Global Information Assurance Certification Paper

GSEC Exam – Option 1
Karen Nelson
Tyson's Corner, Dec. 8-13, 2002

Security Assessment Guidelines for Financial Institutions

Summary

This paper will discuss the following five information security assessment processes, identified by the Federal Financial Institutions Examination Council (FFIEC)[1] and other financial regulators, as core components of a financial institution information security program, especially in fulfilling Gramm-Leach-Bliley Act (GLBA), and relevant with other, similar requirements:

- Identify the risks that may threaten customer information [and the earnings and capital capabilities of the institution],
- Develop a written plan containing policies and procedures to manage and control these risks;
- Implement security controls;
- Test the security to assure that significant controls are effective and performing as intended;
- Monitor and update – "Adjust the plan on a continuing basis to account for changes in technology, the sensitivity of customer information, and internal or external threats to information security."[2]

The paper contains an introduction and two sections. The first section will discuss how to set up a risk assessment and security evaluation program suitable for Financial Institutions. The discussion will include development of the standards, methods, processes and procedures identified for risk assessment, security planning and reviews. The second section will briefly illustrate these concepts by evaluating two fictional MS-SQL Server applications. One application will contain mission critical business data for internal use only and available only on the "trusted" network. The other MS-SQL application will be a Web-based Internet site run by a Service Provider. The methodology discussed can be included during systems development and used to gain approval of review tools and techniques after the move into production.

Introduction

Financial institutions face challenges relative to preserving the safety and soundness of the institution and its ability to manage earnings and capital. New technologies require increased diligence by financial intuitions.

The FBI, in its 2001 report "Financial Institution Fraud and Failure Report," says Financial Institution Fraud (FIF) is a Tier 1 priority in its strategic plan and identifies bank failures, identify theft, check fraud, counterfeit negotiable instruments, check kiting, mortgage and loan fraud as its major areas of investigation and an increasing

importance in its investigations related to emerging technologies and computer-related banking. The FBI reports that throughout the 1980's and early 1990's most of the fraud was a result of abuse by insiders. Today, the dominant schemes result from outsiders. "The pervasiveness of check fraud and counterfeit negotiable instrument schemes, technological advances, as well as the availability of personal information through information networks, has fueled the growth in external fraud."[3]

In addition to direct acts of fraud and abuse, financial institutions often become the instruments of money launders and illegal charitable contributions to terrorist.[4] The International Monetary Fund estimates that money laundering could be anywhere from 2-5% of the world's gross domestic product and has been called "the world's second largest underground economy." Both US and international organizations have placed a burden on financial institutions to detect and deter money laundering and the financing of terrorists. In the U.S., this is accomplished by using software to implement requirements of Section 314 of the Patriot Act and the Office of Foreign Assets Control (OFAC), Compliance Programs Division.

When banks fail to provide adequate control over information technology, they can expect to suffer operational damages from mass attacks launched against the Internet and the nation's critical infrastructure. In January 26, 2003, a "virus-like," worm attack against MS-SQL Server 2000 slowed Internet traffic world-wide and caused technical problems that brought down 13,000 ATM machines of the Bank of American and at Canadian Imperial Bank of Commerce. While these types of vulnerabilities often capture the negative attention of the public, they represent only a small portion of the business risks financial institutions must control.

The Office of the Comptroller of the Currency (OCC) has identified four of the nine categories in its risk framework to which technology-related products, services, delivery channels, and processes are most frequently exposed:

1. Transaction risks – the risks to earnings or capital arising from problems with service or product delivery, for example poorly configured or incompatible internal and external systems and processes.
2. Strategic risks – the risks to earnings or capital arising from adverse business decisions or improper implementation of those decisions.
3. Reputation – the risk to earnings or capital arising from negative public opinion.
4. Compliance – the risk to earnings or capital arising from violations or, non-compliance with prescribed practices or ethical standards.[5] Failure to meet regulatory guidelines can result in severe penalties for financial institutions.

More recently the Office of Thrift Supervision (OTS), has grouped the technology risks faced by financial institutions in three categories:

1. Information Integrity risks – information must be available, accurate, complete, valid and secure.
2. Business continuity risks – the institution's ability to adequately prepare and execute its responsibilities during a disaster.

3. Vendor management risks – the risk that the service provider will not perform the contract terms and conditions as specified causing undesirable consequences for the institution's operations.[6]

This reflects the going requirement for financial institutions to provide Internet-based services, utilize and oversee service providers, and prove, particularly the Board of Directors and Officers, due diligence in protecting customer information and meeting other regulatory requirements.

"Management can reduce a bank's risk exposure by adopting and regularly reviewing its risk assessment plan, risk mitigation controls, intrusion response policies and procedures, and testing processes."[7]

Financial institutions are heavily reliant on external service providers for Web sites and other core information systems. In addition financial institutions have a strong business requirement to analysis daily financial transactions in order to spot portfolio, lending, and financial market trends, customer requirements, and improve services. This requires moving data from multiple transaction-based systems to analytical database applications or data warehouses. MS-SQL server is often used by Service Providers because it is comparatively low in cost; more easily scaled with the introduction of Windows 2000 Data Center, and can be deployed rapidly. Market share for ISP and ASP of this product is on the rise.

Additionally, financial institutions may find it more efficient to use the MS-SQL Server internally to retain possession of certain business data and make it easier to analysis legacy, historical or trend data, while contracting with an ASP to run larger mainframe and multi-tier, integrated applications or Internet sites. The Data Transformation Services (DTS) and other Back Office Products included with MS-SQL Server make it very efficient for use in this manner.

Part 1 – Risk Analysis and Security Planning

Identify the Risks

The data security analyst can play a vital role in assisting the organization in identifying security risks. The business program manager maybe unaware of the potential exposures certain vulnerabilities cause the business application. The project manager may not have been given security requirements useful in selecting appropriate methods to mitigate the risks. The data security analyst fills the gap by providing expertise in technical risk assessment and mitigation. The FFIEC Information Security guidance outlines three phases of risk assement: information gathering, analysis and prioritizing.

