
Technology Risk Controls Program

Examination Objective

To assess the extent to which management identifies and mitigates the institution's primary information technology (IT) risks.

Examination Procedures

Technology risk controls essentially are internal controls that an institution should build into daily operations. This program complements traditional examination procedures in the evaluation of specific activities, such as lending, deposit-gathering, and nondeposit activities. You may need to contact examiners in other examination areas to comprehensively evaluate an institution's activities. In addition, you should coordinate efforts to review written policies, internal controls, and other related functions.

If you note problems or unusual factors, consider referrals to information systems, compliance, and other examiners (for example, capital markets specialists). You may also consult with the Regional IT Manager whenever you need additional technological information.

Interagency Guidelines Establishing Standards for Safeguarding Customer Information

Procedures in this program provide for the review and evaluation of a financial institution's compliance to guidelines establishing standards for safeguarding customer information that implement sections 501(b) and 505 of the Gramm-Leach-Bliley Act (GLB). The Interagency Guidelines Establishing Standards for Safeguarding Customer Information is in three parts consisting of: I. An introduction that describes the scope of the guidelines. II. Standards for Safeguarding Customer Information. III. Development and Implementation of information security program.

Part I - Scope: The guidelines apply to customer information maintained by or on behalf of entities over which OTS has authority. These entities are savings associations whose deposits are FDIC insured and any subsidiaries of such savings associations, except brokers, dealers, persons providing insurance, investment companies, and investment advisers.

Part II – Standards: (A) The savings association shall implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the savings association's size and complexity and the nature and scope of its activities. (B) The savings association shall design the information security program to ensure the security and confidentiality of customer information, protect it against anticipated threats, hazards, and unauthorized access that could result in substantial harm or inconvenience to any customer.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Technology Risk Controls Program

Part III – Development and implementation of information security program: Describes the regulatory agencies' expectations for the creation, implementation, and maintenance of an information security program, consisting of the following:

- A. Involve the Board of Directors
- B. Assess risks to customer information
- C. Manage and control the risks
- D. Oversee related service provider arrangements
- E. Adjust the information security program, as necessary.
- F. Provide a written report to the board regarding the status of the program
- G. Implement the (GLB guideline) standards by July 1, 2001.

To evaluate management's compliance to the GLB guidelines, we include and identify the guidelines in Level I and II procedures under Audit, Management Oversight, Information Integrity, Business Continuity, and Internet Banking.

Level I

Wkp. Ref.

1. Ascertain the institution's IT environment and risks. Review the following documents:
 - Standard scoping materials (prior ROE, Regulatory Profile, supervisory correspondence).
 - Preliminary Examination Response Kit (PERK 005), including information related to the Information Technology Database (ITD). Review ITD data for completeness and accuracy. Forward a copy to the regional office according to local instructions.
 - Internal or external audit reports, third-party reviews, and client control letters.
 - Examination reports (by OTS or other FFIEC agencies) pertaining to the institution's IT environment (service providers, software vendors and others).

-
2. Determine if the institution corrected any previous violations and addressed any criticisms.
-

Exam Date: _____

Prepared By: _____

Reviewed By: _____

Docket #: _____

Technology Risk Controls Program

Wkp. Ref.

3. Gain an understanding of the institution's IT environment and risks, including:
 - Identify mission-critical systems.
 - Develop an understanding of the IT infrastructure, including Local Area Networks (LANS), Wide Area Networks (WANS), and other IT resources.
 - Obtain information on recent, current and planned major IT projects, such as systems conversions, the introduction of a new product, or the introduction or expansion of electronic banking (including websites).
-

Audit

4. Assess the adequacy of audit coverage of the institution's IT-related risks and management's responsiveness to audit issues.
 - Determine whether IT audit plans, schedules, and/or audits completed since the preceding examination are commensurate with the institution's IT environment and IT-related risks. The institution should regularly schedule evaluations of the information security program. (GLB III-C)
 - If audit plans and schedules are appropriate:
 - Determine whether audits have been performed according to plan.
 - Determine whether audits have appropriately addressed the risks identified in this program.
 - Determine whether significant audit concerns are timely reported to senior management and the board of directors.

 5. Assess management's overall responsiveness to audit concerns, including the timeliness of corrective action.
-

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Technology Risk Controls Program

Wkp. Ref.

