Global Information Assurance Certification Paper

Information Security Management System (7799)
For
An Internet Banking System

Hermann Kelley

GIAC Certified ISO-17799 Specialist
Practical Assignment

Version 1.1, February 15, 2005

Table of Contents

Introduction

Banks and other financial institutions are governed by the Gramm-Leach-Bliley Act (GLBA) of 1999. Section 501(b) of the GLBA defines 'Standards for Safeguarding Customer Information'.

In February 2001, a number of government agencies, including the Office of the Comptroller of the Currency (OCC), the Federal Deposit Insurance Corporation (FDIC) and the Office of Thrift Supervision (OTS), collectively published guidelines supporting the GLBA requirements.

Specifically the guidelines address standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.

Most banks allow customers to conduct banking transactions through a Web based Internet interface. The security of this application and customer information associated with it is business critical for banks as security breaches may be considered high-profile. Furthermore, due to the requirements imposed by GLBA, banks need to implement safeguards governing this application and are regularly audited for compliance by the respective government agencies.

This paper develops an ISMS (Information Security Management System) as defined by ISO17799 which will effectively implement GLBA compliance and protect sensitive customer information that is stored as part of an Internet Banking System.

Organization

Secure Bank of Illinois, (SBI) is a community bank with 7 branch offices located in Illinois, Michigan and Indiana. SBI does not perform in-house data processing but historically has outsourced their core banking services to a third party called Reliable Banking Partners, Inc (RBP).

Due to competitive pressure and customer demand, SBI has implemented an Internet Banking System (IBS). The Internet Banking System is a turn-key solution purchased from Quick and Easy Inc. (Q&E), which implements the complete Web interface, management of the Internet Banking System and integration with the core banking system at RBP.

All SBI branch offices connect to the main branch using private leased frame-relay lines. The connection to RBP is a frame-relay line as well.
Bank tellers at the branch offices access the core banking system at the main branch through terminal emulation software. The branch offices do not currently have IT staff. Basic IT and help desk functions are performed by IT staff at the main branch and are partly outsourced to a local consulting company.

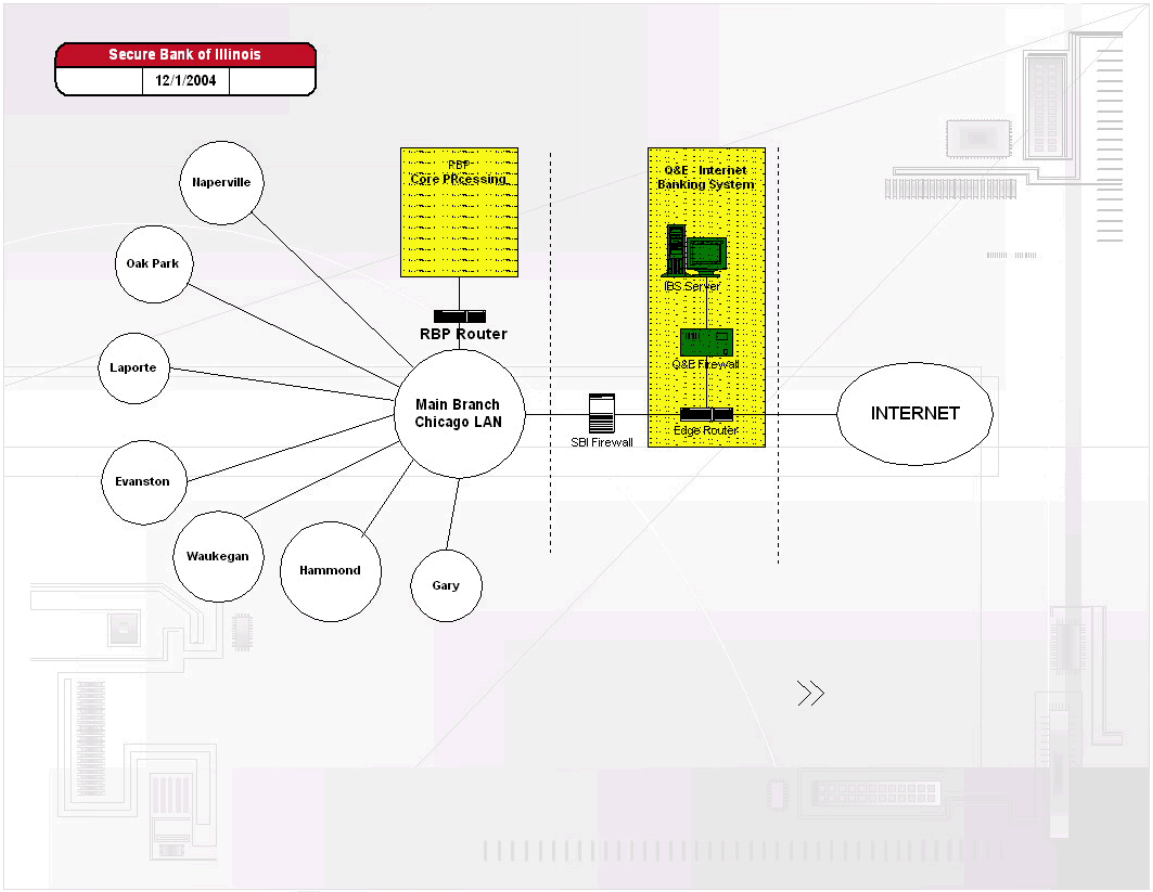
Internet access, as well as access to email, is limited to management and certain members of the IT team. This setup limits SBI's exposure to threats from the Internet.

Internally, SBI uses a system of logging, alerting and regular auditing to detect potential security breaches. Basic patch management and security maintenance procedures as well as security policies are in place.

In the future SBI plans to increase Internet usage throughout the organization. The ISO17799 initiative as it is described in this paper will serve as a blue-print and pilot project for extending strong security management throughout the rest of the organization.

Internet Banking System (IBS)

The diagram below shows how Q&E's Internet Banking System is integrated with SBI's network.