Risk Assessment: Information Gathering

This phase requires the use of interviews, research, and analytical tools to determine the system composition, organization and responsibilities, business objectives and security requirements. To accomplish this, use the following steps:

1. Obtain a listing of assets, including equipment, human resources, and services used or planned for the system.
2. Identify the potential threat agents of the assets -- people with malicious intent, both insiders and outsiders, employees, users and contractors who may accidentally cause harm, service personnel who may gain physical access for other purposes, i.e., air conditioning repair service for the computer room; as well as environmental risks, such as fire hazards, infrastructure failures, natural disasters, etc.
3. Obtain the owner's classification of the data in regards to its sensitivity; i.e., confidential, proprietary, official-transaction-of-record (for example, earnings statements are public but held to a higher degree of accuracy and reliability), public; and functionality – mission critical, value-added service, informative, Enterprise-wide or organizational unit, regulatory or contractual, business or infrastructure requirements.
4. Identify organizational and technical vulnerabilities and obtain the owner's ranking on the impact to the business of a loss in each of the following security objectives:
    a. Availability
    b. Integrity
    c. Confidentiality
    d. Accountability
    e. Assurance
5. Identify the organization's current security policies, standards and procedures relevant to the application under review. Note any gaps where no policy or standard exists that would mitigate the risks.
6. Identify technical and administrative controls available in the present environment that could be used to mitigate risks of vulnerabilities being exploited.
7. Prepare a security control matrix identifying the security requirements, required controls, identifying gaps in the present control framework [development of a written plan is covered in the next section].

It is important that each of these steps be carried out in order to devise an appropriate security strategy. For example, a typical vulnerability scan may reveal that a password has not been changed for some time. By interviewing the administrator, it maybe determined that the ability to login with the account, which is an application account rather than a user account, has been disabled, and that the password is a hard-to-guess, sealed secret. A scan may reveal that SMTP is running and identify exposures. The interview and/or review of the application documentation may reveal that this is a required component, restricted to sending critical event alerts to end user administrators, and protected using encryption. Especially when the review involves a database application, scanners may not be

able to provide sufficient information because the application architecture and security design strategy may not be readily apparent.

Interviews and questionnaires are useful for gaining a basic description of the system and an understanding of its objectives, determining management's intentions for providing controls and for assigning responsibilities, and for gaining an understanding of the sensitivity and importance of the application data. The purpose of the information gathering is to obtain an understanding of the internal controls in use, as well as to identify vulnerabilities and exposures. This information is useful in planning for security testing.

Security scanning and vulnerability testing verify whether management's intentions are being met and whether vulnerabilities exist which have not been discovered. Security testing may include a review of the actual configuration [using scripts or automated tools] and the use of automated vulnerability assessment tools. The security testing methods selected depend on the application environment. Testing maybe performed by internal staff or by contracts with third parties. Network security testing using vulnerability analyzers and other tools is appropriate when attempting to discover weaknesses in your own network and financial institution examiners recommend regular use of these assessment tools.

However, Service Providers typically require independent verification of security controls through a third party review[8]. SAS 70 reviews maybe one of two types: Type 1 and Type II. Type I reports describes the service organization's description of its controls at a specific point in time and result in a written opinion on whether the service provider's description is presented fairly and whether the selected controls were relevant in achieving the control objectives. Type II reports extend the review to include detailed testing of the service provider's controls over a minimum of six months. Service Providers may provide SAS-70 reports that do not cover the system the Institution is assessing. Or if the SAS-70 does not have all the answers required to evaluate the suitable for your organization, the financial institution should prepare additional questions and specific contract terms to ensure their requirements are met. [Though the FFIEC directives make it clear that Service Providers should conduct vulnerability assessments, the SAS-70 reports may not include them.]

Other types of reviews are available. The ISO-17799 reviews can be requested for specific, critical support system (communications links or, in particular, for critical applications or for the entire site(s). For example, a the contract for a Web-hosted site that allows the purchasing organization to maintain administrative control of its server and applications may benefit from a ISO-17799 [BS-7799-2] certification of the communications channel between the corporate site and the web hosting site or service provider. Other frequently used third party reviews include TrueSecure certification, WebTrust and SysTrust. Specific vulnerability and penetration testing may also be requested. The entity requesting the service, under the authorization of the Service Provider, determines the scope of the review. If the Service Provider

initiates, pays for and delivers the third party review, the Service Provider determines the scope. They institution may try to obtain the Service Provider's authorization for a review in which the institution determines scope or test boundaries and methods.

Once the platform is known, research reported vulnerabilities, errors and attacks that maybe likely to occur. The numerous security organizations (SANS, SecurityFocus/Bugtraqs, CERT, etc,) vendor (Microsoft, Sun, IBM, etc,), and financial regulatory bulletin services (NIPC, FFIEC, FINCEN, etc.) also describe steps to take to apply patches and other techniques to mitigate risks. Financial Institutions must use these warnings to target for analysis specific vulnerabilities when conducting vulnerability assessments.

Risk Assessment: Analysis

The information gathered should be the basis for formulating a hypothesis regarding the ranking of data and components according to their sensitivity and importance to operations. Based on the information gathered from interviews and testing, the FFIEC suggests creating and analyzing applicable threat scenarios. The analysis should be useful in explaining to the owner or budget authority reasonable, foreseeable threats and possible attacks against information and systems that may affect the institution's condition and operations or may cause data disclosures that could result in substantial harm, inconvenience, or loss of reputation.[9] The analysis requires identifying the vulnerability, the persons or events that could be used to exploit the vulnerability, the consequences of successful exploit, and the impact to the business.

For example, an Internet based web site that use MS-SQL Server running on Port 1433 was used to spread the Slammer Worm, which caused distributed denial of service. As a result [hypothetical], customers could not access the Web site for about an hour, and the MS-SQL Server had to be removed from the network for patching and hardening, for an additional 4 hours. This resulted in lost business during the weekend peak shopping period.

These vulnerabilities need to be described to business owners in terms of the impact to their operations, the likelihood of occurrence, the benefit that would be added by incurring reasonable costs for controls to mitigate the risks. For example, OCC Alert 2001-4, "Network Security Vulnerabilities," in warning about recent hacker attacks, said "If successful in breaching a system and gaining access to customer records, unauthorized parties may fraudulently withdraw funds from bank accounts, obtain funds through identity theft, or extort funds by threatening public disclosure." The bulletin explains that in addition to conducting their penetration testing and vulnerability assessments, banks should include requirements in contracts with service providers to ensure appropriate performance of security maintenance and

reporting and to notify the bank when security breaches occur that may affect the bank.

