Information Technology Risks and Controls Program

Examination Objectives

To determine whether management effectively identifies and mitigates the association's information technology (IT) risks.

To determine whether the board of directors adopted adequate policies, procedures, and operating strategies appropriate for the size and complexity of the association's IT environment.

To determine whether the association has a written information security program to comply with the requirements of the Interagency Guidelines Establishing Information Security Standards (Security Guidelines), which implement Sections 501(b) of the Gramm-Leach-Bliley Act of 1999 (GLB Act) and 216 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act).

To determine whether the association has a written identity theft prevention program to comply with the requirements of the Identity Theft Red Flags regulation, which implements Section 114 of the FACT Act.

To initiate corrective action when policies, procedures, or controls are deficient or when you note violations of laws or regulations.

Examination Procedures

WKP. REF.

Level I

Level I procedures assess the association's processes for identifying and managing IT risks. Level I procedures are sufficient when an association has an effective internal control environment for IT risks, and there are no findings, which would cause you to expand your scope.

1. Review the association's response to the PERK 05, previous examination reports, including IT Reports of Examination, internal and external audit reports, and supervisory correspondence. After verifying completeness and accuracy of the IT database information, provide this information to your regional office for processing and input.

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

WKP. REF.

2. Determine that the association implemented effective corrective actions for all previously cited IT exceptions, criticisms, or violations. This includes any matters cited in IT Reports of Examination.

3. Determine the complexity of the association's information technology environment. Identify the association's significant systems. Significant means those critical to ensure information security, satisfactory customer service, and continuity of operations. Review the association's networks. Determine what significant applications are processed on the networks.

4. In conjunction with the Examiner-in-Charge (EIC) or examiner(s) performing the other Management programs, review board of directors' minutes of regular, special, and committee meetings for discussion and approval of significant IT matters. Examples of significant IT matters would include the association's written information security program, its written identity theft prevention program, new or ongoing service provider relationships, and the association's business continuity plan.

5. In conjunction with the examiner(s) performing the reviews of Management and Earnings, determine the effectiveness of the board of directors and senior management in implementing strategic planning for IT. Evaluate plans for any significant changes. Review the association's strategic or business plan for IT-related activities.

6. Review the association's policies and procedures for IT. Determine whether these are effective for monitoring and controlling the association's IT risks considering the complexity of its IT environment.

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

WKP. REF.

7. In conjunction with the examiner(s) performing the review of the audit function, assess the adequacy of the association's audit coverage for IT risks. Verify that audit policies, practices, and programs for IT audits or other independent reviews are adequate for the size and complexity of the association's IT environment.

8. Review IT audits or other independent reviews completed since the preceding examination. Determine that IT audit work products are adequate for the size and complexity of the association's IT environment.

9. Assess management's responsiveness to IT audit concerns. Review the timeliness and adequacy of corrective actions. Confirm that the board of directors is informed of significant audit concerns, and that the board ensures completion of corrective actions.

10. Determine that IT audit expertise and training are sufficient for the complexity of the IT risks of the association.

11. Determine the association's compliance with the objectives of the interagency Security Guidelines implementing Sections 501(b) of the GLB Act and 216 of the FACT Act. The Security Guidelines require associations to have a comprehensive, written information security program that includes the administrative, technical, and physical safeguards to achieve the following objectives:

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

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

WKP. REF.

To meet the objectives and comply with the Security Guidelines, an association must:

- Implement a written information security program that the board of directors approved.
- Conduct and prepare a written information security risk assessment.
- Require in contracts that service providers implement appropriate information security programs designed to meet the objectives of the Security Guidelines.
- Monitor, evaluate, and adjust the information security program for changes in the association's IT environment.
- Report to the board of directors annually regarding the association's compliance with the Security Guidelines and the status of the written information security program.

12. Review measures the association has implemented in its written information security program to manage and control risks. Determine that the association considered and adopted, as appropriate:

- Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals.
- Controls and procedures to prevent employees from providing customer information to unauthorized individuals through pretext calling or other fraudulent methods.
- Access restrictions at physical locations containing customer information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals.
- Encryption of electronic customer information, including while in transit or in storage, or on networks or systems, to ensure unauthorized individuals do not gain access.

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

WKP. REF.

- Procedures designed to ensure that modifications to customer information systems are consistent with the association's written information security program.
- Dual control procedures, segregation of duties, and employee background checks for employees with access to customer information to minimize risk of misuse of customer information.
- Monitoring systems and procedures to detect actual and attempted attacks or other intrusions into customer information systems.
- Response programs that specify actions to take when the association 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 and water damage or technological failures.

