

Data Privacy and Gramm- Leach-Bliley Act Section 501(b)

October 2007

Agenda

- Introduction and Fundamentals
- Gramm-Leach-Bliley Act, Section 501(b)
- GLBA Life Cycle
- Enforcement and Criminal Penalties
- Key Compliance Factors
- Q & A

- What is Privacy and Why Does It Matter?
 - The management of sensitive customer information from intake to destruction under secure conditions to improve customer service and maintain public trust in the organization.
 - You can't have privacy without security, but you can have security without privacy.

- **Federal Regulation**

- “Constant vigilance is critical ... The FDIC takes a proactive approach to enforcing data security regulations and guidance.”

Sandra L. Thompson, Deputy Director, FDIC

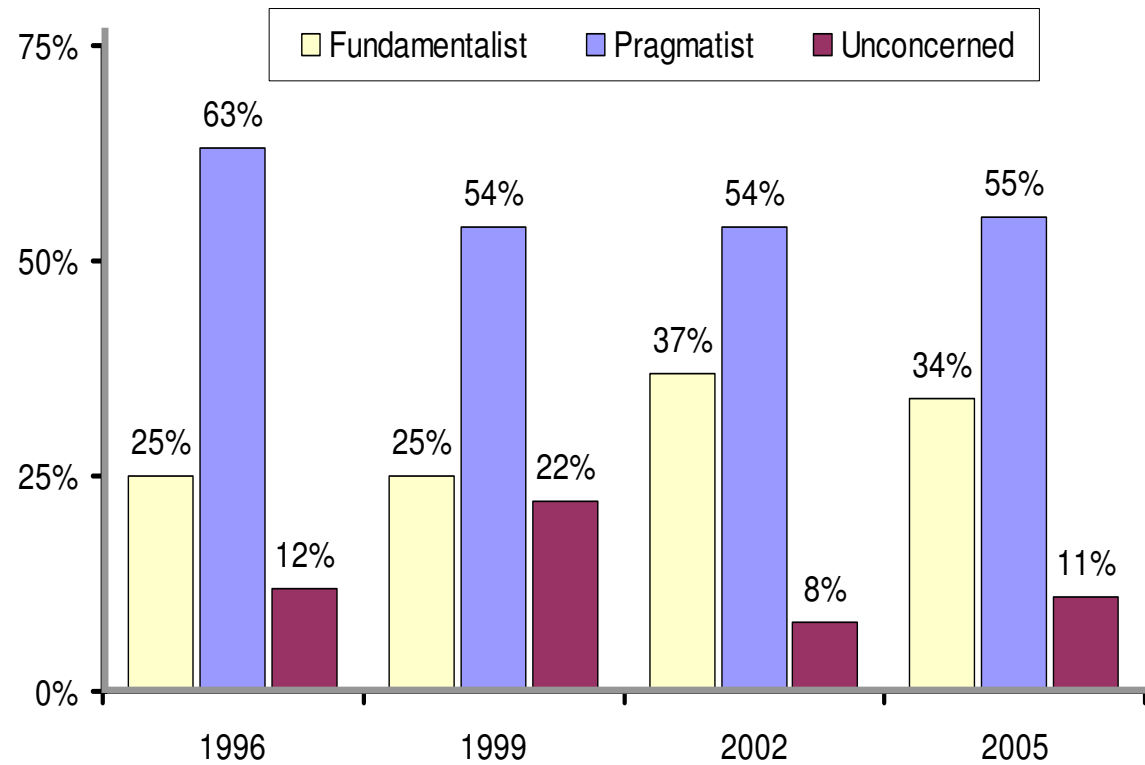
- “If we do nothing, identity theft is going to go through the roof. It really means we should get on the stick and do something here. We’re in the Wild West where companies can do anything they want.”

