

Information Technology Risk Examination (InTREx)
Information Technology Profile

Purpose

To provide insight into the institution's Information Technology (IT) operations in order to ensure appropriate resources are allocated to the examination.

Instructions for Completing the Information Technology Profile (ITP)

The ITP contains questions covering significant areas of an institution's IT function. Accurate and timely completion of the ITP will improve the efficiency of the examination process.

No supporting documentation is requested at this time. Based on the responses to the ITP, a customized risk-focused document request list will be sent to the institution in advance of the onsite examination.

Please type the name of the individual completing this document and the executive officer attesting to its accuracy.

Preparer's Name and Title	Institution's Name and Location
Executive Officer's Name and Title	Date Completed

Information Technology Risk Examination (InTREx)

Information Technology Profile

Core Processing

1. Are any core applications (for example: loans, deposits, investments, trust, or general ledger) processed by an external service provider (including affiliated organizations)?

<input type="checkbox"/>	Yes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No
--------------------------	-----	-------------------------------------	--------------------------	----

If Yes, please list the core service provider(s) and the application(s) serviced.

2. Are any core applications (for example: loans, deposits, investments, trust, or general ledger) processed on in-house computer systems? [Note: a Yes response to both 1 and 2 is possible.]

<input type="checkbox"/>	Yes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No
--------------------------	-----	-------------------------------------	--------------------------	----

If Yes, please list the core applications processed in-house.

3. Has the institution changed any core applications or core service providers since the previous examination, or are plans in place to change within the next 12 months?

<input type="checkbox"/>	Yes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No
--------------------------	-----	-------------------------------------	--------------------------	----

If Yes, please list the systems, applications or service providers that have changed or will change.

4. Are any item processing activities, such as branch capture, merchant remote deposit capture, lockbox, or mobile deposit capture, performed in-house?

<input type="checkbox"/>	Yes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No
--------------------------	-----	-------------------------------------	--------------------------	----

Network

1. Is any part of the network virtualized? (Multiple systems or processes sharing a single physical server or device)

<input type="checkbox"/>	Yes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No
--------------------------	-----	-------------------------------------	--------------------------	----

If Yes, please describe.

Information Technology Risk Examination (InTREx)

Information Technology Profile

2. Is there remote access capability to network resources?

<input type="checkbox"/>	Yes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No
--------------------------	-----	-------------------------------------	--------------------------	----

If Yes, please describe.

3. Does the institution have a wireless network (e.g., internal, guest)?

<input type="checkbox"/>	Yes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No
--------------------------	-----	-------------------------------------	--------------------------	----

If Yes, please describe.

4. Are any systems or applications hosted or processed within a cloud environment?

<input type="checkbox"/>	Yes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No
--------------------------	-----	-------------------------------------	--------------------------	----

If Yes, please describe.

5. Is the network configured and managed in-house?

<input type="checkbox"/>	Yes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No
--------------------------	-----	-------------------------------------	--------------------------	----

6. Are network security systems (e.g., firewall, IDS/IPS) configured and managed in-house?

<input type="checkbox"/>	Yes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No
--------------------------	-----	-------------------------------------	--------------------------	----

Online Banking

1. Does the institution host an informational website in-house? (Informational is generally thought of as static content web pages used for marketing and is differentiated from deposit account access and other transactional applications.)

<input type="checkbox"/>	Yes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No
--------------------------	-----	-------------------------------------	--------------------------	----

Information Technology Risk Examination (InTREx)

Information Technology Profile

2. Are online or mobile banking products offered to consumers?

<input type="checkbox"/>	Yes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No
--------------------------	-----	-------------------------------------	--------------------------	----

If Yes, please describe.

3. Are online or mobile banking products offered to commercial customers (e.g., cash management, ACH, wire transfer)?

<input type="checkbox"/>	Yes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No
--------------------------	-----	-------------------------------------	--------------------------	----

If Yes, please describe.

4. Are any transactional online banking applications hosted in-house?

<input type="checkbox"/>	Yes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No
--------------------------	-----	-------------------------------------	--------------------------	----

If Yes, please describe.

Development and Programming

1. Does the institution use or support any custom software, or engage in any custom software development or programming (either internally or through a vendor)?

<input type="checkbox"/>	No	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Report Development	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Bridging/Middleware	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Ancillary Applications	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Core Applications
--------------------------	----	-------------------------------------	--------------------------	--------------------	-------------------------------------	--------------------------	---------------------	-------------------------------------	--------------------------	------------------------	-------------------------------------	--------------------------	-------------------

If Yes, please describe the applications maintained, developed, or supported internally?

Software and Services

1. Does the institution provide any technology services to other entities (including affiliates)?

<input type="checkbox"/>	Yes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No
--------------------------	-----	-------------------------------------	--------------------------	----

If Yes, please describe.

Information Technology Risk Examination (InTREx)

Information Technology Profile

2. If Yes to question 1, does the institution process critical applications for insured financial institutions (including affiliates)?

<input type="checkbox"/>	Yes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No
--------------------------	-----	-------------------------------------	--------------------------	----

If Yes, please list the serviced financial institutions.

Other

1. Does the institution originate ACH debit transactions using NACHA's ACH Standard Entry Class (SEC) codes of WEB or TEL?

<input type="checkbox"/>	Yes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No
--------------------------	-----	-------------------------------------	--------------------------	----

If Yes, please describe (e.g., types of transactions, monthly volume).

2. Does the institution allow personnel, including directors, to use their own mobile devices for bank functions?

<input type="checkbox"/>	Yes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No
--------------------------	-----	-------------------------------------	--------------------------	----

If Yes, please describe.

3. Does the institution have a customer-facing call center?

<input type="checkbox"/>	Yes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No
--------------------------	-----	-------------------------------------	--------------------------	----

4. Is the institution a merchant acquiring institution?

<input type="checkbox"/>	Yes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No
--------------------------	-----	-------------------------------------	--------------------------	----

5. Besides any changes described in Core Processing #3 above, have there been any significant changes in other technologies or services since the prior exam or are any planned for the next 12 months?

<input type="checkbox"/>	Yes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No
--------------------------	-----	-------------------------------------	--------------------------	----

If Yes, please describe.

Information Technology Risk Examination (InTREx)

Information Technology Profile

6. Does the institution have any foreign-based technology service providers?

<input type="checkbox"/>	Yes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No
--------------------------	-----	-------------------------------------	--------------------------	----

If Yes, please describe.

7. Has the institution assessed its cybersecurity program and risk in the past 12 months?

<input type="checkbox"/>	Yes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No
--------------------------	-----	-------------------------------------	--------------------------	----

8. Has the institution or any of its service providers experienced a cyber attack, significant security event, or operational interruption since the previous examination?

<input type="checkbox"/>	Yes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No
--------------------------	-----	-------------------------------------	--------------------------	----

If Yes, please describe.

9. Have there been any changes in key IT management or personnel since the previous examination?

<input type="checkbox"/>	Yes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No
--------------------------	-----	-------------------------------------	--------------------------	----

If Yes, which positions?



Information
Technology
Risk
Examination

Institution Name: [Click here to enter institution name](#)

Cert# [Click here to enter cert number](#)

Preparer: [Click here to enter preparer name](#)

Start Date: [Click here to select a start date](#)

Core Analysis Decision Factors

Note: refer to the FFIEC IT Examination Handbook - Audit if additional analysis is necessary to complete this module.

Decision Factors - Audit

A.1. The level of independence maintained by audit and the quality of the oversight and support provided by the Board of Directors and management.

[Procedures #1-3 ▼](#)

[Click here to enter comment](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

A.2. The adequacy of IT coverage in the overall audit plan and the adequacy of the underlying risk analysis methodology used to formulate that plan.

[Procedures #4-5 ▼](#)

[Click here to enter comment](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

A.3. The scope, frequency, accuracy, and timeliness of internal and external audit reports and the effectiveness of audit activities in assessing and testing IT controls.

[Procedures #6-8 ▼](#)

[Click here to enter comment](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

A.4. The qualifications of the auditor, staff succession, and continued development through training.

[Procedure #9 ▼](#)

[Click here to enter comment](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

A.5. The existence of timely and formal follow-up and reporting on management's resolution of identified problems or weaknesses.

[Procedure #10 ▼](#)

[Click here to enter comment](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

A.6. If applicable, include a summary comment below for any additional risk factors reviewed or examination procedures performed that may not be directly referenced in the Decision Factors above. (These risk factors and procedures could include, but are not limited to, Supplemental Workprograms, FFIEC workprograms, agency-specific workprograms, and/or new guidance not addressed in the modules.)

[Click here to enter comment](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

Summary Comment - Audit

[Click here to enter comment](#)

URSIT Audit Rating: [Click here to select rating](#)

Complete the following procedures at each examination. The resources listed below are not intended to be all-inclusive, and additional guidance may exist.

Resources

- *FFIEC IT Examination Handbook – Audit*
- *Interagency Policy Statement on the Internal Audit Function and its Outsourcing*
- *Interagency Policy Statement on External Auditing Program of Banks and Savings Associations*
- *Interagency Guidelines Establishing Standards for Safety and Soundness*
- *Interagency Guidelines Establishing Information Security Standards*
- *FDIC Risk Management Manual of Examination Policies - Section 4.2 Internal Routine and Controls*

Preliminary Review

Review items relating to internal or external IT audit, such as:

- Examination reports and workpapers
- Pre-examination memoranda and file correspondence
- IT audit charter and policy
- IT audit schedule
- IT audit risk assessment
- Cybersecurity self-assessments
- Internal and external IT audit reports
- Board/Committee minutes related to IT audits
- Organization chart reflecting the audit reporting structure
- Actions taken by management to address IT audit and examination deficiencies

1. Evaluate the independence of the IT audit function and the degree to which it identifies and reports weaknesses and risks to the Board of Directors or its Audit Committee in a thorough and timely manner. Consider the following:
 - IT auditor reports directly to the Board or the Audit Committee
 - IT auditor has no conflicting duties
 - External IT audit firms do not have conflicts of interest (e.g., IT consulting)

[Decision Factor 1 ▲](#)



Control Test

Review the organization chart, the auditor job description, and Audit Committee minutes to verify the reporting structure and independence of the audit function.

[Click here to enter comment](#)

2. Evaluate the quality of oversight and support provided by the Board of Directors and management. Consider the following:

- The institution has a documented audit policy or charter that clearly states management's objectives and delegation of authority to IT audit
- The audit policy or charter outlines the overall authority, scope, and responsibilities of the IT audit function
- The Board or the Audit Committee review all written audit reports
- Deviations from planned audit schedules are approved by the Board or Audit Committee

[Decision Factor 1 ▲](#)

[Click here to enter comment](#)

3. If IT audit is outsourced, review and evaluate outsourcing contracts, audit engagement letters, and policies. Determine whether the documents include the following:

- Expectations and responsibilities for both parties
- The scope, timeframes, and cost of work to be performed by the outside auditor
- Institution access to audit workpapers

[Decision Factor 1 ▲](#)



Control Test

Review the engagement letters for any current outsourced IT audits. Refer to the Interagency Policy Statement on the Internal Audit Function and its Outsourcing for provisions typically included in engagement letters.

