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.

# Gramm-Leach-Bliley Act Title V Complexities and Compliancy for the Community Banking Sector

Today's small banks are faced with even more daunting tasks in an effort to remain compliant and profitable. With the passage of the Gramm-Leach-Bliley Act of 1999, small community banks are being forced to review their security posture, which historically has tended to be limited in scope and effectiveness. This report will focus on the requirements that are mandated in the legislation as well as the interpretation by federal regulatory agencies such as the FDIC and OCC. We will then discuss what actions community ban...

Copyright SANS Institute
Author Retains Full Rights

AD

ForeScout

# Gramm-Leach-Bliley Act Title V Complexities and Compliancy for the Community Banking Sector

© SANS Institute 2003, Author retains full rights

GIAC Security Essentials Certification (GSEC)
Assignment version 1.4b, Option 1

Joseph Seaman

November 22, 2002

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

## Abstract

Today's small banks are faced with even more daunting tasks in an effort to remain compliant and profitable. With the passage of the Gramm-Leach-Bliley Act of 1999, small community banks are being forced to review their security posture, which historically has tended to be limited in scope and effectiveness. This report will focus on the requirements that are mandated in the legislation as well as the interpretation by federal regulatory agencies such as the FDIC and OCC. We will then discuss what actions community banks can take today to obtain compliance as well as addressing the potential impact on current pending legislation. Even though the effective date for compliance has passed, there are still banks in the market today that have not yet completed the minimum set of requirements and are grappling with how to quickly and effectively satisfy the requirements. The security areas that are addressed in the act are broad and complex and therefore why more and more institutions are seeking help from outside vendors and consultants to help identify and resolve their security issues.

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

## History

The guidelines were created to further clarify the requirements contained in Title V of the Gramm-Leach-Bliley Act (herein "GLB Act"), which was signed into law on November 12, 1999. Section 501 from Subtitle A of the GLB Act is titled, *"Protection of Nonpublic Personal Information*". The relevant text is stated as such:

"It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information. ... each agency ... shall establish appropriate standards ... relating to administrative, technical, and physical safeguards—

(1) to insure the security and confidentiality of customer records and information;
(2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
(3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer." (Senate Banking Committee 1999)

In an effort to clarify the questions surrounding how banks can comply with the GLB Act, guidelines were developed titled, *"Interagency Guidelines Establishing Standards for Safeguarding Customer Information*". The guidelines were developed jointly by the Department of Treasury, Office of Comptroller of the Currency (OCC), Office of Thrift Supervision (OTS), the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation (FDIC) (collectively, the Agencies). Each agency included as an appendix to the guidelines, further clarification for those entities to which it has authority over. However, the text and definition of each of the agency's appendices are for the most part, the same.

## Guideline Requirements

Compliancy with the guidelines and the GLB Act were required by July 1, 2001. Financial institutions were to create, implement and maintain a comprehensive information security program to protect against unauthorized access or use of customers' nonpublic personal information. Most agencies are currently in the process of educating and warning banks for areas of non-compliance to further clarify any questions in the guidelines and how it is applicable to each banks environment.

The guidelines are intended to integrate industry best practices by breaking them down into the following seven steps:

1) Involve the Board of Directors
2) Assess Risk

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

3) Manage and Control Risk
4) Oversee Service Provider Arrangements
5) Adjust the Program
6) Report to the Board
7) Implement the Standards

Each of these steps will be described to understand where and how community banks can achieve compliance.

**1. Involve the Board of Directors**

The Board of Directors, or appropriate bank management that has the authority and accountability to the bank operations, are required to approve the written information security program. The information security program includes, "administrative, technical, and physical safeguards appropriate to the size and complexity of the bank and the nature and scope of its activities." (Federal Register 2001) The Board of Directors is also responsible for ensuring the development, implementation and maintenance of the information security program. Therefore, bank management's first focus should be the selection of appropriate policies and procedures for the information security program.

