently operating procedures that, in some cases, may actually make matters worse.[4]

Formulation of Written Policies and Procedures
A risk analysis serves as a great tool for developing company policies and procedures. Once you have identified the most critical functions of your company you can tailor your written policies and procedures to ensure that the most favorable procedures are followed. How this is done will be readily apparent when we demonstrate the risk analysis process.

Identify Operational Deficiencies
In the same way you can streamline your business processing using a Risk analysis you may also realize certain procedures need to be performed in order to ensure a better final product, maintain the integrity of financial processes, etc. This is generally one of the most recognizable benefits of a typical risk analysis.

Increased Operational Efficiency
The process of identifying risks in your company requires a look at all procedures that are performed in all levels of the company. Many times, redundant procedures are uncovered or procedures with no real value are identified. In addition, you may find that certain areas of your company may be able to address the needs of a business process more efficiently. Eliminating or modifying your current procedures can streamline your business processes and increase productivity.

---

[3] San Francisco Small Business Commission, San Francisco Mayor's Office of Emergency Services. "Disaster, Preparing Your Small Business for Disaster. " URL:http://www.bomasf.org/pdf/news/smallbizdisaster.pdf (7 Feb. 2004)

[4] Gardner, Robert CPP. "Small Business: Reducing the Risk." (1995) URL: http://www.crimewise.com/library/bizrisk.html (7 Feb. 2004)

Information Technology
The risks associated with information technology have been a driving force behind the adoption of risk analysis in many business sectors. Depending upon your company's reliance on information technology this could be the largest area of risk in your company. Performing a risk analysis of your technology processes is vital to the continued health of this area. No matter how small your business is using risk analysis techniques within your IT department can increase operational efficiency and ensure that security vulnerabilities are not missed.

Knowledge
While many small business owners know their business intimately this may change as the business grows. A continuing reevaluation and updating of the companies risk analysis allows the companies owner(s)/manager(s) to see how all functions of the business relate to one another and contribute to the success of the company.

Legal Compliance
Small businesses may not be as heavily regulated by the previously mentioned statues; i.e. the Gramm-Leach-Bliley Act or Sarbanes-Oxley Act, but many still have other regulatory requirements that they must follow. Using a risk analysis to compare these regularity requirements with your current business processes will ensure that your company is fulfilling its legal responsibilities.

Policy Acceptance
Many times companies enact policies and expect these policies to be followed. The threat of unemployment is used to enforce these policies when a more effective alternative is to show low-level managers why these policies are needed. Policies derived from a well thought out risk analysis do just that. It allows managers to see that there is a rational and logical reason for that policy.

Security
Probably the most tangible use of a risk analysis is its use in evaluating the overall security of your company. Whether its security of personnel, inventory, or other physical or intellectual assets, a thorough understanding of their vulnerabilities will ensure that the security you provide is commensurate with its value.

The examples given are just some of the benefits a risk analysis can provide for your business. Now that we have identified some of these benefits we will examine how to perform a risk analysis of your company's processes.

For a risk analysis to be effective it must be organized and concise. A Risk Analysis Matrix is often used to do this. We will use the following table as our matrix.

Ref #	Risk	Risk Type	Level of Risk	Controls \Policies Used to manage risk	Control Procedures	Additional Measures Required?

The “Ref#” column is self-explanatory and is used to track each identified risk. You could easily use letters instead of numbers in this column if you choose.

The “Risk” column notes all things that could go wrong in any of your business processes. This is the primary column we will use when conducting our analyses. The other columns in the matrix all are all derived from the entries here; however, when you are first doing your risk analysis you may place items in the Control Procedures column and trace these procedures back to an identified risk. If you find that there is no risk associated with your procedure you may need to evaluate the necessity of the Control Procedure.

The “Risk Type” column is used to identify the kind of risk you identified in the Risk Column. There are many ways to define type of risk; e.g. human, technical, reputation, natural, monetary, etc. The type of Risk will vary based upon the type of entity you are analyzing. For our purposes we will ignore this column.

The “Level of Risk” column is used to measure the relative impact the identified risk will have on your business processes. Risks are generally measured qualitatively or quantitatively.

A quantitative risk analysis uses computer modeling and statistical analysis based on known data values. A quantitative risk analysis should only be performed with the help of a Risk processional. Qualitative analysis are, generally, less formal and rigid in their design.

> Use a qualitative analysis where the level of risk does not justify the time and resources need for a numerical analysis, where the data is inadequate, or to perform an initial screening of risks.[5]

For a small business performing its first risk analysis with little or no money to spend a qualitative risk analysis is the obvious choice. In the following examples we will now measure risk. We will use High, Medium, and Low to measure the relative value of the risks we identify in our Risk Analysis example found in the Appendix.

