

Examination Procedures to Evaluate Compliance with the Guidelines to Safeguard Customer Information

Background

These examination procedures are derived from the interagency Guidelines Establishing Standards for Safeguarding Customer Information, as mandated by Section 501(b) of the Gramm-Leach-Bliley Act of 1999. The guidelines address standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.

The guidelines require each institution to 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. While all parts of the institution are not required to implement a uniform set of policies, all elements of the information security program must be coordinated.

These examination procedures are intended to assist examiners in assessing the level of compliance with the guidelines. As such, the procedures are annotated, with commentary, to provide guidance regarding the purpose of the examination procedure or as guidance in performing the procedure.

The examination procedures are designed to apply to a wide range of banks. As such, certain procedures may not apply to smaller or less complex institutions. Examiners should take these factors into consideration during their evaluations.

Examination Procedures

Examination Objective: Determine whether the financial institution has established an adequate written Information Security Program and whether the program complies with the Guidelines Establishing Standards for Safeguarding Customer Information mandated by section 501(b) of the Gramm-Leach-Bliley Act of 1999.		
	Key Questions or Considerations	Clarification/Annotation
I.	Determine the involvement of the board.	
A.	Has the board or its designated committee approved a written Corporate Information Security Program that meets the requirements of the Information Security Guidelines (guidelines)?	Review the program to determine if it is appropriate for the size and complexity of the institution and the nature and scope of its activities.
B.	If the board has assigned responsibility for program implementation and review of management reports to an individual or committee, do they possess the necessary knowledge, expertise and authority to perform the task?	
C.	Does the program contain the required elements?	Determine whether the program includes the basic elements of the GLBA requirements.
1.	If more than one information security program exists for the institution, are the programs coordinated across organizational units?	Determine whether an enterprise-wide coordination of information security programs exists. Coordination should encompass all elements of the information security programs. One master program is not required.
D.	Determine the usefulness of reports from management to the board (or its designated committee). Does the report adequately describe the overall status of the program, material risk issues, risk assessment, risk management and control decisions, service provider oversight, results of testing, security breaches and management's response, and recommendations for program changes?	Determine who reviews the reports to ensure they are accurate.
1.	How often does the board (or its designated committee) review reports?	Reports on compliance with guidelines should be presented to the board (or its designated committee) at least annually.
E.	Overall, do management and the board (or its designated committee) adequately oversee the institution's information security program?	Comment on the degree of involvement in the oversight process by the board (or its designated committee) and involvement by senior management.

II.	Evaluate the risk assessment process.	
A.	Review the risk assessment program.	
1.	How does the institution assess risk to its customer information systems and non public customer information?	Review the steps taken to identify reasonably foreseeable threats and the potential damage those threats could cause given the policies, procedures, systems, and other factors that are in place to control risk. Discuss the use of current relevant information such as: hardware and software vulnerabilities, methods of attack, network topology, contractual requirements with outside parties, controls and control environment (e.g., policies, procedures, practices, budgets, organizational charts, and training), and test results.
2.	Has the institution evaluated the risk to the entire customer information system?	The customer information system is broader than automated systems. It includes all methods to access, collect, store, use, transmit, protect, or dispose of customer information.
3.	Has the institution used personnel with sufficient expertise to assess the risks to its systems and customer information on an enterprise-wide basis?	An enterprise-wide risk assessment using skills and knowledge from across the enterprise, from technical staff to management, should be conducted. Institutions may supplement their own knowledge with outside expertise. Less complex institutions may require fewer resources.
4.	Is the risk assessment part of a formal risk assessment process with timelines and milestones? If not, how will management ensure timely completion?	
5.	Does the institution have a process for identifying and ranking its information assets (data and system components) according to sensitivity? How does it use this process in its risk assessment?	The institution should identify the relative sensitivity of its information and customer information system, and use that identification to determine how certain data elements or system components should be protected. No specific process is required; whatever process is used should be logical, supportable, and appropriate for the institution.
B.	Assess adequacy and effectiveness of risk assessment process.	

1.	Does the institution identify all reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems?	Review for reasonableness the threats management has identified.
2.	Does the institution support its estimate of the potential damage posed by various threats?	Review the process management uses to identify the potential risks and to assess the potential damage, if the risk is not mitigated.
3.	Review the institution's existing controls to mitigate risks. Does the institution's analysis consider the current administrative, physical, and technical safeguards that prevent or mitigate potential damage?	
4.	Does the institution use test results to support its assessment of the adequacy and effectiveness of those controls?	
C.	Does the institution identify and prioritize its risk exposure, decide on the risks it must mitigate, and create a mitigation strategy? Is the decision to accept risks documented and reported to the appropriate management levels?	Review factors used to evaluate level of risks and acceptability of risk as a business decision. Assess the reasonableness of documentation used to support this decision. All risk acceptance must be supported adequately and approved by the appropriate level of management.
1.	Does the institution promptly act to mitigate risks that pose the immediate possibility of material loss?	Risk assessments that uncover immediate risks of material loss should be traceable to prompt actions taken to mitigate those risks.
2.	How does the institution demonstrate that the mitigation strategy was reviewed by appropriate officials?	Review documentation.
3.	Does the risk assessment provide guidance for the nature and extent of testing?	
4.	Does the risk assessment include vendor oversight requirements?	

III.	Evaluate the adequacy of the program to manage and control risk.	
A.	Review internal controls and policies. Has the institution documented or otherwise demonstrated, at a minimum, that it considered the following controls, and adopted those it considered appropriate?	Assess the adequacy of controls used to support risk mitigation judgments.