The bank's policies and procedures form the necessary foundation of any security program. It is therefore imperative that all of the necessary policies and procedures are well documented. The worst-case scenario that a bank could face is being legally charged and having to explain to a jury that a particular policy was implied based on moral or ethical standards. In this scenario, the bank's information security program will be subjected to intense examination including all policies, procedures, standards, testing results, and all applicable logs. In addition, the bank should expect questions on every policy such as why the policy was created, who created and approved the policy, and what measures were taken to enforce compliance of the policy.

The best way to address questions on policy development is to incorporate one, or a combination of several, recognized sets of industry "best security practices". Then bank management can tailor them to the bank's unique requirements. Although the security industry has not agreed on a single best set of security practices, there are several common and well- defined standards. A sample list of best security practices sources that community banks can use include the following:

- Common Criteria ver. 2.1 / ISO 15408
- Carnegie Mellon University CERT® Coordination Center
- CIO Council
- Critical Infrastructure Assurance Office
- General Accounting Office
- Information Assurance Technical Framework Forum (IATFF)
- The Internet Engineering Task Force (IETF)
- Internet Security Task Force (ISTF)
- SANS Institute

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

- U.S. Department of Defense Information Assurance Technology Analysis Center
- U.S. Department of Energy Computer Incident Advisory Capability (CIAC)
- The ISO Standard 17799
- Information Systems Audit and Control Association & Foundation's Control Objectives for Information & Related Technology (CobiT)

Banks can then use these sources to not only define the model they are using but have the advantage of applying the lessons learned by other organizations that use the same best practices.

**2. Assess Risk**

The process of assessing risk can be addressed using two different approaches, either vulnerability or asset focused. If using a vulnerability focused assessment the following steps need to be taken:

1. Identify and analyze known vulnerabilities
2. Calculate the severity
3. Identify affected assets
4. Assign potential loss value
5. Consider possible enemies and their motivations (Hacker, Insider, Spy)
6. Assign probability
7. Calculate and report to Board or Management

If using an asset focused assessment the following steps should be taken:

1. Inventory sensitive and critical assets
2. Estimate potential loss value
3. Account for dependencies on technology
4. Identify and analyze known vulnerabilities
5. Consider possible enemies and their motivations (Hacker, Thief, Spy)
6. Assign probability
7. Calculate and report to Board or Management

According to the guidelines each bank shall:

"1. Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems.

2. Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information.

3. Assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks" (Federal Register 2001)

In order to effectively manage the risk that banks face, they must properly identify all of the risks associated with customer information. The bank should review their policies and procedures once the risks are identified. Thus, any changes or modifications to its controls can be applied to limit the potential impact or likelihood of the risk. That is not to say that all risks should be eliminated but rather a way for the board to stay

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

informed of the risks presented and make an informed decision on how best to mitigate or reduce the level of risk. To identify internal and external threats to its customer information systems also implies that banks should have the appropriate means to stay informed on the latest security issues applicable to their environment. This is best achieved by subscribing to mailing lists and news alerts that can direct tailored information based on individual requirements.

**3. Manage and Control Risk**

A critical component of an information security program is a risk management plan. The guidelines require that a bank must do three things to address risk:

(1) "Design its information security program to control the identified risks.
(2) Train staff to implement the bank's information security program.
(3) Regularly test the key controls, systems and procedures of the information security program. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs." (Federal Register 2001)

The designing of the information security program includes the policies and procedures that address the objectives and risks of the bank. The policies and procedures take into account the confidentiality of the bank's information and business processes as well as the complexity of the technical and physical environment. The guidelines specify eight areas, which the agencies expect to be addressed within the bank's information security program. At a minimum, all banks will need to consider appropriate policies and procedures relating to:

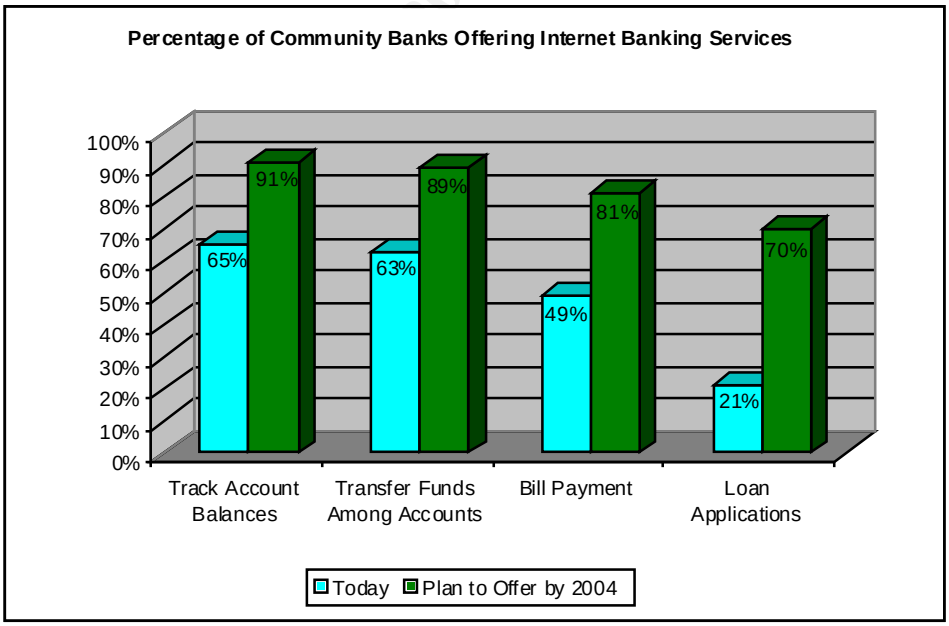
1. "Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals". (Federal Register 2001) These controls can be as simple as one-factor authentication mechanisms, where a user provides an ID or account and a corresponding password in order to authenticate the user. An area that is often overlooked is what particular users can do once they have been authenticated. Banks need to establish a defined access control methodology by using least privilege when establishing access rights. Two of the more common methodologies in use today are Role Based and Discretionary. Role Based Access Control (RBAC) is applying security rights based on specific job roles or functions. Access to files as well as applications is provided to specific roles and users are then assigned to a role. Discretionary Access Control (DAC) is based on individual requirements. It is easy to implement but more difficult to maintain. Access to files and applications is assigned at the discretion of the owner. (Dupuis 2001) In both cases, access should be provided based on least privilege. The default behavior should always be that you would not have access unless you are explicitly given access.

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

2. "Access restrictions at physical locations containing customer information, such as buildings, computer facilities, and records storage facilities." (Federal Register 2001) This is so that banks do not have open access to systems or terminals where either bank personnel or unauthorized individuals do not have a requirement to do so. Most banks have already established appropriate safeguards to the physical access of the building and maintain an appropriate storage mechanism for such items as loan documentation, paper collateral, and bank records. However, due to the nature of community banks and the facilities that they occupy, many did not have the infrastructure or floor design to accommodate a "data center" setup. Servers and routing equipment were often put in closets or in offices that were shared with other functions. This presented scenarios such as the case of office cleaning personnel unplugging a server in order to use the power outlet for the vacuum. Banks need to identify office space that is limited to only authorized personnel that have a legitimate business need to access the computer facilities.

3. "Encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access." (Federal Register 2001) Community Banks are moving more and more to offering a wider array of Internet banking services. Grant Thornton's Ninth Annual Survey of Community Bank Executives surveyed 429 chief executives of community banks. The survey shows the increasing reliance on the Internet to provide additional services and products (see Fig.1). This is also noted in the survey in that 80% of the respondents have a web site as compared to 21% in 1997. (Thornton 2002)

***Fig. 1***




Source: Grant Thornton's Ninth Annual Survey of Community Bank Executives, 2002

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

GLB Act raises the concern of not only protecting data at rest but also data in transit. Banks will need to analyze where encryption should be used beyond just using SSL to access account information. Community Banks need to review what information is being stored on their web server, not only in cache but temp files as well, and how it interacts with the supporting databases and systems that contain customer information. Banks need to look at the entire flow of data and protect all points in the transaction both inside and outside of the bank's network.

4. "Procedures designed to ensure that customer information system modifications are consistent with the bank's information security program." (Federal Register 2001) A proper change control mechanism should be established to account for any authorized changes to customer information systems. This mechanism should account for such things as the impact of change, date of change, approval requirements, rollback or back-out procedures and a detailed description of what the change is and any associated risks. This is to prevent unauthorized changes being made to customer information systems that could adversely affect the stability and security of the bank's systems.