The ISMS defined in this paper will include the Internet Banking System (IBS) as well as customer information that is shared with the core processing system at RBP.

In its current implementation, the IBS is implemented using a setup that closely resembles a DMZ. Although there is limited impact on the rest of the network the IBS is considered a high-risk component since sensitive account information as well as financial transactions are processed here.

Currently Q&E maintains security of the IBS. So far, no controls have been documented by the vendor. As a result, SBI is taking steps in ensuring regulatory compliance by implementing and ISMS protecting this critical system.

The IBS consists of two separate components running on a Microsoft IIS Web Server.

The first component implements a user interface where users can login and view their account statements, view check images, make payments, etc. Since SBI is a community bank verification of the customers' identity is done at the branch. A customer with an existing account will have to visit one of the branch offices and fill out a form requesting access to the IBS. Upon verification of his photo ID and signature a branch employee assigns a user name and a temporary password. Additionally, an email address provided by the customer is included on the application. The original application is stored at the branch office for a month after which it is destroyed. A copy of the original application is sent (as interoffice memo) to the administrator of the IBS. The customer is given another copy of the application and is reminded to change the default password upon first logon.

The second component can be used only by the administrator of the Internet Banking System. Access to these administrative functions is restricted by IP-addresses (the system can only be used from SBI's internal network) and a password which is created during installation of the IBS. The administrator password is unknown to the vendor (Q&E).

The IBS administrator performs a number of daily maintenance tasks some of which are performed at the beginning of each business day and later at 4pm.

The tasks performed at the beginning of each business day include:

- Create a list of unusual transaction for review
    - A list of transactions with and amount of more than $5000 is created and sent to account representatives for review
    - A list of accounts originating or receive more than 5 transactions is created and sent to account representatives for review
- Create a list of users active during the past 24 hours
    - A list of users that logged on during the past 24 hours is created and archived in a daily log file. The log file contains account details as well as the users IP-address and is stored in a specially designed database on the internal network.

The tasks performed at 4pm each day include:

- Setup of new user accounts
  - The IBS administrator creates a new account and sends a confirmation email to the user
- Review of Web server log files
  - Web server log files are manually reviewed to potentially identify signs of abuse. Suspicious activity is forwarded to networking staff for further analysis

Once per week the IBS administrator creates a complete list of transactions originating from the IBS. At the same time the AS/400 administrators create a list of all IBS transactions logged on the core banking system.
The compliance officer compares the number of transaction to detect possible deviations, which might indicate that the IBS has been compromised.

Even thought there are a number of controls in place to ensure fraudulent transactions are detected, there are no mechanisms in place to ensure the IBS system has not been compromised. The vendor of the IBS (Q&E) is responsible for applying security patches to the system and also rolls out new versions of their own software, which may include new vulnerabilities. In case an existing vulnerability on the system is exploited by an external attacker, SBI may suffer a number of significant consequences including:

- Defacement of the Web site
- Theft of user logon credentials
- Access to administrator passwords
- Potential access to internal systems
- Denial of Service (DoS) attacks on the IBS

Event though part of the maintenance on the IBS is handled by an outside vendor, SBI is required by law to protect this critical asset. The objective of fulfilling regulatory requirements has led to the decision of implementing an ISMS that addresses the threats mentioned above.

Staffing

SBI hash about 200 employees with an IT staff of approximately 10 people. Two senior software engineers share the responsibility of maintaining user accounts, reviewing log files and limited software development on the AS/400 programs at RBP. These software engineers also implement day to day automation tasks and are available to provide expertise in the areas of access control, change management and monitoring.

Two network administrators (J. Miller and P. Welsh) are currently in charge of maintaining a secure network infrastructure. Their daily tasks include the review of log files, monitoring of security bulletins, research of security patches, etc. SBI has recently implemented an IDS (Intrusion Detection System) network appliance which is monitored at a NOC (Network Operations Center) which is staffed 24x7. SBI has conducted internal and external tests penetration tests on its network and found that intrusion analysts at the NOC react to alerts in an adequate manner and typically will contact SBI within 10-20 minutes. Both network administrators carry pagers and have remote access to SBI's network. Their work schedules are overlapping in a way that enables SBI to achieve near 24x7 coverage for responding to security alerts.

Throughout the organization SBI has three help-desk employees which respond to user questions, may to a certain extent troubleshoot network problems and are trained to recognize security violations and initiate incident response. One of the help-desk employees also conducts security awareness training twice per year and provides new employee introduction where a recent hire is made familiar with security responsibilities and SBI's information security policy. The help-desk employees also serve as administrators of the IBS and responsibilities are rotated weekly resulting in weekly change of the administrator password and respective audit trails.

The compliance officer (Peter Smith) is the liaison between regulators, such as the FDIC, third party vendors and consulting companies providing IT related services to SBI. He is responsible for scheduling regular security audits, providing appropriate funding and expertise and overseeing remediation efforts when audits discover security vulnerabilities.

The director of HR is responsible for issuing building passes and submitting requests to setup network accounts. All physical and network access is restricted for a certain period of time. Physical access is further controlled across different areas of the main bank building. Network access is based upon an employee's roles and responsibilities. Regular audit logs are generated to verify that old accounts have been deleted and potentially detect suspicious activity.

A few additional employees with limited computer skills are responsible for system backups, installation of new computers and various other maintenance tasks.

SBI's branch offices do not have dedicated IT staff. Maintenance which requires physical presence at the branch locations is performed by employees

commuting to these locations.

Security Posture

Due to regular security awareness training and introduction to security responsibilities at the point of hire, SBI has developed a strong security-focused mentality. Several members of SBI staff have been trained on information security issues, threats and management.

Approximately once per month, although not on an official schedule, security issues are discussed in a staff meeting and the compliance officer will make arrangements for the issues to be solved and/or report to the board. Besides a set of industry standard practices for information security management SBI has a large number of safeguards like intrusion detection, logging and monitoring, incident response plan and regular auditing in place. A basic set of information security policies is in place but outdated. The policies are scheduled to be reviewed and updated during a third party audit in the third quarter of 2005.