[Click here to enter comment](#)

4. Evaluate the IT audit risk assessment process. Consider the following:

- Identification of a comprehensive IT audit universe
- Utilization of a risk scoring/ranking system to prioritize audit resources
- Establishment of Board-approved audit cycles

[Decision Factor 2 ▲](#)

[Click here to enter comment](#)

5. Determine whether the audit plan adequately addresses IT risk exposure throughout the institution and its service providers. Areas to consider include, but are not limited to, the following:

- Information security, including compliance with the *Interagency Guidelines Establishing Information Security Standards*
- Incident response
- Cybersecurity
- Network architecture, including firewalls and intrusion detection/prevention systems (IDS/IPS)
- Security monitoring, including logging practices
- Change management

- Patch management
- Third-party outsourcing
- Social engineering
- Funds transfer
- Online banking
- Business continuity planning

[Decision Factor 2 ▲](#)



Independent audit or review evaluates policies, procedures, and controls across the institution for significant risks and control issues associated with the institution's operations, including risks in new products, emerging technologies, and information systems.

Logging practices are independently reviewed periodically to ensure appropriate log management (e.g., access controls, retention, and maintenance).

The independent audit function validates controls related to the storage or transmission of confidential data.



Control Test

Validate that IT audits have been performed according to the approved audit plan.

[Click here to enter comment](#)

6. Determine whether the actual frequency of IT audits aligns with the risk assessment results and whether the scope of IT audits is appropriate for the complexity of operations.

[Decision Factor 3 ▲](#)

[Click here to enter comment](#)

7. Review IT audit reports issued since the previous examination. Evaluate whether the reports adequately:
- Describe the scope and objectives
 - Describe the level and extent of control testing
 - Describe deficiencies
 - Note management's response, including commitments for corrective action and timelines for completion
 - Detail follow-up/correction of prior IT audit or regulatory examination exceptions

[Decision Factor 3 ▲](#)

[Click here to enter comment](#)

8. Evaluate the ability of the IT audit function to accurately assess, test, and report on the effectiveness of controls. Consider the following:

- IT examination findings
- Cyber incidents
- Other significant IT events

[Decision Factor 3 ▲](#)



Control Test

Sample the audit workpapers for adequacy and completeness.

[Click here to enter comment](#)

9. Determine whether auditor expertise and training is sufficient for the complexity of the IT function in relation to the technology and overall risk at the institution. Consider the following:

- Education
- Experience
- On-going training

[Decision Factor 4 ▲](#)

[Click here to enter comment](#)

10. Evaluate the audit department's process for monitoring audit and regulatory findings until resolved. Consider the following:

- A formal tracking system that assigns responsibility and target date for resolution
- Timely and formal status reporting
- Tracking and reporting of changes in target dates or proposed corrective actions to the Board or Audit Committee
- Process to ensure findings are resolved
- Independent validation to assess the effectiveness of corrective measures

[Decision Factor 5 ▲](#)



Issues and corrective actions from internal audits and independent testing/assessments are formally tracked to ensure procedures and control lapses are resolved in a timely manner.

[Click here to enter comment](#)

End of Core Analysis.



Management

Institution Name: [Click here to enter institution name](#)

Cert# [Click here to enter cert number](#)

Preparer: [Click here to enter preparer name](#)

Start Date: [Click here to select a start date.](#)

Core Analysis Decision Factors

Note: refer to the applicable FFIEC IT Examination Handbooks if additional analysis is necessary to complete this module.

Decision Factors – Management

M.1. The level and quality of oversight and support of IT activities by the Board of Directors and management.

[▼ Procedures #1-3](#)

[Click here to enter comment](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

M.2. The ability of management to provide information reports necessary for informed planning and decision making in an effective and efficient manner.

[▼ Procedure #4](#)

[Click here to enter comment](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

M.3. The adequacy of, and conformance with, internal policies and controls addressing IT operations and risks of significant business activities.

[▼ Procedure #5-6](#)

[Click here to enter comment](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

M.4. The level of awareness of and compliance with laws and regulations.

[▼ Procedures #7-11](#)

[Click here to enter comment](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

M.5. The level of planning for management succession.

[▼ Procedure #12](#)

[Click here to enter comment](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

M.6. The adequacy of contracts and management's ability to monitor relationships with third-party servicers.

[▼ Procedure #13](#)

[Click here to enter comment](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

M.7. The adequacy of risk assessment processes to identify, measure, monitor, and control risks.

[▼ Procedures #14-16](#)

[Click here to enter comment](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

M.8. If applicable, include a summary comment below for any additional risk factors reviewed or examination procedures performed that may not be directly referenced in the Decision Factors above. (These risk factors and procedures could include, but are not limited to, Supplemental Workprograms, FFIEC workprograms, agency-specific workprograms, and/or new guidance not addressed in the modules.)

[Click here to enter comment](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

Summary Comment - Management

[Click here to enter comment.](#)

URSIT Management Rating: [Click to choose a rating](#)

Complete the following procedures at each examination. The resources listed below are not intended to be all inclusive, and additional guidance may exist.

Resources

- *FFIEC IT Examination Handbook – Management*
- *FFIEC IT Examination Handbook – Outsourcing Technology Services*
- *Interagency Guidelines Establishing Standards for Safety and Soundness*
- *Interagency Guidelines Establishing Information Security Standards*
- *Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation*
- *Examination Documentation (ED) Module – Third-Party Risk*
- *FIL-52-2006 Foreign-Based Third-Party Service Providers Guidance on Managing Risk in These Outsourcing Relationships*
- *SR 13-19 Guidance on Managing Outsourcing Risk*

Preliminary Review

Review items relating to Management, such as:

- The committees, names, and titles of the individual(s) responsible for managing IT and information security
- Board and IT-related committee minutes
- IT-related policies
- IT-related risk assessments, including cybersecurity
- Business and IT organization charts
- IT job descriptions
- Qualifications of key IT employees
- IT-related audits
- Insurance policies
- Strategic plans
- Succession plans
- IT budgets

1. Evaluate the quality of Board and management oversight of the IT function. Consider the following:

- Adequacy of the process for developing and approving IT policies
- Scope and frequency of IT-related meetings
- Existence of a Board-approved comprehensive information security program
- Designation of an individual or committee to oversee the information security program, including cybersecurity
- Composition of IT-related committees (e.g., Board, senior management, business lines, audit, and IT personnel)
- Effectiveness of IT organizational structure, including:
 - Direct reporting line from IT management to senior level management
 - Appropriate segregation of duties between business functions and IT functions
 - Appropriate segregation of duties within the IT function
- Adequacy of resources (e.g., staffing, system capacity)
- Qualifications of IT staff, including:

- Training
- Certifications
- Experience
- Technology support for business lines
- Generation and review of appropriate IT monitoring reports
- Adequacy of employee training

Decision Factor 1 ▲



The Board of Directors or an appropriate committee of the Board of each bank 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.*



Designated members of management are held accountable by the Board or an appropriate Board committee for implementing and managing the information security and business continuity programs.

Management assigns accountability for maintaining an inventory of organizational assets.

Processes are in place to identify additional expertise needed to improve information security defenses.

Information security roles and responsibilities have been identified.

Information security risks are discussed in management meetings when prompted by highly visible cyber events or regulatory alerts.

Employee access to systems and confidential data provides for separation of duties.

[Click here to enter comment](#)

2. Evaluate the quality of IT reporting to the Board of Directors. Consider reports such as:

- IT risk assessments
- IT standards and policies
- Resource allocation (e.g., major hardware/software acquisitions and project priorities)
- Status of major projects
- Corrective actions on significant audit and examination deficiencies
- Information security program, including cybersecurity

Decision Factor 1 ▲



Report to the Board. Each bank shall report to its Board or an appropriate committee of the Board at least annually. This report should describe the overall status of the information security program and the bank's compliance with these Guidelines. The report, which will vary depending upon the complexity of each bank's program should discuss material matters related to its program, addressing issues such as: risk assessment; risk management and control decisions; service provider arrangements; results of testing; security breaches or violations, and management's responses; and recommendations for changes in the information security program.



Management provides a written report on the overall status of the information security and business continuity programs to the Board or an appropriate Board committee at least annually.

The institution prepares an annual report of security incidents or violations for the Board or an appropriate Board committee.



Control Test

Review the most recent annual information security program report to the Board and ensure it covers the minimum required elements outlined in the Information Security Standards.

[Click here to enter comment](#)

3. Evaluate the adequacy of the short- and long-term IT strategic planning and budgeting process. Consider the following:

- Involvement of appropriate parties
- Identification of significant planned changes
- Alignment of business and technology objectives
- Ability to promptly incorporate new or updated technologies to adapt to changing business needs
- Coverage of any controls, compliance, or regulatory issues which may arise or need to be considered

[Decision Factor 1 ▲](#)



The budgeting process includes information security related expenses and tools.

[Click here to enter comment](#)

4. Evaluate the adequacy of management information system (MIS) reports (e.g., lending, concentrations, interest rate risk) and the reliability management can place upon those reports in the business decision-making process. Consider the following elements of an effective MIS report:

- Timeliness
- Accuracy
- Consistency
- Completeness
- Relevance

[Decision Factor 2 ▲](#)



Control Test

Obtain feedback from risk management and compliance examiners regarding the quality and usefulness of reports provided for management decisions.

[Click here to enter comment](#)

5. Evaluate management’s ability and willingness to take timely and comprehensive corrective action for known problems and findings noted in previous IT examination reports, audits, service provider/vendor reviews, and internal reviews (e.g., disaster recovery, incident response, cybersecurity tests).

[Decision Factor 3 ▲](#)



Issues identified in assessments are prioritized and resolved based on criticality and within the time frames established in the response to the assessment report.



Control Test

Review the audit tracking report to ensure management is resolving issues in a timely manner.

[Click here to enter comment](#)

6. Evaluate whether written policies, control procedures, and standards are thorough and properly reflect the complexity of the IT environment. Also, evaluate whether these policies, control procedures, and standards have been formally adopted, communicated, and enforced. Consider the following:

- Information security, including cybersecurity
- Network security, including intrusion detection
- Incident response, including Suspicious Activity Reports
- Business continuity
- Acceptable use
- Access rights
- Electronic funds transfer
- Vendor management/Third-party risk
- Remote access
- Bring Your Own Device (BYOD)
- Institution-issued mobile devices
- Anti-virus/Anti-malware
- Patch management
- Unauthorized/Unlicensed software

Decision Factor 3 ▲



The institution has policies commensurate with its risk and complexity that address the concepts of information technology risk management, threat information sharing, and information security.

An information security and business continuity risk management function(s) exists within the institution.

The institution has policies commensurate with its risk and complexity that address the concepts of information technology risk management.