5. "Dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer information." (Federal Register 2001) Even before the tragic events of 9/11, many banks were already obtaining employee background checks and in some cases, expanded the scope of the background check. What becomes difficult to implement are segregation of duties and dual control procedures due to the size of the community bank's organization. "Approximately half (49%) of the banks report that their staff member responsible for online technology has other responsibilities as well." (Thornton 2002) It thus becomes more appropriate for community banks to implement such checks and balances as allowing a system administrator to only create an account for access to customer information systems and then permit an application owner to assign the appropriate rights to the account within the application. This establishes dual control procedure because the process to provide access to customer information requires two steps that are completed by separate parties. It also establishes segregation of duties because the system administrator cannot accidentally create an account and give it permissions that are not appropriate for the new account.

6. "Monitoring systems and procedures to detect actual and attempted attacks or intrusions into customer information systems." (Federal Register 2001) Monitoring could be as simple as reviewing the audit logs to as complex as establishing an enterprise intrusion detection system architecture. Intrusion detection systems ("IDS") are designed to identify suspect activity and alert someone of the risk. They operate in real time and can also perform some of the more mundane, often overlooked tasks such as reviewing system logs to alert for suspicious activity. (See http://www.networkintrusion.co.uk/ids.htm for a comparison of the various IDS in the market today.) IDS have improved greatly over the past few years and are becoming more intelligent to reduce the frequency of false-positives. Although

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

banks do not necessarily have to utilize intrusion detection, they are becoming commonplace in many security programs due to lowered costs, the capability to outsource management and maintenance of devices, and the ever-increasing threats and vulnerabilities.

7. "Response programs that specify actions to be taken when the banks suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies." (Federal Register 2001) Historically, banks have not shared information related to unauthorized access into their computer systems. Part of this has been due to the lack of controls alerting that something has happened and another has been the fear of information leaking to the general public resulting in bad publicity. This is now required for publicly traded banks and should be a part of every incident response plan. An incident response plan is critical to any security program. A well thought out plan would address not only who needs to be informed but also what actions are to be taken and when. You do not want to start asking questions after a breech has occurred. Many banks do not have the expertise or staff to properly handle the forensics or legal requirements of a security breech and as such should seek the assistance of outside consultants or third party companies that specialize in handling such events. Each bank should also begin discussions with their local FBI InfraGard chapter (http://www.infragard.net), which can greatly assist in early warning as well as on-site investigations.

8. "Measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards such as fire and water damage or technical failures." (Federal Register 2001) Many banks have already established a disaster recovery plan to account for malicious or environmental threats. Unfortunately, the lines on when or when not to use the plan become blurred when you start looking at the less obvious threats. It is very easy to decide that the plan should be used when a fire has struck the building but is difficult to define when a computer virus is running wild in the organization. What if the virus is only affecting half of the organization? Do you shut down all systems to limit the continued spread of the virus? If you restore from backup, how do you know that the virus is not time released and infected on the backup files as well? These issues should be addressed in not only the disaster recovery plan but also included in the risk management plan.

Each bank should incorporate these areas into their written policies and procedures while making certain that it is appropriate for their environment.

The second required item of managing and controlling risk is the training of staff to be able to implement the information security program. All bank personnel should be aware of the bank's policy and procedures as well as be able to recognize and respond to any incidents or compromises in security. This is not say that all staff should be versed on the intricacies of how computer hackers work but should be

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

aware of the methods they use to obtain unauthorized access or customer information. The amount and type of training that is covered in the information security program covers many aspects and should be tailored based on each individual's job requirements. One such area for all bank personnel is training on social engineering tactics. Social engineering is using personal or public information to get privileged information and gain access to restricted systems. Hackers employ social engineering to impersonate such common business interactions as help desk engineers, vendors or support technicians. They then use the information gathered to attack vulnerable systems based on the information gathered.

