XXVI Congreso de Seguridad Bancaria
CELAES 2011

Gramm-Leach-Bliley Act Section 501(b)

Silka M. Gonzalez, CPA, CISA, CISSP, CISM, CITP, CRISC
President
Enterprise Risk Management

enterprise risk management
The Control Professionals

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

FLORIDA INTERNATIONAL FIBA BANKERS ASSOCIATION

Agenda

Gramm-Leach-Bliley Act, Introduction and Fundamentals

GLBA Life Cycle

1 - Information Security Program

2 - Risk Assessment

3 - Testing of Information Security Controls

- Vulnerability Assessment
- Penetration testing
- Review of third party provides contracts and SAS 70\SSAE-16

4 - Implementation of Security Controls

5 - Board Directors Involvement

6 - On-going Process

- Information Security Incident Response Plan
- Training and Awareness

Key Compliance Factors

Questions & Answers

Gramm-Leach-Bliley Act

Requires financial institutions to ensure the security, confidentiality and integrity of non-public customer information.

Prohibits financial institutions from sharing any information that is non-public with nonaffiliated third parties.

Applies to institutions “significantly engaged” in providing “financial activities”, that is, financial products or services to consumers. These include:

- Lending
- Transferring
- Economic advisory services
- Brokering loans
- Debt collecting
- Providing real estate settlement services

Gramm-Leach-Bliley Act

In addition to banks, the GLBA applies to businesses that significantly engage in financial activities. For instance:

- Mortgage lender or broker
- Check casher
- Pay-day lender
- Credit counseling service or other financial advisors
- Professional tax preparers
- Retailers that issue credit cards to consumers
- Auto dealers that lease and/or finance

Nonpublic Information

Nonpublic information can include:

- Salary
- Social security number
- Account numbers
- Account balances
- Financial products purchased

Public Information

The term “public information” means any information, regardless of form or format, that an agency discloses, disseminates or makes available to the public.

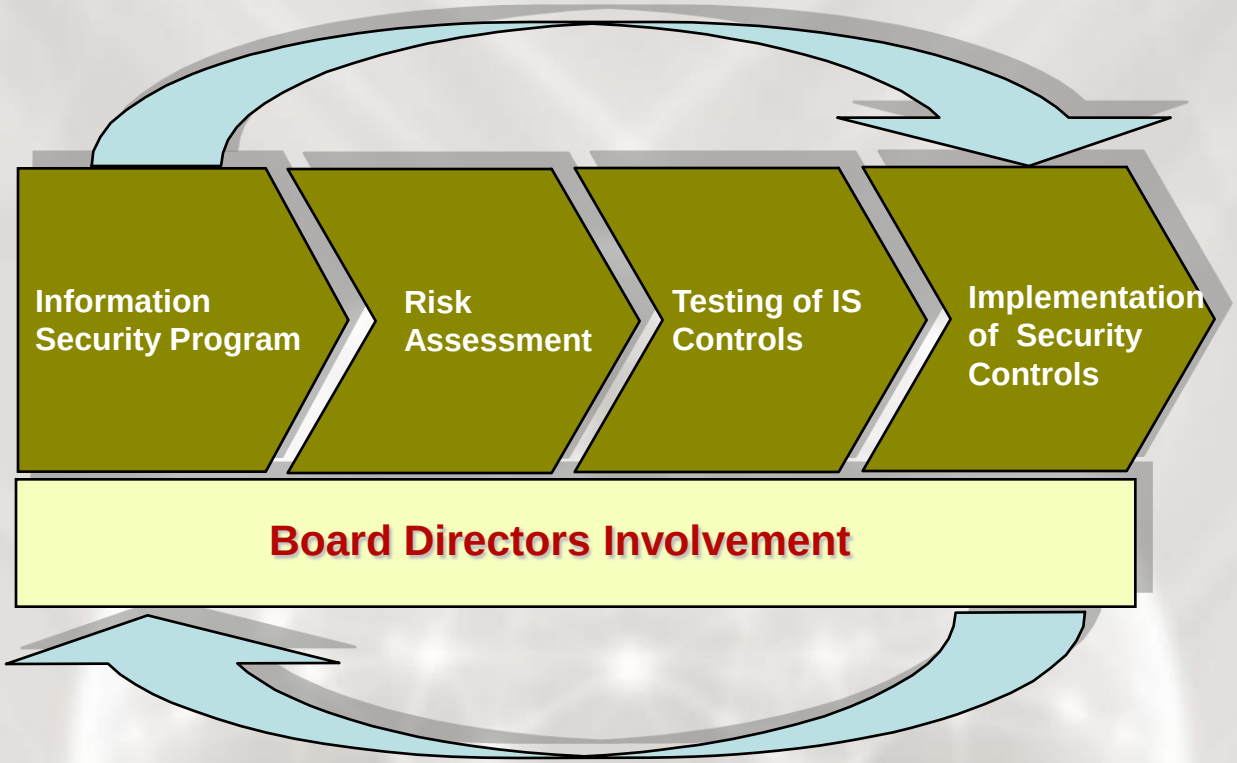
Public information includes:

- Public records (e.g. real estate disclosures, bankruptcy filings, tax liens)
- Information from telephone white pages
- Information from websites with non-restricted access

GLBA Section 501(b)

Section 501 of the Gramm-Leach-Bliley Act requires **Financial Institutions** to follow standards set forth by the Agencies (e.g., FDIC, OCC, OTS, and the Board of Governors of the Federal Reserve System) to protect the security, confidentiality and integrity of non-public customer information through administrative, technical and physical safeguards.

GLBA Life Cycle



On-going Security Reviews and Information Security Program Adjustments

Information Security Program

Each financial institution shall implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the institution and the nature and scope of its activities.

Information Security Program

The information security program shall be designed to:

Ensure the security, confidentiality and integrity of customer information.

Protect against any anticipated threats or hazards to the security, confidentiality and integrity of customer information.

Protect against unauthorized access to or use of customer information which could result in substantial harm or inconvenience to any customer.

Information Security Program

Design the information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the bank's activities.

Each financial institution must consider and adopt those security measures the bank determines are appropriate.

Security measures include:

- Access controls on customer information systems including controls to authenticate and permit access only to authorized individuals.
- Controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means.

Information Security Program

Security measures include:

- Access restrictions at physical locations containing customer information, such as buildings, computer facilities, and records storage facilities.
- Encryption of electronically transmitted and stored customer information.
- Procedures designed to ensure that customer information system modifications are consistent with the bank's information security program.
- Dual control procedures and segregation of duties.
- Employee background checks for employees with responsibilities for or access to customer information.

Information Security Program

Monitoring systems and procedures to detect actual and attempted attacks or intrusions into customer information systems.

Response programs that specify actions to be taken when the bank suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies.

Measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards such as fire, water damage, hurricanes or technological failures.

Information Security Program

The organization applies adequate security measures to the selection and management of third party providers.

Employees have the skill sets to implement the security program.

Security training is provided to the organization's personnel.

Regularly test key controls, systems and procedures.

Risk Assessment

Each Financial Institution shall:

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

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

Assess the sufficiency of security controls in place to control risks.

Risk Assessment

Determines levels of exposure of systems and data to external and internal threats.

Identifies, analyzes, and prioritizes risks that could compromise confidentiality, integrity, and availability of critical systems and data.

Identifies controls that are available and controls that are missing.

Includes a business impact analysis and a gap analysis.

Risk Assessment

Gap Analysis:

Comparison between the controls and safeguards identified in the controls that should be in place.

Document residual risk and the disposition of the risk.

Ensure logical and justifiable reasoning is used to accept risks.

Ensure management formally approves any decision to accept risks.

The result of this phase are working plans with security controls implementation priorities.

Risk Assessment

Perform risk assessments on a regular basis.

As the organization, processes, infrastructure, systems and data change with time, the risk assessment needs to be conducted again to identify new risks.

Risk assessment is an on-going process.

Testing Information Security Controls

Information security controls testing is a broad set of assessments focused on evaluating, testing and reporting on an organization's achievement of control objectives. Among these assessments we can mention:

- Vulnerability Assessment
- Penetration testing
- Review of third party provides contracts and SAS 70\SSAE-16

The assessments in general are performed using a snapshot of the security controls currently in place.

Vulnerability Assessment

Assess the overall adequacy of existing security controls present in the infrastructure and associated processes under review.

The assessment focuses on each individual component's security posture.

Vulnerability assessment can include:

- Operating Systems
- Critical Applications
- Database Systems
- Networking Components
- Interfaces between applications

A vulnerability assessment is NOT exclusively a technical security review. All security controls related to the area under revision should be considered including **Technical** and **Non-Technical**.

Vulnerability Assessment

Identifies potential security weaknesses in the infrastructure and associated processes of an organization.

Identifies existing security controls and whether they are working as expected.

Identifies gaps between existing security configurations, required security standards and industry best practices.

Can assess the security controls implemented in the organization's infrastructure.