13. Confirm that the association has ongoing training for employees that implement and maintain the information security program. Review guidance to association employees for protecting customer and corporate information. Such guidance should describe the employee's responsibilities and consequences of improper actions.

14. Determine that the association has an incident response program consistent with the guidance in CEO Memo 214. Evaluate the effectiveness of the association's program for responding to incidents of unauthorized access to sensitive customer information and providing notification, as required. Confirm that the association's response program contains measures to:

- Assess the nature and scope of the incident.
- Notify OTS, either directly or through the association's service providers.
- Notify law enforcement agencies.
- File Suspicious Activity Reports when required.

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

WKP. REF.

- Control the incidents of unauthorized access.
- Notify customers, when necessary.

15. If the association had incidents of unauthorized access to sensitive customer information, determine that it:

- Conducted a prompt investigation to determine the likelihood the information accessed has been or will be misused.
- Notified customers when the investigation determined misuse of sensitive customer information has occurred or is reasonably probable.
- Delivered notification to customers, when warranted, by means the customer can reasonably be expected to receive, for example, by telephone, mail, or electronic mail.

16. Review the association's customer notice and determine it contains:

- A description of the incident, including type of information subject to unauthorized access.
- Measures taken by the association to protect customers from further unauthorized access.
- Telephone numbers customers can call for information and assistance.
- Reminders to customers to review account statements over a reasonable period – 12-to-24 months – and to report immediately suspicious activity and suspected identity theft incidents.
- A description of a fraud alert and how to place one in a customer's report.
- Recommendations to obtain credit reports from each nationwide credit-reporting agency and have information related to fraudulent transactions deleted.
- An explanation of how customers can obtain free credit reports.

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

WKP. REF.

- Information concerning availability of online guidance by the Federal Trade Commission regarding steps the consumer can take to protect against identity theft.

17. Evaluate the effectiveness of the association's measures to authenticate customers accessing Internet-based services and other electronic banking activities. Ensure that the association's authentication methods and controls specifically address the need for risk-based assessments, customer awareness, and security measures consistent with the guidance in CEO Memo 228. An association should:

- Ensure its information security program identifies and assesses risks associated with Internet-based products and services, identifies risk mitigation actions, and evaluates customer awareness efforts.
- Adjust its information security program for changes in IT, sensitivity of customer information, and internal or external threats to information.
- Implement appropriate risk mitigation strategies.

18. Verify that the association periodically[1] identifies covered accounts it offers or maintains.[2] Verify that the association:

- Included accounts for personal, family, and household purposes that permit multiple payments or transactions; and
- Conducted a risk assessment to identify any other accounts that pose a reasonably foreseeable risk of identity theft, taking into consideration the methods used to open and access accounts, and the association's previous experiences with identity theft.

[1] The risk assessment and identification of covered accounts is not required to be done on an annual basis. This should be done periodically, as needed.

[2] A "covered account" includes: (i) an account primarily for personal, family, or household purposes, such as a credit card account, mortgage loan, auto loan, checking or savings account that permits multiple payments or transactions, and (ii) any other account that the association offers or maintains for which there is a reasonably foreseeable risk to customers or the safety and soundness of the association from identity theft.

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

WKP. REF.

19. Review examination findings in other areas, e.g., Customer Information Security Program, Customer Identification Program and Bank Secrecy Act, to determine whether there are deficiencies that adversely affect the association's ability to comply with the Identity Theft Red Flags Rule (Red Flags Rule).

20. Review any reports, such as audit reports and annual reports prepared by staff for the Board of Directors,[3] or an appropriate committee thereof or a designated senior management employee, on compliance with the Red Flags Rule, including reports that address the following:

- The effectiveness of the association's Identity Theft Prevention Program (Program).
- Significant incidents of identity theft and management's response.
- Oversight of service providers that perform activities related to covered accounts.
- Recommendations for material changes to the Program.

Determine whether management adequately addressed any deficiencies.

21. Verify that the association has developed and implemented a comprehensive written Program, designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or an existing covered account. The Program must be appropriate to the size and complexity of the association and the nature and scope of its activities. Conduct the following procedures:

- Verify that the association considered the Guidelines in Appendix J to the regulation, Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation, in the formulation of its Program and included those that are appropriate.

[3] The term Board of Directors includes: (i) in the case of a branch or agency of a foreign bank, the managing official in charge of the branch or agency, and (ii) in the case of any other creditor that does not have a Board of Directors, a designated employee at the level of senior management.

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

WKP. REF.

