InTREx Information Technology Risk Examination

Information Technology Profile

Purpose

To provide information about the institution's Information Technology (IT) and operations to ensure appropriate resources are assigned to the examination.

Instructions for Completing the Information Technology Profile (ITP)

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

Please enter the name of the individual completing the ITP and the executive officer attesting to its accuracy, their titles, the institution name and location, and the date the ITP was completed.

Preparer Name and Title:

Click here to enter name

Click here to enter title

Institution Name and Location:

Click here to enter a location

Executive Officer's Name and Title:

Click here to enter title

Date Completed:

Click here to select a date

Core Processing

1. Indicate whether core applications are outsourced or hosted in-house (systems hosted by affiliated organizations are outsourced). Check all that apply. Leave blank if not applicable.

	Outsourced	In-House
General Ledger	☐	☐
Loans	☐	☐
Deposits	☐	☐
Investments	☐	☐
Trust	☐	☐

Click here to enter comment

Network

2. Does the institution utilize any of the following types of cloud services? Check all that apply.
   - ☐ Software as a Service (SaaS) ⓘ
   - ☐ Infrastructure as a Service (IaaS) ⓘ
   - ☐ Platform as a Service (PaaS) ⓘ
   - ☐ N/A

3. Who has remote access capability to network resources? Check all that apply.
   - ☐ No one
   - ☐ Vendors
   - ☐ Employees or Board Members (Bank-owned device)
   - ☐ Employees or Board Members (Personal device)

4. Does the institution have a wireless network? Check all that apply.
   - ☐ No
   - ☐ Stand-alone guest network
   - ☐ Production internal network

5. Indicate whether network monitoring (e.g., performance, intrusion detection, web filtering) and network operations are managed in-house or outsourced? Check all that apply.

	Outsourced	In-House
Network monitoring	☐	☐

	Outsourced	In-House
Network operations	☐	☐

Payments and Internet Banking

6. Indicate whether online banking services are outsourced or hosted in-house. Check all that apply. Leave blank if not applicable.

		Outsourced	In-House
Consumer	Internet Banking	☐	☐
	Mobile Banking	☐	☐
	Mobile Deposit	☐	☐
Commercial	Internet Banking	☐	☐
	Mobile Banking	☐	☐
	Remote Deposit Capture	☐	☐

7. What type of ACH origination transactions are processed? Check all that apply.

☐ None
☐ Standard ACH
☐ Same day ACH
☐ Third Party Payment Processor

Development and Acquisition

8. Has the institution engaged in merger or acquisition activity since the previous exam, or plans to do so in the next 6 months?

☐ Yes
☐ No

9. Does your institution provide IT services to other institutions (including affiliates)? Check all that apply.

   ☐ No
   ☐ Network support and applications
   ☐ Core processing
   ☐ Other

10. Does the institution support any custom software or engage in any custom software development? Check all that apply.

	Outsourced	In-House
No software development	☐	☐
Non-critical software or	☐	☐
Critical systems (e.g., custom coded core systems)	☐	☐
API	☐	☐
Other	☐	☐

Click here to enter comment

Cybersecurity

11. Has the institution assessed its cybersecurity risk and preparedness in the last 12 months using FFIEC CAT, Cyber Risk Institute ("CRI") Profile (formerly the FSSCC Profile), NIST or any other assessment tool?

   ☐ Not assessed
   ☐ Assessed

12. Has your institution or any of your service providers experienced a cyber attack, significant security event, or operational interruption since the previous examination? Check all that apply.

- ☐ No
- ☐ Institution
- ☐ Service Provider

Other

13. Have there been any significant changes in technology or services since the previous examination, or are any changes expected in the next 6 months? Check all that apply.

- ☐ No change
- ☐ Core system
- ☐ Significant network
- ☐ Significant application
- ☐ Key IT management or personnel
- ☐ Other new technology or services (e.g. artificial intelligence, blockchain, P2P payments)

Click here to enter comment

InTREx Information Technology Risk Examination **Audit**	**Institution Name:** Click here to enter Institution Name
	Cert/RSSD#:
	Preparer:
	Exam Start Date: Click or tap to enter a date

Core Analysis Decision Factors

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 Programs 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

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

Audit Summary

1-Strong ☐ 2-Satisfactory ☐ 3-Less Than Satisfactory ☐ 4-Deficient ☐ 5-Critically Deficient ☐

Decision Factor 1 – Board and Management Oversight

Strong ☐ Satisfactory ☐ Less Than Satisfactory ☐ Deficient ☐ Critically Deficient ☐

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

Procedure 1 – Audit Independence

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 designated 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)

Click here to enter comments

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 control test comments

Procedure 2 – Board and Management Support

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

- 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

Procedure 3 – Audit Outsourcing

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

Click here to enter comments

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.