6. Determine whether other examiners identified significant IT-related issues such as deficiencies related to data integrity, computer models, or information security in areas of their review. If so, investigate the underlying cause(s) and implications. Consult with the examiner in charge and, if appropriate, the Regional IT Manager.
-

If the thrift has well-qualified staff that conduct a thorough audit of technology risk controls (including the assessment of compliance to GLB information security guidelines), and management responds quickly and appropriately to audit and examination issues, you may conclude this Program now or selectively complete other Level I procedures before concluding.

If an internal or external audit covers technology risk controls, but one or more aspect is weak, lacking, or out-of-date, continue within Level I, and select and complete procedures that correspond to the situation at hand.

If there is no independent review of technology risk controls by an internal auditor, external auditor, or another qualified individual, generally you should complete all of the remaining Level I procedures.

If Level I procedures reveal or suggest weaknesses, complete corresponding Level II procedures.

You may also selectively complete Level II procedures to test Level I findings.

Management Oversight

7. Determine whether the institution has an IT plan appropriate to the size and complexity of its technology environment. Determine whether the board approved the plans, and whether the approval process ensures that the IT plan aligns with the business plan.
-

8. Review minutes of board and management meetings for evidence of involvement in and approval of significant IT matters. Board minutes should reflect the review and approval of the institution's written information security program and continued oversight over the maintenance of the program. (GLB III-A)
-

Exam Date: _____

Prepared By: _____

Reviewed By: _____

Docket #: _____

Technology Risk Controls Program

Wkp. Ref.

Information Integrity

9. Review guidance for employees pertaining to the need to protect the integrity and confidentiality of customer and corporate information. Such guidance may describe the employee's responsibilities and consequences of improper actions. It may also give examples of improper activity, such as, the unauthorized disclosure of customer account information.

10. Determine whether an adequately designed information security program has been established for the institution (GLB III-G requires implementation by July 1, 2001). Information security policies, procedures, and standards now in operation provide for the following (GLB III-B and III-C):

- Implementation and periodic adjustment of a risk assessment process pertaining to customer and corporate information.
- Controlled assignment of user access to customer information and sensitive corporate data.
- Monitoring of access to and use of sensitive or powerful system capabilities (such as the ability to override overdraft or check-cashing limits).
- Internet services access controls.
- Data input quality controls (for new accounts, the interest rate control file, and spreadsheets).

11. Review a sample of user access profiles for conformance to policies and procedures. Include sample profiles of teller, back-office, and security administrator access for at least one of the institution's primary systems (such as the deposit, mortgage loan, general ledger system, or Fedline).

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Technology Risk Controls Program

Wkp. Ref.

Business Continuity

12. Assess the overall policy for disaster recovery (Business Continuity and Business Resumption) to determine management's requirements for departments or other operating units to establish, maintain, and test plans for their areas.

-
13. Review the institution's disaster recovery plans for one or more mission-critical systems and determine if the plans provide for the following (GLB III-C):

- Recovery of lost customer and corporate data.
- A management-approved time line for completion of recovery.
- Testing and periodic updating of the plans.

For internally operated systems selected, also determine if the plans provide for:

- Replacement of damaged resources (such as hardware and software).
 - An alternate processing location.
-

Vendor Management

14. Determine if the institution established adequate vendor-related policies. Ensure that the institution exercises appropriate due diligence in managing and monitoring its service providers. Confirm that the thrift maintains effective information security programs to protect customer information.

-
15. Assess the institution's controls for monitoring its primary service provider's service-level performance.

- Determine whether the institution periodically verifies the service-level performance reports supplied by the service provider.

Exam Date: _____

Prepared By: _____

Reviewed By: _____

Docket #: _____

Technology Risk Controls Program

Wkp. Ref.

- Determine whether executive management is promptly informed of significant deficiencies in vendor performance.
-

Internet Banking

Thrift institutions generally outsource the implementation and operation (“hosting”) of Web sites to one or more Internet Service Providers (ISPs). We limit the scope of this program to the review of controls thrift management established to minimize the risk of operating within an internet environment. However, hardware and software controls related to operation of the ISP service are not within the scope of this program.

If the institution hosts its own web site (i.e., the thrift operates its own computer and software to support its web site), an IT examiner should assess the associated controls.