- Determine whether the Program has reasonable policies, procedures and controls to effectively identify and detect relevant Red Flags and to respond appropriately to prevent and mitigate identity theft. Associations may, but are not required to use the illustrative examples of Red Flags to identify relevant Red Flags Questions as shown in Supplement A to the Guidelines.
- Determine whether the association uses technology to detect Red Flags. If it does, discuss with management the methods by which the association confirms the technology is working effectively to detect, prevent, and mitigate identity theft.
- Determine whether the Program, including the Red Flags determined to be relevant, is updated periodically to reflect changes in the risks to customers and the safety and soundness of the association from identity theft.
- Verify that (i) the Board of Directors, or an appropriate Committee thereof, initially approved the Program; and (ii) the Board, or an appropriate Committee thereof, or a designated senior management employee, is involved in the oversight, development, implementation and administration of the Program.

22. Verify that the association trains appropriate staff to effectively implement and administer the Program.

23. Determine whether the association exercises appropriate and effective oversight of service providers that perform activities related to covered accounts.

24. Review password controls used on the association's operating systems and significant applications. Confirm these address password length, change intervals, composition, history, and reuse or lockout. Assess effectiveness of these controls.

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

WKP. REF.

25. Assess the association's user access assignment policies and procedures for its information systems. Determine that these policies and procedures:

    - Provide for proper segregation of duties and dual controls.
    - Assign processing capabilities according to job responsibilities.
    - Limit system administrator capabilities appropriately.
    - Create user access profiles or user access assignments that are differentiated according to job duties.
    - Ensure that the association periodically reviews and updates user access assignments for job changes and terminations.

26. Review user access profiles or user access assignments for at least one of the association's significant systems, for example, lending, deposits, general ledger, or funds transfers. Determine that system access rights are consistent with the association's policies and procedures for assigning system access.

27. Confirm that the association has current written procedures to ensure security over its funds transfer activities, and that personnel are adequately trained to follow these procedures.

28. Confirm that each authorized user involved in the association's funds transfer activities maintains a unique password known only to the user. Verify that system users change passwords frequently.

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

WKP. REF.

29. Review the association's business continuity plan. Verify that the business continuity plan is based on a business impact analysis and that it identifies recovery priorities. Confirm that the association tested the business continuity plan within the past twelve months and that the board of directors annually approves testing results and the business continuity plan.

30. Review the association's back-up procedures. Determine what data are backed up, the rotation schedule, where the back-up media are stored, and how soon the back-up media are taken offsite.

31. Ensure that the association excercises appropriate due diligence in selecting, managing, and monitoring its service providers. Determine the association has established adequate policies and procedures to manage its service provider or vendor relationships.

32. Determine that the association's contracts with its service providers have clauses that require the vendors to implement measures designed to meet the objectives of the Security Guidelines. Review the association's policies, procedures, and practices used to confirm that its service providers satisfied obligations under the contract regarding customer information.

33. Determine that the association's board of directors, or an appropriate committee, approves new service provider relationships, or significant changes to existing oursourcing arrangements. These changes should be supported by a written risk analysis consistent with the association's business plan and the proposed or planned activity.

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

WKP. REF.

34. Determine that association management and the board of directors periodically review significant service provider contracts and service level agreements.

35. If the association created a transactional website since the previous exam determine that it provided the notice to OTS as required by CEO Memo 109. If the Notice was not timely and satisfactorily filed, contact the regional office to discuss appropriate remediation actions. Discuss with the regional office the need for follow-up review to ensure compliance with the requirements set forth in the CEO memo.

36. Review the association's website to determine there are no inappropriate or misleading website links.

37. Discuss with your EIC any planned or pending system conversion, transactional website plans not previously communicated to or filed with OTS, system-generated errors that affect integrity of management information or regulatory reports, or any other significant IT issues or concerns. After discussion with your EIC, notify your regional IT Examination Manager, as appropriate.

LEVEL II

After you complete the Level I examination procedures, if you need additional review to support an examination conclusion for a particular IT risk, you should review examination guidance and procedures in the FFIEC Information Technology Examination Handbook for the specific subject matter. These FFIEC Information Technology Examination Handbook procedures are considered Level II procedures for Examination Handbook Section 341.

You should complete the examination procedures in the FFIEC Information Technology Examination Handbook you deem necessary to test, support, and present conclusions derived from performing Level I procedures. Level II procedures provide additional verification regarding the level of technology

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

WKP. REF.

risk and the effectiveness of a savings association's risk management processes and controls. You can use the FFIEC examination procedures in their entirety or selectively, depending on the examination scope and need for additional verification.

EXAMINER'S SUMMARY, RECOMMENDATIONS, AND COMMENTS

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