Since most of SBI's core services are outsourced or handled by third party systems, there are no overarching security principles. SBI relies on staff and consultants for keeping systems on their network but has, over the past five years, continued to increase their information security budget continuously. Understanding the need for information security management, the organization will be taken to the next level by adopting the plan-do-check-act philosophy as form of an ISO17799 pilot which later may be extended to larger portions of the enterprise. As pointed out during regulatory audits, SBI needs to strengthen the security of their third party systems, since these pose a high risk.

Plan-Do-Check-Act

ISO17799 defines the PDCA (Plan-Do-Check-Act) methodology for implementing and maintaining ISMS. The remainder of this document will address these four phases.

Phase I – Plan

With few IT resources carrying critical information and limited IT staff, SBI traditionally relied on information security policies and procedures to maintain their systems and regulatory compliance.

Some of the shortcomings identified with the existing system are:

- Policies and Procedures are static. Their effectiveness and compliance is not monitored. Furthermore, a recent audit showed that the policies are outdated.
- Existing policies are inadequate and do not reflect business objectives.
- No reporting structure is in place informing senior management of inadequacies.

SBI management understands that implementing an ISMS will address the above findings, improve security and also achieve the objectives set forward by GLBA.

A work paper detailing “Examination Procedures to Evaluate Compliance with the
Guidelines to Safeguard Customer Information (GLBA)” [1] evaluates achievement of these objectives by requiring auditors to perform some of the following tasks:

- Determine the involvement of the board
- Evaluate the risk assessment procedures
- Evaluate the adequacy of the program to manage and control risk
- Assess measures taken to oversee service providers
- Determine whether an effective process exists to adjust the program

All of these requirements are typically addressed within the scope of an ISMS so ISO17799 seems to be a good methodology for addressing GLBA

requirements.

High Level Security Policy

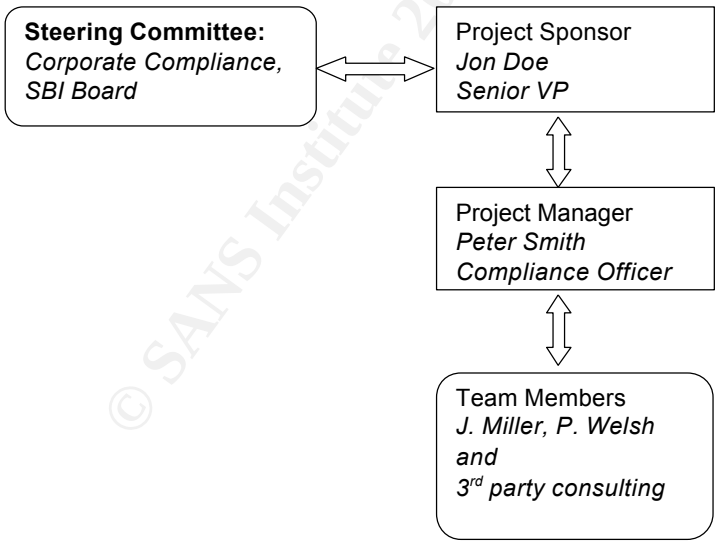
The following high-level security policy (HSLP) has been adopted by SBI management and is carried forward throughout this document. For the purpose of this limited ISMS it is to be applied to the Internet Banking System and GLBA requirements. This HSLP is also designed to support decision making and lower level policy development.

"SBI will practice strong information security and protect customer information as required by GLBA to minimize risks to the Internet Banking System".

ISO17799 – Project Team

SBI has recently performed a policy review and an internal risk assessment. However, these activities have been performed before SBI staff was trained in ISO17799.

The following group of people has been assigned to perform, delegate and implement the steps introduced by the ISO standard.



Team Member Roles and Responsibilities

Project Manager: Peter Smith

The project manager manages team structures, resources and reporting between the groups. Peter will facilitate work and is primarily responsible for executing and reporting on the status of the project. Planning documents are reviewed weekly by the team.

The project manager

- Is responsible for identifying the tasks required to implement the ISMS and assigning appropriate resources. When necessary resources cannot be found in-house he will identify necessary third parties jointly with the project sponsor.
- Is responsible for managing timelines associated with approved tasks
- Is responsible for third party management
- Provides expertise regarding regulatory compliance

Project Sponsor: John Doe

The project sponsor has overall responsibility for successful implementation of the ISMS. As such, Jon

- Is responsible for defining high-level objectives in cooperation with the steering committee
- Is responsible for funding of the project
- Is responsible for reporting progress to the board
- Serves as the main communication channel between the project team and executive management

Team Members

The team members are drawn from different areas within SBI. In later phases J. Miller and P. Welsh may be replaced by other employees or augmented by third party consulting firms.

- Document tasks, status and progress
- Participate in weekly status meetings
- Develop policies and procedures
- Perform research and identify controls to support the ISMS

Team Dynamics

The team does not currently have any fulltime security resources. All members on the team have additional responsibilities. Though this may seem to be a disadvantage it helps spread a security conscious culture throughout the organization since the team was selected from employees that showed strong interest and initiative with regards to information security.

The three main members, Peter Smith, J. Miller and P. Welsh have been with SBI for many years and have jointly built the existing security infrastructure, policies and processes. Jon Doe, the project sponsor, has supported the team over the past five years and is a strong evangelist of this initiative.

During a normal workday J. Miller and P. Welsh will share most of their tasks with each other. Since each of them may have to commute to a branch office it is vital for SBI operations that these two employees function as a team. During a normal workday, without special projects scheduled, one of them will prepare a daily digest of activities and email it to John Doe. Usually once per week, an official status meeting is conducted where issues are prioritized and resources as well as deadlines are assigned.
Peter Smith will be informed by one of the team members should issues arise that may affect his role as compliance officer. Since the successful implementation of the ISMS is very important to SBI, Peter Smith will attend all weekly meetings during the Plan phase of the implementation.
Besides these meetings all team members, including the project sponsor, will follow the meeting schedule described later in the document. Should delays or cancellations occur John Doe will document these exceptions and will be held responsible by the board for timely completion of the project, before an upcoming audit during the third quarter of 2005.