Senator Charles E. Schumer, Senate Banking Committee

- Impacting Customers and Your Bottom Line



- **Consumer Attitudes**





**How much would you pay to stay
off the cover of The Herald?**



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

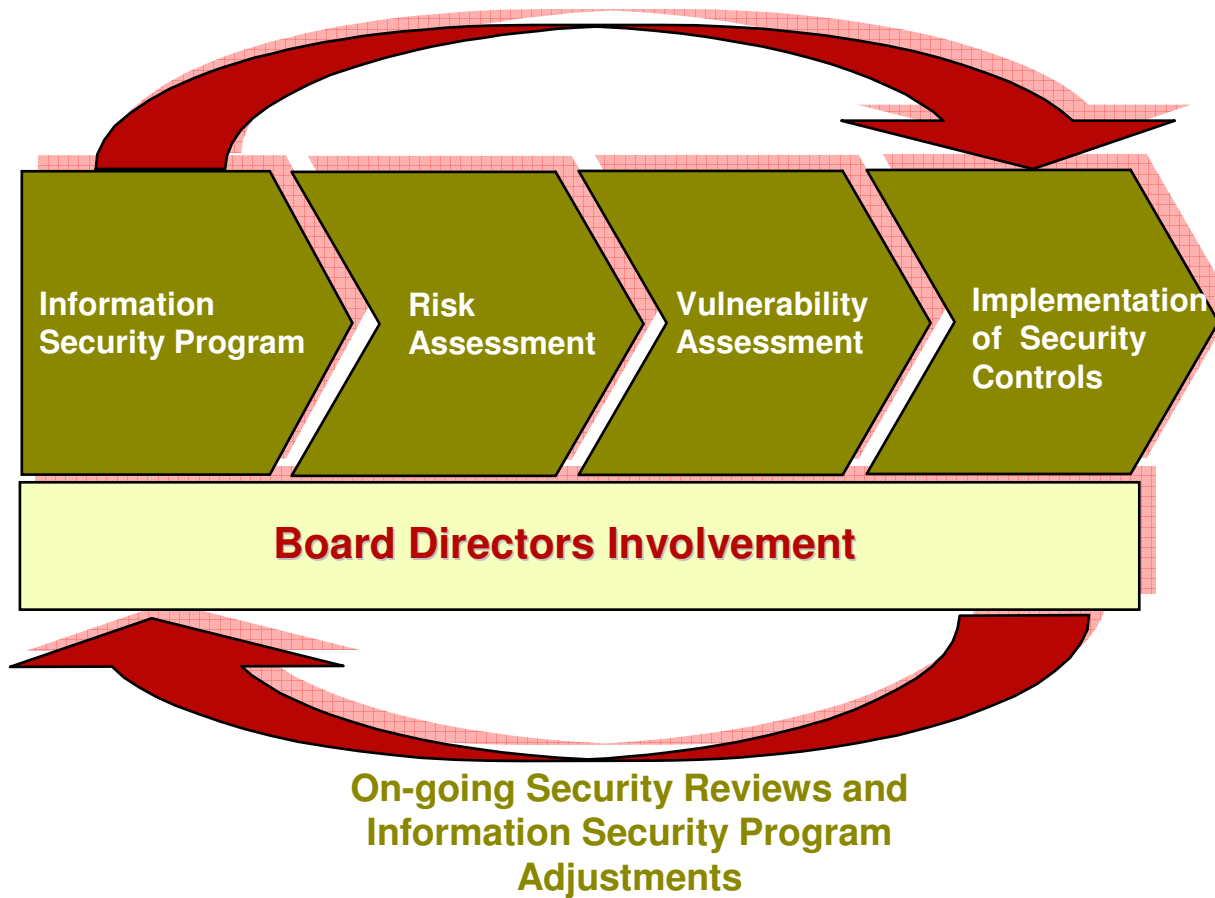
Public Information

- 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

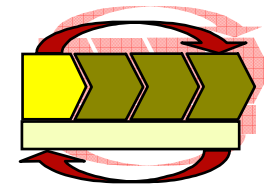
GLBA Section 501 (b)

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.

