Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Conducting an electronic information risk assessment for Gramm-Leach-Bliley Act compliance.

To obtain compliance with the new Gramm-Leach-Bliley privacy regulations, financial institutions need to identify vulnerabilities in electronic systems, assess likelihood and impact of threats, and assess sufficiency of controls to mitigate those risks. In response to these new regulations, I developed a process for conducting an electronic risk assessment in accordance with GLBA, and used it to conduct a risk assessment for Johnson Financial Group. The process involves listing each technology and vendor service and ca...

Copyright SANS Institute

Author Retains Full Rights

AD

Conducting an electronic information risk assessment for Gramm-Leach-Bliley Act compliance.

SANS GSEC Practical Assignment version 1.4b

© SANS Institute 2003, Author retains full rights

Kevin M Bong
GCIA, GCIH, GCFW, MCSE(NT)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Abstract

To obtain compliance with the new Gramm-Leach-Bliley privacy regulations, financial institutions need to identify vulnerabilities in electronic systems, assess likelihood and impact of threats, and assess sufficiency of controls to mitigate those risks. In response to these new regulations, I developed a process for conducting an electronic risk assessment in accordance with GLBA, and used it to conduct a risk assessment for Johnson Financial Group.

The process involves listing each technology and vendor service and categorizing these systems based on the data they process or store. Threats and vulnerabilities are listed for each technology, and then controls are specified for each vulnerability. Controls are categorized, and definitions for control adequacy and residual risk are developed and applied to each technology. Output includes a report showing vulnerabilities, controls, and a risk rating for each technology, a report showing which vulnerabilities have insufficient controls, and others.

Table of Contents

Abstract 2
Table of Contents 2
Purpose 3
Before 3
  Process Foundation 3
  Process Steps and Implementation Considerations 4
During 4
  Step 1. Determine Data Classification Categories 4
  Step 2. Inventory Systems 5
  Step 3. Classify Inventoried Systems 6
  Step 4. Determine Initial Risk of inventoried systems 7
  Step 5. Group Technologies 9
  Step 6. Identify Vulnerabilities and Threats 9
  Step 7. Identify Controls 10
  Step 8. Indicate whether controls are preventative, detective, corrective, or directive 12
  Step 9. Determine Control Adequacy 13
  Step 10. Determine Residual Risk 16
After 17
  Step 11. Apply definitions and logic to the data and create reports 17
  Step 12. Report results to corporate leadership 19
  Step 13. Review and update at least yearly 20
Enhancement Possibilities 20
Appendix A: Automation Tools 21
Appendix B. Relational Database Design 22
Appendix C. REFERENCES 24

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Purpose

The Gramm Leach Bliley Act specifies what financial companies are required to do with regards to protecting the privacy of their customers. One of the primary aspects of the development and implementation of a security program that complies with GLBA is to perform a regular assessment of risk to customer information. This risk assessment needs to include an identification of foreseeable threats, an assessment of the likelihood and potential damage of these threats, and the sufficiency of controls to mitigate risks.[1] GLBA also requires regular reporting of the risk assessment results to corporate leadership.

While the GLBA only specifies a risk assessment of physical and electronic customer data, financial institution examiners are looking for a consolidated risk assessment of all systems that transfer, process, or store electronic data.

From these factors we found the need to develop a risk assessment process for electronic systems that filled the following requirements:

- fulfills the GLBA requirements
- is comprehensive but of reasonable effort
- is easy to understand and explain
- determines residual risk for each system based on data classification, vulnerabilities, and controls
- allows each year's assessment process to build on previous year effort

The process can be useful for any institution for the following reasons:

- It is easy for others to duplicate
- It is flexible to be customized for different organizations' needs
- It is generic enough to be used "out of the box" for many organizations

Before

Process Foundation

The process we developed very closely follows the Information Security Risk Assessment recommendations found in the FFIEC Information Technology Examination Handbook:[2]

- Obtain listings of information system assets (e.g., data, software, and hardware). Inventories on a device-by-device basis can be helpful in risk assessment as well as risk mitigation. Inventories should consider whether data resides in house or at a TSP.

- Determine threats to those assets, resulting from people with malicious intent, employees and others who accidentally cause damage, and environmental problems that are outside the control of the organization (e.g., natural disasters, failures of interdependent infrastructures such as power, telecommunications, etc.).

---

[1] "Interagency Guidelines Establishing Standards for Safeguarding Customer Information." February 1, 2001. <http://www.ffiec.gov/exam/InfoBase/documents/02-joi-safeguard_customer_info_final_rule-010201.pdf> (March 6, 2003)

[2] "Information Security Booklet". *FFIEC Information Technology Examination Handbook.* February 2003 <http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html> (March 6, 2003)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Identify organizational vulnerabilities (e.g., weak senior management support, ineffective training, inadequate expertise or resource allocation, and inadequate policies, standards, or procedures).
- Identify technical vulnerabilities (e.g., vulnerabilities in hardware and software, configurations of hosts, networks, workstations, and remote access).
- Document current controls and security processes, including both information technology and physical security.
- Identify security requirements and considerations (e.g., GLBA).
- Maintain the risk assessment process requires institutions to review and update their risk assessment at least once a year, or more frequently in response to material changes in any of the six actions above.

Process Steps and Implementation Considerations

The process described below could be done manually for a small, simple network. However, the scope of the process makes it well worth the effort to automate. One way to automate is to store the data and perform the calculations in a relational database. A possible relational database schema is shown in Appendix B.