Can verify against a standard or best practice.

Can provide a benchmark.

Vulnerability Assessment

Cannot ensure 100% security.

Cannot assess the “informal” internal processes and procedures (e.g., password sharing).

Cannot detect fraud.

Penetration Testing

The portion of security testing in which the penetrators attempt to circumvent the security features of a system. The penetrators may be assumed to use all system design and implementation documentation, which may include listings of system source code, manuals, and circuit diagrams. The penetrators work under no constraints other than those that would be applied to ordinary users.

Procedures used to test and possibly bypass security measures of a system.

Emulate the same methods used by Hackers.

Discover weaknesses within the technical infrastructure.

Measure an organization's resistance to attacks.

Penetration Testing

Network	**Network:** It is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source.Wardialing: It is a technique used to identify the phone numbers that can successfully make a connection with a computer modem. **Wardriving:** The act of driving around in a vehicle with a laptop computer, an antenna, and an 802.11 wireless LAN adapter to exploit existing wireless networks. **Bluesnarfing**: Bluesnarfing is the theft of information from a wireless device through a Bluetooth connection. **RFID hacking:** The hacking of RFID chips is typically done through the use of a RFID cloner.
Application	It is an attempt to circumvent the security features of an application based on the attacker's understanding of the application design and implementation.
Social Engineering	It is a collection of techniques used to manipulate people into performing actions or divulging confidential information.

Penetration Testing

Zero Knowledge	Partial Knowledge	Full Knowledge
▪ Perform many irrelevant tests. ▪ Failure to test all relevant platforms. ▪ Accidentally damage network devices or servers. ▪ Failure to finish work in a timely manner.	▪ Reduce the amount of irrelevant tests. ▪ Reduce the possibility of damage to network devices or servers.	▪ Tailored test according to the network devices or servers. ▪ More detailed tests. ▪ Ability to identify more issues in platforms that are critical to the organization.

Penetration Testing

Identifies potential security weaknesses in the infrastructure and associated processes of an organization (root cause).

Identifies existing security controls and whether they are working as expected.

Can assess the security controls implemented in the organization's infrastructure.

Cannot ensure 100% security.

Cannot detect fraud.

Third Party Providers – SAS 70 \ SSAE-16

SAS 70 Key Aspects

The Statement on Auditing Standard NO. 70 (SAS 70) was issued by the American Institute of Certified Public Accountants (AICPA) in 1992.

Leading standard regarding assurance reports for service organizations.

SAS 70 report on controls at service organizations.

Many organizations outsource business functions to third party vendors.

The organization performing the outsourced service is called a **service organization**.

The organization using the outsource service is called a **user entity**.

Third Party Providers – SAS 70 \ SSAE-16

SAS 70 Key Aspects

SAS No. 70 provides the **requirements and guidance for CPAs** reporting on controls at **service organizations** and for **user auditors** auditing the financial statements **of user entities** that use a service organization.

Third Party Providers – SAS 70 \ SSAE-16

New Standards Replacing the SAS 70

In the United States the SAS 70 will be replaced by the Statement on Standards for Attestation Engagements 16 (**SSAE 16**).

SSAE 16 was issued by the American Institute of Certified Accountants (AICPA) in April 2010.

Globally, the standard that will be used is the International Standard on Assurance Engagements 3402 (**ISAE 3402**).

There was no global standard prior to the the **ISAE 3402** standard for engagements to report on controls at service organizations.

The ISAE 3402 standard was issued by the International Auditing and Assurance Standards Board (IAASB) in December 2009.

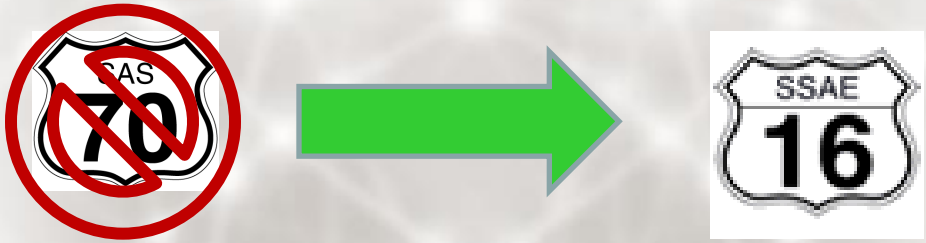
Third Party Providers - SAS 70 \ SSAE-16

New Standards Replacing the SAS 70

The standards are effective for reports with periods ending on or after June 15, 2011.

Early adoption of the standards are permitted.

The SSAE 16 and ISAE 3402 standards are substantially the same with some differences.