16. Assess the institution’s Internet-related information security controls.

- Determine whether the institution is prepared to deal with Internet information security matters through the support and advise of qualified employee(s) or outside consultants.
- Determine whether the thrift has established policies and standards related to the use of Internet facilities and services by its employees. The policies should indicate the user authorization process, the Internet services allowed, and the need for controls such as authentication, firewalls, and encryption. (GLB III-C)
- Assess management’s process for verifying the adequacy of its Internet service provider’s (ISP) information security and transaction verification controls. (GLB III-D)

17. If the institution created a transactional website since the previous exam determine that they provided the notice to OTS as required by CEO memo No. 109. Contact the regional office to determine the need for follow-up to ensure compliance with the requirements set forth in the CEO memo.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Technology Risk Controls Program

Wkp. Ref.

Level II

Management Oversight

- | | |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| 18. Assess the adequacy of IT resource acquisition and outsourcing policy and determine whether it covers cost / benefit analysis; vendor selection and due diligence; management approval (authority limits or guidelines); contract execution; and software licensing. (GLB III-D) | |
| 19. Assess the appropriate corporate policy (IT or other) covering insurance to determine whether IT insurance coverage is periodically reviewed and approved by senior management. | |
| 20. Determine whether management provides the board with report(s) that describe the overall status of the information security program and the institution's compliance with the GLB guidelines. (GLB III-F) | |

Information Integrity

- | | |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| 21. Determine whether the design of the information security program complies with GLB guidelines as regards the scope and standards for safeguarding customer information. (GLB I and II) | |
| 22. Evaluate the customer and corporate information risk assessment process. Management should (GLB III-B): <ul style="list-style-type: none">• Maintain an inventory of all repositories of customer and corporate information. Management should take particular note of non-public customer information and mission-critical corporate information. Repositories include electronic and paper files.• Identify threats to the integrity and confidentiality of the information. | |

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Technology Risk Controls Program

Wkp. Ref.

- Assess the sufficiency of policies and procedures intended to control the risks. Management can accomplish assessments through self-inspection, or through independent audits.
- Monitor, evaluate, and adjust the risk assessment, taking into consideration any change in the IT environment or sensitivity of the information.

23. Assess the user-access assignment process. Determine whether institution managers have (GLB III-C):

- Identified the system's sensitive customer-record fields and powerful transactions.
- Assigned job responsibilities that provide for proper segregation of duties and dual control over sensitive fields and powerful transactions.
- Assigned user information retrieval and transaction processing capabilities according to defined job responsibilities.
- Appropriately limited the assignment of highest user access capabilities (for example, Security Administrator).
- Created and authorized the user access profiles for implementation by the information security officer.

24. Perform sampling tests to verify that user-access assignments are in conformance with management-designed user access profiles (or, in the absence of such profiles, that user access assignments are appropriate).

- Obtain printouts of access profiles of selected users from one of the institution's systems. Include a range of users.
- Ascertain if the system access profiles show inconsistencies with management-designed user access profiles or defined job responsibilities.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Technology Risk Controls Program

Wkp. Ref.

- Identify the sensitive data and transaction processing capabilities of selected users and ascertain if their execution is protected by prudent controls.
-
25. If you find any user access assignments to be inappropriate, determine if the condition was caused by (a) control deficiencies in the granting of user access assignments or (b) deficiencies in the system's security controls (system rules or software).
-
26. Determine if management periodically reviews and updates user-access assignments. (GLB III-E)
-
27. Determine if appropriate controls are in place to monitor activities of employees in areas where proper segregation of duties is not feasible, and of other sensitive activities such as the file maintenance of customer records. (GLB III-C)
-
28. Determine if appropriate user access and monitoring policies and procedures are adequately documented.
-
29. Evaluate information security policies and standards in effect for (GLB III-C):
- User-ID controls.
 - Passwords.
 - System log-on and log-off.
 - Virus-protection.
 - Encryption of sensitive customer or corporate information whether used and stored within the institution or transmitted elsewhere.
 - Destruction or disposal of sensitive customer and corporate information to ensure

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Technology Risk Controls Program

Wkp. Ref.

that the information will not be unintentionally made available to unauthorized persons. Proper disposal could include shredding of paper media, deleting, or degaussing (erasing) of data in electronic media, etc.

30. Assess data-input quality controls. Determine whether controls are in place to verify the completeness and accuracy of sensitive input data that are not readily verifiable by the editing capabilities of the automated system.