Process Overview
1. Determine data classification categories
2. Inventory Systems
3. Classify Data
4. Determine Initial Risk of each system

Vendor Services:
Manage the vendor following a vendor management policy appropriate to their initial risk tier.

Technologies:
5. Group Technologies
6. List vulnerabilities and threats for each system
7. List controls for each vulnerability or threat
8. Classify controls
9. Determine adequacy of controls
10. Determine Residual Risk
11. Generate reports
12. Report results to corporate leadership
13. Repeat annually

During

Step 1. Determine Data Classification Categories

The type of data that a system stores, processes, or transmits determines how critical that system is. Developing classification factors for data helps to determine which

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

systems put the company at a higher risk. Be sure to include classification factors that specify rate the importance of security, reliability, and availability of the data.

Sample classification factors are shown below.

Data Classification Factors

1	Contains non-public personal information about our customers as defined in the GLBA privacy regulations.
2	Contains bank, employee, or customer information that should be restricted to a limited number of our employees.
3	Contains bank, employee, or customer information that should be restricted from non- employees.
4	Contains information that is relied upon for risk management or decision making purposes
5	Contains information that could be altered or tampered with for fraudulent purposes
6	Contains information that could be altered or tampered with for financial gain
7	Contains information that is critical to the our internal operations
8	Contains information that is critical to our ability to service our customers.

Step 2. Inventory Systems

The next step is to generate a list of all systems in use that store, process, or transmit data. The systems list should include hardware, software, and vendor provided services.

At this stage indicate whether the system is a *technology* or a *vendor service*. In this context, a technology is a system for which you have control over the security, integrity, or availability. This normally involves systems managed locally such as server hardware, backup tapes, local databases, and desktop applications. A vendor service is any system for which the vendor has access to the data, or for which you rely on the vendor for integrity or availability. Examples of vendor services include cellular phones, a news or stock feed, or a third party data mining service.

It is important to note that some systems will be both a technology and a vendor service. For example, a Frame Relay line between two corporate sites would be considered a vendor service because we rely on the vendor to keep the line secure and available. However, we have some control over the security in that we can encrypt data before sending it through the line.

Sample Inventory List

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

ID	System	Technology	Vendor
1	Internet T-1		X
2	Network Switches	X	
9	Corporate Mail Server	X	
10	Accounting File Server	X	
11	Backup Server	X	
12	Help Desk Application Server	X	
13	HR File Server	X	
14	Maintenance File Server	X	
15	Marketing Customer Data Mining Service		X
16	Supplier Extranet - Frame Relay	X	X
18	Palm Pilots	X	

Step 3. Classify Inventoried Systems

At this time, indicate which classification categories each technology or vendor service. It may be possible to delegate this responsibility to the appropriate system administrators or vendor relationship managers.

One way to make this step clearer for system administrators and relationship managers is to develop questions for people to ask to determine if a specific category is true for a system.

Some example questions:

- If an attacker gained control of this system, would he have access to customer information? If yes, then the system falls into category 1.
- If this system were unavailable, would we still be able to complete our internal operations? If no, then the system falls into category 7.
- If this system were unavailable, would we still be able to service our customers? If no, then the system falls into category 8.

Sample Data Classification

	GLBA Protected	Restricted to limited employees	Restricted from non-employees	Risk management decision making	Altered for fraud	Altered for financial gain	Critical to operations	Critical to customer service
System	**Cat 1**	**Cat 2**	**Cat 3**	**Cat 4**	**Cat 5**	**Cat 6**	**Cat 7**	**Cat 8**
Internet T-1	X	X	X	X	X	X	X	X
Network Switches	X	X	X	X	X	X	X	X
Corporate Mail Server	X	X						
Accounting File Server	X	X	X	X	X	X	X	
Backup Server	X	X	X	X	X	X	X	X
Help Desk Application Server		X	X					
HR File Server		X	X		X	X	X	
Maintenance File Server		X	X					

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Marketing Customer Data Mining Service	X	X	X	X				
Supplier Extranet - Frame Relay		X	X	X	X		X	
Palm Pilots		X	X					

Step 4. Determine Initial Risk of inventoried systems

First create definitions for "Initial Risk". These definitions should be based on which data classification categories the system falls into.

Being a financial services company, reputation and compliance are among our highest priorities. We determined the attributes of our initial risk categories based on this:

Highest Initial Risk
Failure or compromise of this technology or vendor
- Can cause disclosure of private customer information
- Can cause us not to stay in compliance
- Can cause significant impact on the reputation of the company

Highest Initial Risk
Failure or compromise of this technology or vendor
- Can prevent us from doing business for an unacceptable period of time.
- Can cause significant impact on the reputation of the company
- Can cause significant financial loss for the company

Medium Initial Risk
Failure or compromise of this technology or vendor
- Can cause degraded service to our customers
- Can delay internal operations for a short period of time
- Can minimally impact reputation
- Can cause a small to medium financial loss for the company

Low Initial Risk
Failure or compromise of this technology or vendor will not cause the conditions indicated above.

Correlating the data classification to the attributes above, we find that our Initial Risk definitions based on the data categories are as follows:

Tier 1: Highest Risk
Any system containing **Category 1** data (GLBA protected customer information)

Tier 2: High Risk
Any system containing **Category 7** data (critical to operations) or **Category 8** data (critical to customer service).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Tier 3: Medium Risk
Any system containing data in **Categories 2 through 6**

Tier 4: Low Risk
Any system that does not fulfill any of the classification categories

Each institution will need to define its own initial risk tiers.