1.	Access controls, such as controls to authenticate and permit access to customer information systems to authorized persons only.	Controls include both technical measures and procedures to guard against non-technical attacks, such as impersonation or identity theft.
2.	Access restrictions at physical locations, such as buildings and computer facilities, to permit access to authorized persons only.	Physical locations include all places where customer data is kept in a retrievable form, including document disposal.
3.	Encryption of electronically transmitted and stored customer data.	Review the encryption standards used by the institution. The selection of data to encrypt and the encryption technique and level should be supported by the risk assessment.
4.	Procedures to ensure that systems modifications are consistent with the approved security program.	Discuss changes in control procedures. Determine who has access to make changes to the system, both hardware and software, and how those changes are reviewed and verified.
5.	Dual control procedures, segregation of duties, and employee background checks.	Check standard internal control procedures to minimize fraud and other risks. In general, only employees should have access to customer information or customer information systems necessary to perform job functions.
6.	Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems.	Review monitoring systems and procedures, including network and host intrusion detection systems, network traffic monitoring, manual review of logs, and other information available to assess management's monitoring processes.
7.	Response programs specifying actions to be taken by specific individuals when the institution suspects unauthorized access (i.e., incident response).	Determine whether procedures are in place to isolate, analyze, recover, and appropriately report unauthorized access. Recovery involves technical as well as public relations elements. Consider whether the bank has appropriate internal and external reporting procedures (e.g., regulator, law enforcement, news media).
8.	Measures to protect against destruction, loss, or damage of information from potential environmental hazards, such as fire and water damage or technological failures.	Review data and system backup and business resumption capabilities.
B.	Is staff adequately trained to implement the security program?	Review existing staff qualifications and requirements for ongoing training to ensure that the staff stays abreast of current technology and methods to safeguard customer information.

1.	Obtain from management a listing of the training provided to all users of the institution's system.	Training includes awareness programs as well as classroom instruction. Training should be consistent with user's security-related responsibility and function.
C.	Determine whether key controls, systems, and procedures of the information security program are regularly tested by independent third parties or qualified independent staff in accordance with the risk assessment.	Verify that the institution has identified its key controls, systems, and procedures. Key controls can be both technical and procedural in nature.
1.	Assess whether the nature and frequency of testing is consistent with the risk assessment.	Review scope and test results to ensure they address key risk areas.
2.	Assess whether tests are conducted or reviewed by independent third parties or qualified staff independent of those that develop or maintain the security program.	Tests should be conducted or reviewed by persons independent of those who operate the systems, including the management of those systems.
3.	Assess whether management reviews test results promptly. Assess whether management takes appropriate steps to address adverse test results.	Assess adequacy of corrective actions taken.

IV.	Assess the measures taken to oversee service providers.	
A.	Determine whether the institution exercises due diligence in selecting service providers.	Due diligence should include a review of the measures taken by a service provider to protect customer information.
B.	Determine what information is supplied to service providers.	List vendor(s) and type of data that is shared with them.
C.	Obtain a copy of the contract(s) with the service provider(s). Determine whether contracts require service providers to implement appropriate measures to meet the objectives of the guidelines.	Contracts entered on or before March 5, 2001 must be brought into compliance by July 1, 2003.
D.	If the institution's risk assessment requires monitoring a service provider, then perform the following steps for each applicable service provider.	
1.	Determine whether the service provider contract provides for sufficient reporting from the service provider to allow the institution to appropriately evaluate the service provider's performance and security, both in ongoing operations and when malicious activity is suspected or known.	Review the service provider reporting to ensure it provides the institution with sufficient information to manage the risks of inadequate performance as well as suspected or actual information security compromise.

2.	Determine whether the institution's actions adequately control information supplied to service providers, ensuring that the information is managed and secured properly.		Review vendor management policies and procedures for adequacy, including the appropriateness and completeness of management reviews of service provider audits, test results, or other equivalent evaluations.
3.	Review financial condition of service provider.		

V.	Determine whether an effective process exists to adjust program.		
A.	Does the institution have an effective process to adjust the information security program as needed? Is the appropriate person assigned responsibility for adjusting the information security program?		Regardless of who does the oversight (board, designated committee, or individual), assess adequacy of monitoring, discuss the current program, and identify planned changes to the program.
B.	Review procedures that are in place to ensure that when the institution makes changes in technology and its business function the requirements of the guidelines are also considered. These changes can include: 1) Technology changes (e.g., software patches, new attack technologies and methodologies). 2) Sensitivity of information. 3) Threats (both nature and extent). 4) Upcoming changes to institution's business arrangements (e.g., mergers and acquisitions, alliances and joint ventures, outsourcing arrangements). 5) Upcoming changes to customer information systems (e.g., new configurations or connectivity, new software).		Determine how the responsible individual(s) is (are) informed of changes that might require adjustment to the program.
C.	Determine whether appropriate expertise is applied to evaluate whether changes to the information security program are necessary.		
D.	Determine whether appropriate controls exist to ensure changes to the information security program are properly implemented in a timely, risk-based manner.		The institution should ensure that adequate controls are implemented before the institution changes its systems or environment.

VI.	Summarize and communicate your findings.		
A.	Discuss issues, conclusions, and potential violations with EIC.		

B	Discuss findings with institution management. If you have identified material issues, obtain and document management commitments to address those issues.		
C.	Complete workpapers.		
D.	Detail findings with support in a Summary Comment.		