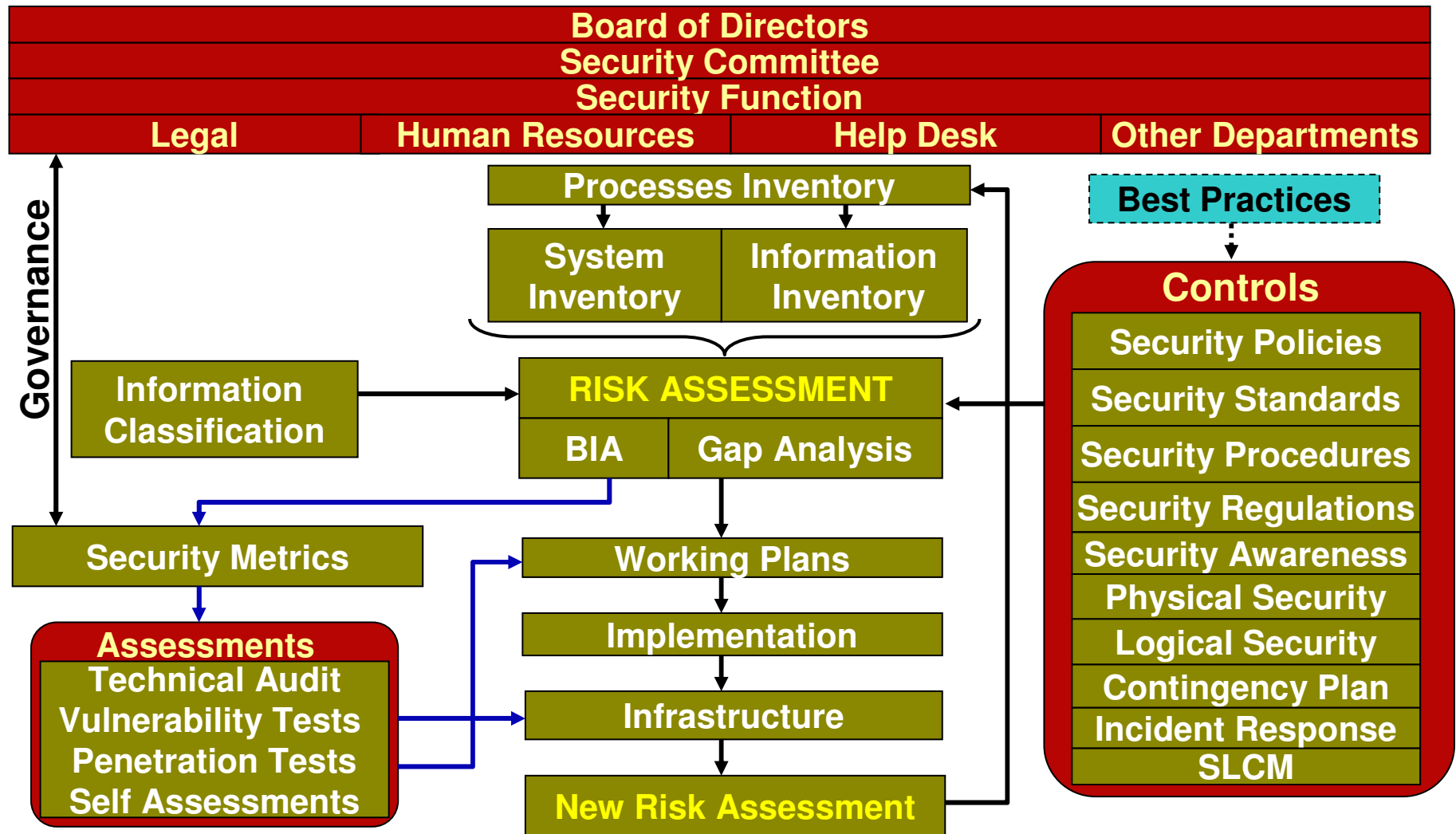
GLBA Life Cycle



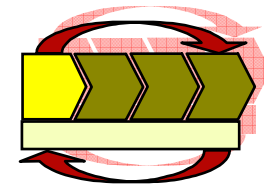
Information Security Program



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.