- A research laboratory may rank restricting research data from competitors above customer service or customer privacy.
- A news website, such as cnn.com, may rank customer service (uptime) or accuracy most highly

Apply the definitions to the classified systems to develop the table below.

Sample Initial Risk Determination

		GLBA Protected	Restricted to limited employees	Restricted from non-employees	Risk management decision making	Altered for fraud	Altered for financial gain	Critical to operations	Critical to customer service
System	Initial Risk	**Cat 1**	**Cat 2**	**Cat 3**	**Cat 4**	**Cat 5**	**Cat 6**	**Cat 7**	**Cat 8**
Internet T-1	Tier 1 - Highest	X	X	X	X	X	X	X	X
Network Switches	Tier 1 - Highest	X	X	X	X	X	X	X	X
Corporate Mail Server	Tier 1 - Highest	X	X						
Accounting File Server	Tier 1 - Highest	X	X	X	X	X	X	X	
Backup Server	Tier 1 - Highest	X	X	X	X	X	X	X	X
Help Desk Application Server	Tier 3 - Medium		X	X					
HR File Server	Tier 2 - High		X	X		X	X	X	
Maintenance File Server	Tier 3 - Medium		X	X					
Marketing Customer Data Mining Service	Tier 1 - Highest	X	X	X	X				
Supplier Extranet - Frame Relay	Tier 2 - High		X	X	X	X		X	
Palm Pilots	Tier 3 - Medium		X	X					

Different processes for technologies and vendor services

At this point, the process diverges for technologies and vendor services. For systems which are solely vendor services, it is important to perform the data classification consistent with the technologies that are managed internally. However, there is not much value in performing and vulnerability and control assessment on vendor services, since we rely on the vendor for the security of those systems.

Vendor management is an integral part of the data security. While this paper will not cover vendor management, one possibility way to correlate vendor management with

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

the rest of your risk management process is to create Tier 1, Tier 2, and Tier 3 vendor management policies to correlate with the Tier 1, Tier 2, and Tier 3 risk ratings that are assigned to those vendors.

The rest of the process described here will deal only with technologies, or those systems for which we have control over the security, availability, and integrity.

Step 5. Group Technologies

To reduce the effort of the risk assessment process by eliminating redundancies, group technologies that are similar in such a way that they will have the same vulnerabilities. For example, all databases on the private network will have basically the same vulnerabilities. Instead of specifying all those vulnerabilities for each database, we will group the database and then relate the vulnerabilities to the group.

There is a trade-off here. A more generic group, such as "all databases on the private network" will include more systems, and result in less work when we list and relate vulnerabilities. More specific groups, such as "Oracle databases on the private network" and "MS SQL databases on the private network" will provide more accuracy, but will also result in more work.

Grouping technologies provides large gains in terms of reducing the effort, but it also adds error to the system. As time and needs allow, you can "fine tune" the technology groups to make them more specific and increase the accuracy to an acceptable level.

Sample Technology Groups

ID	System	Group
1	Internet T-1	Internet Connections
2	Network Switches	Network Infrastructure
9	Corporate Mail Server	Mail Servers
10	Accounting File Server	NT File Servers
11	Backup Server	Backup Servers
12	Help Desk Application Server	Application Servers
13	HR File Server	NT File Servers
14	Maintenance File Server	NT File Servers
16	Supplier Extranet - Frame Relay	Extranet
18	Palm Pilots	Handhelds

Step 6. Identify Vulnerabilities and Threats

List each vulnerability or threat, and indicate which technologies could be compromised.

Sample vulnerability and threat assignment for the technology "NT File Servers"

Vulnerability	Affects NT File Servers?
Capture and decryption of secured data transmissions	
DNS/Website spoofing	

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Dormant user accounts	X
Downloading infected software from Internet	
Email viruses	
Hardware failure of desktops	
Hardware failure of servers	X
Incomplete/Non existent backups	X
Infected Software or Disks on Webservers	
Infected software or disks on Clients	
Infected software or disks on Servers	X
Internet Denial of Service Attack	
IP Spoofing	
Listening Services/Open ports on internal systems	X
Listening Services/Open ports on webservers	
Malicious employee	X
OS/Software installation and patches corrupting data or breaking functionality	X
Password Cracking	X
Password sniffing - Internet	
Password sniffing - Private network	
Physical access to un-secured logged in terminal	X
Power failure	X
Social Engineering	
Unpatched Operating Systems and software -desktops	
Unpatched Operating Systems and software -servers	X
Unprotected shares and trust relationships	
Vulnerable CGI Programs	
Weak passwords/Password Guessing	X
Website defacement of DMZ servers	
Website defacement of Internet Servers	
Wireless access compromise	
Worm or other self-propagating virus	X

Vulnerabilities of “hardware failure of desktops” and “hardware failure of servers” are shown separately above. Originally this was listed as just “hardware failure”, however when I went to relate controls, I found that we had controls in place for servers, such as redundant disks and power supplies, that we did not have for desktops. This is another area where error is added to the system, the best way to limit it is to make the vulnerabilities more specific. As you are entering vulnerabilities and controls, you can go back and fine tune (such as I did by splitting hardware failure into two separate vulnerabilities) until you are satisfied with the level of accuracy.