Control Test

Review procedures for communicating policies to staff.

Review internal audit testing of policy adherence.

[Click here to enter comment](#)

7. Evaluate the written information security program and ensure that it includes administrative, technical, and physical safeguards appropriate to the size and complexity of the institution and the nature and scope of its activities. Consider the following:

- Access controls on customer information systems
- Access restrictions at physical locations containing customer information

- Encryption of electronic customer information, including while in transit or in storage on networks or systems
- Procedures designed to ensure that customer information system modifications are consistent with the institution's information security program
- Dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer information
- Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems
- Incident response programs that specify actions to be taken when the institution 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
- Measures for properly disposing of sensitive customer/consumer data containing personally identifiable information

Decision Factor 4 ▲



A bank's information security program shall be designed to:

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

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

Develop, implement, and maintain appropriate measures to properly dispose of customer information and consumer information

Manage and Control Risk. Each bank shall design its 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.

Adjust the Program. Each bank shall monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and the bank's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to customer information systems.



All elements of the information security program are coordinated enterprise-wide.

Management holds employees accountable for complying with the information security program.

Threat information is used to enhance internal risk management and controls.

The institution has an information security strategy that integrates technology, policies, procedures, and training to mitigate risk.



Control Test

Select a sample of controls or safeguards from the information security program and map the controls back to the threats identified in the risk assessment.

[Click here to enter comment](#)

8. Evaluate the information security training program, including cybersecurity. Consider the following:

- Periodic training of all staff, including the Board
- Specialized training for employees in critical positions (i.e., system administrators, information security officer)
- Distribution of latest regulatory and cybersecurity alerts
- Communication of acceptable use expectations
- Customer awareness program

Decision Factor 4 ▲



Train staff to implement the bank's information security program.



Annual information security training is provided.

Annual information security training includes incident response, current cyber threats (e.g., phishing, spear phishing, social engineering, and mobile security), and emerging issues.

Situational awareness materials are made available to employees when prompted by highly visible cyber events or by regulatory alerts.

Customer awareness materials are readily available (e.g., DHS' Cybersecurity Awareness Month materials).

Information security threats are gathered and shared with applicable internal employees.



Control Test

Review documentation of employee security awareness training.

[Click here to enter comment](#)

9. Evaluate the adequacy of the Identity Theft Prevention / Red Flags Program, including the Program's compliance with regulatory requirements. Verify that the financial institution:

- Periodically identifies covered accounts it offers or maintains. (Covered accounts include accounts for personal, family and household purposes that permit multiple payments or transactions.)
- Periodically conducts 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 institution's previous experiences with identity theft.
- Has developed and implemented a Board-approved, comprehensive written Program designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. The Program should:

- Be appropriate to the size and complexity of the financial institution and the nature and scope of its activities.
 - Have reasonable policies, procedures and controls (manual or automated) to effectively identify and detect relevant Red Flags and to respond appropriately to prevent and mitigate identity theft.
 - Be updated periodically to reflect changes in the risks to customers and the safety and soundness of the financial institution from identity theft.
 - Involves the Board, or a designated committee or senior management employee, in the oversight, development, implementation, and administration of the program.
 - Reports to the Board, or a designated committee or senior management employee, at least annually on compliance with regulatory requirements. The report should address such items as:
 - The effectiveness of policies and procedures in addressing the risk of identity theft.
 - Service provider arrangements.
 - Significant incidents involving identity theft and management’s response.
 - Recommendations for material changes to the program.
 - Trains appropriate staff to effectively implement and administer the Program.
- Exercises appropriate and effective oversight of service providers that perform activities related to covered accounts.

[Decision Factor 4 ▲](#)



*Customer transactions generating anomalous activity alerts are monitored and reviewed.
Customer service (e.g., the call center) utilizes formal procedures to authenticate customers commensurate with the risk of the transaction or request.*

[Click here to enter comment](#)

10. Evaluate the process to address changes to, or new issuance of, laws/regulations and regulatory guidelines.

[Decision Factor 4 ▲](#)

[Click here to enter comment](#)

11. Determine whether management files Suspicious Activity Reports (SARs) for IT or cybersecurity incidents when required.

[Decision Factor 4 ▲](#)



Responsibilities for monitoring and reporting suspicious systems activity have been assigned.



Control Test
Discuss with Risk/BSA examiners to determine whether any IT-related SARs have been filed.

[Click here to enter comment](#)

12. Evaluate management succession and cross training. Consider the following:

- Existence and appropriateness of job descriptions
- Adequacy and training of back-up individuals
- Existence of plans in the event of loss of a key manager or employee

Decision Factor 5 ▲



Control Test

Review the management succession plan to ensure it meets the needs of the institution.

[Click here to enter comment](#)

Vendor Management – Ongoing Monitoring

(See also Development and Acquisition Module – Procedures #2-4 for Vendor Management – Acquisition)

13. Evaluate whether a risk-based vendor management program has been implemented to monitor service provider and vendor relationships (both domestic and foreign-based). Consider the following:

- Coverage of service providers and vendors, including affiliates, in the risk assessment process
- Foreign-based risks, as applicable
- Ongoing monitoring, which may include the following:
 - Financial statements
 - Controls assessments, such as SSAE 16 SOC Reports (Statement on Standards for Attestation Engagement Service Organization Control Reports)
 - Information security program
 - Cybersecurity preparedness and resilience
 - Incident response
 - Internal/external audit reports
 - Regulatory reports
 - Affiliate relationships (e.g., Federal Reserve Regulation W)
 - Consumer compliance
 - Onsite reviews
 - Participation in user groups
 - Business continuity program, including integrated testing with the institution’s plan
 - Service level agreement compliance
 - Vendor awareness of emerging technologies
 - Report to Board of Directors

Decision Factor 6 ▲



Oversee Service Provider Arrangements. Each bank shall:

- *Where indicated by the bank's risk assessment, monitor its service providers to confirm that they have satisfied their obligations. As part of this monitoring, a bank should review audits, summaries of test results, or other equivalent evaluations of its service providers.*



The institution has policies commensurate with its risk and complexity that address the concepts of external dependency or third-party management.

A list of third-party service providers is maintained.

A risk assessment is conducted to identify criticality of service providers.

The third-party risk assessment is updated regularly.

Audits, assessments, and operational performance reports are obtained and reviewed regularly validating security controls for critical third parties.

Ongoing monitoring practices include reviewing critical third-parties' resilience plans.



Control Test

Review a sample of documentation for ongoing monitoring of critical service providers to ensure sufficient monitoring is occurring.

[Click here to enter comment](#)

14. Evaluate the institution's IT risk assessment process. Consider the following:

- Identification of all information assets and systems, including cloud-based, virtualized, and paper-based systems
- Identification of critical service providers
- Gathering of threat intelligence (e.g., FS-ISAC, US-CERT, InfraGard)
- Determination of threats, including likelihood and impact
- Identification of inherent risk levels
- Documentation of controls to reduce threat impact
- Determination of the quality of controls (i.e., testing)
- Identification and evaluation of residual risk levels
- Remediation program for unacceptable residual risk levels
- Updating of the risk assessment promptly for new or emerging risks

Decision Factor 7 ▲



Specific to the customer information security program, each bank shall:

- *Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems.*
- *Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information.*
- *Assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.*

Regularly test the key controls, systems, and procedures of the information security program. The frequency and nature of such tests should be determined by the bank's risk assessment. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs.



A risk assessment focused on safeguarding customer information identifies reasonable and foreseeable internal and external threats, the likelihood and potential damage of threats, and the sufficiency of policies, procedures, and customer information systems.

The risk assessment identifies internet-based systems and high-risk transactions that warrant additional authentication controls.

The institution belongs or subscribes to a threat and vulnerability information-sharing source(s) that provides information on threats (e.g., FS-ISAC, US-CERT).

Threat information is used to monitor threats and vulnerabilities.

The critical business processes that are dependent on external connectivity have been identified.

Data flow diagrams are in place and document information flow to external parties.

An inventory of organizational assets (e.g., hardware, software, data, and systems hosted externally) is maintained.

Organizational assets (e.g., hardware, systems, data, and applications) are prioritized for protection based on the data classification and business value.

Management considers the risks posed by other critical infrastructures (e.g., telecommunications, energy) to the institution.

The risk assessment is updated to address new technologies, products, services, and connections before deployment.

[Click here to enter comment](#)

15. Evaluate the risk monitoring reports provided to the Board and/or senior management. Consider the following:

- Major IT projects
- Security incidents, including cyber incidents
- System availability and capacity
- Network security, including firewalls and intrusion detection/prevention
- Patch management

Decision Factor 7 ▲



Control Test

Review a sample of risk monitoring reports to ensure comprehensive and timely reporting.

[Click here to enter comment](#)

16. Evaluate management’s process for determining the adequacy of IT insurance policies. Consider the following:

- Employee fidelity
- IT equipment and facilities
- Media reconstruction
- E-banking
- Electronic funds transfer
- Business interruptions
- Errors and omissions
- Extra expenses, including backup site expenses

Decision Factor 7 ▲



Control Test

Review insurance policies to ensure coverage of IT activities.

[Click here to enter comment](#)

Supplemental Workprograms (as applicable)

Outsourcing / Vendor Management / Third-Party Risk

Note: Basic outsourcing concepts are addressed in the Management, Support and Delivery, and Development and Acquisition Modules. If expanded examination procedures are warranted, refer to the Expanded Management Module.

Also available are the Third-Party Risk Examination Documentation (ED) Module, the FFIEC IT Examination Handbook - Outsourcing Technology Services, and FIL-3-2012 Revised Payment Processor Relationships Guidance. Coordinate with examination efforts in the areas of risk management, BSA, and consumer protection.

If additional procedures are used, enter a summary of findings below.

[Click here to enter comment](#)

Credit Card Related Merchant Activities

Note: This type of activity relates to credit card payment transactions for merchants. Refer to the Credit Card Related Merchant Activities Examination Documentation (ED) Module and the FFIEC IT Examination Handbook - Retail Payment Systems.

If additional procedures are used, enter a summary of findings below.

[Click here to enter comment](#)

End of Management Core Analysis. If applicable, and as needed based on the extent of the institution’s involvement in the following areas, continue to the Expanded Analysis.

- Cloud Computing
- User Groups
- Vendor Information Security Programs
- Managed Security Service Providers
- Foreign-Based Technology Service Providers
- Vendor Incentive Agreements



Information
Technology
Risk
Examination

Institution Name: [Click here to enter institution name](#)

Cert# [Click here to enter cert number](#)

Preparer: [Click here to enter preparer name](#)

Start Date: [Click here to select a start date](#)

Development and Acquisition

Core Analysis Decision Factors

Note: refer to the FFIEC IT Examination Handbook - Development and Acquisition if additional analysis is necessary to complete this module.

Decision Factors – Development and Acquisition

DA.1. The level and quality of oversight and support of systems development and acquisition activities by senior management and the Board of Directors.