ISMS Scope

As described above the objective of this ISMS is two-pronged. One goal is to strengthen security on the Internet banking part of SBI's business and the other goal is to implement management procedures that satisfy GLBA requirements.

This ISMS will meet both goals by:

- Protecting the IT infrastructure elements of the network segment hosting Q&E's Internet Banking System
- Implementing security management policies, procedures and controls that support GLBA requirements
- Implementing reporting and checking mechanisms that ensure the continuous improvement of the ISMS

Timelines

SBI's board and management have committed to implementing an ISMS as defined in the scope section within a timeframe of six months. The following section describes the resources involved, as well as a schedule that has been reviewed and acknowledged by all members of the project team.

A second phase where the scope of the existing ISMS will be expanded to include other SBI assets is estimated to begin in the third quarter of 2005.

Current Initiatives

The following initiatives are currently being performed by project team members. Should a conflict of interest arise the program manager needs to be informed in a timely manner.

- Corporate Compliance Functions: Current risk analysis efforts (due in February 2005) efforts and policies in development (due in March 2005) will be used as input into the ISMS initiatives.
- A number of operating system upgrades and application roll-outs may impact implementation of monitoring solutions. P. Welsh will coordinate efforts and report on progress.

Scheduled Tasks and Milestones

Date/Time	Duration	Description	Type	Resources
3/2/05, 9am-5pm	All day	Project definition	Planning meeting	J. Doe, P. Smith, J. Miller, P. Welsh
3/9/05, 10am	2 hours	Task and timeline approval	Planning meeting	J. Doe, P. Smith, J. Miller
3/16/05, 10am	1 hour	Program Kickoff	Planning meeting	Steering committee, J. Doe, P. Smith,
4/1/05	n/a	Policy requirements	Milestone	J. Miller, P. Welsh
4/5/05	n/a	Asset identification	Milestone	P. Smith, J. Miller, P. Welsh
4/7/05, 1pm-5pm	4 hours	Risk analysis session	Work session	P. Smith, J. Miller, P. Welsh, 3rd party
4/14/05, 1pm-5pm	4 hours	Risk analysis session	Work session	P. Smith, J. Miller, P. Welsh, 3rd party
4/15/05	n/a	Suggested controls	Milestone	J. Miller, P. Welsh, 3rd party
5/3/05	n/a	Requirement for policies	Milestone	J. Miller, P. Welsh, 3rd party
5/17/05, 1pm-5pm	4 hours	Policy hand-off	Work session	P. Smith, J. Miller, 3rd party
5/24/05	n/a	Delivery of draft policies	Milestone	3rd party

Asset Identification

Although the ISMS will protect the IBS from a number of threats, the main focus is the safeguarding of customer information. The information flows in the below have been used to identify assets which need to be included in the risk analysis process. Furthermore the project team conducted a session where a perceived dollar amount was assigned to the asset.

Assets exceeding a perceived value of $10,000 have been considered for the scope of the ISMS:

- Internet Banking System (the server)
  - Nominated Owner: J. Miller
  - Perceived value: $200,000
  - Scope: In scope
- Access to administrative interface
  - Nominated Owner: J. Miller
  - Perceived value: $50,000
  - Scope: In scope
- Firewall
  - Nominated Owner: P. Welsh
  - Perceived value: $20,000
  - Scope: Out of scope due to strong controls in place
- Security audit results
  - Nominated Owner: J. Miller
  - Perceived value: $10,000
  - Scope: Out of scope due to limited impact
- AS/400
  - Nominated Owner: J. Miller
  - Perceived value: $500,000
  - Scope: Out of scope for ***first*** implementation. Likely to be revised due to perceived value.
- Customer lists
  - Nominated Owner: Peter Smith
  - Perceived value: $500,000
  - Scope: Out of scope for first implementation. Likely to be revised due to perceived value.

Information Flows

This section lists a number of flows of information that have been identified.

1) Maintenance by IBS Manager
2) IBS User checking account
3) IBS User performing transaction
4) Data Backup
5) Security Audit by third party

Maintenance

Maintenance is performed by a manager assigned to the Internet Banking System. The manager performs tasks like adding/deleting users, changing passwords, performing backups etc.

During the maintenance process, the manager may have to access the RBP's core processing system to access/verify user credentials.

This verification is a manual process. All notes or temporary files created during this process must be destroyed after completing the task.

A log file listing only non-sensitive information is kept by the manager and archived for review during the regular audit process.

User Checking Account

When a user logs on to the Internet Banking System, a gateway to the core processing system is used to retrieve current account information. This information is temporarily stored on the Internet Banking System. After the user logs off these temporary files are deleted. However the temporary files are not wiped clear before deletion.

User Performing Transaction

When a user performs a banking transaction, the transaction is not being processed in real time. With the current system, transactions are stored on the Internet Banking System and transferred through the gateway to the core processing system each day at midnight (batch processing).

The current format for these data does not provide for encryption or integrity checking. It is possible to delete these files or modify parts of a transaction while the files are sitting on the IBS waiting to be processed.

Data Backup

During the regular system backup of the Internet Banking System, sensitive client information is stored. These backups are stored separately from normal system backups since regulatory requirements require special care in safeguarding customer information.

Security Audit

Security audits are performed on an on-going basis. The results of a security audit are stored on a dedicated server in encrypted form. The data on the systems performing the audit will be wiped clean after copying the results to the encrypted storage.

Third parties performing vulnerability scanning and security audits must document their data destruction procedures and sign an NDA.