Decision Factor 2 – Audit Planning

Strong ☐ Satisfactory ☐ Less Than Satisfactory ☐ Deficient ☐ Critically Deficient ☐

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

Procedure 4 – Risk Assessment Process

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 plans and schedules based on risk

Procedure 5 – IT Risk Exposure

Determine whether audit plans or audit risk assessments 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
- Security monitoring, including logging practices
- Change management
- Patch management
- Third-party outsourcing
- Social engineering
- Funds transfer
- Online banking
- Business continuity management

Baseline Cybersecurity Statements

Check if <u>not</u> met (x)

☐ *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.

Decision Factor 3 – Audit Reporting and Activities

Strong ☐ Satisfactory ☐ Less Than Satisfactory ☐ Deficient ☐ Critically Deficient ☐

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

Procedure 6 – Audit Frequency

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

Click here to enter comments

Procedure 7 – Audit Reports

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

Procedure 8 – Control Evaluation

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

- IT examination and Audit findings
- Audit risk assessment
- Cyber incidents
- Other significant IT events
- Assessment of potential impact of control deficiencies on other areas of operations

Click here to enter comments

Control Test

Sample the audit workpapers for adequacy and completeness.

Click here to enter control test comments

Decision Factor 4 – Auditor Qualifications

Strong ☐ Satisfactory ☐ Less Than Satisfactory ☐ Deficient ☐ Critically Deficient ☐

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

Click here to enter comments

Procedure 9 – Auditor Expertise and Training

Determine whether auditor expertise and training are 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 for both internal and external personnel as appropriate

Decision Factor 5 – Audit Finding Resolution

Strong ☐ Satisfactory ☐ Less Than Satisfactory ☐ Deficient ☐ Critically Deficient ☐

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

Click here to enter comments

Procedure 10 – Audit Monitoring and Resolution

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

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

Baseline Cybersecurity Statements

Check if <u>not</u> met (x)

☐ *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.*

Decision Factor 6 - Supplemental Risk Factors and Procedures

Strong ☐ Satisfactory ☐ Less Than Satisfactory ☐ Deficient ☐ Critically Deficient ☐

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 comments

End of Audit Core Analysis.

InTREx Information Technology Risk Examination	Institution Name:
	Cert#
	Preparer:
Development and Acquisition	Start Date:

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				
	Strong ☐	Satisfactory ☐	Less than satisfactory ☐	Deficient ☐	Critically deficient ☐
DA.2.	The quality of project management programs and practices. ▼ Procedure #5				
	Strong ☐	Satisfactory ☐	Less than satisfactory ☐	Deficient ☐	Critically deficient ☐
DA.3.	The adequacy of controls over program changes. ▼ Procedure #6				
	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				
	Strong ☐	Satisfactory ☐	Less than satisfactory ☐	Deficient ☐	Critically deficient ☐
DA.5	If applicable, evaluate the adequacy of source code and programming controls. ▼ Procedures #8-9				
	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.)				
	Strong ☐	Satisfactory ☐	Less than satisfactory ☐	Deficient ☐	Critically deficient ☐

Development and Acquisition Summary
URSIT Development and Acquisition 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*
- *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 ▲

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.

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.

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.

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*

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.

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 ▲

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.

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.

End of Development and Acquisition Core Analysis.

InTREx Information Technology Risk Examination	**Institution Name:**
	Cert#
Management	**Preparer:**
	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

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

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

Strong ☐ Satisfactory ☐ Less than satisfactory ☐ Deficient ☐ Critically deficient ☐

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

▼ Procedures #7-11

Strong ☐ Satisfactory ☐ Less than satisfactory ☐ Deficient ☐ Critically deficient ☐

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

▼ Procedure #12

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

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

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.)

Strong ☐	Satisfactory ☐	Less than satisfactory ☐	Deficient ☐	Critically deficient ☐

Management Summary

URSIT Management Rating:

Management

InTREx

Procedures

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*
- *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 ▲

GLBA

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.*

CYBER

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.

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 ▲

GLBA

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.

CYBER

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.

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.

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.

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.

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 ▲

CYBER

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.

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.

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.

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.

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

Decision Factor 4 ▲

11. Determine whether management files Suspicious Activity Reports (SARs) for IT or cybersecurity incidents when required and notifies its primary Federal regulator of incidents that meet the threshold of the Computer-Security Incident Notification rule.