Step 7. Identify Controls

List all of the controls that are in place and indicate which vulnerabilities or threats they impact.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Sample Controls List for the vulnerability "Weak Passwords/Password Guessing"

Control	Mitigates Weak Passwords/Password Guessing?
128 bit encryption on Internet communications	
Account and user rights management	
Authentication event logging	**X**
Authentication required on WAP Dial-up and VPN	
Awareness and appropriate configuration	
Backup generator	
Backup monitoring systems	
Backup policies and procedures	
Backup systems	
Border router access control lists	
Change default passwords	
Close port 80 into service network	
DNS Monitoring	
Desktop Antivirus	
Desktop Antivirus Consolidated Management	
Desktop software installation policy	
Disable or re-name default user accounts	
Disaster Recovery Contract	
Email Antivirus	
Email attachment filtering by file type	
Encryption required on WAP	
Enhanced DNS Monitoring	
Firewall	
HP Openview Monitoring	
Hardware redundancy	
Incident Response Process	**X**
Internet use policy	
Intrusion Detection System	
Locked/logged out servers	
Logfile Monitoring	
Modem pool to limit use of desktop modems	
Multiple locations	
NAT with non-routable addresses	
No Unattended/automatic patch installations	
No use of Remote Services utilities	
Off-site storage	
Periodic forced password changes	**X**
Physical access controls	
Policies against end users setting up WAPs	
Policies to install only necessary services	
Redundant Internet connection	
Redundant systems	
Risk/Testing/Migration/Recovery plan for system installs and upgrades	
Router ACLs	
SMTP Gateway in DMZ	

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

SSL with signed certificates for secure web services	
Security Patch Application	
Security considered when developing programs	
Server Antivirus	
Service Pack/Security Patch Tracking system	
Website content monitoring	
Strong password enforcement	X
Switched Network	
Terminated employee process	
Test lab	
Tier 1 ISP (UUNet)	
Integrity Checking software	
Trust relationships enforced by encrypted passwords	
UPS	
User account monitoring	
User training	X
WAN Provider agreements	
Web server NTFS permissions	
Web server application not running as admin	

Step 8. Indicate whether controls are preventative, detective, corrective, or directive

To adequately control a threat or vulnerability, you need to have tools or processes in place to prevent a compromise from occurring, tools or processes in place to detect and alert you if a compromise has occurred, and tools or processes in place to allow you to recover from a compromise quickly and prevent future occurrences.

Here are the definitions we use to determine which of these categories a control falls into:[3]

Preventative Control - system or technology whose purpose is to prevent an attack attempt or exploit from being successful. Also a system or technology whose purpose is to prevent a hardware failure from impacting service. Examples of preventative controls include: Strong passwords, firewalls, clustered servers, physical access restrictions, and encryption.

Detective Control - system or technology whose purpose is to detect an attack, compromise, or hardware failure and alert an administrator in an appropriate time frame. Examples of detective controls include Intrusion Detection Systems, physical security systems, Centralized management tools, SNMP, automated logfile monitoring, content monitors, virus scanners, and integrity checkers.

Corrective Control - system or technology that enables us to better respond to and recover from an incident, as well as prevent future occurrences. Corrective controls

[3] "Control Types for Information Security". *Computer Operations Security*. <http://www.peacefulpackers.com/it_solutions/xisa0703.htm> (April 6, 2003)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

include incident response programs and systems that record activity, events, or changes for future research.

Directive - The control requires an end user or vendor to follow a policy or contract for it to be effective. We cannot control whether users or vendors follow policies, so policy controls are documented, but are not used in control adequacy calculations. If the policy only applies to IT personnel (such as a policy to disable default user accounts on servers) and I am confident and can verify that the IT personnel are following the policy, then I would not mark it as a policy control because it is effective in mitigating risk.

Note that many controls will fall into more than one category.

Sample of Categorizing Controls

ID	Control	Prevention	Detection	Correction	Direction
1	128 bit encryption on Internet communications	X			
2	Account and user rights management	X			
3	Authentication event logging			X	
4	Awareness and appropriate configuration	X			X
5	Backup generator	X			
6	Backup monitoring systems		X	X	
7	Backup policies and procedures	X			X
8	Backup systems	X			
9	Border router access control lists	X			
10	Change default passwords	X			
11	Close port 80 into service network	X			
12	Desktop Antivirus		X	X	
13	Desktop Antivirus Consolidated Management	X	X	X	
14	Desktop software installation policy	X			X

Step 9. Determine Control Adequacy

At this step determine definitions for “Control Adequacy” in terms of Strong, Adequate, or Weak. We developed different definitions based on the Initial Risk Tier. We found that what is an adequate level of control for medium or low risk systems may not be adequate for higher risk systems.

To come up with our definitions, we first developed an abstract statement regarding what we believe constitutes a strong, adequate, or weak level of control. We then applied this abstract statement to the control categories of preventative, detective, and corrective, to produce “definitions” by which we can calculate the adequacy of the level of control.

