Note: *This mapping is for informational purposes only. It shows what changed between the 2016 and 2023 versions of the InTREx work program.*

1 Audit

Resources

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

Preliminary Review

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

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

Decision Factors

1. The level of independence maintained by audit and the quality of the oversight and support provided by the Board of Directors and management.
2. The adequacy of IT coverage in the overall audit plan and the adequacy of the underlying risk analysis methodology used to formulate that plan.

3. The scope, frequency, accuracy, and timeliness of internal and external audit reports and the effectiveness of audit activities in assessing and testing IT controls.
4. The qualifications of the auditor, staff succession, and continued development through training.
5. The existence of timely and formal follow-up and reporting on management's resolution of identified problems or weaknesses.
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.)

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 ~~its~~ 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)

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.

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

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

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.

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 ~~cycles~~plans and schedules based on risk

Procedure 5 – IT Risk Exposure

Determine whether ~~the~~ 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 ~~(IDS/IPS)~~
- Security monitoring, including logging practices
- Change management
- Patch management
- Third-party outsourcing
- Social engineering
- Funds transfer
- Online banking
- Business continuity ~~planning~~management

Control Test

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

Procedure 6 – Audit Frequency

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

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 on 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

Control Test

Sample the audit workpapers for adequacy and completeness.

Procedure 9 – Auditor Expertise and Training

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

- Education
- Experience
- On-going training for both internal and external personnel as appropriate

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 in 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

2 Management

Resources

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

Preliminary Review

Review items relating to Management, such as:

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

Decision Factors

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

2. The ability of management to provide information reports necessary for informed planning and decision making in an effective and efficient manner.
3. The adequacy of, and conformance with, internal policies and controls addressing IT operations and risks of significant business activities.
4. The level of awareness of and compliance with laws and regulations.
5. The level of planning for management succession.
6. The adequacy of contracts and management's ability to monitor relationships with third-party servicers.
7. The adequacy of risk assessment processes to identify, measure, monitor, and control risks.
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.)

Procedure 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

Procedure 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

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.

Procedure 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

Procedure 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

Control Test

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

Procedure 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).

Control Test

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

Procedure 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

Control Test

Review procedures for communicating policies to staff.

Review internal audit testing of policy adherence.

Procedure 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

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.

Procedure 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

Control Test

Review documentation of employee security awareness training.

Procedure 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.

Procedure 10

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

Procedure 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.

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.

Procedure 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

Control Test

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

Procedure 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 evaluation the quality of the bank's vendor management relative to that rating.

Control Test

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

Procedure 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

Procedure 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

Control Test

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

Procedure 16

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

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

Control Test

Review insurance policies to ensure coverage of IT activities.

Supplemental Workprograms

Outsourcing / Vendor Management / Third-Party Risk

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

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

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

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.

3 Support and Delivery

Resources

- FFIEC IT Examination Handbook – Architecture, Infrastructure, and Operations (AIO), Information Security, and Business Continuity ~~Planning~~ 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~~FFIEC Guidance on Authentication in an Internet Banking Environment (2005 and 2011)~~

Preliminary Review

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

- Prior examination reports and workpapers
- Pre-examination memoranda and file correspondence
- Operations-related policies
- Network topology
- Cybersecurity self-assessments
- Reports of any significant cyber-attacks, security events, or operational interruptions
- Internal and external IT audit reports
- Board~~/~~ and ~~C~~committee minutes related to IT
- Information Technology Profile
- ~~Disaster recovery/b~~Business continuity management plan
- Network vulnerability assessments/penetration tests
- Regulatory reports ~~(e.g., TSP 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.

Decision Factors

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

~~2.~~ ~~T~~the adequacy of data controls over preparation, input, processing, and output; ~~.~~

~~3.~~1. and ~~T~~the quality of assistance provided to users, including the ability to handle problems.

~~4.~~2. The adequacy of ~~corporate contingency planning and business resumption for data centers, networks, service providers, and business units~~resilience, continuity, and response capabilities to safeguard personnel, customers, and products and services.

~~5.~~3. The adequacy of network architectures and the security of connections with public networks

~~6.~~4. The quality of physical and logical security, including the privacy of data.

~~7.~~5. The adequacy of controls over electronic funds transfers and electronic banking activities.

~~8.~~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.)