---

[5] The State of Queensland (Department of Education). “Integrated Risk Management in Education Queensland.” (2001) URL: http://education.qld.gov.au/strategic/policy/guidelines/risk/qualitative.html. (7 Feb. 2004)

The “Control\Policies Used to Manage Risk” column is, generally, a broad statement as to how your business will mitigate the Risk Identified in the “Risk” Column. This column can and should be correlated with your companies written polices to ensure that formal procedures are developed to mitigate your companies risks.

The “Control Procedures ” column is used to identify actual actions performed in your business units. These actions should mitigate the risks identified in the Risk Column and should be derived from the “Control\Policies Used to Manage Risk”

The final column “Additional Measures Required” can be used, as a checklist, to ensure that the necessary policies and procedures have been developed to mitigate the risks identified.

Now that we have seen the basic framework used for performing a risk analysis we can follow the process using real world examples.

Your first step should be to gather as much information about your business processes as possible. The information gathering phase should encompass internal as well as external sources. For instance, a risk analysis of a banks’ e-business unit would include internal sources such as current procedures, company policies, and interviews with personnel, as well as external sources such as regulatory requirements, audit recommendations and competitors product information.

A trucking business may use business contracts and labor agreements. A landscaping may obtain information from growing and planting books. A deli may use FDA food handling guidelines. Typically, all companies can use the information found in existing policies and procedures, interviews and questionnaires, insurance documents, disaster preparedness information, and federal labor laws. Other sources depending on the type of business may include government regulations, legal contracts, trade restrictions, and/or past legal precedents. The key is to look at your business processes from as many angles as possible and identify the risks that are inherent your business.

In theory, your business should identify risks, formulate policies based on those risks and then develop procedures to ensure that the risks are properly mitigated. In reality; however, it is generally easier and less time consuming to begin with what you already do to make sure things don’t go wrong and work from there. After all, you probably already have established procedures in your company to make sure most risks can be handled without disrupting your business.

In our first example, we will use information obtained from current operating procedures and enter these in our matrix. Please note in our examples we will ignore the Ref#, Type of Risk, Level of Risk, and the Additional Measures

Needed columns. For our purposes, which are to examine the flow of risk identification to actual control procedures, these columns are not needed.

In your own analysis you will use the columns Level of Risk and Additional Measures Needed column to identify the risks that could have a serious effect on your business processes and what risks you still need to address. As previously stated, a complete E-Banking Risk Analysis Matrix, which includes these risk rankings, can be found in the Appendix.

Our first example will rely on current procedures involving the Companies E-Banking business. We will use these procedures to populate our matrix with applicable risks. These procedures are as follows:

- All changes to the Bank's E-Banking website are approved in advance by the Bank's Marketing Department.
- Security and Hardware are in place to ensure all activity regarding the bank's E-Banking systems is logged.
- Data on the bank's E-banking systems is backed up daily.

We will enter these procedures in our matrix as follows:

#	Risk(s)	Risk Type	Lvl of Risk	Controls \Policies Used to manage risk	Control Procedures	Additional Measures Required?
					All changes to the Bank's E-Banking website are approved in advance by the Bank's Marketing Department.	
					Security and Hardware are in place to ensure all activity regarding the bank's E-Banking systems is logged.	
					Data on the on the bank's E-Banking system is backed-up daily.	

The next step is to ask, "Why are we doing these procedures?" The answer will, generally, identify a risk to your business process. We will enter these risks in the "Risk" column.

#	Risk(s)	Risk Type	Lvl of Risk	Controls \Policies Used to manage risk	Control Procedures	Additional Measures Required?
	Intentionally or unintentionally changing the E-Banking web site design could cause damage to the reputation of the bank or a loss of business.				All changes to the Bank's E-Banking website are approved in advance by the Bank's Marketing Department.	
	System files\account records may be intentionally \unintentionally modified causing a loss of data integrity, potentially flawed decision making, financial losses, and/or loss of reputation.				Security and Hardware are in place to ensure all activity regarding the bank's E-Banking systems is logged.	
	Inadequate backups could cause loss of data confidentiality, integrity, and systems availability.				Data on the on the bank's E-Banking system is backed-up daily.	

The final step in our first example is to formulate policies to ensure that all levels of the company address identified risks.

#	Risk(s)	Risk Type	Lvl of Risk	Controls \Policies Used to manage risk	Control Procedures	Additional Measures Required?
	Intentionally or unintentionally changing the E-Banking web site design could cause damage to the reputation of the bank or a loss of business.			Before being posted, all changes to the E-Banking web page must be approved by the Marketing Department. Changes to the web page(s) of the Bank must be verified by a second person before and after posting.	All changes to the Bank's E-Banking website are approved in advance by the Bank's Marketing Department.	
	System files\account records may be intentionally \unintentionally modified causing a loss of data integrity, potentially flawed decision making, financial losses, and/or loss of reputation.			All computerized systems must include logs which record changes to critical application system files Periodic reviews of production operating systems and network operating systems must be conducted to ensure that only authorized changes have been made.	Security and Hardware are in place to ensure all activity regarding the bank's E-Banking systems is logged.	
	Inadequate backups could cause loss of data confidentiality, integrity, and systems availability.			To prevent loss, all data stored on the Bank's E-Banking systems must be copied to tape or other storage media.	Data on the on the bank's E-Banking system is backed-up daily.	