Sample Control Adequacy Definitions

Higher Risk Systems (Tier 1 and Tier 2)

Strong

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- In the abstract, assumes layered security, a reliable means for detecting and alerting to a compromise or failure, a means for tracking events and changes or researching past events, and a process to respond, recover, and prevent future occurrences.
- For a given vulnerability, there exists
  - at least two layers of preventative controls which directly prevent exploit of this vulnerability
  - at least one detective control which will reliably detect an exploit of this vulnerability in a very short time
  - at least two corrective controls which will improve our ability to respond, recover, and prevent future occurrences

Adequate

- In the abstract, assumes there is a control in place preventing every threat or vulnerability from being successful, as well as a means for detecting and responding to compromise or failure.
- For a given vulnerability, there exists
  - at least two preventative controls which directly prevent exploit of this vulnerability
  - at least two corrective controls which will improve our ability to respond, recover, and prevent future occurrences

    OR
  - at least one preventative control which directly prevents exploit of this vulnerability
  - at least one detective control which will reliably detect an exploit of this vulnerability
  - at least two corrective controls which will improve our ability to respond, recover, and prevent future occurrences

Weak

Does not meet the criteria above

<u>Medium-Low Risk Systems (Tier 3 and Tier 4)</u>

Strong

- In the abstract, assumes layered security, a reliable means for detecting and alerting to a compromise or failure, a means for tracking events and changes or researching past events, and a process to respond, recover, and prevent future occurrences.
- For a given vulnerability, there exists
  - at least two layers of preventative controls which directly prevent exploit of this vulnerability
  - at least one detective control which will reliably detect an exploit of this vulnerability
  - at least one corrective controls which will improve our ability to respond, recover, and prevent future occurrences

    OR
  - at least two layers of preventative controls which directly prevent exploit of this vulnerability
  - at least two corrective controls which will improve our ability to respond, recover, and prevent future occurrences

Adequate

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- In the abstract, assumes there is a control in place preventing every threat or vulnerability from being successful, as well as a means for detecting or responding to and correcting compromise or failure.
- For a given vulnerability, there exists
  - at least one preventative controls which directly prevents exploit of this vulnerability
  - at least one detective control which will reliably detect an exploit of this vulnerability
  - at least one corrective controls which will improve our ability to respond, recover, and prevent future occurrences

    OR
  - at least one preventative control which directly prevents exploit of this vulnerability
  - at least two corrective controls which will improve our ability to respond, recover, and prevent future occurrences

Weak
Does not meet the criteria above

Here is the calculation for "**Hardware Failure of Servers**" as it affects the Accounting File Server.

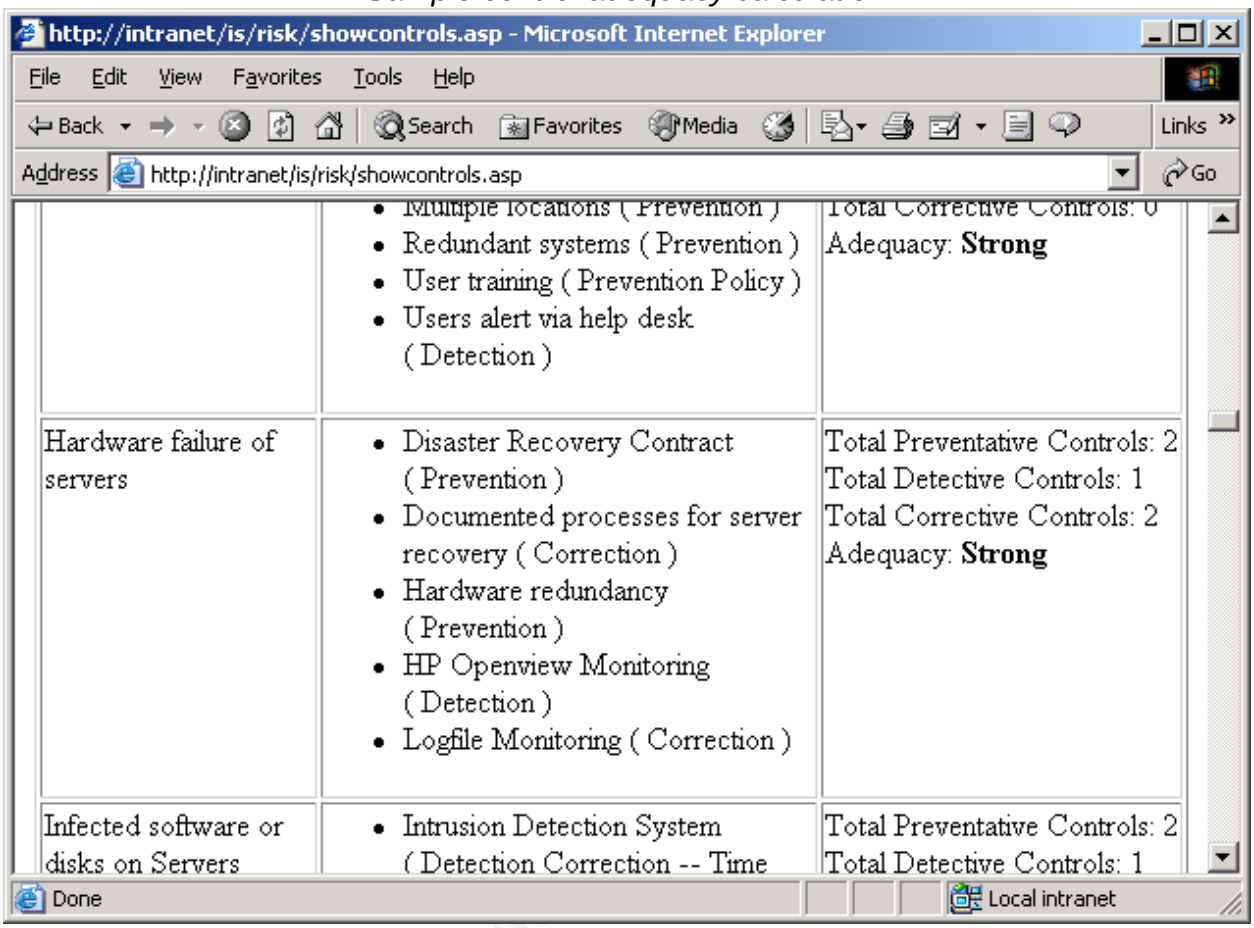
The accounting file server is a "Tier 1 - highest risk" system.
For this vulnerability, there are:
- two preventative controls (Hardware redundancy, and a third part Disaster Recovery contract)
- one detective control (HP Openview will send an alert on hardware failure)
- two corrective controls (Logfiles allow us to track and determine cause of failures, and documented recovery processes allow us to recover quickly)

Applying the logic for control adequacy calculation, this results in a **Strong Control Adequacy** of our protection against server hardware failure.