If the business owner is not motivated by technical descriptions of vulnerabilities, you may need to ask the owner's opinion on the impact to the business should certain events occur. The Information Security Forum (ISF) has some a simple approach for clarifying risks and control requirements for non-technical business managers. A few examples, are presented in the table below[10]:

Table 1. Sample Questions Excerpted from Information Security Forum (ISF) Simplified, Practical Risk Analysis Methodology (SPRINT).

Impact to the business from a loss of Confidentiality	**Manager's Rating – Would it…**
FRAUD If information is disclosed, could funds be improperly diverted?	Threaten Business Survival Cause Serious Damage Cause Significant Damage Be a Minor Impact Negligible Affect
PUBLIC CONFIDENCE If information is disclosed, what damage could there be to customer confidence; public image; or shareholder or supplier loyalty?	Threaten Business Survival Cause Serious Damage Cause Significant Damage Be a Minor Impact Negligible Affect
Impact to the business from a loss of Integrity	**Manager's Rating – Would it…**
MANAGEMENT DECISIONS Could incorrect business decisions be made as a result of errors in or unauthorized changes to information?	Threaten Business Survival Cause Serious Damage Cause Significant Damage Be a Minor Impact Negligible Affect
FRAUD Could fraudulent diversion of funds arise from or be concealed by unauthorized changes to information?	Threaten Business Survival Cause Serious Damage Cause Significant Damage Be a Minor Impact Negligible Affect
Impact to the business from a loss of Availability (identify duration of outage)	**Manager's Rating – When Would it…**
PUBLIC CONFIDENCE Could customer confidence, public image and reputation, or shareholder or supplier loyalty be damaged if the application is unavailable?	Threaten Business Survival (More than 1 day) : Negligible Affect (less than 0.5 hour)
LEGAL LIABILITY Could legal, regulatory or contractual obligations be breached through a loss of the availability of	Threaten Business Survival (More than 1 day) :

the application?	Negligible Affect (less than 0.5 hour)

Following the business impact analysis, a simple threat assessment is performed. The threat assessment asks business managers to assign a vulnerability rating indicating the likelihood of occurrence of commonly occurring threats. For example, "How probable would it be unauthorized entry into premises could be used to compromise confidentiality?" "Consider such factors as the restrictions on access to premises; quality of physical security staff; sharing of premises; employee termination procedures; use of external contractors for maintenance and cleaning, storage of documents and printouts, the use of non-disclosure agreements with contractor staff." For the factors that the manager considers at high risk, control requirements are identified. The result is a summary of critical business impacts, threats and vulnerabilities and an action plan for implementing controls selected to mitigate these risks. The more detailed technical vulnerability assessment and this simple risk analysis can be used together or separately to summarize the risks to business management and to clarify for IT technical staff why action is required.

Risk Assessment: Prioritize

Once all threat and vulnerability assessments are identified and classified according to outcome and probabilities, management may decide additional controls are required. By including the cost of implementing the control against the potential loss it is easier to determine which actions should have immediate priority, and which actions should become part of long-range plans. The remedial actions are identified, responsibilities and milestones assigned.

Develop a Written Plan

"Financial institutions should develop a strategy that defines control objectives and establishes an implementation plan…." "An Information security strategy is a plan to mitigate risks while complying with legal, statutory, contractual and internally developed requirements."[11] The strategy should be documented in a written security plan, and a written security plan is required to fulfill requirements for financial privacy requirements of the Gramm-Leach-Bliley Act (GLB).

If the Institution has published data security policies, standards and procedures, it is easier to develop the written plan. "Policies are the primary embodiment of strategy….and specify the mechanisms through which responsibilities can be met, and provide guidance in acquiring, configuring, and auditing information systems."[12] The policies become part of the written plan for internal applications and part of the contractor capabilities analysis and during contract negotiations. The Service Provider should be capable of providing services and solutions that meet the organization's security standards as well as regulatory requirements, particularly for financial privacy. A written plan can be used during reviews as discussed in the next

section. The written plan documents for the infrastructure support systems, for applications, or for the site the most likely threats and vulnerabilities to occur and the actions taken to mitigate the risk to an acceptable level. It is a method of obtaining business and information system management's acknowledgement of the risk, and their responsibility for overseeing and authorizing maintenance of security controls.

The "National Information Assurance Certification and Accreditation Process (NIACAP), (NSTISSI No. 1000)," the NIST SP-800-18 "Planning Guide for Developing Security Plans for Information Technology Systems," the British Standards Institute BS-7799 "Code of Practice for Information Security Management – Part 2," and the FFIEC "Information Security Booklet – December 2002" of the IT Examination Handbook, offer similar guidance but with varying degrees of formality, ascertainment and documentation in developing security plans. The NSTISSI distinguishes three types of accreditations that could be applied to financial institutions: major application, general support system, and site. The security plan documents the following:

- The boundary of the system to be included in the plan,
- The description of the system and its critical interfaces,
- A description of the owners and the business purpose for the application, support system, or site;
- The operating environment, risks and threats;
- The security architecture and controls selected,
- The assignment of responsibilities among critical resources, such as engineering, development, operations, administration, end users, security, service providers, etc.;
- Actions that must be taken for the system to meet the identified security requirements and deadlines for completion,
- Documentation of the security plans, test plans and procedures, results of security certification or acceptance, and the residual risk;
- The baseline security configuration document.

The OTS Handbook 341 describes and explains the selection and use of administrative, operational and procedural controls to mitigate technology risks. The controls selected should be part of the security plan. The security plans should be used in conjunction with additional certification statements that clarify for the owner or designated authority their responsibilities in authorizing the actions in the plan to mitigate the risk identified. The owner is ultimately responsible for the success of the system operations, and any due diligence [or negligence] taken to reduce the level of harm that may occur from incidents that may occur during its operations. In regulated institutions this responsibility is extended to include the measures taken or those that were neglected that hold a potential for harming the institution or the public. Failure to comply can result in substantial penalties.