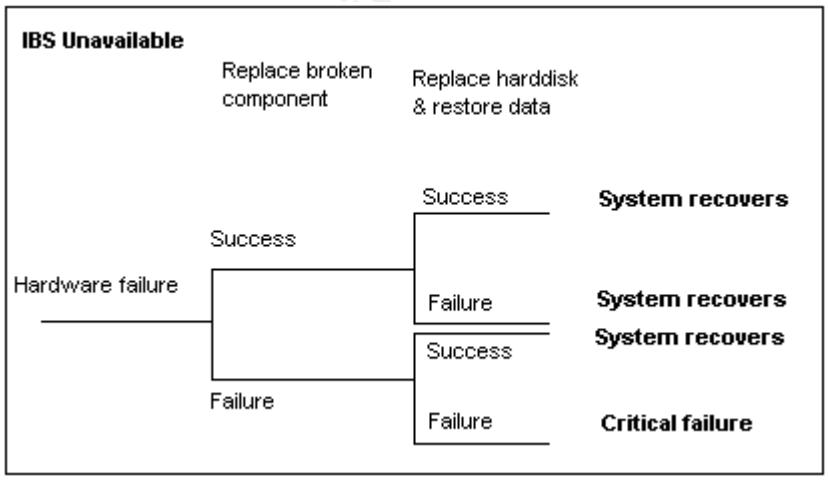
Risk Analysis Approach

Since the bank regularly performs risk analysis on the business side, the compliance department has a risk analysis specialist on staff. After consulting with the specialist the SBI team members decided that a qualitative risk analysis will work best for the Internet Banking System. The reasons for this decision were:

- After going through several rounds of exercises the team had a short list of high priority risks/items
- The team believes that the qualitative approach is adequate for the threats identified and
- A qualitative approach will yield the quickest result (management is still somewhat skeptical regarding the Risk Analysis). The team will consider a different methodology during phase two, when the scope of the ISMS is expanded

Consequence Cause Analysis

A pilot initiative is currently being conducted to further identify risks using CCA (Consequence Cause Analysis). Future iterations of these models will be folded into the ISMS. Since no team members are currently trained appropriately, an outside consultant will be used to assist with the risk analysis. The following fault tree has been generated by the project team to give guidance for the examination of additional scenarios:



The risk matrix below shows threat items which that have been identified during the risk analysis phase. All the items listed have significant or severe damages

should the threat be realized.

Risk Matrix

This section lists risks that have been identified during the qualitative risk analysis phase. The risks are related either the Internet Banking System (IBS) or compliance requirements defined by GLBA.

Threat	Vulnerability	Likelihood	Risk Level	Control	Mitigated risk level
IBS unavailable	System failure	Medium	High	BS7799, 7.2.2 Power supplies & 7.2.4 Equipment Maintenance	Medium
	Software update failure	Medium	High	BS7799, 10.5.1 Change Control Procedures	Medium
	Denial of Service of existing configuration	Medium	High	BS7799, 8.2.1 Capacity Planning	Medium
IBS Web site defaced	Missing patch/software update	Medium	High	BS7799, 8.3.1 Control against malicious software	Medium
Confidential data from IBS leaked to outside attacker	Missing patch/software update	Medium	High	BS7799, 8.3.1 Control against malicious software & 10.5.1 Change Control procedures	Medium
Unauthorized access causes publicity damage	Missing patch/software update	Medium	High	BS7799, 8.3.1 Control against malicious software & 10.5.1 Change Control procedures	Low
	Bad user passwords	High	High	BS7799, 6.2.1 Information security education and training	Medium
	Social engineering of SBI employees	Low	High	BS7799, 6.2.1 Information security education and training and 6.1.1 Including security in job responsibilities	Low

Unauthorized user initiates transaction	Missing patch/software update	Low	High	BS7799, 8.3.1 Control against malicious software & 10.5.1 Change Control procedures	Low
System Intrusion goes unnoticed	Log files are not reviewed	Medium	High	BS7799, 6.3.1 Reporting Security Incidents & 8.1.3 Incident Management Procedures	Medium
Not meeting regulatory requirements	Not aware of requirements	High	High	BS7799, 12.1.1 Identification of applicable legislation	Low
	Not enough resources	Low	High	BS7799, 12.2.1 Compliance with Security Policy	Low
	No support from management	Low	High	BS7799, 12.2.1 Compliance with Security Policy & 12.3.1 System audit Controls	Low

Selected Controls

As shown in the matrix above most identified risks receive a significant reduction on risk level after an appropriate control is applied. To further reduce the risk levels associated with some of the remaining threats, management decided to implement additional controls for:

- IBS Web site defaced
- Unauthorized user initiates transaction
- Not meeting regulatory requirements

Risk Management

Required Policies

This section describes the additional policies needed to support the above controls.

Incident Response Policy

Purpose: The existing incident response policy will be expanded to include a section on monitoring a potential Web site defacement.

Audience: This document is intended for the information security/incident response team.

Areas of Standard: The policy addresses section 8.1.3 'Incident Management Procedures' of the ISO17799 standard.

Implementation Detail: SBI will implement file integrity checking software to detect modifications to publicly accessible Web pages. The software creates MD5 or similar checksums on each critical file defined in a database. An alert is sent to the information security team when a critical file is modified. The assigned incident handler (J. Miller or P. Welsh) will conduct a brief investigation of the incident (less than 15 minutes) and restore the modified files from a backup. Additionally the incident will be investigated and escalated until the vulnerability is fixed. Should the team not be able to remedy the situation within 24 hours, John Doe may elect to take the system offline until a solution is found.

Application Access Policy

Purpose: The existing application access policy for clients will be expanded to include a section on logging user access.

Audience: This document is intended for the information security team and the audit team.

Areas of Standard: The policy addresses section 9.6 ‘Application Access Control and section 9.7.2 ‘Monitoring System Use’ of the ISO17799 standard.

Implementation Detail: SBI will log user access and cross-reference with IP-addresses. This information may be critical for identifying system abuse and will aid with prosecution. P. Welsh will generate a monthly audit on these files and generate statistics on the user/IP pairs. If a single IP is found to log into more than 5 different user accounts, the users will be investigated. Should abuse be detected the incident is escalated, users are contacted, the accounts are blocked and the IP-address is restricted on the firewall. Similarly, if there are more than 10 failed login attempts from a single IP within 24 hours an incident investigation is launched and potentially escalated.