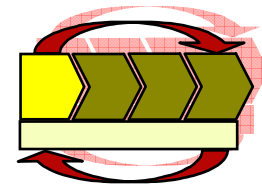
Information Security Program



The information security program shall be designed to:

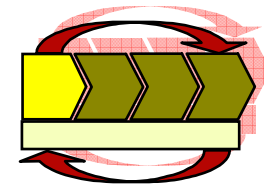
- Ensure the security, confidentiality and integrity of customer information.
- Protect against any anticipated threats or hazards to the security, confidentiality and integrity of customer information.
- Protect against unauthorized access to or use of customer information which could result in substantial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

Information Security Program



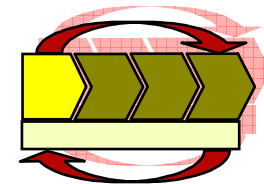
- Design the information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the bank's activities.
- Each financial institution must consider and adopt those security measures the bank determines are appropriate.
- 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



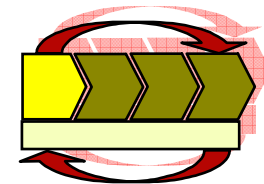
- Access restrictions at physical locations containing customer information, such as buildings, computer facilities, and records storage facilities.
- Encryption of electronically transmitted and stored customer information.
- Procedures designed to ensure that customer information system modifications 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



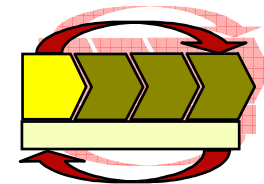
- Monitoring systems and procedures to detect actual and attempted attacks or intrusions into customer information systems.
- Response programs that specify actions to be taken when the bank suspects or detects that unauthorized individuals have gained access to customer information systems, including 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.

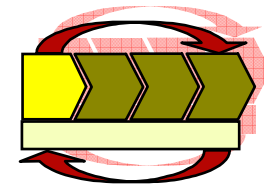
Information Security Program



Security Fundamental Principles:

- **Confidentiality**
 - Information should be accessed only by authorized individuals.
 - Prevent unauthorized access to information.
- **Integrity**
 - Changes to information are performed by authorized individuals using authorized procedures.
 - In addition, information should be consistent, in both internal and external form.
- **Availability**
 - Information is available when needed.

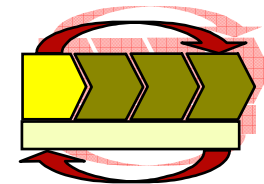
Information Security Program



Organizational Departments:

- The Information Security Program will impact all departments.
- Some departments are more involved than others.
- Legal Department:
 - Evaluate third party contracts
 - Support for incident response situations
 - Review laws and regulations
 - Interact with other lawyers and with law enforcement

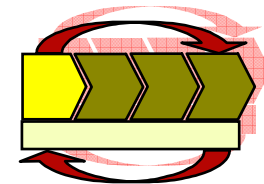
Information Security Program



Organizational Departments:

- Human Resources Department
 - Process employees when they are hired, transferred to a new position and terminated
- Help Desk Department
 - Identify Information Security Help Desk persons responsible for answering information security related problems
 - Provide the first line of defense for information security – social engineering

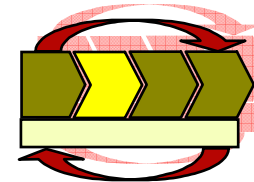
Information Security Program



Security Metrics:

- Information systems security metrics provide a practical approach to measuring information security within the organization.
- Good metrics tie closely to business strategies, objectives, program maturity and the company's control environment.
- Some security metrics include:
 - Time to install software patches (if the business units apply their own patches)
 - Lost or stolen mobile computers
 - Rogue wireless access points discovered
 - Delay between employee termination and manager seeking access shutoff

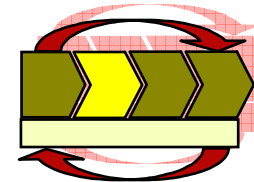
Risk Assessment



Each Financial Institution shall:

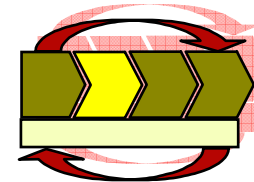
- Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information systems.
- Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information.
- 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.

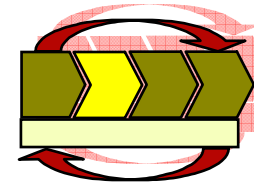
Risk Assessment



Methodology:

- Phase 1: Inventory of information assets
 - Systems and applications
 - Electronic documents
 - Manual documents
- Phase 2: Classification of information assets
 - Sensitivity of asset
 - Public, confidential or top secret
 - Security component
 - Confidentiality, integrity and availability

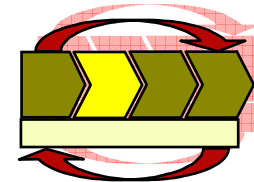
Risk Assessment



Methodology:

- Phase 3: Threat analysis
 - Probability that the threat will occur
 - Various levels ranging from low to high
 - Impact on institution if threat materializes
 - Low, medium or high
- Phase 4: Controls/safeguards analysis
 - Existence and degree of security controls currently in place
 - Yes, no or partial
 - **Integrates results from vulnerability assessment**

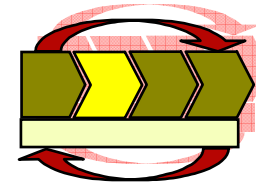
Risk Assessment



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.

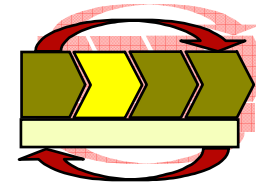
Risk Assessment



Gap Analysis:

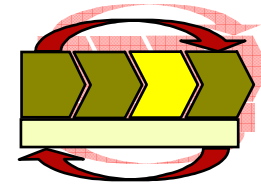
- Ensure management formally approves any decision to accept risks.
- The result of this phase are working plans with security controls implementation priorities.

Risk Assessment



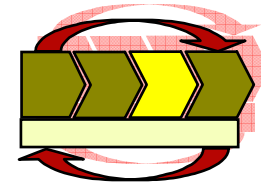
- Perform risk assessments on a regular basis.
- As the organization, processes, infrastructure, systems and data change with time, the risk assessment needs to be conducted again to identify new risks.
- Risk assessment is an on-going process.

Vulnerability Assessment



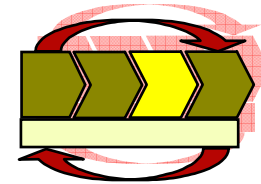
- Assess the overall adequacy of existing security controls present in the infrastructure and associated processes under review.
- The assessment is performed using a snapshot of the security controls currently in place.
- The assessment focuses on each individual component's security posture.
- Vulnerability assessment can include:
 - Operating Systems
 - Critical Applications
 - Database Systems
 - Networking Components
 - Interfaces between applications

Vulnerability Assessment



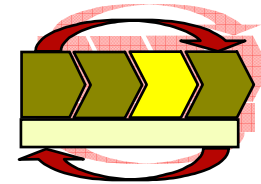
- A vulnerability assessment is NOT exclusively a technical security review.
- All security controls related to the area under revision should be considered including:
 - Technical
 - Non-Technical

Vulnerability Assessment



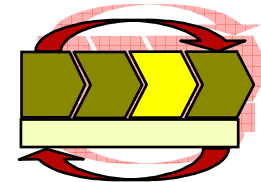
- Identifies potential security weaknesses in the infrastructure and associated processes of an organization.
- Identifies existing security controls and whether they are working as expected.
- Identifies gaps between existing security configurations, required security standards and industry best practices.