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Sample control adequacy calculation



http://intranet/is/risk/showcontrols.asp - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://intranet/is/risk/showcontrols.asp

	• Multiple locations (Prevention) • Redundant systems (Prevention) • User training (Prevention Policy) • Users alert via help desk (Detection)	Total Corrective Controls: 0 Adequacy: **Strong**
Hardware failure of servers	• Disaster Recovery Contract (Prevention) • Documented processes for server recovery (Correction) • Hardware redundancy (Prevention) • HP Openview Monitoring (Detection) • Logfile Monitoring (Correction)	Total Preventative Controls: 2 Total Detective Controls: 1 Total Corrective Controls: 2 Adequacy: **Strong**
Infected software or disks on Servers	• Intrusion Detection System (Detection Correction -- Time	Total Preventative Controls: 2 Total Detective Controls: 1

Done Local intranet

Step 10. Determine Residual Risk

Create definitions for residual risk based on the Initial Risk Tiers and the Control Adequacy. The residual risk definitions are in terms of **High** residual risk, **Moderate** residual risk, and **Low** residual risk. We use a "weakest link" philosophy, if there is even one weakly controlled vulnerability for a technology, then that technology has weak controls overall. For a technology to have strong controls overall, every vulnerability must be strongly controlled.

Residual Risk Rating Definitions

<u>High Residual Risk</u>

- Any system of Tier 1 (Highest) , Tier 2 (High), or Tier 3 (Medium) Initial Risk with Weak controls to threats and vulnerabilities

<u>Moderate Residual Risk</u>

- Any system of Tier 1 (Highest) or Tier 2 (High) Initial Risk with Adequate controls to threats and vulnerabilities

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Any system of Tier 4 (Low) Initial Risk with Weak controls to threats and vulnerabilities

Low Residual Risk

- Any system (Tier 1 through 4) Initial Risk with Strong controls to threats and vulnerabilities
- Any system of Tier 3 (Medium) or Tier 4 (Low) Initial Risk with Adequate controls to threats and vulnerabilities

This may be more clearly understood in the following table.

Residual Risk Matrix

	Tier 1 (Highest) Initial Risk	Tier 2 (High) Initial Risk	Tier 3 (Medium) Initial Risk	Tier 4 (Low) Initial Risk
Strong Controls	Low Residual Risk	Low Residual Risk	Low Residual Risk	Low Residual Risk
Adequate Controls	Moderate Residual Risk	Moderate Residual Risk	Low Residual Risk	Low Residual Risk
Weak Controls	High Residual Risk	High Residual Risk	High Residual Risk	Moderate Residual Risk

After

Step 11. Apply definitions and logic to the data and create reports

Once your correlate all the data, you fill find that a great deal of information is generated. We created a web interface to display and navigate the data.

Sample Technologies Summary Report

System	Initial Risk	Control Adequacy	Residual Risk
Internet T-1	Tier 1 - Highest	Strong	Low
Network Switches	Tier 1 - Highest	Adequate	Moderate
Corporate Mail Server	Tier 1 - Highest	Adequate	Moderate
Accounting File Server	Tier 1 - Highest	Adequate	Moderate
Backup Server	Tier 1 - Highest	Adequate	Moderate
Help Desk Application Server	Tier 3 - Medium	Weak	High
HR File Server	Tier 2 - High	Strong	Low
Maintenance File Server	Tier 3 - Medium	Strong	Moderate
Supplier Extranet - Frame Relay	Tier 2 - High	Weak	High
Palm Pilots	Tier 3 - Medium	Adequate	Moderate

This screen shows each system, its initial risk, overall control adequacy, and calculated residual risk. If you click on the technology name, you can drill down and get the detail report showing how the Initial Risk, Control Adequacy, and Residual Risk ratings were calculated.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Sample Technology Detail Report

http://intranet/is/risk/bigreport2.asp?Technology=Email and scheduling (Microsoft Exchan...

File Edit View Favorites Tools Help Links »

Technology:	**Email and scheduling (Microsoft Exchange/Outlook)**
Provided By:	**Microsoft**
Type:	Transmitting
Initial Risk:	Medium
Calculated Residual Risk:	Low

Has the following attributes:
Contains bank, employee, or customer information that should be restricted to a limited number of our employees.
Contains bank, employee, or customer information that should be restricted from non-employees.
Contains information that is relied upon for risk management or decision making purposes
Contains information that could be altered or tampered with for fraudulent purposes
Contains information that could be altered or tampered with for financial gain.
Contains information that is likely to be specifically targeted by attackers (either internal or external)
Contains frequently changing data that cannot be re-created from other sources (Intra-day data loss is a concern)

Vulnerability	Controls	Adequacy
Dormant user accounts	• Account and user rights management (Prevention) • Authentication event logging (Correction) • Enhanced User Account and	Total Preventative Controls: 2 Total Detective Controls: 1 Total Corrective Controls: 2 Adequacy: **Strong**