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 or Computer-Security Incident Notifications have been filed within designated timeframes.

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.

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
- If available, read the report(s) of examination of any examined service provider(s) to the bank rated composite 3, 4, or 5 (Uniform Rating System for Information Technology) at the most recent examination, and evaluate the quality of the bank's vendor management relative to that rating.

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.

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.

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.

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

- Employee fidelity
- IT equipment and facilities
- Media reconstruction
- Online and mobile 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.

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 and the FFIEC IT Examination Handbook - Outsourcing Technology Services. 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.

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.

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

InTREx Information Technology Risk Examination **Support and Delivery**	**Institution Name:**
	Cert# Click here to enter Cert/RSSD #
	Preparer:
	Exam Start Date:
Core Analysis Decision Factors	

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 – Architecture, Infrastructure, and Operations (AIO), Information Security, and Business Continuity Management booklets*
- *Interagency Guidelines Establishing Standards for Safety and Soundness*
- *Interagency Guidelines Establishing Information Security Standards*
- *Interagency Statement on Pandemic Planning*
- *FFIEC Guidance on Authentication and Access to Financial Institution Services and Systems*
- *Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers*

Preliminary Review

Review items relating to 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
- Reports of any significant cyber-attacks, security events, or operational interruptions
- Internal and external IT audit reports
- Board and committee minutes related to IT
- Information Technology Profile
- Business continuity management plan
- Network vulnerability assessments/penetration tests
- Regulatory reports

If available, read the report(s) of examination of any examined service provider(s) to the bank rated composite 3, 4, or 5 (Uniform Rating System for Information Technology) at the most recent examination.

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

Support and Delivery Summary

1-Strong ☐ 2-Satisfactory ☐ 3-Less than satisfactory ☐ 4-Deficient ☐ 5-Critically deficient ☐

Decision Factor 1 – Performance and Data Controls

Strong ☐ Satisfactory ☐ Less than satisfactory ☐ Deficient ☐ Critically deficient ☐

Evaluate the quality of processes or programs that monitor capacity and performance; the adequacy of data controls over preparation, input, processing, and output; and the quality of assistance provided to users, including the ability to handle problems.

Click here to enter comments

Procedure 1 – Operational Controls

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)

Baseline Cybersecurity Statements

Check if <u>not</u> met (x)

☐ *Data is disposed of or destroyed according to documented requirements and within expected time frame.*

Control Test

Review sample documentation for each of the above-mentioned controls.

Procedure 2 – Imaging

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 (e.g. back office conversion, accounts receivable conversion, mobile banking)

Control Test

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

Enter Control Test notes here, if performed

Decision Factor 2 - Business Continuity Management (BCM)

Strong ☐ Satisfactory ☐ Less than satisfactory ☐ Deficient ☐ Critically deficient ☐

The adequacy of resilience, continuity, and response capabilities to safeguard personnel, customers, and products and services.

Procedure 3 – BCM Governance

Determine whether the board and senior management periodically review and approve the following:

- BCM responsibility and accountability
- BCM resource allocation
- Alignment of business strategy and risk appetite
- Business continuity risks and adopting policies and plans to manage events
- Business continuity exercise/test strategy
- Business continuity training strategy
- Business continuity operating/performance results, including exercise/test results
- Resolution plan(s) for identified weaknesses

Baseline Cybersecurity Statements

Check if <u>not</u> met (x)

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

Procedure 4 – Business Impact Analysis

Determine whether adequate business impact analyses for all business functions 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) and comprehensiveness of management's review
- Identification of critical business functions and interdependencies across business units prioritization of processes, systems, and applications for recovery
- Analysis of reasonably foreseeable disruptive events, including:
  - natural events (e.g., fires, floods, severe weather)
  - technical events (e.g., communication or power failure)
  - malicious events (e.g., fraud, theft, cyber-attacks)
  - international events (e.g., political instability, economic disruptions), and
  - low likelihood/high impact events (e.g., terrorist acts, pandemics)
- Reasonableness 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 service providers and vendors in the business impact analyses/risk assessments

Control Test

Review a sample of business impact analyses and risk assessments.