31. Assess personnel access restrictions at locations containing customer or corporate information, such as buildings, computer facilities, work areas, and records storage facilities. (GLB III-C)

Business Continuity Risk

32. Assess the institution's disaster recovery plans and testing related to outsourced systems. Obtain and review the institution's service provider-related contingency plan to determine if it (GLB III-C):

- Identifies all the categories and sources of data input into the service provider's systems by the thrift.
- Describes the steps required to recover previously input data and prepare them for resubmission when requested by the service provider.
- Identifies the person or teams responsible for executing the recovery steps.
- Provides a management-approved time line for input resubmission.

33. Determine if the institution periodically reviews the plan to help ensure that it is current and effective. (GLB III-E)

Exam Date: _____

Prepared By: _____

Reviewed By: _____

Docket #: _____

Technology Risk Controls Program

Wkp. Ref.

34. Assess the institution's disaster recovery plans and testing related to internally operated systems. Obtain and review the plan for a selected mission critical system, and determine if the plan provides for (GLB III-C):
- The recovery of key resources, including the computer, operating system software, application system software and data.
 - An alternate processing site/work area.
 - Staff assignments, contact lists, and other recovery related provisions as indicated in OTS CEO Memo 72.
 - A management-approved recovery time line for the completion of recovery.
 - Storage of backup files at a safe location.
 - Updated inventory of files maintained at backup sites.
-
35. Determine if the plan is reviewed periodically to help ensure that it is current and effective. (GLB III-E)
-
36. Determine if there is adequate protection against destruction of institution-maintained customer or corporate information against potential physical hazards such as fire and water damage (GLB III-C).
-

Vendor Management Risk

37. Evaluate the appropriateness of existing contracts. Determine if contracts adequately define performance measures related to vendor commitments and if contracts include recommended contract provisions such as those in TB 46 and CEO Memo 133. Also, determine if there are contract provisions and oversight mechanisms to protect the security of customer information maintained or processed by the service providers.
-

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Technology Risk Controls Program

Wkp. Ref.

38. Assess the institution's controls for monitoring vendor performance and ascertain whether (GLB III-D):
- The institution verifies periodic performance level reports supplied by the service provider.
 - The unit that monitors vendor performance verifies and approves vendor charges for routine and special services.
 - The institution adequately monitors delivery of nonproduction deliverables.
 - Senior management is being promptly informed of significant deficiencies in vendor performance.
-

Internet Banking

Vendor-Related Controls (GLB D)

39. Review documentation of any due diligence review related to the adequacy of prospective ISPs' information security controls. If you identify significant weaknesses, ascertain their status of resolution. Potential areas of weakness are:
- Authentication controls
 - Firewall controls
 - Encryption controls
 - Intrusion-detection controls
 - Incidence-handling controls.
-

40. Assess the effectiveness of controls for the ongoing verification of the adequacy of the ISP's information security program.
-

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Technology Risk Controls Program

Wkp. Ref.

41. Assess management's process for verifying the adequacy of its ISP's business continuity plans. Determine whether management has obtained documented assurance from ISPs that customer transactions are adequately backed up to ensure that they are recoverable in the event of a disaster affecting the ISP.

42. Determine if management monitors the results of tests of the ISP's disaster recovery plans.

43. Assess the appropriateness of the terms and conditions of existing ISP contracts.

44. Assess management's process for monitoring ISP service-level performance.

Institution Controls (GLB III-C)

45. Determine if the institution established policies and procedures to deal with its contractual responsibilities related to outsourced services such as Internet banking, customer bill payment, etc. Procedures should be in place to deal with problem transactions for which the institution is responsible and related customer service activities.

46. Assess controls over the institution's web site systems administrators, if any. The number of administrators should be limited and management should review and approve their web site maintenance capabilities.

47. Determine if the institution's firewall control parameters (i.e., "filters") are described in a document that management reviewed and approved.

Exam Date: _____

Prepared By: _____

Reviewed By: _____

Docket #: _____

Technology Risk Controls Program

Wkp. Ref.

48. Determine if there are modems in PCs or workstations that would allow unauthorized Internet users (e.g., hackers) to circumvent the institution's firewall. If yes, assess existing controls or management's action plan, to mitigate the risk.
-

Conclusions

49. Summarize findings, obtain management responses, and update programs and the continuing examination file (CEF), if applicable, with any information that will facilitate future examinations. File exception sheets in the general file.
-

50. Ensure that your review meets the Objectives of this Handbook Section. State your findings and conclusions, appropriate recommendations for any necessary corrective measures, on appropriate work papers and report pages.
-

Examiner's Summary, Recommendations, and Comments

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____