Internal Audit Policy

Purpose: The purpose of this policy is to give the internal auditor guidance on how to evaluate existing policies for ensuring regulatory compliance.

Audience: This document is intended for the internal audit team.

Areas of Standard: The policy addresses section 12.1 ‘Compliance with Legal Requirements’ of the ISO17799 standard.

Implementation Detail: After each review the internal auditor will file a compliance assessment report. The compliance assessment report is reviewed by Peter Smith who develops a summary and forwards to the project team within on week of receiving the initial report. After team has had a chance to review the summary (or a maximum of two weeks) a meeting is conducted to prioritize items and identify remedies. The remedies are approved by John Doe and timelines are set for implementation. I case the management team decides to accept the shortcoming are report explaining the reasoning is created and forwarded to the board.

ISMS Management structure

After successful implementation Peter Smith (Compliance Officer), will conduct monthly meetings to monitor the progress of the ISO17799 program at SBI. The meeting is attended by J. Miller and P. Welsh. If 3rd parties are invited to the meeting an NDA (non-disclosure agreement) must be signed by the 3rd party. Numerous other meetings will be part of the ISMS and are described in their respective sections of the document.

The goal of this meeting mentioned above is to report progress to the steering committee and identify any issues with the implementation of the program.

The team members (Miller and Welsh) may at any given point in time report issues or request additional to/from the project sponsor John Doe.

Since GLBA compliance is one of the main goals of this ISMS, we do not need to define a committee to oversee management of the ISMS. Regular reviews, project management and reporting to top level management are an inherent part of GLBA. The main reason for this decision is a constraint in resources. After the first three phases Plan-Do-Check of the PDCA cycle are completed, selected members of the team and steering committee will be appointed to a new a committee for overseeing the ISMS.

Phase II – Do

This section describes the action items required to implement the ISMS as describe in the section above.

Implementation Plan

Problem: IBS, Limited Security Management

The Internet Banking Systemic implemented by the vendor (Q&E) provides a limited set of controls for implementing strong security. Software updates and operating system configuration are handled by the vendor. However, the vendor does not provide any intrusion detection or even auditing/monitoring functions for this critical asset.

Action Plan: Implement Additional Logging and Monitoring

To improve security of the IBS and satisfy the intrusion detection, logging and monitoring requirements SBI will implement a set of security technologies and security management procedures.

Action Steps

1. Obtain vendor permission to increase security of the system by installing additional software and implementing patch management procedures
2. Obtain vendor documentation on operating system security configuration
3. Identify, train and assign staff for incident response
4. Define incident response and escalation procedure
5. Select file integrity checking software
6. Implement file integrity checker and setup alerting
7. Identify requirements for customer login/IP-address mapping
8. Design and implement system defined under ‘7’.
9. Identify requirements for wiping temporary files
10. Design and implement system defined under ‘9’.
11. Design a system that will use the file integrity checker to mitigate the risk of transaction files being modified before batch submission (see information flows section for details)

`

Problem: IBS, Missing Abuse Detection

The Internet Banking Systemic is limited to preventative controls. Detective controls to alert to potential system abuse, which may in turn lead to fraudulent transactions are not in place.

Action Plan: Implement Additional Logging and Auditing

To be able to detect system abuse (or attempted system abuse) SBI will implement a system that will track successful and unsuccessful logon attempts. A monthly audit will detect suspicious user patterns and lead to incident follow-up and escalation.

Action Steps

1. Design software to extract logons and logon attempts from Web server log files. The system will store its information on the Web server.
2. Design a system that duplicates the information collected in '1' on a secure internal server in case the IBS gets compromised and log files are erased.
3. Implement the systems designed in '1' and '2'.
4. Design analysis procedure and thresholds for incident investigation
5. Define incident response and escalation procedure
6. Define reporting structure
7. Train two employees on usage of the system
8. Assign responsibilities and audit schedule

Problem: Missing Reporting Structure

Though information security policies, procedures and controls have been developed to protect customer information other GLBA requirements like reporting and regular reviews have not been developed.

Action Plan: Create Templates and Timelines

The requirements for reporting and regular reviews as described in GLBA are inherent to and ISO17799 ISMS. The Plan-Do-Check-Act cycle will also satisfy the regulatory compliance requirement.
However, to fully implement the ISMS, some additional policies need to be developed, additional policies need to be amended, controls need to put in place and staff needs to be trained and assigned.

Action Steps

1. Setup schedule for compliance meetings
2. Setup training schedule for J. Miller and P. Welsh
3. Develop standardized templates for reporting
4. Define reporting schedule and obtain commitment to deadlines
5. Perform gap analysis on existing policies
6. Review gap analysis created in '5', prioritize and develop additional policies
7. Amend the following policies to reflect requirements:
    - Incident Response Policy
    - Application Access Policy
    - Internal Audit Policy
8. Research current legal and regulatory requirements
9. Provide regular reports to steering committee

Statements of Applicability

ISO17799, Section 10.5.1 – Change Control Procedures

Description: This control minimizes the risk that vulnerabilities are introduced into a system. Change control also documents the specifics (who, what, when and why) of a configuration change or software update.

Reason for implementing: Since the IBS vendor (Q&E) regularly updates software and also installs operating system patches, we need change control procedures in place. Proper change control will result in accountability for bugs introduced to the system as well as for missing security patches which should have been installed.

Implementation: Control will be implemented

Implementation method: This control will be implemented by

- Writing change control procedures that are mandatory for Q&E as well as SBI
- Working with Q&E to understand and accept procedures
- Review specifics of each change control request

ISO17799, Section 12.1.1 – Identification of Applicable Legislation

Description: This control minimizes liability.

Reason for implementing: Since one of the two main goals for implementing and ISO17799 ISMS was achieving GLBA compliance other legislation an regulatory requirements is also of concern.