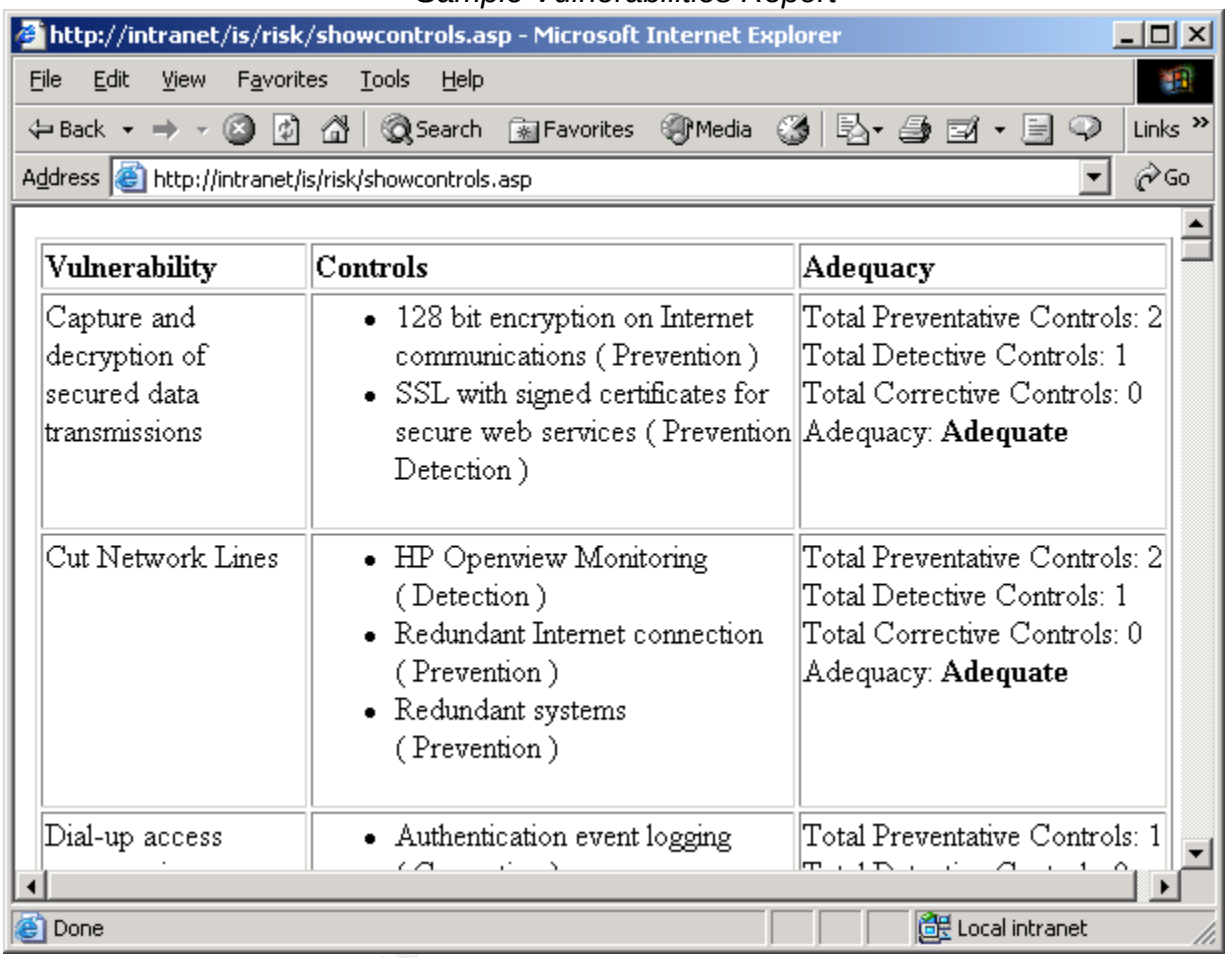
Done Local intranet

This view is available for every technology. In this case is shows an Initial Risk of Medium and a Residual Risk of Low. It lists the characteristics of the system, and then lists each vulnerability, the corresponding controls, and the control adequacy calculation. Our system also records and displays the vendor of the technology, as well as the type of service (Storage, Processing, or Transmitting), but these factors are not used in the risk calculations.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Another useful report we generate lists each vulnerability in the system the corresponding controls, and the control adequacy calculation. This report is useful in summarizing where security weaknesses lie.

Sample Vulnerabilities Report



Vulnerability	Controls	Adequacy
Capture and decryption of secured data transmissions	• 128 bit encryption on Internet communications (Prevention) • SSL with signed certificates for secure web services (Prevention Detection)	Total Preventative Controls: 2 Total Detective Controls: 1 Total Corrective Controls: 0 Adequacy: **Adequate**
Cut Network Lines	• HP Openview Monitoring (Detection) • Redundant Internet connection (Prevention) • Redundant systems (Prevention)	Total Preventative Controls: 2 Total Detective Controls: 1 Total Corrective Controls: 0 Adequacy: **Adequate**
Dial-up access	• Authentication event logging	Total Preventative Controls: 1

Step 12. Report results to corporate leadership

GLBA requires annual reporting to corporate leadership of
- status of information security program
- compliance with Interagency Guidelines
- risk assessment
- risk management and control decisions
- service provider arrangements
- security violations and management response
- recommendations for changes to the info security program[4]

[4] "Interagency Guidelines Establishing Standards for Safeguarding Customer Information." February 1, 2001. <http://www.ffiec.gov/exam/InfoBase/documents/02-joi-safeguard_customer_info_final_rule-010201.pdf> (March 6, 2003)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Step 13. Review and update at least yearly

The structure of this risk assessment process allows you to build on the previous years' results rather than start over from scratch each year. The extra time saved by not repeating the effort can be used to "fine tune", or make the groups and vulnerabilities more specific to obtain more accurate results.