Implement and Test Security Controls

Typically, the internal controls, highlighted below, and explained in detail in the FFIEC Handbook, should be selected from the following,[13] based on results of risk

assessment, knowledge of the business objectives, and contractual, legal or regulatory obligations:

Logical and Administrative Controls

- Access Rights Administration
- Authentication
- Acceptable Use Policy
- Network Access
- Operating System Access
- Application Access
- Remote Access

Physical Security

- Physical security zones, i.e., data center vs. branches
- Controls for environmental hazards, such as fire, flooding (halo gas, smoke alarms, raised flooring, heat sensors, etc;
- Power outages and fluctuations
- Alarms, surveillance cameras, synchronized lighting, and other intruder detection devices
- Backup communications
- Vaults, locked cabinets, equipment and paper storage, media storage
- Locks or other devices for PC, laptops, PDS, hand-held devices, etc.
- Protected cabling, routing of cabling wire rooms locks, Infrared or wireless equipment, frequency emissions both wireless and unintentional emissions from unshielded equipment
- Badges and physical ID controls

Encryption

- Transmission
- Storage
- Key Management
- Uses by Type
    - Hashes: verify file and message integrity and passwords from disclosure
    - Symmetric keys: used with asymmetric keys, which perform key exchange to establish encrypted session with symmetric key
    - Asymmetric or Public keys – PKI, key exchange,

Anti-Virus and other controls against malicious code

- Antivirus, Code Blocking, Content Management, Email scanners
- Firewall, gateway rules and/or filters
- Policies and procedures

Systems Development, Acquisition, and Maintenance

- Security requirements specified during SDLC requirements definition phase, designed, developed, tested and implemented as part of the overall process
- Independent evaluation and security accreditation of purchased software
- Problem and change management procedures established
- Version control and audit
- Source code review and testing

- Segregation of duties by restricting vendor/developer access to production source code and systems and monitoring their access to development
- Perform security tests to verify that the security requirements are met before implementing software in production
- Remove services and components of COTS that are not required.
- Implement security provided with the COTS package, if it would meet your security requirements, not introduce new vulnerabilities to the rest of the networked systems, the value exceeds the costs of implementation.
- For COTS software, determine if the vendor's certification requirements [specification of baseline configuration required to meet support requirements] include sufficient measures for patching against security alerts and vulnerabilities.
- System and patch maintenance procedures ensure integrity, reliability, and successful operations without introduction of new vulnerabilities.

Personnel Security Controls

- Background checks and screening
- Confidentiality, nondisclosure, authorized use agreements
- Job descriptions
- Training in security awareness and compliance

Electronic and Paper-based Media Handling

- Handling and storage
- Disposal
- Transit

Logging and Data Collection

- Identify components to be logged (i.e., firewall events, network traffic, intrusion detection system events, application and operating systems, etc.)
- Specify information to be logged
- Protect logged data from destruction or manipulation
- Review and analysis of logs, escalation procedures and required responses and reporting.

Service Provider Oversight

- Due diligence in researching and selecting service providers
- Contractual assurances for complying with the organization's security policies and requirements
- Capabilities for conducting or obtaining third party reports and reviews that adequately test the controls of the application and/or services to be provided in the agreement

Intrusion Detection and Response

- Type of Intrusion detection system to use -- heuristic or signature – based on objectives
- Proper placement of Intrusion detection system
- Apply various countermeasures on typical methods used to defeat the IDS or to generate false positives or false negatives;

The controls selected for use in an application or support system security plan should be based on the results of the risk analysis, any regulatory or contractual obligations and the business goals. The test plan should verify whether or not the controls are in place, whether the controls are working effectively and efficiently in mitigating the risks, and whether or not further action should be taken to mitigate the residual risk. The test plan should look at administrative, technical and operational controls.

The written test plan may include the following:

- Statement of the risk to be analyzed,
- Statement of expected control,
- Description, procedures and tools to be used to test the controls,
- Results of testing,
- Consequences, exposure or business impact if left unchecked,
- Recommendations for implementing controls to mitigate the risks.

The written test plan should be agreed to with an appropriate level of management. When using automated vulnerability scanners and penetration testing tools a written agreement and explanation of use should be obtained from an appropriate level of management for periodic use. Most of these agreements include a disclaimer intended to absolve the tester of damages that occurred during the testing period. Those responsible for testing should consider the timing of the tests, and the extent of testing. For example, using some dictionary attacks embedded in vulnerability scanners that would lock out all users from the database and disrupt operations would not be wise under certain conditions. Test procedures can include the use of automated tools, such as, port scanners, vulnerability scanners, database and network sniffers, host-based and network-based intrusion detection, penetration tests, automated security configuration analyzers and/or scripts. It can include reviewing accounts, authorization and access, maintenance; access control logs, change management authorizations, file and program access controls; technical walk-throughs and use-case scenarios.

Monitor and Update the Security Plan

Analysis and update the Security Plan based on current information. Once the baseline security plan has been agreed, it becomes a basis for monitoring and reviewing the effectiveness of existing security controls. Based on the information gathered about new threats and vulnerabilities, actual attacks or incidents, changes in performance or business requirements, and changes in regulatory requirements, the plan should be analyzed and updated. The FFIEC guidelines in its Information Security Booklet include security self-assessment, security personnel access to and use of automated tools appropriate for complex financial institution systems, automated security policy and security log analysis, configuration management procedures, vulnerability and patch management, maintenance of authentication and access control systems, maintenance of use of intrusion detection, firewall, and other security appliances; activity related to oversight of service providers and vendors.

Part 2 - Example Using SQL

In order to meet the guidelines in this assignment, only the highlights of a risk assessment and review will be presented. Also the scope will be limited to analyzing risks associated with the SQL Server only, rather than a comprehensive review which would include environmental, administrative and operational controls.

This section will briefly review two applications, which require MS-SQL Server. One application is managed internally and the requirements permit the use of Integrated NT Security. The other is managed by a Service Provider and requires the use of MS-SQL Server mixed mode security. Information similar to this and additional details would be part of the written security plan.

Internally managed SQL Server Application

The specifications for the Internal Application (IA) are summarized as follows:

Business Objective: Provide 500 retail banking analyst with information on activity of demand deposit customers for targeted marketing, collections, inquiries, providing added services, analysis of financial performance and impact to the bank's future business plans.

Sensitive Data: customer account numbers, social security information, personal identity information, financial information, and other details. Includes required regulatory reporting and actions relative to financial privacy.

Targets: Retail banking analysts and other specialized staff, the bank's technical support staff and developers, the COTS vendor's technical support staff (including developers), customers, intruders ("insiders" more likely than "outsiders").