Now that we have completed our matrix it is time to evaluate it. Ask yourself "Are there more risks we have not identified? Do the procedures and policies in place properly address all the risks? Are there procedures in place we

have missed that will help mitigate these risks? Do we need another procedure(s) to help mitigate these risks?" Starting with procedures you already have makes answering these questions and filling in the gaps much easier. Here is a look at a completed analysis of these same risks.

#	Risk(s)	Risk Type	Lvl of Risk	Controls \Policies Used to manage risk	Control Procedures	Additional Measures Required?
	Intentionally or unintentionally changing the E-Banking web site design could cause damage to the reputation of the bank or a loss of business.			Before being posted, all changes to the E-Banking web page must be approved by the Marketing Department. Changes to the web page(s) of the Bank must be verified by a second person before and after posting.	All changes to the Bank's E-Banking website are approved in advance by the Bank's Marketing Department. Changes are reviewed and approved in writing by the Marketing Department upon completions	
	System files\account records may be intentionally \unintentionally modified causing a loss of data integrity, potentially flawed decision making, financial losses, and/or loss of reputation.			All computerized systems must include logs which record changes to critical application system files Periodic reviews of production operating systems and network operating systems must be conducted to ensure that only authorized changes have been made.	Security and Hardware are in place to ensure all activity regarding the bank's E-Banking systems is logged. Computer generated activity logs are reviewed daily. Current computer system configurations are compared to a baseline at least monthly.	
	Inadequate backups could cause loss of data confidentiality, integrity, and systems availability. Intentional or unintentional deletion of important files may cause increased expenses or loss of reputation			To prevent loss, all data stored on the Bank's E-Banking systems must be copied to tape or other storage media. The Bank requires the use of at least five sets of backup media to be used in rotation. Backup Up media should be stored in fireproof safes, at a separate location System managers are responsible for ensuring that periodic backups of the E-Banking systems are performed.	Data on the on the bank's E-Banking system is backed-up daily. Backup procedures are reviewed and approved by E-Banking management. E-Banking backups are checked daily for propriety. Backup tapes are restored quarterly to backup systems to ensure integrity of backup process. Backup tapes are removed from rotation after one year of use. Backup tapes are stored off-site in fireproof vaults.	

Our next method will assume you have gathered information regarding your business from outside sources and are using these sources to identify potential risks to your own business. Using outside sources helps save time and allows you to view the risks to your business from an alternative angle. We will

use the E-Banking Booklet contained in the FFIEC's IT Examination Handbook. A section of this handbook reads as follows:

> Financial institution directors and senior management should ensure the information security program addresses these challenges and takes appropriate actions….
>
> ♦Implement security controls sufficient to manage the unique security risks confronting the institution. Control considerations include….
>
> •Ongoing awareness of attack sources, scenarios, and techniques….
>
> •Hardened systems with unnecessary or vulnerable services or files disabled or removed….
>
> •Physical security of all e-banking computer equipment and media..[6]

As you can see this source offers three areas we can use to identify potential risks. We'll enter these potential risks in our matrix.

#	Risk(s)	Risk Type	Lvl of Risk	Controls \Policies Used to manage risk	Control Procedures	Additional Measures Required?
	New security threats could compromise system integrity before applicable system defenses are put in place.					
	Hardware or Software features not used in the E-Banking environment may be used to gain unauthorized access to the Bank's systems causing loss of production capabilities and/or damage to the reputation of the Bank.					
	In adequate physical controls of E-Banking hardware and media could result in loss of production capabilities and/or the compromise of customer information. The theft of confidential information could result in the bank's E-Banking customers being victims of identity theft thereby damaging the Bank's reputation and increasing legal fees.					

[6] Federal Financial Institutions Examination Council. "FFIEC E-Banking IT Examination Handbook." (August 2003):pg. 26

Once we have identified the risks we need to ensure that we relay this information to our company via Company policies; i.e. Controls \Policies Used to Manage Risk. Company policies give direction as to the types of procedures that should be in place; i.e. Control Procedures. We'll enter both of these in our matrix.