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)

Control Test

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

Procedure 2 – Imaging

Evaluate the adequacy of controls for item processing functions, including check imaging~~document imaging and management systems~~. Consider the following:

- ~~Indexing controls (i.e., organized and easily accessible)~~
- ~~Limitations on the ability to alter scanned documents (particularly important if relying on documents for legal purposes)~~
- ~~Record retention requirements (i.e., compliance with State and Federal regulations)~~

- ~~Error handling and readability of images (i.e., quality assurance process)~~
- ~~Controls over the destruction of source documents after being scanned~~
- ~~Inclusion of imaging systems in the information security risk assessment if documents include personally identifiable information~~
- ~~Inclusion of imaging systems in business continuity planning~~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.

~~Procedure 3~~

~~Evaluate the adequacy of controls for item processing functions, including check imaging. Consider the following:~~

- ~~Controls over teller/branch imaging~~
- ~~Security over the capture, storage, and transmission of images~~
- ~~Controls over the destruction of source documents after being scanned~~
- ~~Dual control or independent review over the processing of reject, re-entry, and unposted items~~
- ~~Physical controls over negotiable items~~
- ~~Controls over cash letters (e.g., reconcilements, segregation of duties)~~

~~Procedure 4~~

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

- ~~Training~~
- ~~Problem resolution~~
- ~~Overall support~~

~~Control Test~~

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

Procedure 3 – BCM Governance~~5~~

Determine whether the Board and senior management ~~annually~~ periodically review and approve the following:

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

Procedure 4 – Business Impact Analysis~~6~~

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

- Input from all integral groups (e.g., business line management, risk management, IT, facilities management, and audit) and comprehensiveness of management's review
- Analysis of reasonably foreseeable threats, including natural events, technical events, pandemics, malicious activity, and cyber threats
- Utilization of the business impact analysis to identify critical business assets and prioritize recovery of processes, systems, and applications
- ~~Identification~~ 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 vendors or service providers in the business impact analyses/risk assessments

Control Test

Review a sample of business impact analyses and risk assessments.

Procedure 5 – Business Continuity Plan (BCP)~~7~~

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

- ~~Identification of alternate locations for business operations and IT recovery~~
- ~~Backup of data, operating systems, applications, and telecommunication~~
- ~~Offsite storage of backup media, supplies, business continuity plan, and system documentation~~
- ~~Existence of alternate power supplies (e.g., uninterruptable power supply [UPS], generators)~~
- ~~Procedures and priorities for returning to permanent and normal operations~~
- ~~Designation of business continuity personnel and responsibilities~~
- ~~Adequacy of service providers' business continuity programs, including cyber resilience and preparedness~~
- ~~Process for updating plans as needed~~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~~8~~

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

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

Procedure 7 – Business Continuity Strategies~~9~~

Determine whether ~~the business continuity plan effectively addresses pandemic issues~~management can effectively respond to wide-scale disruptions in order to meet resilience and recovery objectives. ~~Consider the following~~Do the strategies:

- ~~Planning~~
- ~~Preparing~~
- ~~Testing~~
- ~~Responding~~
- ~~Recovering~~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

~~Procedure 10~~

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

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

Procedure 8 – BCM Testing and Exercises~~11~~

Determine whether the business continuity exercise/test~~ing~~ program is sufficient to demonstrate the ~~financial institution's~~ ability to meet its continuity objectives. Consider the following:

- ~~Regular testing of varying scenarios, including cyber attacks, based upon risk assessment~~
- ~~Testing of critical business lines, systems, and operations, such as:~~
    - ~~Core systems~~
    - ~~Networks~~

- ~~Funds transfer~~
- ~~Telecommunications~~
- ~~Testing of internal interdependencies between business units and processes~~

- ~~Documentation of all facets of the continuity testing program, including:~~
  - ~~Test scenarios~~
  - ~~Plans~~
  - ~~Scripts~~
  - ~~Results~~
  - ~~Reporting, including Board reporting~~
- ~~Employee familiarity with the written plans and their individual responsibilities~~
- ~~Analysis of test results and resolution of any identified issues~~
- ~~Use of offsite resources (e.g., backup data) to conduct the recovery test~~
- ~~Testing with critical third-party service providers, including at a minimum:~~
  - ~~From the institution's primary location to the TSPs' alternative location~~
  - ~~From the institution's alternative location to the TSPs' primary location~~
- ~~Testing the adequacy of remote access infrastructure and capacity, if being relied upon for critical business continuity processes in a pandemic or other scenario~~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

Control Test

Review BCP testing documentation to determine adequacy.