System Description: Windows 2000 Server, MS-SQL Server 2000, COTS [Visual Basic], TCP/IP network. Requires transferring data from an IBM MVS mainframe application to the SQL Server. Only authorized DOMAIN users running the required COTS [Visual Basic] client can access the MS-SQL application and server from a corporate LAN. The COTS application cannot be updated directly by the vendor. Patches and upgrades are sent to engineering to test before installation.

Threat Scenario: Identity Theft and Pre-text Calling: A hacker breaks into a Career Website and steals identity information of a bank customer. The hacker then calls the financial institution, posing as a customer or someone authorized to have the customer's information, and convinces a retail bank consultant to release confidential customer identity information and to change the customer's address. The hacker then uses the information to commit loan fraud accepting in cash the proceeds from the loan.

Compensating Controls: Train retail bank staff in procedures to use in verifying identity of the requestor and legitimacy of the claim. Set up audit trails, triggers and

procedures to record events based on "red flags." Use object permissions and triggers to prevent staff from making changes that have not been independently verified. Use caller-id software with the applications. Report suspicious activity in required SAR reports to FINCEN. [Note more controls would be selected.]

Service Provider managed SQL Server Application

The specifications for the Service Provider Application (SPA) transaction web site are as follows:

Business Objective: Offer mortgage loans over the Internet. This would include qualifying applicants, making competitive offers, completing processes required to approve the loan, including processing critical documents relative to loan approval.

Sensitive Data: customer account numbers, social security information, personal identity information, financial information, and other details. Mortgage offers are public until consumer decides to apply for mortgage. Then the consumer must register with the site and provide confidential information to use in processing the loan request.

Targets: Lending officers of the bank and its subcontractors, consumers, ISP staff, staff of ancillary services, i.e., credit bureaus, title search, appraisers, etc; competitors, intruders (outsiders more likely than insiders).

System Description: Windows 2000 Server, MS-SQL Server 2000, IIS Server with ASP COTS application on public and private TCP/IP network. Requires links and/or interfaces with multiple servicing organizations. The Service Provider performs upgrades and patches.

Threat Scenario: Loan Fraud: The financial institution contracts with a Service Provider to provide loan origination, qualification, processing and preparation services. The bank furnishes the Service Provider its lending policies and rates. An evildoer obtains a false identity, then poaches on the Service Provider's web site to determine how to manipulate the site and the links required to get a loan approval. The evildoer gets the link for requests for appraisals and for credit ratings, sets up a bogus site and link. The evildoer then enters the Service Providers site and makes a loan request on a property. The property that was purchased previously by the seller, the evildoer's partner, for $100,000 is to be sold for $220,000. The evildoer diverts requests for appraisals to the bogus website, which automatically provides comparables that will be approved by the lender. The lender wires the funds to the evildoer's seller. The borrower will eventually default on the loan.

Compensating Controls: Install network and host-based intrusion detection and monitor activities of evildoers, collect data to trace evildoer's IP address(es). Obtain information on Web linking and trace activity through the links. Use encryption to authenticate the linked sessions. Set file permissions on web server data and

application files to prevent unauthorized access, data manipulation, and insertion. More controls would be selected.

Security Objectives

Using the information gathered and the preliminary risk scenarios, set some high-level security objectives for the application. A sample of objectives appears below.

Table 2 – Identify High Level Security Objectives Applicable to Applications

High Level Objectives	**Internal Application (IA)**	**Service Provider Application (SPA)**
Confidentiality	Customer data must be kept confidential, particularly information regarding identity.	Loan applicant data must be kept confidential.
Integrity	Customer account data must be accurate and complete. Changes of address and other critical data should not be made without independent verification and authorization.	Loan applicant data must be accurate and complete, must not be falsified by participants in the lending process. Transaction web site links must be protected from unauthorized modification and abuse. Web links must clearly distinguish between the bank and third party service.
Availability	Must be available throughout the normal business day. Service would be impacted after 4 hours and business threatened after a couple of days.	Must be available 24x7. Service would be impacted after one hour and business threatened after a day.
Accountability	Auditing should be sufficient to trace activity to its source. Intrusions should be detected. Vulnerabilities should be spotted and patched.	Auditing should be sufficient to trace activities to its source and to follow the transfer of critical data through interconnected systems. Intrusions, enumeration and unauthorized scanning should be detected. Vulnerabilities should be spotted and patched.
Assurance	Selection of controls is documented in the security plan. Semi-annual security testing and monitoring are conducted to verify, validate and update	The Service Provider(s) have been subject to a third party review. Contractual arrangements require the Service Provider to use procedures and policies

	plans. Security controls to prevent Identity theft and pre-text calling must be tested and verified following regulator guidelines and requirements.	that enforce the organization's security policies. The Service Provider has provided written documentation of its security policies and security architecture. SLA's and regular monitoring are provided. The SP provides incident response reports when major incidents occur that could impact the service. Security controls protecting identity, transaction web links must be tested and verified following regulator guidelines and requirements.

Risk Analysis – Overview

MS-SQL Server has been identified as one of the top 10 Windows security threats by the SANS Institute. During 2002 Microsoft issued 11 security bulletins requiring patches to multiple vulnerabilities open in the SQL Server, compared to only three from June 1998 to June 1999. Though a small number of patches were released, during 1998/99 notable criminal activity occurred on Internet web sites running poorly configured and administered IIS and MS-SQL Servers. Hackers such as Maxus stole credit card numbers from several sites, attempted to extort the business owners, and released the stolen credit card numbers to the public and/or underground when the legitimate businesses failed to pay. "Though CISP [VISA's Cardholder Information Security Processing] and SDPS [Mastercard's Site Data Protection Service] focus on network security – from the transport layer to the physical security policies – these practices do not address payments for products and services via stolen or generated credit-card numbers, which constitute the majority of B2C transactions."[14] These types of attacks maybe reduced somewhat by controls coded into the applications and the database to prevent credit card theft and exploitation.

With Microsoft SQL Server 2000 it has been easy to exploit several types of buffer overflows that may not require authentication and may result in escalation of privileges for the attacker. Some buffer overflow attacks may disable (by writing over) or make ineffective the security parameters in what was thought to be a "hardened" or securely configured Server.