You can also add technologies, vulnerabilities, and controls throughout the year as changes are made within the corporation, and then regenerate the reports to determine how overall risk has been impacted.

Enhancement Possibilities

What-If Scenarios
The system could be used to evaluate the impact of new technologies on overall risk. During vendor selection or a technology implementation for a new system or service, enter the system into the risk assessment process, categorize the data, relate the vulnerabilities and controls, and display how the overall risk has changed.
It would also be beneficial to evaluate new security controls in this way. By putting a security control into the system, you can show which vulnerabilities or threats it impact, and which technologies or systems it impacts.

You could also do what-if scenarios for new vulnerabilities. When a new vulnerability is identified, enter it into the system and relate it to the appropriate technologies and controls. Then view the reports to see how the Residual Risk Level has changed.

One enhancement to the system that would make "what if" scenarios easier would be the ability to take a "snapshot" of the state of the system before applying changes such as new technologies, vulnerabilities, and controls. After the changes are made, the new state could be compared to the snapshot programmatically, generating a new report only showing those things that changed.

Include Physical Security
GLBA requires that your electronic data security program be coordinated with your physical data security program. It could be possible to extend the structure outlined above to include physical security. This will likely involve developing new control adequacy definitions to support physical security controls, but many other aspects would likely need to change very little.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Appendix A: Automation Tools

http://www.johnsonintl.com/SANS/Risk

SANS *Audit & Security Controls that Work* Presentation on the risk assessment process
400 KB Microsoft Powerpoint
This presentation was given at the SANS Audit & Security Controls that Work conference, April 5 2003. It walks through the risk assessment process described above.

Sample Inventory Worksheet
28 KB Microsoft Word
This template can be provided to IT support personnel, system administrators, and vendor relationship managers to develop an inventory of systems in use and the type of data each system has access to.

Sample Risk Assessment Database
450 KB Microsoft Access
This database shows how the process can be automated. It allows for definition of the logic to be used in the process, entry of inventory and data classifications, entry of vulnerabilities and controls, specifying the relationships between systems, vulnerabilities, and controls, and finally generation of reports.

Sample Inventory and Classification Report
4 KB PDF Document
This report shows the systems and associated data classification categories, as well as the Initial Risk Rating of each system.

Sample General Control Adequacy Report
36 KB PDF Document
This report shows each vulnerability or threat, all the controls in place to prevent exploitation of each vulnerability, and whether that vulnerability is Strongly, Adequately, or Weakly controlled.

Sample System Summary Report
3 KB PDF Document
This report shows each system, the calculated Initial Risk Rating, the weakest Control Adequacy for vulnerabilities affecting that system, and the resulting Residual Risk based on the Initial Risk and Control Adequacy.

Sample System Detail Report
40 KB PDF Document
For each system, this report shows classification categories, vulnerabilities, controls, and the calculated Initial and Residual Risk Ratings.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Appendix B. Relational Database Design

Definition Files:

tblClassificationCategories
classificationCategoryID
classificationCategoryName

tblTiers
tierID
tierName

tblClassificationTierRelationship
classificationID
tierID

tblControlAdequacyMatrix
tierID
minimumPreventativeControls
minimumDetectiveControls
minimumCorrectiveControls
resultingControlAdequacy

tblResidualRiskMatrix
tierID
controlAdequacy
resultingResidualRisk

Data Files:

tblSystemsList
systemID
systemName
technologyGroupID

tblSystemsClassification
systemClassificationID
isCategory1
isCategory2
isCategory3
…
isCategoryN

tblTechnologyGroups
technologyGroupID
technologyGroupName

tblVulnerabilities
vulnerabilityID
vulnerabilityName

tblTechnologyGroupRelateVulnerabilities
technologyGroupRelateVulnerabilityID
technologyGroupID
vulnerabilityID

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

tblControls
controlID
controlName
isPreventative
isDetective
isCorrective
isPolicy

tblVulnerabilitiesRelateControls
vulnerabilityRelateControlID
vulnerabilityID
controlID

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Appendix C. REFERENCES

"Control Types for Information Security". *Computer Operations Security*. <http://www.peacefulpackers.com/it_solutions/xisa0703.htm> (April 6, 2003)

"Interagency Guidelines Establishing Standards for Safeguarding Customer Information." February 1, 2001. <http://www.ffiec.gov/exam/InfoBase/documents/02-joi-safeguard_customer_info_final_rule-010201.pdf> (March 6, 2003)

"Information Security Booklet". *FFIEC Information Technology Examination Handbook.* February 2003 <http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html> (March 6, 2003)

OCC2001-35 Examination Procedures to Evaluate Compliance with the Guidelines to Safeguard Customer Information. Office of the Comptroller of Currency. <http://www.occ.treas.gov/ftp/bulletin/1002-35a.pdf> (March 6, 2003)

"Interagency Guidelines Establishing Standards for Safeguarding Customer Information." February 1, 2001. <http://www.ffiec.gov/exam/InfoBase/documents/02-joi-safeguard_customer_info_final_rule-010201.pdf> (March 6, 2003)

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 24th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced