# Global Information Assurance Certification Paper

GSEC Certification Practical Assignment
GSEC v.1.4b Option 2 – Case Study in Information Security

**EVOLUTION OF A WRITTEN INFORMATION SECURITY PROGRAM**

Bill Havlin
January 7, 2003

## Introduction

The Gramm-Leach-Bliley Act (GLBA) was enacted as Public Law No: 106-102 on November 12, 1999. Financial institutions were given until July of 2001 to gain compliance with the act. However, when the financial institution where I am employed underwent a routine examination performed by the Federal Reserve Board in August 2002, it became apparent that we had overlooked a critical section of this legislation. According to the Federal Examiners conducting the Examination, this was a fairly common occurrence among the financial institutions they had recently reviewed. Title V, section 501b of the GLBA addresses the implementation of appropriate administrative, technical and, physical safeguards to ensure the protection of non-public, personal customer information. The purpose of this particular section of the GLBA was to ensure that financial institution customers were properly notified regarding how their private information was treated and that this information was appropriately safeguarded from unauthorized access.

Most financial institutions reacted quickly and appropriately to the privacy notification portion of this section of the act, however, many organizations apparently overlooked or simply failed to comply with the guidelines regarding the safeguarding of this information. In fact, the Legal department of my company had reviewed the legislation, prepared a privacy notification document, notified our customers of our practices, updated our Service Provider contracts, and felt that we had met the requirements of the GLBA appropriately. However, as we were preparing for a routine examination by the Federal Reserve Board, we realized that we had overlooked Section 501b of Title V of the GLBA regarding the establishment of a written Information Security Program.

This paper outlines the actions that were taken to develop a written Information Security Program compliant with the GLBA guidelines and how information security awareness was raised to a higher level within our organization during the process.

## How It All Started (Before)

When the GLBA was enacted, our organization did not have any specific focus on information security. Like most organizations, security measures were left to be instituted by Information Technology system administrators, developers, and Facilities management staff. Our Legal and Regulatory Compliance areas reviewed the GLBA legislation and the legal privacy notification information was developed accordingly. A plan to distribute this information to our customers was developed and a notification was added to our public website. As far as we were concerned, we had met our compliance obligations, according to our interpretation, well before the established deadline of July 1, 2001.

When the Federal Reserve Board notified us that they would be conducting a General Controls Examination of our company in the Fall of 2002 (including a review of GLBA compliance), we decided to review the requirements of the GLBA to make sure that we hadn't missed anything. It was at this time that we realized that we had, in fact, overlooked a key requirement of the GLBA regarding the implementation of an Information Security Program. In June of 2001, one month before full compliance was mandated, a project team was assembled to address the Information Security Program requirements. The project team seemed to be appropriately staffed with representatives from Information Technology, Human Resources, Legal, Training, and the business units, and they quickly determined that we needed to develop a written Employee Security Policy. Unfortunately, there was no clear owner or direction of the project, so the team struggled and eventually disbanded without completing any deliverables.

In October of 2001, I was appointed as the company's Information Security Officer in response to an internal audit recommendation and requirements of the GLBA. I was immediately tasked with completing the development of the Employee Security policies, which, at the time, we believed would fulfill the requirements of the GLBA.

My research into the GLBA requirements found that the Information Security Program referenced in the legislation was much more comprehensive than a simple Employee Security policy, and so I began to gather more information to develop an appropriate plan.

## Evolution of a Plan (During)

My first step was to gather as much information from the previous project team as I could find and begin to assimilate the information again. In conjunction with this, I needed to find out as much as possible regarding the GLBA requirements to ensure that the plan to be developed would be in compliance.

The information I gathered from the previous project team turned up a conglomeration of security policies and operational procedures. So, I hit the Internet to research what other companies had done to create an Information Security Program. Not surprisingly, I found a wide variety of solutions ranging from a short two-page outline of "acceptable use" to a multi-page, integrated web site covering virtually every aspect of information security. While this exercise resulted in a lot of good information, I unfortunately didn't find anything that I could easily modify to meet the needs of our organization.

So, I continued to review the information that I had gathered. It finally occurred to me that one of the challenges faced by the previous project team was that they were trying to develop a single, comprehensive document to address what appeared to me to be three separate areas:

- General Information Technology policies and procedures
- Information Security guidelines for employees
- An over-arching Information Security program

Now I was on to something! With this minor epiphany, I was able to organize the information I had into each of these three categories and, suddenly, I had some structure and meaning to the work at hand. Of course, this also meant that I had created three individual spin-off projects, but each of these had a much more defined purpose.

## Start with What You Know (During)

Since my background was in Information Technology and systems administration, I decided to tackle the Information Technology Policies and Procedures document first. A lot of the relevant information had already been gathered, so I just needed to organize the information in a sensible manner.

I won't spend a lot of time rehashing the development of this document. Suffice it to say that this was the most laborious task I encountered in the evolution of our Information Security Program. In order to complete this task I had to don my auditor's cap and conduct numerous interviews of all levels of Information Technology personnel. This actually proved to be a very valuable experience, as it helped me to better understand the myriad activities that occurred each day in the department. Consequently, by the time I had compiled a decent first draft of the document, many of the procedures had been modified based on the results of these discussions and the constantly changing technology environment. Keeping the document current on an on-going basis has proven to be a formidable task, but the addition of two staff members in the Fall of 2002 has proven considerably helpful.

The following is a summary of the different sections of the manual including a brief description of the contents. I offer this as a guideline for others to follow in developing a similar document.

**Information Technology** – This section includes an overview of the organization of the Information Technology department including organizational chart, job descriptions, and a generic diagram of our private network. The network diagram was intentionally stripped of specific addresses, product names, and vendor information. I find this diagram very useful to share with vendors and consultants to help them understand our network without divulging any compromising information.

**System Standards and Conventions** – This section outlines corporate naming conventions for network devices, servers, use accounts, etc. Workstation and server configuration standards are also covered here.

**Security Administration** – This section describes the manner in which the variety of security administration functions are performed within the department including the administration of user accounts, anti-virus software, intrusion detection system, physical access to the Data Center, UPS system, operational back-ups, etc.

**System Administration** – Included here is an overview of system and database administration procedures for each unique operating system and corporate application. Topics covered include performance monitoring, capacity planning, routine maintenance and procedures for evaluating and applying service packs, security patches, etc.

**Hardware and Software Asset Management** – This section describes procedures for asset requisition, maintenance, and tracking. Also covered in this section are guidelines for how product licensing, support, and vendor contracts are managed and maintained.

**System Development Life Cycle** – The various products and procedures used to ensure that programming changes are created, modified, tested, and promoted through development, testing, and production environments in a consistent and routine manner is covered in this section.

**Business Continuity and Disaster Recovery** – Business Continuity and Disaster Recovery are two very distinct, but related processes. This section helps to explain the differences between the two. Topics covered include system backup and restore procedures, annual testing procedures, and media storage guidelines.

**Technical Support** – The manner in which end-user technical support is requested, prioritized, escalated, and resolved is covered in this section.

The focus of this particular document is to describe the high-level policies and procedures that define the manner in which routine Information Technology functions are completed. This is not a step-by-step guide for completing these functions, but an overview of functions and their purpose.

While the creation of this document was a huge step forward for the Information Technology department, it represented only a small portion of the overall Information Security Program that was my ultimate goal. So, I turned my focus to the development of the Employee Security Policies document.

## Security Guidelines for Employees (During)

Stage two of the plan involved developing and distributing a document for employees outlining acceptable use of corporate resources and guidelines for security-conscious behavior. I knew the document would have to be both as brief as possible and as comprehensive as possible to ensure that all employees would actually take the time to read it and that it was a meaningful document.

There are a wide variety of resources available on this particular topic. The sources that I found most useful are listed in the references at the end of this paper. My final document was ten pages long, including the cover and acknowledgment pages. That was a little longer than I really wanted it to be, but I couldn't find anything that could be cut out.

Here, again, I offer a summary of the contents of the final product as an aid for others.

> **Introduction** – This section establishes that the purpose of the document is to provide guidance for employee behavior to ensure the privacy and integrity of confidential corporate and customer information as well as preserving the company's good name and investment in technology.
>
> **Responsibility and Accountability** – This section clearly identifies that the responsibility for understanding and following the security guidelines rests with each employee. Secondarily, management personnel are identified as the enforcers of the policy. This helps alleviate the roll of enforcement from the Information Security Officer.
>
> **Acceptable Use** – This section establishes guidelines for responsible and appropriate use of corporate resources and provides a reminder that their primary purpose is to conduct corporate business. Moderate personal use may be allowed as long as production systems or other employees are not impacted.

**System and Application Security** – This section outlines proper safeguarding of account access codes and passwords, establishes that the employee to whom an account is issued is responsible for all activity associated with account, and urges the creation of strong passwords.

**Remote Access** – This section addresses the manner in which employees can securely connect to corporate applications utilizing an Internet connection. Specific security software is required, including corporate anti-virus, desktop firewall software, and a corporate issued VPN account. Access from non-corporate equipment (home PC's) is not allowed.

**Virus Protection** – This section outlines the dangers of virus activity and how to respond if a virus is suspected to exist on a corporate resource.

**Internet and Electronic Messages** – This section reminds employees that e-mail is a privilege that can be revoked if used inappropriately. Employees are advised that e-mail is not necessarily encrypted and should not be used to transmit confidential customer or corporate information.

**Internet Based Messaging and File Sharing Systems** – This section outlines the dangers inherent with Instant Messaging systems and Peer-to-Peer file sharing systems on the Internet. Their use is expressly forbidden.

**Corporate Mailing Lists** – I had to throw in a little blurb here to remind employees to use corporate-wide mailing lists only for corporate business and only with management approval.

**Unauthorized Hardware and/or Software Modifications** – This section reminds employees that they should not install any hardware or software on their corporate computers without consulting the Information Technology department in order to avoid software conflicts and copyright violations.

**Copyrights and Software Licensing** – This section expands upon the previous section to remind employees that the company strongly adheres to all copyright and licensing agreements and that all contracts and licenses will be stored and managed by the Information Technology department.

**Information Maintenance** – This was one of the most difficult sections to write. It outlines how both physical and electronic data should be stored while it is useful and how it should be destroyed when it becomes no longer useful. The next revision of this document will include a data-classification model as well, which should help to better clarify the maintenance procedures.

**Physical Security** – This section reminds employees that they are responsible to ensure that confidential customer and corporate information, both physical and electronic, should be properly secured when not in use. Specific references to branch site procedures is also included here.

**Privacy Laws and Individual Rights** – The Legal department helped to write this clause which states that the company has the right to review any and all information passing through or stored on a corporate resource and that employees should have no expectation of privacy in this regard.

**Monitoring** – A follow-up to the previous section explaining that duly authorized representatives of the company can and will monitor e-mail, Internet, and other network activity. This section also outlines the proper procedures for management to follow to request copies of this information.

**Public Representations** – This section reminds employees that the Public Relations department must approve any public use of the corporate logo and/or any other representation on behalf of the company.

**Reporting Security Incidents** – A brief description of how to identify a security incident and a copy of our Security Incident Report form. This section also explains how to report an incident via our corporate Intranet site.

**Acknowledgment Page** – Finally, the acknowledgement page reminds the employee that by signing the document, they acknowledge that they have reading, understand, and agree to abide by the Security Policies and that they are aware of the consequences should they fail to abide by the guidelines.

Once I had completed the Employee Security Policies document, I had to find a way to distribute it to approximately 1,800 employees in thirty-eight states and somehow get all those signatures.

Since I had also been working on the development of an Information Security Awareness web site on our corporate Intranet, I decided to utilize this site to promote the newly developed employee security policies and to offer employees the ability to review and electronically acknowledge the document.

An e-mail message was distributed to all employees announcing the Employee Security Policies and included instructions on how to log-in to the website to review and acknowledge them. Our information security program was given additional merit through an endorsement from the CEO in his monthly Intranet address to employees.

At last, our Information Security Program was gaining some momentum! Unfortunately, the Federal Reserve Examiners were not satisfied with the few security-specific documents that we presented to them and the loosely organized security processes throughout the company, so they informed us that we really needed to put together a written document outlining a comprehensive information security program.

## Finally, a Written Information Security Program (During)

As mentioned, the Federal Reserve Examiners showed up for their review of our operations in August 2002. At this point, I had officially been in the role of Information Security Officer for nearly a year and the Privacy Team, responsible for developing and administering the Information Security Program, had been established for a little over one month. While we had made great strides in enhancing the security posture of our organization over the last year, the review by the Federal Reserve Examiners would be our first objective third-party audit.

The Federal Reserve review was quick, but painful. In the course of four days, the Federal Reserve Examiners conducted a very cursory review of our Information Technology and Security operations and were able to identify seven pages of concerns and recommendations. Compliance with Title V Section 501b of GLBA was only one of the eighteen concerns noted in their final report.

Fortunately, the Federal Reserve Examiners were very understanding and helpful and directed us to a couple of government web sites providing guidelines established by the Federal Reserve Board of Governors and other banking regulatory groups.

One of the more succinct and helpful references, was written by Michael J. Zamorski, Acting Director of the Federal Deposit Insurance Corporation (FDIC) in his March 14, 2001 Financial Institution Letter to Banking CEOs and Compliance Officers. Mr. Zamorski's letter noted that there were essentially four basic requirements outlined within Title V Section 501b of the GLBA:

***The guidelines also describe the oversight role of the institution's board of directors in this process and its continuing duty to evaluate and oversee the program's overall status. Institutions are required to:***

- ***identify and assess the risks that may threaten customer information;***
- ***develop a written plan containing policies and procedures to manage and control these risks;***
- ***implement and test the plan; and***
- ***adjust the plan on a continuing basis to account for changes in technology, sensitivity of customer information, and internal or external threats to information security.***

Using this information and several other documents from a variety of federal and legal resources, the following written Information Security Program was developed. I present the document in its entirety, followed by a discussion regarding how the process of developing this document enhanced the overall security process of our organization.

**PURPOSE OF THE PROGRAM**

It is the purpose of this program to outline the administrative, technical, and physical safeguard procedures designed to:

- Ensure the security and confidentiality of Irwin Mortgage customer information
- Protect against any anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

**ASSIGNMENT OF RESPONSIBILTY**

The Board of Directors has appointed the Privacy Team to be responsible for implementing and administering the Information Security Program. The Privacy Team consists of the Chief Information Officer, Senior Corporate Counsel, Lead Information Technology Counsel, and the Information Security Officer.

The Privacy Team will report to the Board annually with the overall status of the Information Security Program including:

- Current risk assessment, management, and control activities
- Service Provider arrangement concerns
- Overview and status of known security breaches, violations, or other concerns
- Summary results of security testing procedures
- Recommendations for program modifications or enhancements

**RISK ASSESSMENT**

A complete internal and external vulnerability assessment will be conducted on at least an annual basis. The annual assessment will be designed to identify technical and procedural vulnerabilities as well as the effectiveness of existing security policies and procedures.

Additionally, the Privacy Team will maintain a Corporate Risk Assessment Grid comprised of various anticipated risk factors, weighted with their forecasted probability, resulting in a calculated risk value for a variety of technology systems, procedures, and data sources. The Risk Assessment Grid will be reviewed and updated on a quarterly basis.

## RISK MANAGEMENT AND CONTROL PROCEDURES

The following security measures will be routinely employed to ensure the security, confidentiality, and integrity of all non-public customer and corporate information:

- All corporate applications will require individual user access controls and only specific access required to perform assigned duties will be granted.
- Security awareness issues will be communicated to all employees to reduce the probability of unauthorized individuals fraudulently gaining application access information.
- Physical security measures will be implemented at all locations where customer information is stored and at all corporate data center locations.
- Encryption technology will be employed any time confidential corporate or customer information is transmitted electronically.
- A change management process will be implemented to ensure that all production system modifications are consistent with the Information Security Program.
- Information systems will be actively monitored to detect actual or attempted attacks on or intrusion into customer system information systems.
- An incident response procedure will be implemented to outline specific actions to be taken when a suspected or actual security breach or unauthorized access of customer or confidential corporate information has occurred.
- Corporate business continuity and disaster recovery programs will be established and maintained.

## ROUTINE TESTING OF KEY CONTROLS, SYSTEMS, AND PROCEDURES

The effectiveness of the Information Security Program will be regularly evaluated and tested through the use of internal audits, external audits, and operational testing where appropriate.

The Privacy Team will ensure that all internal and external audits and Federal examinations are completed in a timely, accurate, and efficient manner.

Where possible and appropriate, security procedures will be tested and verified annually in a test or isolated environment.

## SECURITY TRAINING AND AWARENESS

The Privacy Team will endeavor to promote on-going information security awareness through the following channels:

- Distribution of Employee Security Policies manual to all employees requiring annual sign-off of agreement and compliance.
- Implementation of a security and privacy awareness Intranet web site including safeguarding customer data guidelines, incident reporting form, e-mail virus and hoax information, and other related topics.
- Regular articles published in the corporate newsletter.
- Information security bulletins distributed to all employees to address security policy modifications, security alerts, and other urgent security issues.

**OVERSIGHT OF SERVICE PROVIDERS**

The Privacy Team will ensure that due diligence is exercised in selecting Service Providers and will maintain appropriate supporting documentation for all major corporate Service Providers.

All Service Provider contracts will require that a corporate Confidentiality Agreement be signed. When appropriate, proof that the Service Provider has met the requirements of the Gramm-Leach-Bliley privacy act will be required. Acceptable forms of proof are Service Provider audit reports, SAS 70 reports, or summaries of other equivalent tests or evaluations.

**SECURITY PROGRAM EVALUATION AND ADJUSTMENT**

The Privacy Team will continually monitor, evaluate, and adjust the Information Security Program to account for technology changes, emerging vulnerabilities and threats, and any other relevant factors that may have an impact on the security or integrity of confidential corporate or customer information.

The above plan was submitted and approved by the Board of Directors at their October meeting. We finally had a GLBA-compliant Information Security Program, but were we really any better off because of it? I'll finish up with a review of how the process of developing a written information security plan did, in fact, increase the security posture of our organization.

## Lessons Learned – Improvements Made (After)

The written Information Security Program, in and of itself, did not create any greater security for our company. However, the yearlong process and evolution of the program afforded us the opportunity to review and examine the security environment of our company, which had had no previous specific focus on information security.

While researching the requirements of Section 501b of the GLBA and preparing for the review by the Federal Reserve Examiners, we had the opportunity to examine several aspects of our corporate security posture. Consequently, we were able to implement significant changes and enhancements based specifically on the guidelines provided in Section 501b of the GLBA as outlined below:

**PURPOSE OF THE PROGRAM**
**ASSIGNMENT OF RESPONSIBILTY**

These two sections of the Information Security Program allowed us to create and define two key roles responsible for establishing the direction and administration of our budding information security program.

The position of Information Security Officer was established, initially within the Technology Operations division of the Information Technology department. During the year, this position developed and grew into a stand-alone division reporting directly to the CIO and was afforded a staff of four employees.

Additionally, a corporate Privacy Team was established, consisting of members from Senior Management, Information Technology, Information Security and Legal departments.

The creation of these two groups coupled with the mandatory requirement of involvement from the Board of Directors allowed our company to take a serious look at our security posture and the ability to implement the necessary actions to mitigate identified risks.

## RISK ASSESSMENT

This requirement helped to bring a new perspective of risk assessment to the forefront of our company. Our previous actions in this regard relied primarily on internal auditors and our annual financial audit performed by a third party. The GLBA guidelines required that we take a more active approach and review both technological and procedural risks associated with the safeguarding of our confidential customer and corporate data.

This required us to conduct a full-scale vulnerability assessment of our public and private networks, which had never been considered in the past. This turned out to be both challenging and enlightening. Challenging in that we had to work closely with our vendor to ensure that the assessment produced a meaningful result with a prioritized action list. Enlightening in that we discovered several well-known vulnerabilities that we believed had been addressed by our current administrative procedures.

Additionally, the Privacy Team was able to develop a risk assessment grid listing a variety of “high-profile” information systems and security processes cross-referenced by associated risk factors. When weighted by their estimated probability of occurrence, this grid provides a prioritized listing of the company’s most probable information security risks.

## RISK MANAGEMENT AND CONTROL PROCEDURES

This was an area that we were pleasantly surprised to find already significantly in compliance with the GLBA guidelines. Many of the routine Information Technology system administration procedures already in place were identified in this section.

However, there were some key areas that we found lacking, specifically intrusion detection and security monitoring. Unfortunately, as our security initiatives were prioritized during the year, these were deemed less feasible due primarily to the financial and resource cost associated with their implementation. Conversely, funds were budgeted and these initiatives were made a priority for the following year.

## ROUTINE TESTING OF KEY CONTROLS, SYSTEMS, AND PROCEDURES

This was an area that we also found to be significantly in compliance with the GLBA guidelines. As a financial institution, we have always been subjected to various routine internal and external audits. However, the GLBA requirements will bring much more focus on reviewing security administration practices in addition to other routine Information Technology and financial reviews.

## SECURITY TRAINING AND AWARENESS

I believe that this particular section of the GLBA guidelines had the greatest impact on our organization. In order to fulfill this requirement several key activities and communication channels were implemented.

The announcements of the appointment of an Information Security Officer and the development of the Privacy Team were the first steps establishing the importance of information security to the company. This was followed up by additional e-mail notifications from the Information Security Officer regarding security guidelines for common issues and concerns.

The security focus of the company was given its greatest boost with an announcement from the CEO introducing an Information Security Awareness Intranet site and the distribution of the Employee Security policies.

Ongoing awareness is promoted through pertinent articles in the company monthly newsletter and occasional Information Security Bulletin e-mail reminders from the Information Security Officer.

## OVERSIGHT OF SERVICE PROVIDERS

As we reviewed our compliance with this section of the GLBA guidelines, we were somewhat surprised that our current measures were insufficient. Our legal department had addressed all contractual issues regarding the safeguarding of our customer information shared with Service Providers, but our internal management and oversight of these Service Providers and other contractors and vendors was lacking structure and consistency.

This was another area whose priority was shifted into the following year.

## SECURITY PROGRAM EVALUATION AND ADJUSTMENT

This final provision of the GLBA guidelines ties in very closely to the initial requirement of assigning responsibility for the program. As Information Security Officer and a key member of the Privacy Team, I will be responsible for ensuring that each of the objectives listed above is addressed, reviewed, and implemented appropriately.

## Conclusion

As I look back over what I have written here, I consider changing the title to "A Year in the Life of an Information Security Officer". The past year has been both challenging and exciting for me as I try to take my fifteen years of experience in Information Technology and System Administration and focus more keenly on Information Security.

My intent with this paper was to provide others who may find themselves in this situation, faced with developing a security posture within a company with no previous focus on security, an outline of the trials and successes that I faced. I believe that much of what was achieved in the course of the year is summed up in the written Information Security Program that we were required to develop to gain compliance with the GLBA.

I hope others find this helpful.

## References


"Bill Summary & Status for the 106th Congress". Thomas Legislative Information on the Internet. Library of Congress.
URL: http://thomas.loc.gov/cgi-bin/bdquery/z?d106:s.900:

Gramm-Leach-Bliley. "Title V – Privacy, Subtitle A – Disclosure of Non-Public Information, Sec. 501. Protection of nonpublic personal information". November 12, 1999.
URL: http://www.senate.gov/~banking/conf/fintl5.pdf

Zamorski, Michael J. "Security Standards for Customer Information". Financial Institution Letters. Federal Deposit Insurance Corporation. March 14, 2001.
URL: http://www.fdic.gov/news/news/financial/2001/fil0122.html

Hibbs Brody, Melanie – Kirkpatrick & Lockhart. "Banking Agencies Issue Gramm-Leach-Bliley Act Administrative, Technical and Physical Safeguards Guidelines". Mortgage Banking Commentary. March 7, 2001.
URL: http://www.kl.com/files/tbl_s48News/PDFUpload307/7085/MBG030701.pdf

Spillenkothen, Richard. "Standards for Safeguarding Customer Information". 2001 Supervision and Regulation Letters. May 31, 2001.
URL: http://www.federalreserve.gov/boarddocs/SRLetters/2001/sr0115.htm

Jenkins, George/Wallace, Michael. IT Policies & Procedures: Tools & Techniques That Work. Paramus, NJ: Prentice Hall, 2002.