With Microsoft SQL Server it has been easy to exploit poorly designed and administered systems. The business requirements for the use of newer versions of Microsoft SQL Server, which emphasized its strength in sharing and transferring data over the network between applications running on the same and different

platforms, seemed to gain acceptance more rapidly than the technical administrator's capability of configuring it securely. Many business applications for SQL Server are written in Visual Basic – one of the world's most popular programming languages, and therefore, more knowledgeable users are available to hack it. SQL Server Internet applications may use weak authentication procedures, which permit the SQL Server to run with weak or blank passwords on highly privileged accounts such as 'sa.' The SQL Server may allow submission of SQL queries through Web-based forms or at the URL command line. The table below identifies some commonly occurring vulnerabilities and threats. "Probability of occurrence" is measure as "High (H)," "Medium (M)," and "Low (L)." "Impact to the Business" is measured as "Survival Threatened (H)," "Serious Damage (M)," "Significant Damage (L)," "Minor Impact (VL)".

Table 3 – Preliminary Risk Analysis – Probability of Occurrence

Security Objectives	Vulnerabilities & Threats Identified	Probable Occurrence		Impact to Operations	
		IA	SPA	IA	SP
Confidentiality	Identity Theft	H	H	H	H
	Password Cracking	L	H	M	H
	Spoofing	L	H	M	H
	Privilege Escalation	L	H	M	H
	Extortion or Fraud	L	H	M	H
	Buffer Overflow	L	H	M	H
	SQL Injection	L	H	M	H
	Malicious Code	M	H	H	H
	Unauthorized use of services	M	H	H	H
	Web link exploitation	M	H	M	H
	----------[15]	L	H	M	H
	Outsiders gain site of private data	H	H	M	H
	Disclosure by staff of sensitive information	L	L	L	L
	Unauthorized entry into premises	H	H	H	H
	Unauthorized access to data by insiders	L	M	L	H
	Unauthorized access to data by outsiders	M	H	M	H
	Problems with interconnected systems	M	M	M	H
	Interception of communication links	L	L	L	L
	Electronic emanations	L	L	L	L
Integrity	Identity Theft	L	H	H	H
	Manipulation of data	M	H	H	H

Security Objectives	Vulnerabilities & Threats Identified	Probable Occurrence		Impact to Operations	
		IA	SPA	IA	SP
	Corruption of destruction of data	M	H	H	H
	Buffer Overflow	L	H	M	H
	SQL Injection	L	H	L	H
	Malicious Code	M	H	M	H
	Unauthorized use of services	M	H	H	H
	Transaction Web link exploitation ----------[15]	L	H	M	H
	Input Errors	M	M	L	M
	Program Errors	M	M	L	M
	Operator Errors	M	M	L	M
	Manipulation or suppression of input documents	M	M	L	L H
	Unauthorized use of transaction facilities	M	H	M	H
	Unauthorized modification of programs	M	H	L	M
	Unauthorized modification of files	M	H	L	M
	Manipulation of jobs, schedulers, change control automation	M	H	H	L
	Manipulation of computer equipment or media	M	L	H	M
	Integrity problems with feeder systems	M	H	M	M
Availability	Inadequate Redundancy or Fail Over	M	H	M	H
	Inadequate Backup & Restore	L	M	M	M
	Denial of Service & Distributed Does Syn Attacks	L	M	L	M
	Unauthorized use of services ----------[15]	M	M	M	M
	Major Disasters – Natural, Accidents, Acts of War or Terrorism	L H	M H	L L	L L
	Inadequate contingency arrangements	M M	M M	M M	L L
	Inadequate business continuity plans	L	L	L	L

Security Objectives	Vulnerabilities & Threats Identified	Probable Occurrence		Impact to Operations	
		IA	SPA	IA	SP
	Day-to-day System Outages Degraded System Performance Other threats	L ? 	L L 	L ? 	L ?
Accountability	Inadequate audit trail. Audit trail and logs are not secured.	H H	H H	H H	H H
Assurance	Security management plan is not available. No third party review exists.	L M	M H	M H	M H

SQL Server Security Policies

Thus far the review has identified high-level security objectives for the application and many types of threats that would be likely to occur against these applications. The list below provides a set of baseline security standards to use in evaluating the security configuration of the SQL Server in order to determine the likelihood of preventing, detecting or correcting attacks and weaknesses[16]. The actual security configuration can be reviewed against the list of baseline controls. Additional controls, such as improved third party authentication devices or encryption of stored data, can be recommended in order to adequately secure the application.

1. The SQL Server Service runs in the security context of a domain account, with appropriate rights and permissions assigned to the account. [The public SPA application may need to run with a Workgroup account in a peer-to-peer relationship or to utilize the trust relationships available in Windows/NT domains between the IIS Servers and SQL Servers. Note the Public Site should be separate from any internal sites.]
2. The SQL Server Agent Service runs in the security context of a domain account, with appropriate rights and permissions assigned to the account. [Public SPA application may require a local account or to utilize the trust relationships available through Windows/Nt domains between the IIS Servers and the SQL Servers.]
3. The SQL Server 'sa' account has been password protected with a difficult-to-guess password, at least 12 characters in length.
4. User accounts must meet the organization's password control standards, such as, at least 7 mixed characters. Windows/NT account management controls are utilized.
5. The internal server runs in Windows integrated mode as part of a domain or workgroup. [The Public server may have to run in mixed mode – avoid if possible.]
6. Current service packs and patches have been applied and configured appropriately.

7. The production installation does not include components that are not required, such as the development tools, code samples, etc. Some tools cannot be removed without reinstalling the SQL Server.
8. When possible Windows 2000 global groups are used to grant access to users with common requirements, then the global groups are added to the local groups on the SQL Server.
9. The local group account are added to the SQL Server login and mapped to an appropriate database user.
10. If using Windows NT 4, create local groups on the SQL Server and add the domain accounts to the SQL Server logins. Map the login accounts to database user accounts. Set permissions on roles and assign the roles to the appropriate database user accounts.
11. Application roles are used to restrict access to table data through specific applications and to revoke or deny direct access from user accounts.
12. The use of statement permissions has been revoked for all but emergency support accounts on the production database.
13. Object permissions are based on need to know and access strategy.
14. The Windows NT/2000 Administrator account has been renamed on the public SQL server.
15. Internet-facing applications use the Web server on the public network and the SQL Server on the private network.
16. SQL Server enumeration has been disabled to hide the SQL Server Service in the domain.
17. Ingress and egress filtering have been enabled on ports 1433 and 1434 on the firewall.
18. The use of shared SQL Server tools and command line utilities has been restricted based on user responsibilities, i.e., dba or technical support. Procedures are in place to control and authorize use by developers.
19. Auditing of successful and unsuccessful attempts to login to the SQL Server has been enabled.
20. The SQL Profiler utility along with C2 auditing of security events, such as, the use of grant, revoke, deny commands, user and role activity, additions, removals and modifications of the configuration; has been enabled and automated alerts have been configured to warn the DBA/Security when audit logs reach a specific size. Incident handling procedures have been developed for use with the SQL profiler.[17]
21. The Windows/NT guest user account has been disabled and the guest account has been dropped from production databases.
22. The Windows/NT Guest and anonymous accounts has been denied login to the Server. If required, deny or revoke login to other appropriate accounts.
23. Only designated users and accounts have been assigned to fixed server roles, especially sysadmin.
24. Access has been restricted to the SQL Server registry hives, such as HKLM\Software\Microsoft\MSSQLServer and HKML\System\CurrentControlSet\MSSQLServer.