#	Risk(s)	Risk Type	Lvl of Risk	Controls \Policies Used to manage risk	Control Procedures	Additional Measures Required?
	New security threats could compromise system integrity before applicable system defenses are put in place.			E-Banking security administrators must develop procedures to ensure that system security is relevant to current threats.	E-Banking administrators belong to mailing lists that inform them of new virus or security threats. Administrators attend annual security conferences to stay informed of the latest security threats.	
	Hardware of Software features not used in the E-Banking environment may be used to gain unauthorized access to the Bank's systems causing loss of production capabilities and/or damage to the reputation of the Bank.			Features, which are unnecessary in the Bank's E-Banking computing environment, must be disabled when the software or hardware is installed.	Setup checklists provided by software\hardware vendors and\or other security organizations are used to setup new systems. Periodic review of E-Banking system security is performed by third parties. Internal audits of internal computer systems are performed.	
	In adequate physical controls of E-Banking hardware and media could result in loss of production capabilities and/or the compromise of customer information. The theft of confidential information could result in the bank's E-Banking customers being victims of identity theft thereby damaging the Bank's reputation and increasing legal fees.			E-Banking hardware should be kept in secured areas that require card or key access to only authorized personnel. When confidential information is no longer needed it must be destroyed according to approved methods. If confidential information is disclosed, or is suspected of being disclosed to unauthorized parties, the E-Banking department must be notified immediately.	E-Banking computer equipment is kept in a locked room. Only E-Banking personnel responsible for system maintenance has access to Computer equipment. All discarded reports and other confidential information is securely stored until it can be destroyed. Employees will secure all reports and documents in their possession, prior to leaving for the day. Procedures are in place to notify customer s should confidential information be disclosed.	

As we have demonstrated a small paragraph from an outside source can identify many areas of risk in your company. The alternative perspective outside sources give allows you to effectively begin discussions and brainstorm with

others in your company to begin or complete the risk analysis process. Use these sources to save time and to identify risk areas you may have missed.

Once you have completed the basics risk analysis matrix you should evaluate each risk and assign it a value. The value assigned is relative to the type of business you are analyzing. Start by ranking your risks using basic measurements; i.e. high, medium, low. Ranking the risks will allow you to focus on the most important ones before wasting resources on lower ranked risks. You may even choose to ignore some low level risks due to practical or monetary considerations. As you continue to expand on your risk evaluations you may choose to become more detailed in your assignment of risk levels using a more quantitative approach. If you choose to do this, resources of a risk professional are highly desirable.

The final step in completing a risk analysis of your business is evaluating what functions\ processes and\or policies of your company need to be modified to effectively mitigate the identified risks. The Risk Analysis Matrix streamlines this process and is an effective tool to use to identify areas that still need work. Use the “Additional Measures Required?” column to denote what areas effectively mitigate identified risks and what areas still need work.

As we have demonstrated the act of performing a basic risk analysis of your business need not be an overly complicated venture. Using current procedures, outside sources and most of all the intimate knowledge owners\managers have of their business a thorough analysis of a companies risk environment can be performed.

Bibliography

COBRA. "Security Risk Analysis & Assessment, and ISO 1799/B57799 Compliance." URL: http://www.riskworld.net/benefits.htm (7 Feb. 2004)

COBRA. "Security Risk Analysis & Assessment, and ISO 1799/B57799 Compliance." URL: http://www.riskworld.net/benefits.htm (7 Feb. 2004)

San Francisco Small Business Commission, San Francisco Mayor's Office of Emergency Services. "Disaster, Preparing Your Small Business for Disaster. " URL:http://www.bomasf.org/pdf/news/smallbizdisaster.pdf (7 Feb. 2004)

Gardner, Robert CPP. "Small Business: Reducing the Risk." (1995) URL: http://www.crimewise.com/library/bizrisk.html (7 Feb. 2004)

The State of Queensland (Department of Education) "Integrated Risk Management in Education Queensland." (2001) URL: http://education.qld.gov.au/strategic/policy/guidelines/risk/qualitative.html. (7 Feb. 2004)

Federal Financial Institutions Examination Council "FFIEC E-Banking IT Examination Handbook." (August 2003):pg. 26

Decisioneering. "Risk Analysis Overview. What is Risk?" (2003) URL: http://www.decisioneering.com/risk-analysis.htlm. (7 Feb. 2004)

Wood, Charles. "Information Security Policies Made Easy" Baseline Software. Susalito, California (1997)

Nelson, Karen. "Security Assessment Guidelines for Financial Institutions." (2002) Sans Reading Room URL: http://www.sans.org/rr (6 Feb 2004)

Bong, Kevin. "Conducting an Electronic Information Risk Assessment for Gramm-Leach Act Compliance." (2003) Sans Reading Room URL: http://www.sans.org/rr (6 Feb. 2004)

Visintine, Vishal. "An Introduction to Information Risk Assessment" (2003) Sans Reading Room URL: http://www.sans.org/rr (6 Feb 2004)

Candela Solutions. "Internal Control Documentation Evaluation" URL: http://www.candelasolutions.com/popup.asp?ID=3 (7 Feb 2004)

Teal, Kelly. "Sorting Out Sarbanes-Oxley Vague Law, Varied Solutions Cause Confusion for Public Telcos" (Feb. 2004) URL: http://www.phoneplusmag.com/articles/421feat02.html (7 Feb. 2004)