The commitment in resources and money to company security training is of utmost importance. Access to critical systems and applications are provided mostly to internal bank employees. Internal employees are also a tremendous risk as they provide the capability to introduce virus, worms, and Trojan horses that can severely disrupt the integrity, confidentiality and availability of critical systems. That is why it is so important to train employees on how to avoid these pitfalls associated with using only a web browser or email.

The third required area of a bank's risk plan addresses the need to perform continued testing on its controls, systems and procedures. The guidelines state,

"The frequency and nature of such tests should be determined by the bank's risk assessment." (Federal Register 2001)

The frequency of the testing is a continual process that needs to be addressed as risk levels or infrastructure change. Therefore, banks must be able to demonstrate that they are aware of the risks and have taken appropriate action to reduce the risk to acceptable levels.

Since it is rare for a community bank to have a separate auditing staff that is not responsible for the information security program, many banks look to third party companies that specialize in performing these tests. However, community banks continue to struggle with this requirement in that "fewer than four in ten (37%) community banks reported that their Web site either has an independent security certification seal or will have one by the end of this year. Two-thirds (65%) of banks test their Web sites for vulnerabilities at least once a year." (Thornton 2002) Many companies offer these types of testing and audit services and banks should consider implementing a formalized testing model that includes the following:

- Network Vulnerability Assessments
- Penetration Testing
- Intrusion Detection System Testing
- Social Engineering Testing of employees
- Service Provider Compliance Testing
- Policy and Procedure testing

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

Regardless of the type or frequency with which the tests are performed, the results of the tests must be reported to the board.

**4. Oversee Service Provider Arrangements**
The next area that the guidelines address is the bank's duty to oversee its service provider arrangements. Under the guidelines, it is the bank's responsibility to protect its customer's data regardless of who maintains it or where it is located.

The banks shall, "require its service providers by contract to implement appropriate measures designed to meet the objectives of these guidelines and where indicated by the bank's risk assessment, monitor its service providers to confirm that they have satisfied their obligations. As part of this monitoring, a bank should review audits, summaries of test results or other equivalent valuations of its service providers." (Federal Register 2001)

The intent here is that banks cannot shift all liability to its service provider if they have not performed due diligence in its selection of its service provider. The guidelines are also not meant to have all banks hire an independent agency audit the service provider thereby causing unnecessary burden to the service provider. What Community Banks will be asked of is how they determined the service provider is upholding its obligation to secure customer information. This can be accomplished by requesting copies of security audit reports or test results that the service provider has completed with independent agencies.

**5. Adjust the Program**
The guidelines also account for changes in the technology as well as the bank. Rather than prescribe specific solutions to technological issues that can become quickly outdated, the guidelines establish a mechanism for the bank to make the appropriate changes based on changes in the bank's position as relating to administrative, physical and technical controls. It is the banks responsibility to "Monitor, evaluate, and adjust the information security program in light of any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information and the banks own changing business arrangements". (Federal Register 2001) This requires the bank to stay informed and abreast of relevant security issues and make the necessary changes to mitigate the risk associated with the relevant threat.

**6. Report to the Board**
The guidelines specify that on an annual basis, bank management will report to its board the status of the information security program and the bank's compliance with the guidelines. The report will consist of such items as:

(1) Risk assessment;
(2) Risk management and control decisions;
(3) Service provider arrangements;
(4) Results of testing;
(5) Security breaches or violations and management's responses;

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

(6) Any recommendations for changes in the information security program.

As part of the responsibility of the board to perform due care, the board or appropriate management will need this information to make an informed decision on how best to maintain or improve its risk associated with access to customer information. The process of due care is stated as such (FDIC, 1992):

"The duty of care requires directors and officers to act as prudent and diligent business persons in conducting the affairs of the bank." "This means that directors are responsible for selecting, monitoring, and evaluating competent management; establishing business strategies and policies; monitoring and assessing the progress of business operations; establishing and monitoring adherence to policies and procedures required by statute, regulation, and principles of safety and soundness; and for making business decisions on the basis of fully informed and meaningful deliberation."

"The FDIC will not bring civil suits against directors and officers who fulfill their responsibilities, including the duties of loyalty and care, and who make reasonable business judgments on a fully informed basis and after proper deliberation."