Enter Control Test notes here, if performed

Procedure 5 – Business Continuity Plan (BCP)

Evaluate the adequacy of the business continuity plan. Consider the following:

- Authorities, responsibilities, and relocation strategies
- Communication protocols, event management, and business continuity
- Incident response, disaster recovery, and crisis (emergency) management
- Liquidity concerns before and after an adverse event
- Alternatives for payment systems, facilities and infrastructure, data center(s), and branch relocation during a disaster

Procedure 6 – Backup Recovery

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

- Remote access connectivity
- 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

Procedure 7 – Business Continuity Strategies

Determine whether management can effectively respond to wide-scale disruptions in order to meet resilience and recovery objectives. Do the strategies:

- Address personnel, processes, technology, and facility issues
- Address critical business risks in the operating environment
- Outline a combination of backup, replication and storage methods for data protection
- Integrate with disaster recovery services to protect against data destruction
- Provide for high redundancy levels in the data/telecommunications infrastructure, including connections with critical third-party service providers
- Utilize a consistent change management process
- Include alternatives for proprietary systems/applications
- Designate emergency personnel, including critical business process-level employees

Baseline Cybersecurity Statements

Check if <u>not</u> met (x)

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

Procedure 8 – BCM Testing and Exercises

Determine whether the business continuity exercise/test program is sufficient to demonstrate the ability to achieve the continuity objectives. Consider the following:

- Provisions for exercises and tests occurring at appropriate intervals and when significant changes affect the entity's operating environment
- Comprehensive program objectives and plans of exercises and tests to validate the ability to restore critical business functions in a timely manner
- An exercise and test process that provides assurance for the continuity and resilience of critical business functions, without compromising production environments
- Authorities and control over exercises and tests
- Exercise and test policies, expectations, and strategies that demonstrate the entity's ability to utilize alternate facilities
- Exercise and test objectives for resilience, system monitoring, and the recovery of business processes and critical system components
- Exercise and test scenarios, including exercise and test assumptions, objectives, expectations, and assessment metrics
- Types of exercises (e.g., full scale, limited scale, tabletop) and tests
- Exercises and tests related to interaction with third parties, industry-wide testing, and core and significant firms
- Documentation of issues identified through exercises and tests, and action plans and target dates for resolution

Baseline Cybersecurity Statements

Check if <u>not</u> met (x)

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

Control Test

Review BCP testing documentation to determine adequacy.

Enter Control Test notes here, if performed

Procedure 9 – BCM Training

Evaluate the adequacy of the business continuity training program for all stakeholders. Consider the following:

- Alignment of training with strategies
- Training objectives
- Training format
- The extent to which various stakeholders (e.g., the board, business continuity program staff, incident response team, general personnel) are trained
- Process for reviewing/updating the training program

Decision Factor 3 – Network Architectures

Strong ☐ Satisfactory ☐ Less than satisfactory ☐ Deficient ☐ Critically deficient ☐

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

Procedure 10 – Network Architecture and Configurations

Review the network architecture and configurations with management. Consider the following:

- Critical systems and components (e.g., servers, firewall, routers, switches, IDS/IPS)
- Connection points
- Network segmentation (e.g., demilitarized zone [DMZ], virtual local area network [VLAN], wireless)
- Documentation of network topology

Control Test

Review network topology and other documentation. Determine whether the documentation is accurate and current.

Enter Control Test notes here, if performed

Procedure 11 – Remote Access

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

Baseline Cybersecurity Statements

Check if <u>not</u> met (x)

☐ *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*

Decision Factor 4 – Physical and Logical Security

Strong ☐ Satisfactory ☐ Less than satisfactory ☐ Deficient ☐ Critically deficient ■

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

Procedure 12 – Security Monitoring and Malware Protection

Determine the adequacy of security monitoring for the network, critical systems and applications. Also determine whether sufficient controls are in place to protect against malware. Consider the following:

- Existence of systems to detect or prevent unauthorized network access (e.g., intrusion detection/prevention)
- Virus/malware detection practices (e.g., frequency and scope of scans)
- 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

Baseline Cybersecurity Statements

Check if <u>not</u> met (x)

- ☐ *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*
- ☐ *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 periodically*
- ☐ *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 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.

Enter Control Test notes here, if performed

Procedure 13 – Incident Response

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. Consider the Computer-Security Incident Notification rule.
- 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

GLBA (Information Security Standards Response Program)

Consistent with the Information Security Standards and GLBA, 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 additional information 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.

Baseline Cybersecurity Statements

Check if <u>not</u> met (x)

☐ *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*
☐ *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 action*
☐ *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 Test

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.

Enter Control Test notes here, if performed

Procedure 14 – User Access Rights

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

Baseline Cybersecurity Statements

Check if <u>not</u> met (x)

☐ *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*

Procedure 15 – Privileged User and Accounts

Evaluate the controls over privileged users and accounts (e.g., database, network, system administrators, and hypervisors/virtual hosts). 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

Baseline Cybersecurity Statements

Check if <u>not</u> met (x)

☐ *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.