Doherty, Sean. "Feds Reach Out and Touch IT." (July 10, 2003) URL: http://www.parnold.com/articles/handysoft/hsnetworkcomputing.htm

Appendix E-Banking Risk Analysis Matrix

#	***Risk***	Type of Risk	Lvl of Risk	Control(s)/Policies Used to Manage Risk	Control Procedures	Additional Measures Needed (Yes/No)*
1	Failure of important hardware and software vendors to remain financial stable could cause a loss of systems support, and increase costs associated with system upgrades.	Technical	H	Source code for all mission critical file management and database software is held in escrow.	The bank uses standard Web Design software in its web page development. Code for the E-Banking application is held in escrow	No
2	System files/account records may be intentionally/unintentionally modified causing a loss of data integrity, potentially flawed decision making, financial losses and/or a loss of reputation.	Human Reputation	H	All Bank computerized production systems must include logs which record, changes to critical application system files. Periodic reviews of production operating systems and network operating systems must be conducted to ensure that only authorized changes have been made.	Security hardware and software is in place to ensure all activity regarding the bank's E-banking systems is logged. Computer generated activity logs are reviewed daily. Current computer system configurations are compared to a baseline analysis at least monthly.	No
3	Software/programming errors may cause system degradation, interruption in system services, a loss of input data and/or erroneous output data.	Technical	H	The E-banking systems must employ a documented change control process, which is used to ensure that only authorized changes are made.	All changes to the Bank's E-business systems are performed on test systems before they are implemented on live systems. Mangers must approve these tested changes before they are put on live systems.	No
4	Improper documentation of systems and system's integration may cause a lack of management oversight and/or could effect the timely restoration of system resources in the event of a system or component failure.	Technical	M	Documentation reflecting all significant changes to the Bank's E-banking systems must be prepared within a week from the time that a change took place. This documentation must reflect the proposed change, management approval, and the way in which the change was performed.	E-banking equipment and system changes are documented in the E-Banking Hardware and Software Changes Log.	No

#	***Risk***	Type of Risk	Lvl of Risk	Control(s)/Policies Used to Manage Risk	Control Procedures	Additional Measures Needed (Yes/No)*
5	Malicious software (e.g., virus, Trojan horse, logic bomb, worm) could be introduced into the system via internet download, floppy disk, or E-mail, causing system failures, damage to data files, damage to the bank's reputation, and/or exposure of the banks assets to unauthorized personnel.	Technical	M	Virus checking programs approved by the E-Banking Department must be continuously enabled on all E-banking systems. Users must not intentionally write, generate, compile, copy, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any computer's memory, file system, or software.	Virus protection software is loaded on all E-banking systems. E-Banking administrators belong to mailing lists that inform them of new virus or computer systems threats. Users check external media; e.g. cd-rom, diskettes, before files are transferred to any E-banking system. All employees sign a "code of conduct letter" stating that they will not engage in nefarious computer activity while an employee of the bank.	No
6	Unauthorized or improper modifications to system hardware or software could cause system failures, unauthorized access to system resources, and/or loss of quality in output products.	Human	M	Periodic reviews of production operating systems and network operating systems must be conducted to ensure that only authorized changes have been made. The Bank's information systems must employ industry-specific information security standards. In addition, all Bank information systems must include standard controls found in organizations in similar circumstances. Unique risks faced by the Bank must be addressed via custom solutions.	The E-banking manager signs off on all changes to the E-banking systems. E-banking security administrators periodically attend banking seminars regarding E-banking.	No
7	Improper implementation of software changes, upgrades, or modifications could result in system failures.	Technical	M	Executable programs provided by external entities must be tested before installation on any E-Banking system All E-Banking systems must employ a documented change control process.	A test environment is utilized before changes, upgrades or modifications go live. Bugtraq or similar databases are reviewed before purchase of new production software. All system changes to E-Banking systems are documented and approved.	No

#	***Risk***	Type of Risk	Lvl of Risk	Control(s)/Policies Used to Manage Risk	Control Procedures	Additional Measures Needed (Yes/No)*
8	Inadequate documentation of program changes could effect the timely restoration of system resources in the event of a component(s) failure resulting in monetary losses.	Technical	M	Documentation reflecting all significant changes to the Bank's information systems must be prepared within a week from the time that a change took place. This documentation must reflect the proposed change, management approval, and the way in which the change was performed.	The IS or DP Manager signs off on any program changes in the E-Banking Hardware and Software Changes Log.	No
9	Security features may not be adequate or properly enabled on systems exposing the banks assets and resources to unauthorized access.	Technical	M	Information systems security products on the market less than a year must not be used as an integral component of any E-banking system	A thorough review of new security software is performed which includes a written report before any system is adopted. Information Security periodicals as well as Hacker/Cracker sites are reviewed before selecting a new security system.	No
10	Unauthorized disclosure of customer information via improper handling/ storage/ disposal of input and output data, including locked storage of sensitive paper and electronic media could result in claims of negligence and/or damage to the bank's reputation.	Human Reputation	M	Information that can be directly linked to a specific customer must only be released to third parties if the customer has provided written consent or the Bank is legally required to disclose the information. Third parties may be given access to internal information only when a demonstrable need-to-know exists, and when such disclosure has been expressly authorized by management. All waste copies of secret and confidential information must be destroyed according to approved procedures.	E-Banking maintains a shredder that is used to destroy all documents containing users and/or system information. Shredders and shredding boxes are provided for proper disposal of customer information A Privacy Program was presented to all employees to train them on this matter.	No

#	***Risk***	Type of Risk	Lvl of Risk	Control(s)/Policies Used to Manage Risk	Control Procedures	Additional Measures Needed (Yes/No)*
11	Inadequate backups could cause loss of data confidentiality, integrity, and system availability. Intentional or unintentional deletion of important files may cause increased expenses or loss of reputation.	Technical Human	H	The Bank requires the use of at least five sets of backup storage media to be used in rotation. Back-up media should be stored in fireproof safes, at a separate location. To prevent loss, all data stored on the Bank's E-Banking systems must be copied to tape or other storage media. System managers are responsible for ensuring that periodic backups of the E-banking systems are performed.	E-Banking is able to restore files from nightly backups. Backup logs are checked daily for propriety. Backup tapes are restored quarterly to backup systems to ensure integrity of backup process. Backup tapes are removed from rotation after 1 year of use. Backup tapes are stored of-site in Fireproof vaults. All data files for the primary bank systems are backed-up daily and stored off-site. Data on the E-Banking systems are backed up daily. Backup procedures have been reviewed and approved by E-Banking management	No
12	Computer hardware components failure may cause a loss of data integrity, increase in processing time, loss of software capabilities, interruption of services, and/or a degradation of system performance.	Technical	M	Preventive maintenance must be regularly performed on all computer systems according to recommended service intervals and maintenance specifications. Authorized personnel must perform repairs and servicing of equipment.	Contracts are in place for mission critical systems. The Disaster Plan covers recovery of systems and data.	No
13	A break in the power continuity caused by high-voltage spikes or "brownouts" that is sufficient to cause operational interruption may cause a loss of input data or shutdown the systems.	Technical	M	All E-Banking must be outfitted with either uninterruptible power supply (UPS) systems, electrical power filters, or surge suppressers which have been approved by the management.	UPS devices are installed on all Network equipment. Backup generators are in use and tested annually.	No

#	***Risk***	Type of Risk	Lvl of Risk	Control(s)/Policies Used to Manage Risk	Control Procedures	Additional Measures Needed (Yes/No)*
14	An inadequate or outdated business recovery plan may delay resumption of business activities causing monetary losses and damage to the reputation of the bank.	Technical	M	A standard process for developing and maintaining computer and communication system contingency plans must be documented and maintained by the E-Banking Department.	Business/Disaster Recovery Plan is updated and reviewed by management annually.	Yes
15	Inadequate testing of the business recovery plan may delay resumption of business activities causing monetary losses and damage to the reputation of the bank.	Technical	M	Computer and communication system contingency plans must be tested at regular intervals to assure that they are still relevant and effective. Each such test must be followed by a brief report to management detailing the results of the test and any remedial actions that will be taken.	Testing at an off-site location is performed biannually. The results of these tests are provided to the Board of Directors.	No
16	Inadequate planning during system design or software implementation may result in a lack of internal controls.	Technical	M	Whenever major system changes involving sensitive information take place an analysis of the potential security-related impacts must first be performed. The analysis should address security risks and service interruption at a minimum.	Third-party reviews are performed during planning stages. Management signs off on all system changes.	No
17	Intentionally or unintentionally changing the E-Banking web site design could cause damage to the reputation of the bank or a loss in business.	Technical Monetary	M	Before being posted, all changes to the E-Banking web page must be approved by the Marketing Department. Changes to the web page(s) of the Bank must be verified by a second person before and after posting.	All changes are approved in advance in writing by the Marketing Department. Changes are reviewed and approved in writing by the Marketing Department upon completion.	No