Thus, in order for board directors to fulfill their responsibility to make "reasonable business decisions on the basis of fully informed and meaningful deliberation" in regards to the information security program, they must first be informed on the issues involved in the development, maintenance and adjustments to the program.

**7. Implement the Standards**

Each bank was required to implement an information security program by July 1, 2001. There is a grandfather clause with respect to contracts entered with service providers before March 5, 2001 that allows for compliance relative to service providers to be completed by July 1, 2003.

## Next Steps

The FDIC has setup examination procedures (FDIC 2001) to help ensure that the institution has appropriate measures to validate the compliance to GLBA Title V. The procedures are broken down into 5 main categories as follows:

1. Determine involvement of the board
2. Evaluate the risk assessment process
3. Evaluate the adequacy of the program to manage and control risk
4. Asses the measure taken to oversee service providers
5. Determine whether an effective process exists to adjust the program

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

They are tailored to the requirements established in the guidelines and all bank personnel should be aware of the procedures to identify areas of improvement. Community Banks need to stay informed of the issues regarding privacy and security. With the passage of the USA PATRIOT Act (Department of the Treasury 2002) and the pending approval of the Homeland Security Act (Department of Homeland Security 2002), the banking sector will be called upon and relied upon heavily to contribute to the war on terrorism.

The President's Critical Infrastructure Protection Board (PCIPB 2002) has recently published, "*National Strategy to Secure Cyberspace—Draft for Comment*". The board has identified the Treasury Department to oversee the financial services sector with respect to this draft. This may lead to a day when the Treasury can issue rules requiring enforcement by institutions to this strategy. (ICBA 2002) Richard Clarke, chairman of the President's Critical Infrastructure Board, is also proposing several ideas on how to make corporations more responsible for their security. One idea is to increase the liability of corporate officers for failing to provide adequate security. Another is to have CEO's certify their Info-security on their SEC filings. (Prince 2002) All of these issues are having a profound impact on the banking industry as well as our personal lives. It is thus imperative that the banking industry continues to be the leaders in securing critical servers and data.

Community Banks must realize that security is not a destination but a continuous journey that needs to have the necessary attention and support of all members of the banking community.

© SANS Institute 2003, Author retains full rights.

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

## References

Department of Homeland Security. "Information Analysis and Infrastructure Protection". June 2002
URL: http://www.whitehouse.gov/deptofhomeland/sect6.html (November 22, 2002)

Department of the Treasury. "Treasury and Federal Financial Regulators Issue Patriot Act Regulations on Customer Identification". July 17, 2002
URL: http://www.treas.gov/press/releases/po3263.htm (November 22, 2002)

Dupuis, Clement. "Access Control Systems and Methodology". Version 1.0. April 14, 2001
URL: http://comsec.theclerk.com/CISSP/Domain_1.doc (November 22, 2002)

FDIC Financial Institution Letter (FIL--87--92). "Statement Concerning the Responsibilities of Bank Directors and Officers". December 3, 1992
URL: http://www.fdic.gov/regulations/laws/rules/5000-3300.html (November 22, 2002)

FDIC Financial Institution Letter (FIL-68-2001). "Examination Procedures to Evaluate Compliance with the Guidelines to Safeguard Customer Information". August 24, 2001
URL: http://www.fdic.gov/news/news/financial/2001/fil0168a.html (November 20, 2002)

Federal Register Part II 12 CFR Part 30, et al.
"Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness: Final Rule". February 1, 2001
URL: http://www.fdic.gov/regulations/information/ebanking/66FR8615.pdf (November 22, 2002)

Independent Community Bankers of America (ICBA). "Network and Cyberspace Security Resources".
Non-Geek Speak Technology Newsletter for the CEO October 2002: 2
URL: http://www.icba.org/tech/gs1002.pdf (November 22, 2002)

PCIPB, President's Critical Infrastructure Protections Board. "National Strategy to Secure Cyberspace—Draft for Comment". September 2002
URL: http://www.whitehouse.gov/pcipb/cyberstrategy-draft.html (November 22, 2002)