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

Procedure 10 – Network Architecture and Configurations~~2~~

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

- ~~Date of last update~~
- ~~Identification of all c~~Critical systems and components (e.g., servers, firewall, routers, switches, IDS/IPS)
- ~~Identification of all c~~Connection points
- ~~Identification of n~~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.

Procedure 11 – Remote Access~~3~~

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

Procedure 12 – Security Monitoring and Malware Protection4

Determine the adequacy of security monitoring for the network and all 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

~~Procedure 19~~

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

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

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.

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

Procedure 13 – Incident Response~~5~~

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

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.

Procedure 14 – User Access Rights~~6~~

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

Control Test

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

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

Procedure 15 – Privileged User and Accounts~~7~~

Evaluate the controls over privileged users/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

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.

Procedure 16 – Authentication Controls~~8~~

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

~~Procedure 19~~

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

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

~~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.~~

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

~~Procedure 20~~

~~Assess system configuration procedures. Consider the following:~~

~~Configurations based upon industry standards/vendor recommendations~~

~~Configurations standards approved and settings audited~~

~~Unnecessary ports and services disabled~~

~~Default passwords and accounts changed/disabled~~

- ~~Adequacy of automated tools (if being used) to enforce secure configurations~~

Control Test

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

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

Procedure 17 – Patch Management~~21~~

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

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

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.

Procedure 18 – Encryption~~22~~

Evaluate the institution's use of encryption for sensitive institution and customer data at rest and in transit. Consider the following:

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

Procedure 19 – Physical Controls~~23~~

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

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

Control Test

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

Procedure 20 – Electronic Funds Transfer~~24~~

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

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

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 ~~is probably not sufficient in and of itself~~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/or the FFIEC IT Examination Handbook – Retail Payment Systems at institutions with high volume ~~and/~~or complex EFT activities. Significant findings and conclusions should be pulled forward from those workprograms into the comment box below.

~~Procedure 25~~

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

- ~~Due diligence in selecting the electronic banking third-party service provider (if applicable)~~
- ~~Electronic banking risk assessment process~~
    - ~~Inclusion of all products, services, and channels offered (or contemplated) by the financial institution~~
    - ~~Procedures to update the risk assessment at least annually to address:~~
        - ~~Changes in the threat environment, customer base, and/or electronic banking functionality~~
        - ~~Actual incidents of security breaches, identity theft, or fraud experienced by the financial institution or the industry~~
- ~~Authentication and authorization process for customers~~
    - ~~Enrollment procedures~~
    - ~~Authentication parameters and requirements~~

- Enhanced authentication for higher risk activities, such as external transfer of funds
- Re-authentication after period of inactivity
- Procedures to adjust authentication controls based on risk assessments

- Transaction risk
  - Ability to detect, prevent, and respond to fraudulent or anomalous activity
  - Ability to leverage location features for fraud detection
- Customer education
  - Social engineering
  - Phishing
  - Anti-virus/malware
  - Public Internet access
- Compliance and Legal risks
  - BSA/AML compliance (recordkeeping, screening, and reporting requirements)
  - Consumer and privacy disclosures
- Reputation risk
  - Cyber threats
  - Lack of availability

Control Test

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

Procedure 26

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

- On-device data security
  - Customer education regarding the use of PINs or passwords on devices
  - Controls to avoid retaining unnecessary sensitive information on devices
  - Encryption of any sensitive information stored on devices
  - Secure wiping of sensitive information from memory upon exiting the application
  - Authentication when re-entering the application

- Ability to quickly deregister a device if reported lost or stolen

- Mobile application security
  - Secure coding practices
  - Testing for vulnerabilities
  - Ability to patch quickly
- Mobile application delivery/marketplace
  - Customer education on downloading application and any subsequent updates/patches only from a reputable source
- Mobile device malware and viruses
  - Customer education on installing anti-malware on devices
- SMS-based products
  - For communication of non-sensitive information only since SMS is unencrypted
  - Customer education about social engineering, phishing, and other malicious activities
- Data transmission security
  - Customer education on risks of public Wi-Fi

Supplemental Workprogram

E-Banking

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

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

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.

4 Cybersecurity

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

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

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

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

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

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

Procedure 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.

5 ~~Notes~~Unaffected Sections

There were no changes to the following sections of the InTREx program:

- Development and Acquisition Core Module
- Management Expanded Analysis
- Support and Delivery Expanded Analysis
- Information Security Procedures