Implementation: Control will be implemented

Implementation method: This control will be implemented by

- Assigning and training staff
- Performing yearly internal audits and reviews
- Regularly contacting outside consulting companies to review policies
- Identifying staff for attending industry conferences

ISO17799, Section 9.5.4 – Password Management System

Description: A password management system increases password strength by enforcing string passwords, forcing users to change passwords on a regular basis, etc.

Reason for implementing: Will not be implemented.

Implementation: Control will not be implemented

Justification of Non-Applicability: Though weak user passwords have been identified as a high risk to the IBS, SBI decided to mitigate the risks associated with this by creating user awareness, regular password audits and procedures for monitoring system abuse.

Phase III – Check

Even though the scope of this ISMS is limited to the Internet Banking System and regulatory compliance, a large number of audit sections from the BS7799 checklist are applicable. When increasing the scope of the ISMS in a later phase this section needs to be reviewed and amended.

The following audit checklist focuses on the audit questions that most closely relate to the main goals (security for the IBS and GLBA compliance).

Audit Checklist

`

Audit Type	BS7799 – Audit Checklist Section	Reason for Audit	Action Items	Frequency
Information Security Policy	1.1.1	To ensure the policy is up to date and the correct messages are communicated to all employees	• Review policy document [1)] • Interview/test users [2)]	Yearly
Information Security Policy Review and Evaluation	1.1.2	To verify the principles of the HSLP are reflected accurately in the lower level policies	• Review third party audit reports [3)] • Review incident reports [4)] • Interview users [2)]	Yearly
Information Security Education and Training	4.2.1	To ensure managements vision of security is understood throughout the entire organization	• Review policies regarding information security training [1)] • Review training schedule [5)] • Interview or poll users regarding effectiveness of the training program [2)] • Consider an information security quiz to test effectiveness of the training program [2)]	Yearly

Incident Management Procedures	6.1.3	To ensure the policies and procedures are effective and adequate	• Review incident management procedures [6)] • Review incident reports [7)] • Consider testing of procedures using a 'mock incident' [8)]	Yearly
Information Handling Procedures	6.6.3	GLBA requires that customer information is protected	• Review data handling policies and procedures [9)] • Review data destruction policies and procedures [9)] • Interview management regarding data classification [10)]	Yearly
Review of User Access Rights	7.2.4	To ensure that critical systems, especially the IBS, are properly secured.	• Review third party audit reports [3)] • Review access rights documentation [11)]	Yearly
Monitoring System Use	7.7.2	To determine whether there are adequate procedures to detect system abuse	• Review incident reports [7)] • Review monitoring policies and procedures [12)] • Interview IS management regarding compliance with policies and procedures [12)]	Quarterly
Change Control Procedures	8.5.1	To ensure that the right processes are in place to secure critical systems.	• Review change control procedures [9)] • Review change control log [9)]	Semi-annually

Technical Review of Operating System Changes	8.5.2	To ensure that critical systems, especially the IBS, are properly secured.	• Perform vulnerability scan [13)] • Review third party audit reports [3)] • Review patch management procedures [14)]	Semi-annually
Identification of Applicable Legislation	10.1.1	Since one of the main goals of the ISMS is regulatory compliance SBI needs to assign the necessary resources to compliance issues	• Review third party audit reports [15)] • Review action items derived from previous audits [9)] • Ask if staff has enough resources, training, time, support, etc [16)]	Yearly
Data Protection and Privacy of Personal Information	10.1.4	The main focus of GLBA is on protection of personal information	• Obtain list of personal information in use at SBI [17)] • Obtain policy documents [17)] • Review documentation [17)] • Review controls or conduct management interview regarding controls [17)]	Yearly

Compliance with Security Policy	10.2.1	All areas of SBI are required to regularly review security policy. Verifying Compliance with the policy will ensure the policies are adequate and effective	• Obtain policy documents [18)] • Obtain incident reports [18)] • Review documentation [18)] • Conduct interviews with management [18)] • Conduct interviews (random sample) with a number of employees [2)] • Generate compliance report [19)]	Yearly

Detailed Checklist Procedures

1. Peter Smith and J. Miller will both review the policy document(s) and forward improvement suggestions to the project team. The team will prioritize improvements.
2. An outside consulting company will be used to conduct user interviews and summarize responses.
3. Peter Smith and J. Miller will review audit reports and summarize findings. The project team will prioritize improvements.
4. J. Miller and P. Welsh will summarize events. The project team will develop a list of potential policy improvements.
5. J. Miller will review the training schedule. John Doe will adjust according to budget.
6. Either J. Miller or P. Welsh will review management procedures and develop a develop a testing plan
7. The person ***not*** reviewing under [6)] will review incident reports and summarize for team review. The project team will develop a list of potential policy improvements.
8. The person developing the testing plan under [6)] will review incident reports create 'mock incidents' and document responses and present to the project team which will develop a potential list of improvements for the incident response plan.
9. Peter Smith will collect documentation and grade each relevant section. The team will prioritize graded items and develop a list of improvements.
10. J. Miller and P. Welsh will develop a list of information assets. John Doe will present the list to the board for prioritization. Upon prioritization the team may implement additional policies and/or procedures for data handling.
11. P. Smith and J. Miller will review documentation and document changes in requirements. The project team will develop a list of potential policy improvements or additional procedures.
12. Peter Smith will review monitoring procedures and interview IS management regarding compliance and effectiveness of existing procedures. He will summarize shortcomings and verify changed regulatory requirements. P. Smith and J. Miller will develop a list of potential improvements. The team will prioritize improvements.
13. J. Miller will perform a vulnerability scan using Eeye's Retina Security Scanner. After removing false positives he will create a remediation report and the team will assign resources and deadlines for remediation.
14. P. Welsh will review patch management procedures and summarize shortcomings. The team will develop and prioritize improvements.