25. Application roles and stored procedures are used whenever possible. The application role password is encrypted.
26. Views and stored procedures are used instead of direct table access and users are denied direct access to tables.
27. If sensitive data requires encryption, consider utilizing one of many third party products designed to encrypt MS-SQL Server data.
28. Setting up linked servers using Windows authentication mode, which requires the ability to perform security account delegation. Security account delegation is the ability to connect to multiple servers, and with each server change, to retain the authentication credentials of the original client. To use delegation, all servers that you are connecting to must be running Microsoft® Windows® 2000, with Kerberos support enabled, and you must be using Microsoft Active Directory™,
29. Inactive linked server definitions that are no longer needed have been removed.
30. Deny EXECUTE permissions on high-risk stored procedures, like xp_cmdshell, the OLE automation stored procedures, and others listed on the high-risk list[18].
31. Developers have used NT integrated authentication when hard coding connection authentication details. This eliminates the requirement for including a password in the script, ODBC and UDF definition files. The programmed or scripted connection authorizations should be tracked and protected by a change control process.
32. The following MS-SQL directories or their contents have been protected from deletion: Binn, Data, Ftdata, HTML, or 1033. You may lose functionality.
33. Full Backups are conducted nightly and incremental backups every 2 hours. The backups are password protected.
34. The backup plan includes frequent backup of translation logs.
35. Restoration of the database is tested every 6 months and the integrity of the backups is tested daily.
36. Restrictions protect the use of the Data Transformation Service (DTS) -- a password is specified for DTS packages. Procedures are in place that require submission of requests and change control by designated officials in order to use the packages.
37. On the Internal application special NT accounts have been set up for replication services between networked SQL Servers.
38. When installed on a Windows 2000 server, encrypt the database files using the SQL service accounts.
39. If required, use third party products or the Microsoft CryptoAPI to encrypt table data.
40. Direct SQL queries from the URL command line have been prevented.
41. See that applications include controls to prevent buffer overflows, a common vulnerability of MS SQL Servers. For example, do not allow the use of the Visual C++ strcopy() and strcat() functions since they do not check input length. Instead, use strncpy() and strncat(), which do check for input length. Use the MAXSIZE attribute for fields used on a form.

42. The applications use server-side validation techniques for data submitted through forms, URL or SQL injection. The server-side validation techniques should reject data that does not meet length, type, and content requirements. The error message should not reveal information about the SQL Server and should prompt the user for valid input.
43. Installation files that may reveal the system or installation account password, such as setup.iss, have been removed.
44. The BUILT-IN\Administrators group from the SQL Server logins has been removed.
45. Sending and receiving email by the SQL Server Service and SQL ServerAgent Service through account and permissions management is prevented or restricted.
46. The use of job tools and scheduling tools has been restricted to authorized staff or specially designated accounts and change control procedures have been setup for submitting and scheduling jobs based on authorizations.

Test Procedures

A variety of test and test tools are available. The FDIC offers guidance in "Risk Assessment Tools and Practices for Information Systems Security," FIL-68-99, as does the NIST[19] in its new SP-800-42.[20] For example port scanners, such as nmap and Superscan, list all hosts, ports and services running on an identified subnet or network. Some scanners provide operating system fingerprinting and "banner grabbing" to obtain additional information. Port scanners do not identify vulnerabilities and rely on the user's knowledge for estimating risk. Vulnerability scanners identify potential vulnerabilities and exposures, known security flaws and bugs, known attacks and exploits. Typically they classify the exposure as low, medium or high risk and provide guidance on how to correct the weakness. A good vulnerability scanner, such as ISS Database Scanner or NetIQ's Security Manager, can perform this more quickly and accurately than running a series of scripts individually or walking through each configuration option with a DBA or Administrator. [In either case, the results of testing must be presented to the DBA or Administrator in order to clarify and verify interpretation. The Microsoft Baseline Security Analyzer, a free tool, can detect weaknesses in the operating system (NT 4 and Windows 2000), IIS Server and SQL Server configurations and provides recommendations for hardening the configuration. Both the ISS Database Scanner and the Microsoft Scanner test password strength and ISS include a dictionary attack tool (be careful how and when you use it).

Vulnerability assessments should be run on a periodic basis. Vulnerability assessment tools can be host-based or network-based. Host based tools run on a host, usually a server, but also firewalls, routers or desktops; while network tools reside on the network and look for network-based attacks by examining packets for denial of service, spoofing, worms, and other attacks. The accounts listed and permissions matrix that can be constructed using the scanner results should be discussed with end user managers and DBA's in order to determine whether the configuration supports the security requirements.

Penetration tests use automated tools in attempts to circumvent the existing controls. The results of the penetration tests can be used to help the end user see the system through the eyes of a hacker rather than through those of a legitimate business user. The penetration tests goes further than a vulnerability scanner by actually exploiting the vulnerability.

Reports from host-based intrusion detection devices can indicate suspicious activity, such as enumeration of account information and failed attempts to directly access to tables. Intrusion detection devices use three different methods to detect intrusions: attack signatures, system misuse such as unauthorized access, and anomalies or abnormal behavior. New technology discussed on the SANS website called "Anti-Vulnerability Technology," consists of a logic engine and vulnerability warehouse that can be shared by multiple security devices, such as scanners, IDS, firewalls, and other appliances.

SQL Server includes several stored procedures designed to provide information about the configuration. They all start with "sp_help," and provide information on the accounts, roles, statement and object permissions, jobs, etc. [Most are Executable by 'PUBLIC' – what would happen if you denied or revoked PUBLIC access? Be sure to DENY LOGIN to the SQL Server to the anonymous-type accounts and control the use of the superuser accounts.]