Vulnerability Assessment



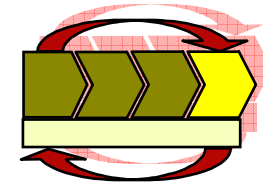
- Can assess the security controls implemented in the organization's infrastructure.
- Can verify against a standard or best practice.
- Can provide a benchmark.

Vulnerability Assessment



- Cannot ensure 100% security.
- Cannot assess the “informal” internal processes and procedures (e.g., password sharing).
- Cannot detect fraud.

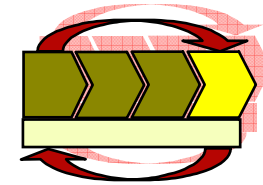
Implementation of Security Controls



Working Plans:

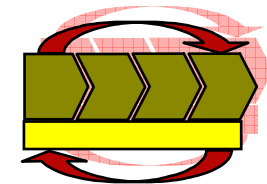
- Working plans must be developed prior to the implementation of security controls.
- Develop strategic and detailed plans addressing the areas where security is required to mitigate the risks found during the risk assessment and vulnerability assessment.
- Develop detailed plans per area and include 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.

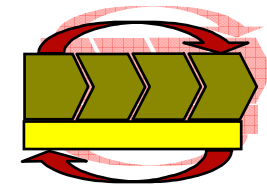
Board Directors Involvement



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

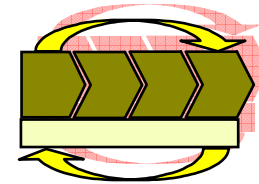
- Approve the bank's written information security program.
- Oversee the development, implementation, and maintenance of the bank's information security program, including assigning specific responsibility for its implementation and reviewing reports from management (e.g., risk assessment and vulnerability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

Board Directors Involvement



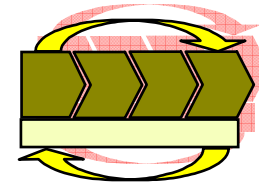
- The success of the Information Security Program will depend on the support, direction and management of the board of directors and management.
- Entities should have an adequate security structure within their board of directors and throughout the organization as a whole.

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.

Enforcement

- The GLB Act gave the Bank Regulatory Agencies (OCC, FDIC, etc.) enforcement authority.
- The bank regulators are taking both informal and formal enforcement actions against banks who fail to comply with the GLBA.

Enforcement

- If regulators find inadequacies in the financial institution's program for securing customer data, the regulators may pursue an informal agreement to remedy the security weaknesses.
- For example, in a recent examination of an institution, the FDIC required improvements with respect to risk assessment and controls.

Enforcement

- Formal enforcement actions include written agreements, cease and desist orders and civil money penalties.
- For example, the FDIC has issued a cease and desist order requiring periodic penetration tests.

Criminal Penalties

- It is a crime for anyone to knowingly and intentionally obtain or cause the disclosure of customer information through fraudulent means.
- For smaller offenses, the maximum sentence is 5 years imprisonment and a \$250,000 fine for individuals, and a \$500,000 fine for corporations.
- For aggravated offenses, the maximum sentence is 10 years imprisonment and a \$500,000 fine for individuals, and a \$1,000,000 fine for corporations.

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

How Can ERM and GT Help?

- **Design a comprehensive security program.**
- **Perform risk assessments.**
- **Perform vulnerability assessments.**
- **Implementation of required automated and manual security controls.**
- **Assist with security training.**
- **Assist with on-going security log monitoring.**
- **Periodic on-going review and guidance.**

Q&A

www.emrisk.com
info@emrisk.com
305.447.6750