[▼ Procedures #1-4](#)

[Click here to enter comment](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

DA.2. The quality of project management programs and practices.

[▼ Procedure #5](#)

[Click here to enter comment](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

DA.3. The adequacy of controls over program changes.

[▼ Procedure #6](#)

[Click here to enter comment](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

DA.4. The development of information technology solutions that meet the needs of end users.

[▼ Procedure #7](#)

[Click here to enter comment](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

DA.5. If applicable, evaluate the adequacy of source code and programming controls.

[▼ Procedures #8-9](#)

[Click here to enter comment](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

DA.6. If applicable, include a summary comment below for any additional risk factors reviewed or examination procedures performed that may not be directly referenced in the Decision Factors above. (These risk factors and procedures could include, but are not limited to, Supplemental Workprograms, FFIEC workprograms, agency-specific workprograms, and/or new guidance not addressed in the modules.)

[Click here to enter comment](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

Summary Comment – Development and Acquisition

Click here to enter summary comment

URSIT Development and Acquisition Rating: [Click to choose a rating](#)

Complete the following procedures at each examination. The resources listed below are not intended to be all-inclusive, and additional guidance may exist.

Resources

- *FFIEC IT Examination Handbook – Development and Acquisition*
- *Interagency Guidelines Establishing Standards for Safety and Soundness*
- *Interagency Guidelines Establishing Information Security Standards*
- *FIL 49-99 Bank Service Company Act*

Preliminary Review

Review items relating to Development and Acquisition, such as:

- Change management policy and procedures
- Project management policy and procedures
- Vendor management policy and procedures (as related to acquisition)
- Products and Services Template
- Board and IT-related committee minutes
- IT-related contracts and license agreements
- IT-related audits

1. Assess the level and quality of oversight and support of acquisition activities by senior management and the Board of Directors. Consider the following:

- Alignment of business and technology objectives
- Establishment of project, technology committee, and Board reporting requirements
- Commitment of the Board and senior management to promote new products
- Level and quality of Board-approved project standards and procedures
- Assignment of personnel to address information security, audit, and testing for technology-related projects
- Establishment of segregation of duties or compensating controls
- Identification and replacement of systems nearing or at end-of-life

Decision Factor 1 ▲

[Click here to enter comment](#)

Vendor Management - Acquisition *(See also Management Module – Procedure #13 for Vendor Management – Ongoing Monitoring)*

2. Evaluate the due diligence process in selecting key vendors. The reviews should focus on an entity's financial condition, relevant experience, knowledge of applicable laws and regulations (e.g., transactions with affiliates), reputation, scope of operations, and effectiveness of controls. Consider management's review of the following:

- Financial statements (e.g., annual reports and SEC filings)
- Experience and ability to implement and monitor the proposed activity
- Business reputation, status in the industry, and sustainability
- Qualifications, training, and experience of the company's principals and staff
- Strategies and goals, including service philosophies, quality initiatives, efficiency improvements, and employment policies
- Existence of significant complaints, litigation, or regulatory actions against the company
- Ability to perform proposed functions using current systems or the need to make additional investments
- Use of other parties or subcontractors by the third party
- Scope of internal controls, information security, privacy protections, and audit coverage
- Business resumption strategies and contingency plans
- Knowledge of relevant consumer protection regulations
- Adequacy of management information systems
- Insurance coverage
- Eligibility to perform as a service provider given the existence of any outstanding enforcement actions against the third party, and the requirements of Section 19 of the FDI Act that may apply to institution-affiliated parties
- Record retention and maintenance practices
- Identification of potential conflicts of interest
- Impact of proposed contracts on the third-party's operations and financial condition

Decision Factor 1 ▲



Oversee Service Provider Arrangements. Each bank shall:

- *Exercise appropriate due diligence in selecting its service providers*



Risk-based due diligence is performed on prospective third parties before contracts are signed, including reviews of their background, reputation, financial condition, stability, and security controls.



Control Test

Review due diligence documentation for any vendors or service providers added or renewed since the prior examination to ensure the depth of the due diligence aligns with the criticality of the services to be provided.

[Click here to enter comment](#)

3. Determine whether the following topics are considered when contracts are being structured. The applicability of each topic is dependent upon the nature and significance of the third-party relationship. Contracts should clearly set forth the rights and responsibilities of each party, including the following:

- Timeframe covered by the contract
- Frequency, format, and specifications of the service or product to be provided
- Other services to be provided by the third party, such as software support and maintenance, training of employees, distribution of required disclosures to institution's customers, and customer service
- Adequate and measureable service level agreements (SLAs)
- Requirement that the third party comply with all applicable laws, regulations, and regulatory guidance

- Authorization for the institution and appropriate Federal and State regulators to have access to the records of the third party as necessary to evaluate compliance with laws, rules, and regulations
- Identification of which party will be responsible for delivering any required customer disclosures
- Insurance coverage to be maintained by the third party
- Terms relating to any use of premises, equipment, or employees
- Permissibility/prohibition of the third party to subcontract or use another party to meet its obligations
- Authorization for the institution to monitor and periodically review the third party for compliance with its agreement
- Independent validation of security controls
- Indemnification or other compensation for contract violations
- Confidentiality and security of information
- Notification of any information security or business continuity incident in a timely manner
- Exit/Deconversion costs and responsibilities

Decision Factor 1 ▲



Oversee Service Provider Arrangements. Each bank shall:

- *Require its service providers by contract to implement appropriate measures designed to meet the objectives of these Guidelines.*



Formal contracts that address relevant security and privacy requirements are in place for all third parties that process, store, or transmit confidential data or provide critical services.

Contracts acknowledge that the third party is responsible for the security of the institution's confidential data that it possesses, stores, processes, or transmits.

Contracts stipulate that the third-party security controls are regularly reviewed and validated by an independent party.

Contracts identify the recourse available to the institution should the third party fail to meet defined security requirements.

Contracts establish responsibilities for responding to security incidents.



Control Test

Review a sample of critical vendor contracts entered into since the previous examination to determine whether they meet the criteria above.

[Click here to enter comment](#)

4. Evaluate the process for identifying, documenting, and reporting service provider relationships (both domestic and foreign-based) to primary Federal and State regulators.

Decision Factor 1 ▲



Control Test

Obtain documentation verifying that regulators were notified of new service provider relationships entered into since the prior examination. Refer to the Bank Service Company Act.

[Click here to enter comment](#)

Project and Change Management

5. Evaluate the institution's program for managing significant projects (e.g., system conversions, product enhancements, infrastructure upgrades, system maintenance). Consider the following:

- Specifications and requirements
- Risk assessments
- Feasibility studies
- Cost/benefit analyses
- Vendor reviews
- Contract reviews
- End-user involvement
- Project plans
- Project status reports
- Test plans
- Test results
- Post-implementation reviews

Decision Factor 2 ▲



Control Test

Review a sample of documentation for significant technology projects, including the following:

- *Initial budgets and projected timelines versus actual results*
- *Project management and technology committee reports*
- *Test documentation, including plans, scripts, results, and error rates*
- *Post-conversion reports*
- *Suspense accounts for outstanding items*

[Click here to enter comment](#)

6. Evaluate change management procedures (e.g., software updates, vendor releases, and emergency program changes) for all critical systems and applications. Consider the following:

- Request and approval
- Testing
- Implementation
- Backup and backout
- Documentation
- User notification and training

If all software updates and vendor releases have not been installed, review management's documentation supporting the delay.

Decision Factor 3 ▲



A change management process is in place to request and approve changes to systems configurations, hardware, software, applications, and security tools.



Control Test

Review a sample of change management documentation for software updates and/or emergency program changes.

[Click here to enter comment](#)

7. Assess the ability of information technology solutions to meet the needs of the end users. Consider the following:

- Satisfaction of end users
- Quality of reporting tools used by management
- Issues noted in meeting minutes

Decision Factor 4 ▲

[Click here to enter comment](#)

If applicable, answer the following questions relating to source code and programming controls.

8. If critical vendor software is used in-house, determine whether the software contract or license agreement addresses the following:

- Possession of current source code or provision that the code is held in escrow
- The right to obtain, use, and modify the software in the event the software vendor is unable or unwilling to properly maintain the program(s)

Decision Factor 5 ▲



Intellectual property and production code are held in escrow.



Control Test

Verify the institution has obtained confirmation from the escrow agent that the current version of the source code is held in escrow.

[Click here to enter comment](#)

9. If the institution is using or supporting custom software, engaging in custom software development or programming, or contracting with third parties for the development of custom software (e.g., report development/queries, bridging/middleware/interfaces, ancillary applications), evaluate the following systems development life cycle (SDLC) processes and procedures:

- Segregation of duties and other security concerns
- Software documentation
- Version control
- Quality assurance and user-acceptance testing
- Emergency software fixes, including having a timely independent review of the fix and updating

documentation

- Restrictions on developer access, with no access to the quality control or production environment
- Masking of customer data to protect sensitive customer information in the development environment
- Independent reviews of software before migration into the production environment to ensure there are no security or integrity issues

For institutions with significant in-house programming, this core procedure may not be sufficient in and of itself. Examiners should utilize the FFIEC IT Examination Handbook – Development & Acquisition for more in-depth examination procedures at institutions with significant in-house programming. Overall findings and conclusions should be pulled forward from that workprogram into the comment box below.

[Decision Factor 5 ▲](#)



Developers working for the institution follow secure program coding practices, as part of a system development life cycle (SDLC), that meet industry standards.

The security controls of internally developed software are periodically reviewed and tested.

The security controls in internally developed software code are independently reviewed before migrating the code to production.

Production and non-production environments are segregated to prevent unauthorized access or changes to information assets.



Control Test

Review periodic tests of the security controls over internally developed software and independent reviews of software integrity prior to placing into production.

[Click here to enter comment](#)

End of Core Analysis.



Information
Technology
Risk
Examination

Support and Delivery

Institution Name: [Click here to enter institution name](#)

Cert# [Click here to enter cert number](#)

Preparer: [Click here to enter preparer name](#)

Start Date: [Click here to select a start date](#)

Core Analysis Decision Factors

Note: refer to the applicable booklets within the FFIEC IT Examination Handbook if additional analysis is necessary to complete this module.

Decision Factors – Support and Delivery

SD.1. The quality of processes or programs that monitor capacity and performance.

[▼ Procedure #1](#)

[Click here to enter comments](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

SD.2. The adequacy of data controls over preparation, input, processing, and output.

[▼ Procedures #2-3](#)

[Click here to enter comments](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

SD.3. The quality of assistance provided to users, including the ability to handle problems.

[▼ Procedure #4](#)

[Click here to enter comment](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

SD.4. The adequacy of corporate contingency planning and business resumption for data centers, networks, service providers, and business units.

[▼ Procedures #5-11](#)

[Click here to enter comment](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

SD.5. The adequacy of network architectures and the security of connections with public networks.

[▼ Procedures #12-13](#)

[Click here to enter comment](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

SD.6. The quality of physical and logical security, including the privacy of data.