Third Party Providers – SAS 70 \ SSAE-16

Re-Defining a SSAE 16 Engagement

A SSAE 16 engagement can no longer be used to report on anything other than a system relevant to internal control over financial reporting.

All other assurance services on other subject matter must be performed in accordance with Attestation Standards.

Includes the effectiveness of controls over privacy and compliance with laws, regulations, and contracts as well as controls over security, availability, processing integrity, and confidentiality.

The SSAE 16 engagement now called a Service Organization Control (SOC) engagement has been divided in three different types SOC1, SOC2, and SOC3.

Third Party Providers – SAS 70 \ SSAE-16

Suggestions for User Organizations

Initiate discussions with auditors to obtain an understanding of the new SSAE 16 standard and its implementation requirements.

Ensure the service organization report is performed by reputable and qualified professionals.

Ensure the service organization provides a type II report.

Ensure the service organization provides a report developed in accordance to the new SSAE 16 standard.

Ensure the report covers a scope that is adequate for your organization.

Third Party Providers – SAS 70 \ SSAE-16

Suggestions for User Organizations

Ensure the report covers the control objectives required by your organization.

Ensure the report covers the regulations required by your organization.

Ensure the period covered is adequate for your organization.

Ensure adequate control testing is performed.

Ensure the contracts with service organizations address the new SSAE 16 standard.

Ensure proper assignment of someone at the organization to be responsible to handle aspects related to the service organization report.

Implementation of Security Controls

Working Plans

Working plans must be developed prior to the implementation of security controls.

Develop strategic and detailed plans addressing the areas where security is required to mitigate the risks found during the risk assessment and vulnerability assessment.

Develop detailed plans per area and include specific tasks to be performed, individual responsible and due dates.

Perform periodic reviews to identify the progress and issues related to each security plan.

Inform executive management and the board of directors on the progress and issues related to the security plans.

Implementation of Security Controls

Once the risks are fully identified, the team can select controls (safeguards, standards, rules, etc.) that best protect against the specific risk.

Controls will cover automated and manual controls.

A repository or database of security controls and their status should be implemented and updated periodically.

Implement in a test environment, evaluate and migrate into the production environment.

Board Directors Involvement

The board of directors or an appropriate committee of the board of each Financial Institution shall:

Approve the bank's written information security program.

Oversee the development, implementation, and maintenance of the bank's information security program, including assigning specific responsibility for its implementation and reviewing reports from management (e.g., risk assessment and vulnerability assessment).

The success of the Information Security Program will depend on the support, direction and management of the board of directors and management.

Entities should have an adequate security structure within their board of directors and throughout the organization as a whole.

On-going Process

Perform on-going periodic reviews and adjustments of the security program.

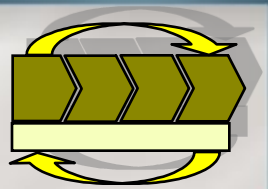
Perform on-going evaluations of existing security controls.

Perform on-going implementations of required controls.

Perform on-going updates to the central repository or database of security controls.

Maintain the board of directors informed of the activities related to the security initiatives.

On-going Process



Assessments

- Assessments should be performed at least yearly for critical areas.
- It is recommended to combine different types of assessments throughout the year.
- Every time a new application is deployed in production environment, it is a good practice to perform a security assessment.

Information Security Incident Response Plan

Incident Response means any actions taken to deal with an incident that occurs.

Information Technology Infrastructure Library(ITIL) defines an incident as "any event which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in, the quality of service."Incident management, therefore, is basically the process of restoring operations as quickly as possible with minimal adverse impact on business operations.

The Incident response plan defines what constitutes a security incident and outlines the incident response phases.

The incident response plan discusses how information is passed to the appropriate personnel, assessment of the incident, minimizing damage and response strategy, documentation, and preservation of evidence.

The incident response plan defines areas of responsibility and establish procedures for handing various security incidents.

Information Security Incident Response Plan

Incident Definition

- Define what are acceptable and unacceptable behaviors.

- The organization has to be prepare to handle the most common type of incidents such as Denial of Services, Malicious Code, Unauthorized access, Inappropriate usage, etc.

Incident Planning

- Define roles and responsibilities

- Define the computer incident response team

- Establish procedures detailing actions taken during the incident.

- Define the escalation procedure based on the type of incident.

Information Security Incident Response Plan

Incident Response Life cycle

Preparation – This phase is the most vital and time consuming step in developing a CIRT team. The preparation step will never be completed as technology and attacks change, so will the documentation and tools necessary to prepare for an investigation. You will continue to review this step of the process and make changes as needed. Documentation is the key for this step as it will direct the actions taken for the remaining step in the process.