#	***Risk***	Type of Risk	Lvl of Risk	Control(s)/Policies Used to Manage Risk	Control Procedures	Additional Measures Needed (Yes/No)*
18	Bank employees may attempt to test and/or compromise internal controls thereby exposing the Bank's assets to unauthorized access.	Human	M	Workers must not acquire, possess, trade, or use hardware or software tools that could be used to evaluate or compromise information systems security. Workers must not test, or attempt to compromise internal controls unless properly approved. Users must not exploit vulnerabilities or deficiencies in information systems security.	Unauthorized attempts are logged and reviewed by the E-Banking Security Administrator daily. Each user logs into E- Banking systems with a pre-assigned user profile that limits the ability of the user to compromise controls. Employees must sign a "Code of Conduct" letter as a condition of employment	No
19	Social engineering may be used to obtain unauthorized access to the Bank's systems causing a loss of production capabilities, physical damage to hardware, and/or damage to the reputation of the Bank via theft of private information.	Human	M	Security Administrators must not reveal a password unless the involved user has first been identified. Passwords may only be disclosed when a user ID is being assigned or to an identified user who has been locked out of his account. Public Tours of major computer and communications facilities are prohibited. Individuals who are not trusted employees, authorized consultants and /or authorized contractors must be supervised whenever they are in restricted areas. Unescorted visitors must be escorted to a reception desk, guard station, or to the person that they came to see. Visitors and other third parties must not be permitted to use employee entrances or other uncontrolled pathways leading to areas containing sensitive information.	**WE MUST IMPLEMENT CONTROL PROCEDURES!!!**	Yes

#	***Risk***	Type of Risk	Lvl of Risk	Control(s)/Policies Used to Manage Risk	Control Procedures	Additional Measures Needed (Yes/No)*
20	Hardware or Software features not used in the E-banking environment may be used to gain unauthorized access to the Bank's systems causing loss of production capabilities and/or damage to the reputation of the Bank.	Technical	M	Features, which are unnecessary in the Bank's E-Business computing environment, must be disabled when the software or hardware is installed.	Setup checklist provided by software vendors and\or other security organizations are used to setup new systems. Third parties perform periodic reviews of the security of E-Banking systems. Internal audits of internal systems are performed.	No
21	The theft of confidential information could result in the banks E-banking customers being victims of identity theft thereby damaging the Bank's reputation and increasing legal fees.	Human	M	When confidential information is no longer needed it must be destroyed according to approved methods. If confidential information is lost, is disclosed, or is suspected of being lost or disclosed to unauthorized parties, the information owner and the E-Banking department must be notified immediately.	All discarded reports and other confidential information is securely stored until it can be destroyed. Employees will secure all reports and documents in their possession, prior to leaving for the day. The ability to download data from the bank's system is restricted to those few employees that have a need to do so. Procedures are in place to notify customers should confidential information be disclosed.	No

#	***Risk***	Type of Risk	Lvl of Risk	Control(s)/Policies Used to Manage Risk	Control Procedures	Additional Measures Needed (Yes/No)*
22	The purposeful destruction of customer data could result in the bank being unable to charge customers for withdrawals, or credit customers for deposits causing financial loses and damage to the Bank's reputation..	Human	M	Users must not intentionally write, generate, compile, copy prorogate, execute, or attempt to introduce any virus, worm, or Trojan horse to the Bank's computer system. To prevent loss, all data stored on the Bank's E-Banking systems must be copied to tape or other storage media. If any unauthorized use of the Bank's information systems has taken place, or is suspected of taking place, the E-Banking Department must be notified immediately.	To protect against external hackers, the bank has installed an Internet firewall and an Intrusion Detection System. Software scans for viruses on all E-banking systems All data files for the primary bank systems are backed-up daily and stored off-site. Unauthorized access attempts are reviewed on a daily basis to ensure that information assets are not compromised.	No
23	Failure to adequately document user actions via audit trails could result in a loss of accountability, jeopardize legal proceedings and/or effect the ability to maintain/upgrade system integrity.	Technical	L	All privileged system commands issued by information security administrators, internal auditors, systems programmers, local area network administrators, etc. must be traceable to specific individuals via the use of comprehensive logs. All Bank computerized production systems must include logs which record, changes to critical application system files, changes to user privileges, system start-ups and shut-downs, and the user session activity; i.e. user-IDs, log-in date/time, log-out date/time, applications invoked. Records tracing security relevant activities to specific users must be retained for at least six (6) months or as required by applicable regulations.		Yes

#	***Risk***	Type of Risk	Lvl of Risk	Control(s)/Policies Used to Manage Risk	Control Procedures	Additional Measures Needed (Yes/No)*
24	Hardware and/or software may become obsolete causing the bank to become less competitive.	Technical	L	When selecting equipment and software, the life of such is anticipated in order to avoid untimely technological obsolescence.	The E-Banking staff attends seminars and trade shows to keep abreast of hardware and software solutions.	No
25	Improper software licensing could cause legal penalties and reputation risk to the bank.	Technical	L	The Bank maintains strict adherence to software license agreements. Management will establish controls to monitor and meter license usage to avoid unintentional violations. Intentional and willful violation of software copyright agreements by any employee of the Bank will be deemed sufficient grounds for termination of employment.	Licenses are purchased on an as-needed basis and are logged by invoice number.	No
26	System resources may not be available to facilitate the timely processing of customer and/or bank data resulting in financial losses and/or damage to the bank's reputation.	Technical	L	The E-Banking Division management is required to maintain reasonable contingency plans for equipment failures, software failures, telecommunication failures, and power failures to minimize the disruption to the Bank's E-Banking activities.	System resources are monitored for capacity planning. The E-Banking areas has written backup/recovery plans. RAID or backup servers are in places on the E-Banking systems.	No
27	Personnel may be unable to continue ongoing operations do to external factors; i.e., snow, floods, earthquakes, etc., resulting in financial losses and damage to the reputation of the bank.	Natural	L	For computer and communications systems, management must prepare, periodically update, and regularly test contingency plans. These plans must provide for the continued operation of mission critical systems in the event of an interruption or degradation of service.	A contract with an off-site vendor is in place for contingency planning and off-site operations	No