[▼ Procedures #14-23](#)

[Click here to enter comment](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

SD.7. The adequacy of controls over electronic funds transfers and electronic banking activities.

[▼ Procedures #24-26](#)

[Click here to enter comment](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

SD.8. If applicable, include a summary comment below for any additional risk factors reviewed or examination procedures performed that may not be directly referenced in the Decision Factors above. (These risk factors and procedures could include, but are not limited to, Supplemental Workprograms, FFIEC workprograms, agency-specific workprograms, and/or new guidance not addressed in the modules.)

[Click here to enter comment](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

Summary Comment – Support and Delivery

[Click here to enter comment](#)

URSIT Support and Delivery Rating: [Choose a rating.](#)

Complete the following procedures at each examination. The resources listed below are not intended to be all-inclusive, and additional guidance may exist.

Resources

- *FFIEC IT Examination Handbook – Operations, Information Security, and Business Continuity Planning Booklets*
- *Interagency Guidelines Establishing Standards for Safety and Soundness*
- *Interagency Guidelines Establishing Information Security Standards*
- *Interagency Statement on Pandemic Planning*
- *FFIEC Guidance on Authentication in an Internet Banking Environment (2005 and 2011)*

Preliminary Review

Review items that may identify support and delivery issues, such as:

- Prior examination reports and workpapers
- Pre-examination memoranda and file correspondence
- Operations-related policies
- Network topology
- Cybersecurity self-assessments
- Internal and external IT audit reports
- Board/Committee minutes related to IT
- Information Technology Profile
- Disaster recovery/business continuity plan
- Network vulnerability assessments/penetration tests
- Regulatory reports (e.g., TSP reports)

1. Determine whether there are adequate controls to manage operations-related risks. Consider whether appropriate daily operational controls and processes have been implemented, such as:

- Monitoring tools to detect and preempt system problems or capacity issues
- Daily processing issue resolution and appropriate escalation procedures
- Secure handling, distribution, and disposal of equipment, media, and output (electronic and physical)
- Independent review of master file input and file maintenance changes (e.g., new loan and deposit accounts, address changes, due dates)
- Independent review of global parameter changes (e.g., interest rate indices for loans and deposits, fee structure, service charges)

Decision Factor 1 ▲



Data are disposed of or destroyed according to documented requirements and within expected time frames.



Control Test

Review sample documentation for each of the above-noted controls and processes for adequacy.

[Click here to enter comment](#)

2. Evaluate the adequacy of controls for document imaging and management systems. Consider the following:
- Indexing controls (i.e., organized and easily accessible)
 - Limitations on the ability to alter scanned documents (particularly important if relying on documents for legal purposes)
 - Record retention requirements (i.e., compliance with State and Federal regulations)
 - Error handling and readability of images (i.e., quality assurance process)
 - Controls over the destruction of source documents after being scanned
 - Inclusion of imaging systems in the information security risk assessment if documents include personally identifiable information
 - Inclusion of imaging systems in business continuity planning

[Decision Factor 2 ▲](#)



Control Test

Verify that scanned items are destroyed in a manner and within the timeframe outlined in institution policy.

[Click here to enter comment](#)

3. Evaluate the adequacy of controls for item processing functions, including check imaging. Consider the following:
- Controls over teller/branch imaging
 - Security over the capture, storage, and transmission of images
 - Controls over the destruction of source documents after being scanned
 - Dual control or independent review over the processing of reject, re-entry, and unposted items
 - Physical controls over negotiable items
 - Controls over cash letters (e.g., reconcilements, segregation of duties)

[Decision Factor 2 ▲](#)



Control Test

Verify that scanned items are destroyed in a manner and within the timeframe outlined in institution policy.

[Click here to enter comment](#)

4. Evaluate the quality of assistance provided to end users, considering both internal and external resources (e.g., Help/Support Desk, vendor support, online help/training materials). Consider the following:
- Training
 - Problem resolution
 - Overall support

[Decision Factor 3 ▲](#)



Control Test

Review Help Desk ticketing reports or other end-user problem logs (if available) to ensure that issues are resolved in a timely and comprehensive manner.

[Click here to enter comment](#)

Business Continuity Planning/Disaster Recovery

5. Determine whether the Board and senior management annually review and approve the following:

- Enterprise-wide business continuity plan
- Business impact analysis
- Risk/threat assessment, including cyber risks/threats
- Testing program
- Testing results

Decision Factor 4 ▲



A formal backup and recovery plan exists for all critical business lines.

[Click here to enter comment](#)

6. Determine whether adequate business impact analyses and risk assessments have been completed. Consider the following:

- Input from all integral groups (e.g., business line management, risk management, IT, facilities management, and audit)
- Analysis of reasonably foreseeable threats, including natural events, technical events, pandemics, malicious activity, and cyber threats
- Utilization of the business impact analysis to identify critical business assets and prioritize recovery of processes, systems, and applications
- Identification of key recovery metrics, such as allowable downtime for critical business functions, acceptable levels of data loss and backlogged transactions, recovery time objectives (RTOs), recovery point objectives (RPOs), and costs associated with downtime
- Inclusion of IT services provided by third-party vendors or service providers in the business impact analyses/risk assessments

Decision Factor 4 ▲



Control Test

Review a sample of business impact analyses and risk assessments.

[Click here to enter comment](#)

7. Evaluate the adequacy of risk management over the business continuity process. Consider the following:

- Identification of alternate locations for business operations and IT recovery
- Backup of data, operating systems, applications, and telecommunication
- Offsite storage of backup media, supplies, business continuity plan, and system documentation
- Existence of alternate power supplies (e.g., uninterruptable power supply [UPS], generators)
- Procedures and priorities for returning to permanent and normal operations
- Designation of business continuity personnel and responsibilities
- Adequacy of service providers' business continuity programs, including cyber resilience and preparedness
- Process for updating plans as needed

Decision Factor 4 ▲

[Click here to enter comment](#)

8. Determine whether the business continuity process includes appropriate recovery operations at the backup location. Consider the following:

- Conditions under which the backup site would be used
- Decision-making responsibility for use of the backup site
- Procedures for notification of the backup site
- A checklist of data files, programs, and other items to be transported to the backup site
- Provisions for special forms and backup supplies
- Remote access connectivity
- Processing instructions and priorities
- Geographic diversity between the backup site and the primary location
- Adequacy of backup site hardware, including capacity and compatibility
- Sufficient processing time for the anticipated workload based on emergency priorities
- Availability of the backup site until the institution achieves full recovery from the disaster and resumes activity at the institution's own facilities.

Decision Factor 4 ▲

[Click here to enter comment](#)

9. Determine whether the business continuity plan effectively addresses pandemic issues. Consider the following:

- Planning
- Preparing
- Testing
- Responding
- Recovering

Decision Factor 4 ▲

[Click here to enter comment](#)

10. Determine whether business continuity strategies are designed to achieve resilience, such as the ability to effectively respond to wide-scale disruptions, including cyber attacks and attacks on multiple critical infrastructure sectors. Consider the following:

- Protections against backup data destruction/corruption
- Alternative telecommunications
- Forensic strategy

Decision Factor 4 ▲



The institution plans to use business continuity, disaster recovery, and data back-up programs to recover operations following an incident.

[Click here to enter comment](#)

11. Determine whether the business continuity testing program is sufficient to demonstrate the financial institution's ability to meet its continuity objectives. Consider the following:

- Regular testing of varying scenarios, including cyber attacks, based upon risk assessment
- Testing of critical business lines, systems, and operations, such as:
 - Core systems
 - Networks
 - Funds transfer
 - Telecommunications
- Testing of internal interdependencies between business units and processes
- Documentation of all facets of the continuity testing program, including:
 - Test scenarios
 - Plans
 - Scripts
 - Results
 - Reporting, including Board reporting
- Employee familiarity with the written plans and their individual responsibilities
- Analysis of test results and resolution of any identified issues
- Use of offsite resources (e.g., backup data) to conduct the recovery test
- Testing with critical third-party service providers, including at a minimum:
 - From the institution's primary location to the TSPs' alternative location
 - From the institution's alternative location to the TSPs' primary location
- Testing the adequacy of remote access infrastructure and capacity, if being relied upon for critical business continuity processes in a pandemic or other scenario

Decision Factor 4 ▲



*Scenarios are used to improve incident detection and response.
Business continuity testing involves collaboration with critical third parties.
Systems, applications, and data recovery is tested at least annually.*



Control Test

Review BCP testing documentation to determine adequacy.

[Click here to enter comment](#)

Information Security

12. Review the network topology with management. Consider the following:

- Date of last update
- Identification of all critical systems and components (e.g., servers, firewall, routers, switches, IDS/IPS)
- Identification of all connection points
- Identification of network segmentation (e.g., demilitarized zone [DMZ], virtual local area network [VLAN], wireless)

[Decision Factor 5 ▲](#)

[Click here to enter comment](#)

13. Assess remote access practices used to authenticate, monitor, and control vendor/employee remote access. Consider the following:

- Disabling remote communications if no business need exists
- Controlling access through management approvals and subsequent audits
- Implementing robust control over configurations at both ends of the remote connection to prevent potential malicious use
- Logging and monitoring remote access activities, particularly for vendors and privileged users
- Using strong authentication and encryption to secure communications
- Enabling vendor remote access accounts only when necessary

[Decision Factor 5 ▲](#)



Remote access to critical systems by employees, contractors, and third parties uses encrypted connections and multifactor authentication.

The institution is able to detect anomalous activities through monitoring across the environment.

Access to critical systems by third parties is monitored for unauthorized or unusual activity.

[Click here to enter comment](#)

14. Determine the adequacy of security monitoring for the network and all critical systems and applications. Consider the following:

- Existence of systems to detect or prevent unauthorized network access (e.g., intrusion detection/prevention)
- Ability to detect and prevent the unauthorized removal of data from the network (e.g. data loss prevention)
- Ability to detect and respond to anomalous activity
- Ability to prevent or detect unauthorized devices or software
- Knowledge and expertise of security personnel
- Adequacy and frequency of network vulnerability assessments and penetration tests
- Adequacy of processes for managing network security devices (e.g., firewall, IDS, VPN)
- Adequacy of log monitoring program
- Adequacy of automated tools (if being used) to support security monitoring, policy enforcement, and reporting
- Appropriateness of wireless configuration and monitoring

Decision Factor 6 ▲



Network perimeter defense tools (e.g., border router and firewall) are used.

Systems that are accessed from the Internet or by external parties are protected by firewalls or other similar devices.

Controls are in place to restrict the use of removable media to authorized personnel.

All ports are monitored.

Wireless network environments require security settings with strong encryption for authentication and transmission.

Independent testing (including penetration testing and vulnerability scanning) is conducted according to the risk assessment for external-facing systems and the internal network.

A normal network activity baseline is established.

Processes are in place to monitor for the presence of unauthorized users, devices, connections, and software.

Audit log records and other security event logs are reviewed and retained in a secure manner.