Prince, Frank. "Security Through Executive Liability"
*CISO Magazine* August 2002 (2002): 13
URL: http://www.cisomagazine.com/2002/aug/news-briefing.shtml (November 2, 2002. Link and magazine publication have been suspended at the time of this report)

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

Senate Banking Committee posting of Gramm-Leach-Bliley Act. "Title V – Privacy Subtitle A – Disclosure of Nonpublic Personal Information". November 1, 1999
URL: http://www.senate.gov/~banking/conf/fintl5.pdf (November 22, 2002)

Thornton, Grant. "Grant Thornton's Ninth Annual Survey of Community Bank Executives". February 2002
URL: http://www.grantthornton.com/content/13466.asp (October 23, 2002)

© SANS Institute 2003, Author retains full rights

Last Updated: September 2nd, 2015

# Upcoming SANS Training

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

| | | | |
|---|---|---|---|
| SANS Crystal City 2015 | Crystal City, VAUS | Sep 08, 2015 - Sep 13, 2015 | Live Event |
| SANS Network Security 2015 | Las Vegas, NVUS | Sep 12, 2015 - Sep 21, 2015 | Live Event |
| SANS Seoul 2015 | Seoul, KR | Sep 14, 2015 - Sep 19, 2015 | Live Event |
| Data Breach Investigation Summit & Training | Dallas, TXUS | Sep 21, 2015 - Sep 26, 2015 | Live Event |
| SANS Baltimore 2015 | Baltimore, MDUS | Sep 21, 2015 - Sep 26, 2015 | Live Event |
| SANS Perth 2015 | Perth, AU | Sep 21, 2015 - Sep 26, 2015 | Live Event |
| SANS Tallinn 2015 | Tallinn, EE | Sep 21, 2015 - Sep 26, 2015 | Live Event |
| SANS ICS Amsterdam 2015 | Amsterdam, NL | Sep 22, 2015 - Sep 28, 2015 | Live Event |
| SANS Bangalore 2015 | Bangalore, IN | Sep 28, 2015 - Oct 17, 2015 | Live Event |
| SANS DFIR Prague 2015 | Prague, CZ | Oct 05, 2015 - Oct 17, 2015 | Live Event |
| SANS Seattle 2015 | Seattle, WAUS | Oct 05, 2015 - Oct 10, 2015 | Live Event |
| SANS Tysons Corner 2015 | Tysons Corner, VAUS | Oct 12, 2015 - Oct 17, 2015 | Live Event |
| SOS: SANS October Singapore 2015 | Singapore, SG | Oct 12, 2015 - Oct 24, 2015 | Live Event |
| SANS Gulf Region 2015 | Dubai, AE | Oct 17, 2015 - Oct 29, 2015 | Live Event |
| SANS Cyber Defense San Diego 2015 | San Diego, CAUS | Oct 19, 2015 - Oct 24, 2015 | Live Event |
| SANS Tokyo Autumn 2015 | Tokyo, JP | Oct 19, 2015 - Oct 31, 2015 | Live Event |
| SANS South Florida 2015 | Fort Lauderdale, FLUS | Nov 09, 2015 - Nov 14, 2015 | Live Event |
| SANS Sydney 2015 | Sydney, AU | Nov 09, 2015 - Nov 21, 2015 | Live Event |
| SANS London 2015 | London, GB | Nov 14, 2015 - Nov 23, 2015 | Live Event |
| Pen Test Hackfest Summit & Training | Alexandria, VAUS | Nov 16, 2015 - Nov 23, 2015 | Live Event |
| SANS Hyderabad 2015 | Hyderabad, IN | Nov 24, 2015 - Dec 04, 2015 | Live Event |
| SANS Cape Town 2015 | Cape Town, ZA | Nov 30, 2015 - Dec 05, 2015 | Live Event |
| SANS San Francisco 2015 | San Francisco, CAUS | Nov 30, 2015 - Dec 05, 2015 | Live Event |
| SANS Milan 2015 | OnlineIT | Sep 07, 2015 - Sep 12, 2015 | Live Event |
| SANS OnDemand | Books & MP3s OnlyUS | Anytime | Self Paced |