Enter Control Test notes here, if performed

Procedure 16 – Authentication Controls

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:

- Configurations based upon industry standards/vendor recommendations, including virtual machines and hypervisors
- Configurations standards approved and settings audited
- Unnecessary ports and services disabled
- Adequacy of automated tools (if being used) to enforce secure configurations
- Default passwords and accounts changed/disabled
- Password controls (expiration period, re-use and history, reset procedures, complexity)
- Failed login settings (number of attempts and lockout period)
- Automatic timeouts
- Use of tokens
- Biometric solutions
- Time-of-day and day-of-week restrictions

Baseline Cybersecurity Statements

Check if <u>not</u> met (x)

☐ *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*

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

☐ *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

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

Enter Control Test notes here, if performed

Procedure 17 – Patch Management

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

Baseline Cybersecurity Statements

Check if <u>not</u> met (x)

☐ *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 Test

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.

Enter Control Test notes here, if performed

Procedure 18 – Encryption

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

Baseline Cybersecurity Statements

Check if <u>not</u> met (x)

☐ *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*

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

Procedure 19 – Physical Controls

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

Baseline Cybersecurity Statements

Check if <u>not</u> met (x)

☐ *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.

Enter Control Test notes here, if performed

Decision Factor 5 – Electronic Funds Transfer (EFT)

Strong ☐ Satisfactory ☐ Less than satisfactory ☐ Deficient ☐ Critically deficient ☐

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

Procedure 20 – Electronic Funds Transfer

Evaluate the adequacy of EFT oversight and controls. 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/Disaster Recovery plans
- Scope and frequency of EFT audit coverage

Examiners should document the conclusions of the evaluation of the EFT oversight and controls here and elsewhere as applicable within the workpapers. Examiners are reminded that EFT activity can have an impact on other examination areas including, but not limited to, Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT), Asset Quality, Liquidity, and Sensitivity to Market Risk. Examiners reviewing EFT may observe suspicious activity, loan participation activity, borrowing activity, brokered deposits, and other inflows and outflows. When observed, examiners should share appropriate information with other examiners reviewing those respective areas.

For institutions with significant or complex EFT activity, this core procedure may need to be augmented with additional procedures that address more complex risks. Examiners should utilize the Electronic Funds Transfer Risk Assessment ED Module and the FFIEC IT Examination Handbook – Retail Payment Systems as resources at institutions with high volume or complex EFT activities. Significant findings and conclusions should be pulled forward from those workprograms into the comment box below.

Decision Factor 6 – Additional Information

Strong ☐ Satisfactory ☐ Less than satisfactory ☐ Deficient ☐ Critically deficient ☐

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.)

Supplemental Workprogram

(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 and Access to Financial Institution Services and Systems, and other outstanding guidance.

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

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, and other outstanding guidance.

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

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.

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

InTREx Information Technology Risk Examination	Institution Name:
	Cert#
	Preparer:
Information Security Standards	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.

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.

InTREx 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
Cybersecurity	**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 the FFIEC Cybersecurity Assessment Tool maps the baseline declarative statements to existing guidance in the FFIEC IT Examination Handbook.

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.				
Strong ☐	Satisfactory ☐	Less than satisfactory ☐	Deficient ☐	Critically deficient ☐	

End of Workpaper.

InTREx Information Technology Risk Examination	**Institution Name:** Click here to enter institution name
	Cert# Click here to enter cert number
Management: Expanded Analysis	**Preparer:** Click here to enter preparer
	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 Management Expanded Analysis.

InTREx Information Technology Risk Examination **Support and Delivery:** Expanded Analysis	**Institution Name:**
	Cert#
	Preparer:
	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

Strong ☐ Satisfactory ☐ Less than satisfactory ☐ Deficient ☐ Critically deficient ☐

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

▼ Procedure #3

Strong ☐ Satisfactory ☐ Less than satisfactory ☐ Deficient ☐ Critically deficient ☐

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

▼ Procedure #4

Strong ☐ Satisfactory ☐ Less than satisfactory ☐ Deficient ☐ Critically deficient ☐

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

▼ Procedure #5

Strong ☐ Satisfactory ☐ Less than satisfactory ☐ Deficient ☐ Critically deficient ☐

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

▼ Procedure #6

Strong ☐ Satisfactory ☐ Less than satisfactory ☐ Deficient ☐ Critically deficient ☐

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

▼ Procedure #7

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

InTREx

Procedures

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 ▲

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 ▲

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 ▲

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 ▲

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 ▲

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 ▲

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 ▲

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 ▲

End of Support and Delivery Expanded Analysis.