Firewall rules are audited or verified at least quarterly.



Control Test

Verify that management obtains, reviews, and acts upon alerts from intrusion detection/prevention systems and other security systems.

Verify that management tracks and remediates findings from vulnerability assessments and penetration tests.

Verify that management obtains and reviews security logs/monitoring reports for operating systems, application systems, and networks.

[Click here to enter comment](#)

15. Evaluate the incident response plan. Consider whether the plan:

- Includes senior leadership
- Includes representatives from various areas (e.g., management, IT, public relations, business units, legal)
- Defines responsibilities and duties
- Defines communication paths for employees and customers to report information security events
- Establishes alert parameters that prompt mitigating actions
- Includes processes and resources to contain incidents and remediate resulting effects
- Outlines internal escalation procedures, including when to notify senior management and the Board
- Details when to notify law enforcement, regulators, and customers
- Contains procedures for filing Suspicious Activity Reports (SARs), if necessary
- Includes recovery strategies for critical systems, applications, and data
- Addresses response to and recovery from a cybersecurity event
- Identifies third parties who can provide mitigation strategies
- Includes a process to classify, log, and track incidents
- Addresses incidents at third-party service providers
- Requires periodic testing

Decision Factor 6 ▲



At a minimum, an institution's response program should contain procedures for the following:

Assessing the nature and scope of an incident, and identifying what customer information systems and types of customer information have been accessed or misused.

Notifying its primary Federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information.

Consistent with the Agencies' Suspicious Activity Report ("SAR") regulations, notifying appropriate law enforcement authorities, in addition to filing a timely SAR in situations involving Federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing.

Taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information, for example, by monitoring, freezing, or closing affected accounts, while preserving records and other evidence.

Notifying customers when warranted.

Where an incident of unauthorized access to customer information involves customer information systems maintained by an institution's service providers, it is the responsibility of the financial institution to notify the institution's customers and regulator. However, an institution may authorize or contract with its service provider to notify the institutions' customers or regulator on its behalf.

NOTE: For incidents related to the Interagency Guidelines Establishing Information Security Standards, refer to Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice.



Roles and responsibilities for incident response team members are defined.

The response team includes individuals with a wide range of backgrounds and expertise, from many different areas within the institution. (e.g., management, legal, public relations, as well as information technology).

Logs of physical and/or logical access are reviewed following events.

Computer event logs are used for investigations once an event has occurred.

Tools and processes are in place to detect, alert, and trigger the incident response program.

Mechanisms (e.g., anti-virus alerts, log event alerts) are in place to alert management to potential attacks.

Alert parameters are set for detecting information security incidents that prompt mitigating actions.

System performance reports contain information that can be used as a risk indicator to detect information security incidents.

Appropriate steps are taken to contain and control an incident to prevent further unauthorized access to or use of customer information.

Communication channels exist to provide employees a means for reporting information security events in a timely manner.

A process exists to contact personnel who are responsible for analyzing and responding to an incident.

Procedures exist to notify customers, regulators, and law enforcement as required or necessary when the institution becomes aware of an incident involving the unauthorized access to or use of sensitive customer information.

Incidents are classified, logged, and tracked.

The institution has documented how it will react and respond to cyber incidents.



Control Testing

Review documentation of security incidents to determine whether required procedures were followed.

Review incident response testing documentation to ensure the tests adequately cover all aspects of the plan.

[Click here to enter comment](#)

16. Evaluate the effectiveness of administering user access rights. Consider the following:

- The process to add, delete, and change access rights for core banking systems, network access, and other systems
- Removal/restrictions when users permanently leave employment or are absent for an extended period of time (i.e., immediate notification from the Human Resources Department to delete/disable a user ID)
- Periodic reviews and re-approvals of employee access levels on all IT systems, including the network, core banking systems, and any other critical applications
- Assignment of unique user IDs to provide employee-specific audit trails (i.e., no sharing of generic IDs for employees with input or change capabilities)
- Assignment of user rights based upon job requirements

Decision Factor 6 ▲



Changes to physical and logical user access, including those that result from voluntary and involuntary terminations, are submitted to and approved by appropriate personnel.

Administrative, physical, or technical controls are in place to prevent users without administrative responsibilities from installing unauthorized software.

Employee access is granted to systems and confidential data based on job responsibilities and the principles of least privilege.

User access reviews are performed periodically for all systems and applications based on the risk to the application or system.

Identification and authentication are required and managed for access to systems, applications, and hardware.



Control Test

Select a sample of users to determine the appropriateness of access rights.

Select a sample of separated users to verify that their access was removed or restricted.

[Click here to enter comment](#)

17. Evaluate the controls over privileged users/accounts (e.g., database/network/system administrators).

Consider the following:

- Limiting access based upon the principles of least privilege
- Establishing a unique user ID separate from the ID used for normal business
- Prohibiting shared privileged access by multiple users
- Maintaining a level of authentication commensurate with privileged users' risk profiles
- Logging and auditing the use of privileged access
- Reviewing privileged user access rights regularly

Decision Factor 6 ▲



Access to make changes to systems configurations (including virtual machines and hypervisors) is controlled and monitored.

Elevated privileges are monitored.

Elevated privileges (e.g., administrator privileges) are limited and tightly controlled (e.g., assigned to individuals, not shared, and require stronger password controls).



Control Test

Review privileged user access reports to determine whether access rights are commensurate with job responsibilities/business needs.

Verify that management obtains and reviews activity logs/monitoring reports of privileged users.

[Click here to enter comment](#)

18. Determine whether authentication controls are adequate and whether configuration parameters meet institution policy and current industry standards for all critical IT systems. Consider the following:

- Length and complexity of password (alphanumeric, uppercase/lowercase, special characters)
- Password expiration period
- Password re-use and history
- Failed login settings (number of attempts and lockout period)
- Screen saver passwords
- Automatic timeouts
- Password reset procedures
- Use of tokens
- Biometric solutions
- Time-of-day and day-of-week restrictions

[Decision Factor 6 ▲](#)



System sessions are locked after a pre-defined period of inactivity and are terminated after pre-defined conditions are met.

Access controls include password complexity and limits to password attempts and reuse.



Control Test

Verify that adequate password control settings are in place for the core system, network, and other critical IT applications.

[Click here to enter comment](#)

19. Determine whether sufficient controls are in place to prevent the corruption of data and software and to correct problems caused by computer viruses or malware. Assess the following:

- Virus/malware detection practices (e.g., frequency and scope of scans)
- Virus/malware update practices for remote access devices
- Processes for updating virus detection applications (i.e., virus signature and scan engines)
- Automated tools to filter email and web traffic

[Decision Factor 6 ▲](#)



Up-to-date anti-virus and anti-malware tools are used.

Anti-virus and anti-malware tools are used to detect attacks.

E-mail protection mechanisms are used to filter for common cyber threats (e.g., attached malware or malicious links).



Control Test

Verify virus signatures are current on a sample of servers and clients.

[Click here to enter comment](#)

20. Assess system configuration procedures. Consider the following:

- Configurations based upon industry standards/vendor recommendations

- Configurations standards approved and settings audited
- Unnecessary ports and services disabled
- Default passwords and accounts changed/disabled
- Adequacy of automated tools (if being used) to enforce secure configurations

[Decision Factor 6 ▲](#)



Systems configurations (for servers, desktops, routers, etc.) follow industry standards and are enforced. Ports, functions, protocols, and services are prohibited if no longer needed for business purposes. All default passwords and unnecessary default accounts are changed before system implementation. Programs that can override system, object, network, virtual machine, and application controls are restricted.



Control Testing

Review management's documentation comparing actual configuration settings to documented and approved standards.

[Click here to enter comment](#)

21. Determine whether sufficient patch management policies and procedures are in place to protect computer systems against software vulnerabilities. Consider the following:

- Assignment of responsibilities for patch management
- Documentation of reasons for any missing or excluded patches
- Tests of patches prior to implementation
- Installation of vendor-supplied patches for:
 - Operating systems
 - Firewalls
 - Routers
 - Switches
 - Intrusion detection/prevention systems (IDS/IPS)
 - Applications
 - Workstation products (e.g., Adobe, Microsoft Office, Java)
 - Other critical systems
- Validation that system security configurations remain within standards after patch installation
- Documented reviews of vendor-provided patch reports, if patch management is outsourced
- Adequacy of automated tools (if being used) to implement patches, to audit for missing patches, and to validate secure configurations after patching
- Adequacy of the vulnerability management program in validating the effectiveness of patch management

[Decision Factor 6 ▲](#)



A patch management program is implemented and ensures that software and firmware patches are applied in a timely manner.

Patches are tested before being applied to systems and/or software.

Patch management reports are reviewed and reflect missing security patches.



Control Testing

Review and discuss the patch exception report with management.

If the patch reports are unavailable, select a sample of servers/workstations/network devices and review patch status.

[Click here to enter comment](#)

22. Evaluate the institution’s use of encryption for sensitive institution and customer data at rest and in transit.

Consider the following:

- Databases
- Mobile devices
- Email
- Back-up media and storage devices
- Transmissions with third parties
- Password databases

Decision Factor 6 ▲



All passwords are encrypted in storage and in transit.

Confidential data are encrypted when transmitted across public or untrusted networks (e.g., Internet).

Mobile devices (e.g., laptops, tablets, and removable media) are encrypted if used to store confidential data.

[Click here to enter comment](#)

23. Determine whether adequate physical and environmental monitoring and controls exist. Consider the following:

- Access to equipment rooms (including telecommunication closets) limited to authorized personnel
- Adequate HVAC
- Alarms to detect fire, heat, smoke, and unauthorized physical access
- Computer/server rooms uncluttered and hazard free
- Sufficient uninterrupted power supplies (i.e., UPS)
- Presence of adequate fire suppression
- Protection of equipment from water damage
- Environmental sensors where needed (e.g., temperature, humidity, water)
- Security cameras

Decision Factor 6 ▲



The physical environment is monitored to detect potential unauthorized access.

Physical security controls are used to prevent unauthorized access to information systems and telecommunication systems.



Control Test

Perform a site/premise inspection to determine the existence of physical protection and detection controls.

[Click here to enter comment](#)

Electronic Funds Transfers and Electronic Banking

24. Evaluate the adequacy of electronic funds transfer (EFT) oversight and controls, taking into consideration the nature and volume of wire transfer and ACH activity. Consider the following:

- Adequacy of policies and procedures
- Appropriateness of risk limits and tolerances
- Segregation of duties
- Adequacy of physical and logical security over EFT systems and applications
- Adequacy of logging, reporting, and reconciling processes
- Ability to prevent, detect, and respond to anomalous or fraudulent activity
- Inclusion of EFT in BCP/DR plans
- Scope and frequency of EFT audit coverage, including a NACHA self-assessment if required

For institutions with significant or complex EFT activity, this core procedure is probably not sufficient in and of itself. Examiners should utilize the Electronic Funds Transfer Risk Assessment ED Module and/or the FFIEC IT Examination Handbook – Retail Payment Systems at institutions with high volume and/or complex EFT activities. Significant findings and conclusions should be pulled forward from those workprograms into the comment box below.