15. Peter Smith will review audit reports, identify applicable legislation and potential shortcomings. John Doe will summarize and present to the board. The boards will prioritize and the team will jointly develop additional policies and controls.
16. Peter Smith will interview IS staff regarding training, resources and effectiveness and summarize for John Doe. Upon review by the team John Doe will present to the board.
17. Peter Smith will collect documentation, conduct interviews and review relevant policy documents and grade each relevant section. J. Miller and P. Welsh will review existing controls and prioritize graded items. The team will jointly develop a list of improvements.
18. Peter Smith and John Doe will collect documentation, conduct interviews and review relevant policy documents and grade each relevant section. The team will jointly develop a list of potential improvements. J. Miller and P. Welsh will prioritize and the team will develop a plan for implementing improvements. John Doe will document improvements which will not be implemented during this round and report to the board.
19. Peter Smith will create a compliance report (developed from the findings in [18)] and present to the board and file for presentation to auditors from a regulatory agency.

Phase IV – Act

The ISMS currently in development defines a large number of audit steps (listed in the previous section) that are designed to lead to continuous improvement of the ISMS.

The following table gives brief recommendations as to what steps SBI might take when an audit result was not satisfactory.

Audit Results and Action Items

`

Audit Type	BS7799 Section	Audit finding	Action Items
Information Security Policy	1.1.1	• Policies missing • Users knowledge of procedures not satisfactory	• Update policy document [1)] • Improve training program [2)]
Information Security Policy Review and Evaluation	1.1.2	• Policies are inefficient or inadequate	• Perform risk analysis, review of HSLP, controls review. [3)] • Update policies and adjust controls [4)]
Information Security Education and Training	4.2.1	• Users fail to answer basic security questions correctly.	• Improve training program [2)]
Incident Management Procedures	6.1.3	• Response time/quality, etc. inadequate	• Improve procedures (improvements have been developed in the 'check section) [5)]
Information Handling Procedures	6.6.3	• Procedures are inadequate	• Perform risk analysis [3)] • Improve procedures (improvements have been developed in the 'check section) [5)]

Review of User Access Rights	7.2.4	• Access rights are inadequate	• Implement stronger access control [5)] • Perform asset risk analysis [3)]
Monitoring System Use	7.7.2	• System is being abused • Monitoring procedures inadequate	• Implement policies or controls to improve situation (improvements have been developed in the 'check section) [5)] • Implement additional controls (improvements have been developed in the 'check section) [5)]
Change Control Procedures	8.5.1	• Procedures are inadequate or a hindrance to operations	• Improve procedures or change policies (improvements have been developed in the 'check section) [1) or 5)]
Technical Review of Operating System Changes	8.5.2	• System has high-risk vulnerabilities	• Update patch management program [6)] • Consider hiring a consulting firm [7)]
Identification of Applicable Legislation	10.1.1	• Applicable legislation is not known or not taken into consideration	• Inform board [8)] • Train staff [9)] • Consider hiring a consulting firm [10)]
Data Protection and Privacy of Personal Information	10.1.4	• Customer data is not adequately protected	• Implement additional controls (improvements have been developed in the 'check section) [11)] • Perform risk analysis [3)]
Compliance with Security Policy	10.2.1	• Parts of the organization are not compliant`	• Perform risk analysis [3)] • Consider updating policy or implementing additional controls. [11)] • Train users [2)]

Note: These are just examples for improving the ISMS. SBI may choose to address the findings with different action items as long as the rational is documented.

Responsibilities for Action Items

1. Peter Smith will oversee and delegate improvements to policy document. If necessary external consultants will be used to incorporate changes.
2. John Doe will evaluate training requirements, present to the board and request additional funding if necessary.
3. J. Miller or the newly trained resource will lead the risk analysis sessions conducted attended by John Doe, Peter Smith, J. Miller and P. Welsh
4. Peter Smith will oversee and delegate improvements to policy document. J. Miller and P. Welsh will implement new controls.
5. J. Miller and P. Welsh will document and implement new procedures.
6. J. Miller and P. Welsh will evaluate best practices and patch management solutions. If additional budget is required for implementation, John Doe will report to the board.
7. J. Miller and P. Welsh will evaluate best practices. If outside resources are required for fixing vulnerabilities, John Doe will request funding from the board.
8. The board is informed of failing audit and will decide whether outside expertise or training will be used to remedy the situation.
9. John Doe will request funding from the board and train selected personnel.
10. John Doe and Peter Smith will select a consulting company to provide additional expertise. Selection of expertise is based on the audit results.
11. Peter Smith will oversee improvements. J. Miller and P. Welsh will implement new controls.
12. If policies need to be updated Peter Smith will oversee and delegate improvements to policy documents. If necessary external consultants will be used to incorporate changes. If additional controls are necessary will oversee improvements. J. Miller and P. Welsh will implement new controls.

Additional Action Items

The following additional items will be addressed before completion of the first full PDCA cycle.

- John Doe will schedule and lead the formation a formal ISMS committee after the first three phases (Plan-Do-Check) of the PDCA cycle are completed. A new schedule of tasks and milestones will be developed and responsibilities will be reassigned during weekly half-day sessions.
- John Doe will summarize accomplishments and improvements after each 'Act' cycle and communicate to the board after review by the committee.
- Formal risk analysis will be introduced and led by a newly trained resource

Regardless of the audit findings above, SBI will address the following items during the next 'Act' cycle of the PDCA system:

- Extend the scope of the ISMS to included additional information assets
- Perform a more thorough risk analysis of the entire organization
- Establish roles and responsibilities for ISMS management and add to job descriptions
- Request feedback and continued support from management
- Adjust audit findings to satisfy requirements of upcoming audits by FDIC, FFIEC (Federal Financial Institutions Examination Council) or OCC
- Consider integrating results from FDIC, FFIEC or OCC audit into ISMS

References

[1] SANS G17799 Course Material - Volumes 11.1-11.6, SANS Institute 2004

[2] Information Security Management- BS 7799.2:2002 - Audit Check List, Val Thiagarajan & Algis Kibirkstis, with the permission of BSI under license number 2003DH0251

[3] FFIEC - GLBA Section 501(b) Examination Procedures, FFIEC, 2001

[4] Stan Poszywak, OCC - GLBA Section 501(b) Examination Procedures, OCC, 2001