Reporting

The results of testing should be discussed with the affected parties: owners, program managers, administrators, and others and an appropriate security plan devised. This may include recommendations or action plans that outline specific corrective actions to be taken and responsibilities of all parties. The selection of controls is based on the results of the risk assessment, the cost of the controls and the expected benefit of implementing the controls. All the most relevant information is then summarized in the written security plan. Often it is good to include with the written plan, a control matrix to use in tracking progress in actions to be taken and to use in the periodic reviews of controls. If completed during development, this is a good opportunity to test tools used and obtain agreement on their use during production. This can be documented in an appendix to the plan.

Additional REFERENCES

"Information Security: Vulnerability Scanning Requirements for GISRA Under OMB-M-02-09," SANS 02-103. http://www.sans.org/top20/GISRA_NASA.pdf

Financial Institution References

Federal Financial Institution Resources
http://www.ffiec.gov/ffiecinfobase/html_pages/re_01.html#FFIEC

- "Risk Assessment Tools and Practices for Information Systems Security," FIL-68-99, FDIC. http://www.ffiec.gov/ffiecinfobase/resources/info_sec/fdi-fil-68-99-risk_assessment_tools_and_practices.pdf
- "Security Monitoring of Computer Networks," FIL-67-2000, FDIC. http://www.ffiec.gov/ffiecinfobase/resources/info_sec/fdi-fil-67-2000-security_monitoring_computer_nets.pdf
- "Privacy of Consumer Financial Information," FIL-73-2001, FDIC. http://www.ffiec.gov/ffiecinfobase/resources/info_sec/joi-privacy_final_rule_000601.pdf
- "Risk Management of Outsourcing Technology Services," OCC Advisory Letter 2000–12, http://www.ffiec.gov/ffiecinfobase/resources/info_sec/occ-al_2000_12_risk_mang_outsourc_tech_service.pdf

Microsoft SQL Server References

- "Attack Snarls Web Traffic, E-mail, ATMS," AP Technology Writer, , Jan 26, 2003. http://home.verizon.com/
- NGSSoftware Insight Security Research Advisory, "Unauthenticated Remote Compromise of MS SQL Server 2000," http://www.ngssoftware.com/vna/ms-sql.txt
- "Port 1434 MS-SQL Worm", www.incidents.org
- "Retina Sapphire SQL Worm Scanner," http://www.eeye.com/html/Research/Tools/Download.asp?file=RetinaSapphireSQL
- "Microsoft SQL Server Passwords," www.ngssoftware.com
- "SQL Injection," www.ngssoftware.com
- Microsoft SQL Server 2000 System Administration Training Kit, Microsoft Press, Redding,2001.
- Microsoft SQL Server 2000 Database Design and Implementation, Microsoft Press, Redding, 2001.
- Inside Microsoft SQL Server 2000, Microsoft Press, Redding, 2001.

[1] IT Examination Handbook Information Security, December 2002, Federal Financial Institution Examination Council (FFEIC), pages 7-12. – one of a series of updates to 1996 FFIEC Handbook, which updates and rescinds security guidelines in the previous book.
[2] Office of Thrift Supervison (OTS) Regulatory Handbook 341.1, "Chapter: Management, Section: Technology Risk Controls" OTS, January 2002, page 341.6. *http://www.ots.treas.gov/docs/429091.pdf*
[3] "Federal Financial Institution Fraud and Failure Report, 2000/1"., U.S. Department of Justice, Federal Bureau of Investigation.
[4] "Money Laundering: A Banker's Guide to Avoiding Problems," Office of the Comptroller of the Currency, Washington, DC, December 2002, page 3.
[5] "Technology Risks Management," OCC 98-3, Office of Comptroller of the Currency, http://www.ffiec.gov/ffiecinfobase/resources/info_sec/occ-bu98-3_technology_risk_management.pdf
[6] Office of Thrift Supervison (OTS) Regulatory Handbook 341.1, "Chapter: Management, Section: Technology Risk Controls" OTS, January 2002, page 341.7.
[7] "Infrastructure Threats – Intrusion Risks," OCC 2000-14, http://www.ffiec.gov/ffiecinfobase/resources/info_sec/ occ-bul_2000_14_infrastructure_threats_intrusion_risks.pdf
[8] The federal agencies providing guidance to financial institutions say that the reviews can be done by the institution's staff or by a third party. The institution's contract should provide an appropriate level of flexibility depending on whether the application is a dedicated or shared service.
[9] FFEIC Information Security Handbook, pages 9-10.
[10] Information Security Forum, Simplified, Practical Risk Analysis Methodology (SPRINT) User Guide, pages 43-57. Also see Fundamental Risk Management series, ISF.
[11] FFEIC Information Security Handbook, page 13.
[12] FFEIC Information Security Handbook, page 14.
[13] FFEIC Information Security Handbook, pages 15-77.
[14] Lori MacVittie, "Online Fraud Detection Takes Diligence," http://www.networkcomputing.com/, February 18, 2002.
[15] Below the line, SPRINT User Guide, ISF, pages 43-57.
[16] Adapted from various SQL Server security guides, such as:

- SQL Server Security http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=0&tabid=1
- "Overview of the SQL Server Security Model and Security Best Practices," Vyas Kondreddi, http://www.sql-server-performance.com/vk_sql_security.asp."
- Microsoft

[17] Karen Nelson, "Designing Secure SQL Server Databases," 75-20-52, Auerbach Publishing; and

- Karen Nelson, "Securing MS-SQL Internet Applications That Use XML: Part 1," EDP Auditing 75-20-50, Auerbach Publications, New York.
- Karen Nelson, "Securing MS-SQL Internet Applications That Use XML: Part 2," EDP Auditing 75-20-51, Auerbach Publications, New York.

[18] MS SQL Server Security, http://www.sqlsecurity.com
[19] http://csrsc.nist.gov/publications/nistpubs/index.htm

- Risk Management Guide, SP-800-30, NIST, http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

- Guideline on Network Security Testing, SP-800-42, NIST (No longer listed on web site.)
- Guide for Developing Security Plans for Information Technology Systems, SP-800-18, NIST. http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.PDF

[20] Tools should not be used without written consent and limitations of liability.