Identification – The identification of an event or incident will come from various sources such as Intrusion Detection, Monitoring systems, Firewall, Vendor Alerts and employees are all sources of identification.

Containment – The containment phase must include all steps necessary to further reduce the chance that the event or incident will spread throughout the company. This step is also vital to maintain the appropriate level of confidentiality of the investigation.

Information Security Incident Response Plan

Incident Response Life cycle

Eradication – The Eradication phase allows the safe removal of the event or incident from the environment without compromising the evidence of the event or incident.

Recovery – The recovery phase allows the environment to restored to the original state prior to the event or incident. This step should also be used to put measures in place to mitigate the event from occurring in the future.

Lessons Learned – The last step in this process is to review the investigation and identify improvements and process changes to improve the process.

Information Security Incident Response Plan

Common Mistakes in the Incident Response

- Failure to Prepare
- Failure to Address the Risk
- Failure to Communicate
- Failure to Document
- Failure to Learn from the Past
- Failure to Protect Potential Evidence

Training and Awareness

Objectives of the security awareness

- Confronting employees with their own responsibilities.
- Indicating the authority and responsibility of the corporate security officer, security forum, security department etc.
- Making employees knowledgeable of the proper security related escalation and reporting procedures within the organization.

Training and Awareness

Need for a Security Awareness Program

It is the people who create, administer and deal with information which makes them a potential vulnerability

It is estimated that 30-50% of information security breaches occur within the organization.

Breaches include intentional fraud, theft and abuse. Often times, accidental, ignorant or well-meant actions may cause security breaches.

Many outside threats such as viruses or Trojans received through e-mails require human intervention.

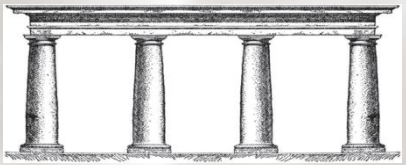
It is estimated that with the improvements in security technologies, hackers will turn more and more to exploiting the human element of security through Social Engineering.

A security awareness program helps to reduce the “people vulnerability”

Training and Awareness

The Foundations of Security Awareness

- Support of executive management
- Behavioral Accountability
- Dedicated resources
- A formal, continuous security awareness program
- Involvement of other departments



Training and Awareness

Formal Security Awareness Program

A security awareness program is a clearly and formally defined plan, a structured approach, and a set of related activities and procedures with the objective of realizing and maintaining a security aware culture.

- Helps attain and sustain security awareness at all times
- Is a continuous process and not a one time effort
- Each security awareness program consists of a number of security awareness campaigns

Focus is the protection of corporate information assets.

Training and Awareness

Requirements of a Security Awareness Program

An effective security awareness program requires the consideration of several elements:

- Analysis of audience composition
- Determination of program content
- Development of awareness program tools and techniques
- Packing and implementing the overall program

Training and Awareness

Awareness Program Tools and Techniques

The communication media selected will determine the effectiveness of the overall awareness program.

The techniques should reflect the personality, traditions, and budget of the organization, as determined by the organization's established policy.

Awareness program tools and techniques:

- ***Presentations***
- ***Videos***
- ***Posters***
- ***Booklets***
- ***Newsletters***
- ***Articles in internal publications***
- ***Special-alert memos***
- ***Electronic bulletin boards/Intranet***
- ***Small handouts***

Training and Awareness

Benefits of a Security Awareness Program

- Mitigation of overall security risk
- Increased confidence of customers, suppliers and shareholders
- Better protection of the confidentiality of critical information
- Increased reliability of information
- Better assurance of availability of information

Training and Awareness

Benefits of a Security Awareness Program

- Better and earlier detection of the remaining security incidents
- Improvement of employee morale (employees are proud to work for a secure organization.)
- Compliance with laws and regulations such as GLBA, FACT Act, SOX, HIPAA, European Data Protection Directive and Canadian Privacy Act
- Fewer internal incidents, errors and omissions

Key Compliance Factors

Degree of board involvement.

Quality of risk assessment and security control testing.

Adequacy of security program in managing and controlling risk.

Effectiveness of third party provider oversight measures.

Quality and effectiveness of the training and security awareness

Existence and enforcement of change management procedures to accommodate on-going changes to the security program.

Contact ERM

By Phone: 305.447.6750

By E-mail: info@emrisk.com

Voted *Best Boutique Risk Management Firm* by *South Florida CEO Magazine*