#	***Risk***	Type of Risk	Lvl of Risk	Control(s)/Policies Used to Manage Risk	Control Procedures	Additional Measures Needed (Yes/No)*
28	Electronic Banking controls may be inadequate resulting in financial losses, damage to the bank's reputation, and failure to comply with banking regulations.	Technical	L	Methods must be in place to ensure that all input to production computer systems that have been submitted for processing have been properly authorized. Transactions affecting sensitive, critical, or valuable information must only be processed if the originating individual or system is authorized to submit such transactions. Authorization can take the form of a signature, secret password, etc. All transactions to be input to a multi-user computer system must first be subjected to reasonableness checks, edit checks, and/or validation checks.	Changes to the E-Banking systems require the user to signon to the system. Reports are produced by the E_Banking system and distributed to for review by applicable areas; e.g. E-Banking, Accounting, etc.	No
29	Third parties may abuse system access privileges, damaging computer operations and/or the Bank's reputation, and/or causing financial losses.	Human	L	Third party vendors must only be given in-bound dial-up privileges when the system manager determines that they have a legitimate business need. These privileges must be enabled only for the time required to accomplish approved tasks. Before vendors or other third party users are permitted to reach the Bank's systems via real-time computer connections specific written approval of the E-Banking Department Manager is required.	Vendor User profiles are disabled until the vendor is ready to dialin. Dial-In lines or Firewall modifications that allow third-parties to access the banks E-Banking systems are changed when not in use.	Yes

#	***Risk***	Type of Risk	Lvl of Risk	Control(s)/Policies Used to Manage Risk	Control Procedures	Additional Measures Needed (Yes/No)*
30	Confidential information may be improperly disclosed to unauthorized parties damaging the Bank's reputation and/or causing the banks information controls to be compromised.	Human	L	Employees and vendors in custody of the Bank's sensitive information must take appropriate steps to ensure that these materials are not available to unauthorized persons. If secret or confidential information is lost or is disclosed to unauthorized parties, the information owner and the E-Banking Department must be notified. Before being released to third parties, all documentation that describes the Bank's systems or systems procedures must be reviewed by the Manager of E-Banking.	A contract outlining third parties responsibilities within the E-Banking systems must be signed before admittance is given to these systems.	No
31	Miscommunications between the Bank and its Vendors concerning the use of the Bank's E-Banking systems could result in damage to the Bank's reputation via unapproved release of information or financial and operational losses due to faulty vendor actions.	Technical	L	An agreement specifying the terms of the software and/or data exchange, as well as, the ways in which it will be used must be obtained before an exchange can take place.	Vendor contracts must include a privacy addendum.	No

#	***Risk***	Type of Risk	Lvl of Risk	Control(s)/Policies Used to Manage Risk	Control Procedures	Additional Measures Needed (Yes/No)*
33	**In adequate physical controls of E-Banking hardware and media could result in loss of production capabilities and/or the compromise of customer information.** The theft of confidential information could result in the bank's E-Banking customers being victims of identity theft thereby damaging the Bank's reputation and increasing legal fees.	Technical Monetary	H	E-Banking hardware should be kept in secured areas that require card or key access to only authorized personnel. When confidential information is no longer needed it must be destroyed according to approved methods. If confidential information is disclosed, or is suspected of being disclosed to unauthorized parties, the information owner and the E-Banking department must be department must be notified immediately.	**E-Banking computer equipment is kept in a locked room.** **Only E-Banking personnel responsible for system maintenance has access to Computer equipment.** **All discarded reports and other confidential information is securely stored until it can be destroyed.** **Employees will secure all reports and documents in their possession, prior to leaving for the day.** **Procedures are in place to notify customer s should confidential information be disclosed.**	No
34	**New security threats could compromise system integrity before applicable system defenses are put in place.**	Technical	H	**E-Banking security administrators must develop procedures to ensure that system security is relevant to current threats.**	E-Banking administrators belong to mailing lists that inform them of new virus or security threats. Administrators attend annual security conferences to stay informed of the latest security threats.	No

Last Updated: July 25th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event