Decision Factor 7 ▲

[Click here to enter comment](#)

25. Evaluate the adequacy of electronic banking oversight and controls. Consider the following:

- Due diligence in selecting the electronic banking third-party service provider (if applicable)
- Electronic banking risk assessment process
 - Inclusion of all products, services, and channels offered (or contemplated) by the financial institution
 - Procedures to update the risk assessment at least annually to address:
 - Changes in the threat environment, customer base, and/or electronic banking functionality
 - Actual incidents of security breaches, identity theft, or fraud experienced by the financial institution or the industry
- Authentication and authorization process for customers
 - Enrollment procedures
 - Authentication parameters and requirements
 - Enhanced authentication for higher risk activities, such as external transfer of funds
 - Re-authentication after period of inactivity
 - Procedures to adjust authentication controls based on risk assessments
- Transaction risk
 - Ability to detect, prevent, and respond to fraudulent or anomalous activity
 - Ability to leverage location features for fraud detection
- Customer education
 - Social engineering

- Phishing
- Anti-virus/malware
- Public Internet access
- Compliance and Legal risks
 - BSA/AML compliance (recordkeeping, screening, and reporting requirements)
 - Consumer and privacy disclosures
- Reputation risk
 - Cyber threats
 - Lack of availability

Decision Factor 7 ▲



Customer access to Internet-based products or services requires authentication controls (e.g., layered controls, multifactor) that are commensurate with the risk.



Review the electronic banking risk assessment for compliance with the FFIEC Guidance on Authentication in an Internet Banking Environment (2005 and 2011).

[Click here to enter comment](#)

26. In addition to the electronic banking controls listed above, evaluate the adequacy of the following controls specific to mobile banking:

- On-device data security
 - Customer education regarding the use of PINs or passwords on devices
 - Controls to avoid retaining unnecessary sensitive information on devices
 - Encryption of any sensitive information stored on devices
 - Secure wiping of sensitive information from memory upon exiting the application
 - Authentication when re-entering the application
 - Ability to quickly deregister a device if reported lost or stolen
- Mobile application security
 - Secure coding practices
 - Testing for vulnerabilities
 - Ability to patch quickly
- Mobile application delivery/marketplace
 - Customer education on downloading application and any subsequent updates/patches only from a reputable source
- Mobile device malware and viruses
 - Customer education on installing anti-malware on devices
- SMS-based products
 - For communication of non-sensitive information only since SMS is unencrypted
 - Customer education about social engineering, phishing, and other malicious activities
- Data transmission security
 - Customer education on risks of public Wi-Fi

Decision Factor 7 ▲

[Click here to enter comment](#)

SUPPLEMENTAL WORKPROGRAMS (as applicable)

E-Banking

Note: After completion of the core electronic banking procedure, if additional examination work is needed, refer to available resources such as the FFIEC IT Examination Handbook, FFIEC Guidance on Authentication in an Internet Banking Environment, and other outstanding guidance.

If additional procedures are used, enter a summary of findings below.

[Click here to enter comment](#)

Mobile Banking

Note: After completion of the core mobile banking procedure, if additional examination work is needed, refer to available resources such as the FFIEC IT Examination Handbook, mobile banking workprograms, and other outstanding guidance.

If additional procedures are used, enter a summary of findings below.

[Click here to enter comment](#)

Remote Deposit Capture

Note: This type of activity refers to a deposit transaction delivery system that allows customers to deposit items electronically from remote locations. Refer to available resources such as the FFIEC IT Examination Handbook, remote deposit capture workprograms, and other outstanding guidance.

If additional procedures are used, enter a summary of findings below.

[Click here to enter comment](#)

End of Support & Delivery Core Analysis. If applicable, and as needed based on the extent of the institution's involvement in the following areas, continue to the Expanded Analysis.

- Wireless
- Virtualization
- Voice over Internet Protocol (VoIP)
- ATM Operations
- Customer-Facing Call Center
- Internal IT Help Desk
- Servicing Provided to Others



Information
Technology
Risk
Examination

Information Security Standards

Institution Name: [Click here to enter institution name](#)

Cert# [Click here to enter cert number](#)

Preparer: [Click here to enter preparer name](#)

Start Date: [Click here to select .a start date.](#)

Workpaper

INTERAGENCY GUIDELINES ESTABLISHING INFORMATION SECURITY STANDARDS

The Interagency Guidelines Establishing Information Security Standards (Information Security Standards) set forth standards pursuant to section 501(b) of the Gramm-Leach-Bliley Act (GLBA). These Information Security Standards address developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. They also address the proper disposal of consumer information pursuant to sections 621 and 628 of the Fair Credit Reporting Act. The Information Security Standards are set forth in:

FDIC - Rules & Regulations Part 364, Appendix B
Federal Reserve - Regulation H, Appendix D-2



Information security principles and standards, contained within the Information Security Standards, are interspersed throughout all areas of the information technology examination modules. Examination procedures that are applicable to the Information Security Standards are marked with this GLBA icon.

The Information Security Standards compliance comment contained in this workpaper should be a concise summary of the findings noted during the evaluation of the GLBA-related factors and procedures contained in the Core Modules.

Note: Each requirement contained in the Information Security Standards is tied to the examination procedure most applicable to that requirement. However, examiners should recognize that additional procedures may also tie to each Guideline requirement.

**Summary Comment – GLBA Information Security Standards
(Comment should be included in the Report of Examination)**

IS.1. After completing the GLBA-related examination procedures contained in the Core Modules, summarize the institution’s compliance with the Interagency Guidelines Establishing Information Security Standards.

[Click here to enter comment](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

Background

The following information is a summary of the Information Security Standards and is intended to serve as an examination resource.

Assessing the Institution's Compliance with the Information Security Standards

The Information Security Standards require each institution to establish a formal information security program that meets the following objectives:

- Ensures the security and confidentiality of customer information
- Protects against any anticipated threats or hazards to the security or integrity of customer information
- Protects against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer
- Ensures the proper disposal of customer information and consumer information
- Implements appropriate response programs for unauthorized access

In reviewing the institution's program, examiners should consider the following:

- Comprehensiveness of the written information security program
- Involvement of the Board (or an appropriate committee thereof)
- Assignment of specific responsibility for implementing the program
- Reasonableness and sufficiency of the risk assessment process
- Ability of the program to control and mitigate the risks
- Awareness and training of staff
- Testing of controls via audit or independent staff
- Proper disposal of consumer information
- Oversight of service providers
- Ability to adjust the program in response to relevant changes
- Adequacy of required annual reports to the Board or designated committee on material matters
- Appropriateness of incident response programs

The information security program represents the standards, policies, procedures, and guidelines defining the institution's security requirements. These security requirements are direct reflections of an institution's risk assessment and risk management practices.

A risk assessment is a multi-step process of identifying and assessing risks to information and infrastructure assets. One of the primary goals of a risk assessment is to identify feasible risk-reduction solutions. These solutions, often in the form of logical and physical controls, are the key defenses in protecting the confidentiality, integrity, and availability of information assets. The institution should continuously gather and analyze information regarding new threats and vulnerabilities, actual attacks, and the effectiveness of the existing security controls. Management should use this threat intelligence information to update the risk assessment, strategy, and controls. Regardless of the method used, the risk assessment provides the critical input for the controls, which become part of an institution's information security program.

The institution should provide an independent framework for assessing, testing, and reporting the effectiveness of controls. A reliable testing program provides reasonable assurances that management's information security program is effective and being followed. Without some form of testing and assessment, management will not be able to determine the adequacy and effectiveness of the information security program.

Management should establish and maintain a formal vendor management program that defines the framework for controlling the external dependency risks associated with key vendors and service providers. For example,

contracts should be established that include service level agreements, audit expectations, and confidentiality/nondisclosure statements. The program should require service providers and vendors to maintain security programs that comply with requirements outlined in the Information Security Standards. Also, management should be aware of the increased risks associated with foreign service providers, and ensure that appropriate controls are in place to mitigate those risks. In summary, the vendor management program should require security standards that meet or exceed the institution's own standards.

Finally, management should ensure that an appropriate incident response program is in place that specifies the actions to be taken when the institution suspects or detects unauthorized access to customer information or customer information systems. These actions should include assessing the nature and scope of the incident, identifying the systems and information that have been accessed or misused, taking appropriate steps to contain and control the incident, notifying regulators and law enforcement authorities (including filing Suspicious Activity Reports), and notifying customers when warranted.

End of Workpaper.



Information
Technology
Risk
Examination

Cybersecurity

Institution Name: [Click here to enter institution name](#)

Cert# [Click here to enter cert number](#)

Preparer: [Click here to enter preparer name](#)

Start Date: [Click here to select a start date.](#)

Workpaper

CYBERSECURITY

In light of the increasing volume and sophistication of cyber threats, institutions should have programs and/or processes in place to oversee and manage cybersecurity and mitigate cyber risks.

The National Institute of Standards and Technology (NIST) defines cybersecurity as “the process of protecting information by preventing, detecting, and responding to attacks.” As part of cybersecurity, institutions should manage internal and external threats and vulnerabilities to protect infrastructure and information assets. The definition builds on information security as defined in FFIEC guidance.

Cyber incidents can have financial, operational, legal, and reputational impact. As such, cybersecurity needs to be integrated throughout an institution as part of enterprise-wide governance processes, information security, business continuity, and third-party risk management. For example, an institution’s cybersecurity policies may be incorporated within the information security program. In addition, cybersecurity roles and processes may be separate roles within the security group (or outsourced) or may be part of broader roles across the institution.

The FFIEC Cybersecurity Assessment Tool (CAT) is one possible tool that institutions can use in assessing their cybersecurity preparedness. The content of the tool is consistent with the principles of the *FFIEC Information Technology Examination Handbook (IT Handbook)* and the NIST Cybersecurity Framework, as well as industry-accepted cybersecurity practices. However, institutions are not required to use the CAT, and examiners should not criticize management if management chooses to use other appropriate tools, frameworks, or processes to assess a financial institution’s cyber risks and cybersecurity preparedness. Appendix A of FIL-28-2015 Cybersecurity Assessment Tool maps the baseline declarative statements to existing guidance in the FFIEC IT Examination Handbook. Examiners should reference this guidance, not the CAT, when citing cybersecurity deficiencies in examination comments.



Cybersecurity principles and standards are not stand-alone, independent principles and standards. They are part of the overall information security and technology oversight function. Therefore, in lieu of having a stand-alone cybersecurity workprogram, those examination procedures in the other InTReX modules that are applicable to cybersecurity are marked with this icon.

The Cybersecurity conclusion comment contained in this workpaper should be a concise summary of the findings noted during the evaluation of the cybersecurity-related factors and procedures contained in the Core Modules.

Summary Comment - Cybersecurity

(Cybersecurity assessment comment should be included in the Report of Examination)

C.1. After completing the cybersecurity-related examination procedures contained in the Core Modules, summarize the adequacy of the institution's cybersecurity preparedness, including risk identification processes and mitigating controls.

[Click here to enter comment](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

End of Workpaper.



Information
Technology
Risk
Examination

Institution Name: [Click here to enter institution name](#)

Cert# [Click here to enter cert number](#)

Preparer: [Click here to enter preparer](#)

Management: Expanded Analysis

Start Date: [Click here to select a start date](#)

Expanded Analysis Decision Factors

This section provides additional examination procedures for IT products and services not specifically addressed in the Core Modules or that may need additional analysis.

Expanded Decision Factors – Management

E.M.1. The adequacy of controls over cloud computing.

[▼ Procedures #1-2](#)

[Click here to enter comment](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

E.M.2. The adequacy of involvement in service provider user groups.

[▼ Procedure #3](#)

[Click here to enter comment](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

E.M.3. Oversight of critical service providers' information security programs.

[▼ Procedure #4](#)

[Click here to enter comment](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

E.M.4. The adequacy of controls over managed security service providers.

[▼ Procedure #5](#)

[Click here to enter comment](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

E.M.5. The adequacy of controls over Foreign-Based Technology Service Providers.

[▼ Procedure #6](#)

[Click here to enter comment](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

E.M.6. Oversight of incentive compensation agreements within IT service provider contracts.

[▼ Procedure #7](#)

[Click here to enter comment](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

Consider the findings in these areas in the overall Management assessment; no summary comment is needed here.

1. Determine whether the following policies and processes address cloud computing. Consider the following:

- Information Security Risk Assessment
- Technology Outsourcing (Vendor Management) Policy
- Information Security Policy
- Security Incident or Customer Notification Policy
- Business Continuity Plan

Decision Factor 1 ▲

[Click here to enter comment](#)

2. For cloud computing, determine that inherent risks have been comprehensively evaluated, control mechanisms have been clearly identified, and residual risks are at acceptable levels. Consider the following:

- Data in the cloud is identified and appropriately classified
- Controls are commensurate with the sensitivity and criticality of the data
- Effectiveness of the controls are tested and verified
- Institution's business continuity plan addresses contingencies for cloud services
- Institution has an exit strategy, including a de-conversion plan, for cloud services

Decision Factor 1 ▲

[Click here to enter comment](#)

3. Evaluate the institution's participation in user groups to monitor and influence critical service providers.

Decision Factor 2 ▲

[Click here to enter comment](#)

4. For critical service providers or vendors with access to sensitive customer information, evaluate management's assessment of these vendors' written information security programs. Consider the following:

- Physical, logical, and environmental controls
- Encryption of electronic customer information
- Dual control procedures, segregation of duties, and employee background checks
- Monitoring systems and procedures to detect actual and attempted attacks or intrusions
- Incident response program that specifies actions to be taken when the vendor suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to the institution, regulators, and law enforcement agencies
- Training, including cybersecurity, for vendor employees

Decision Factor 3 ▲

[Click here to enter comment](#)

5. Evaluate the institution's use of a managed security service provider (MSSP). In addition to the standard vendor management controls in the core modules, consider the following:

- Type and frequency of security reports
 - Quality of logs
 - Separate client logs
 - Security information and event management reports
- In-house expertise to manage MSSP
 - Conformance with institution's information security program
- Responsiveness to audit findings (e.g., penetration test, vulnerability assessment, SSAE 16)
- Clear assignment of responsibilities and accountability
 - Incident response
 - Security alerts
 - Forensic
- Service availability
- Disaster recovery
- Secure handling of sensitive data

If additional examination procedures are necessary, refer to the FFIEC IT Examination Handbook Outsourcing - Technology Services Booklet, Appendix D: Managed Security Service Providers.

Decision Factor 4 ▲

[Click here to enter comment](#)

6. In addition to the vendor management controls outlined in the core module, evaluate the adequacy of additional oversight and controls relating to foreign-based technology service providers (FBTSP). Consider the following:

- Familiarity of FBTSP with U.S. banking laws and regulations
- Contract elements specifically addressing:
 - Access to and location of data
 - Choice of governing law (U.S. law is preferred)
 - Right of U.S. regulators to audit
- Inclusion of FBTSPs in the institution's vendor management program

Decision Factor 5 ▲

[Click here to enter comment](#)

7. For development or other IT-related contracts, incentives embedded in contracts might encourage the service provider to take imprudent risks, resulting in reputational damage, increased litigation, or other risks to the institution. Evaluate the process to review and approve any incentive compensation in contracts.

Decision Factor 6 ▲

[Click here to enter comment](#)

End of Expanded Analysis.



Institution Name: [Click here to enter institution name](#)

Cert# [Click here to enter cert number](#)

Preparer: [Click here to enter preparer name](#)

Start Date: [Click here to select a start date](#)

Expanded Analysis Decision Factors

This section provides additional examination procedures for IT products and services not specifically addressed in the Core Modules or that may need additional analysis.

Expanded Decision Factors – Support and Delivery

E.SD.1. The adequacy of controls over wireless networks.

[▼ Procedures #1-2](#)

[Click here to enter comment](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

E.SD.2. The adequacy of controls over virtualization.

[▼ Procedure #3](#)

[Click here to enter comment](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

E.SD.3. The adequacy of controls over Voice over Internet Protocol (VoIP).

[▼ Procedure #4](#)

[Click here to enter comment](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

E.SD.4. The adequacy of controls over ATM operations.

[▼ Procedure #5](#)

[Click here to enter comment](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

E.SD.5. The adequacy of controls over customer-facing call center operations.

[▼ Procedure #6](#)

[Click here to enter comment](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

E.SD.6. The adequacy of controls over internal IT Help Desk operations.

[▼ Procedure #7](#)

[Click here to enter comment](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

E.SD.7. The adequacy of controls over services provided to other entities.

[▼ Procedure #8](#)

Support and Delivery



Expanded Analysis Procedures

[Click here to enter comment](#)

Strong Satisfactory Less than satisfactory Deficient Critically deficient

Consider the findings in these areas in the overall Support and Delivery assessment; no summary comment is needed here.

1. Determine if the oversight of wireless technology is adequate. Consider the following:

- Management approval of the use of wireless networks
- Adoption of appropriate policies and procedures governing wireless access
- Approval of a minimum set of security requirements for wireless networks
- Periodic security testing of wireless networks

[Decision Factor 1 ▲](#)

[Click here to enter comment](#)

2. Evaluate the configuration of and controls over guest wireless networks. Consider the following possible security controls (not all may be applicable):

- Ensure that wireless access points are physically secured
- Disable unnecessary applications, ports, protocols, and services on wireless access point devices
- Appropriately segment guest wireless networks from the internal network and accurately depict on the network topology diagram
- Change the default password for the administrator account
- Enable strong authentication for remote management (if used)
- Change the default IP address for the wireless router
- Present guests with a legal disclaimer and option to agree to terms and conditions
- Provide guests with terms and conditions for use
- Monitor guest network traffic for unapproved activity
- Additional configuration considerations: hours of availability, broadcast range, web filtering

[Decision Factor 1 ▲](#)

[Click here to enter comment](#)

3. Evaluate the adequacy of oversight and controls relating to virtualization. Virtualization refers to running multiple operating systems (virtual machines) on a single machine (host machine). In general, the same physical and logical security controls that exist in a physical environment should exist in the virtual environment. Consider the following controls for both the host and virtual machines:

- Accuracy of network topology in depicting virtualized environment
- Access rights administration
- Monitoring of privileged users
- Use of standard secure builds for virtual machines (i.e., hardened images)
- Operating system and application licensing
- Patch management
- Business continuity and disaster recovery considerations, including data backup, licensing, and testing
- Capacity monitoring
- Use of standard security controls (e.g., firewalls, anti-virus, encryption)
- Security monitoring
- Auditing and logging practices
- Inclusion of the virtual environment in penetration testing and vulnerability assessments

- Hypervisor management, including encryption and authentication controls over any remote access
- Physical security of the data center/server rooms housing the virtual machines

[Decision Factor 2 ▲](#)

[Click here to enter comment](#)

4. Evaluate the adequacy of controls over Voice over Internet Protocol (VoIP). Consider the following:

- Physical and logical security controls
- Inclusion in patch management and operating system updates
- Privacy and record retention
- Network segmentation
- Inclusion in security testing
- Emergency service communications

[Decision Factor 3 ▲](#)

[Click here to enter comment](#)

5. Evaluate the adequacy of controls over ATM operations. Consider the following:

- Physical controls (e.g., cameras, lighting, alarms, and anti-skimming controls)
- Logical security controls (e.g., access to administrative console, network segmentation)
- Inclusion in patch management and operating system updates
- Dual control over cash (e.g., reloading and balancing)
- Card issuance procedures, including PIN issuances

[Decision Factor 4 ▲](#)

[Click here to enter comment](#)

6. Evaluate the oversight and controls relating to customer-facing call center operations. Consider the following:

- Types and frequency of reports provided to management
- Method for prioritizing calls
- Ability to identify systemic and high-risk issues
- Controls in place to prevent unauthorized access to and manipulation of customer data by call center personnel
- Controls over data theft or extraction (e.g., restrictions on portable media devices, cell phones, tablets, and email)
- Redaction of unnecessary customer information on screens viewed by call center personnel
- Procedures to verify the identity of the caller
- Administration of access rights, including timely removal of rights when employees leave
- Background checks on call center personnel
- Scope and frequency of call center audits

[Decision Factor 5 ▲](#)

[Click here to enter comment.](#)

7. Evaluate the oversight and controls relating to internal IT Help Desk operations. Consider the following:

- Types and frequency of reports provided to management
- Adequacy of the ticketing/issue tracking system
- Method for prioritizing calls and tickets
- Ability to identify systemic and high-risk issues
- Controls in place to prevent Help Desk personnel from seeing user passwords or asking for user passwords
- Controls over reissuance of passwords (e.g., one-time passwords)
- Controls in place to prevent unauthorized access to and manipulation of customer data by Help Desk personnel
- Procedures to verify the identity of the caller
- Administration of access rights, including timely removal of rights when employees leave
- Ability to log and audit Help Desk activities
- Scope and frequency of Help Desk audits

[Decision Factor 6 ▲](#)

[Click here to enter comment](#)

8. Evaluate the oversight and controls over servicing provided by the institution to other entities, including affiliates. Consider the following:

- Adequacy of contracts
- Compliance with service level agreements (SLAs)
- Audit coverage of services provided
- Availability of audits to serviced clients
- Risk assessment considerations, including cybersecurity
- Business continuity and disaster recovery considerations
- Insurance coverage for services provided
- Security of client data and reports, including encryption over data at rest and in transit
- Types and frequency of reports provided to management relating to the services provided to others

[Decision Factor 7 ▲](#)

[Click here to enter comment](#)

End of Expanded Analysis.