Appendix A: Examination Procedures

EXAMINATION OBJECTIVE: Determine the quality and effectiveness of the organization's business continuity planning process, and determine whether the continuity testing program is sufficient to demonstrate the financial institution's ability to meet its continuity objectives. These procedures will disclose the adequacy of the planning and testing process for the organization to recover, resume, and maintain operations after disruptions, ranging from minor outages to full-scale disasters.

This workprogram can be used to assess the adequacy of the business continuity planning process on an enterprise-wide basis or across a particular line of business. Depending on the examination objectives, a line of business can be selected to sample how the organization's continuity planning or testing processes work on a micro level or for a particular business function or process.

This workprogram is not intended to be an audit guide; however, it was developed to be comprehensive and assist examiners in determining the effectiveness of a financial institution's business continuity planning and testing program. Examiners may choose to use only certain components of the workprogram based upon the size, complexity, and nature of the institution's business.

The objectives and procedures are divided into Tier I and Tier II:

- Tier I assesses an institution's process for identifying and managing risks.
- Tier II provides additional verification where risk is eviden

Tier I and Tier II objectives and procedures are intended to be a tool set examiners may use when selecting examination procedures for their particular examination. Examiners should use these procedures as necessary to support examination objectives.

TIER I OBJECTIVES AND PROCEDURES

Examination Scope

Objective 1: Determine examination scope and objectives for reviewing the business continuity planning program.

1. Review examination documents and financial institution reports for outstanding issues or problems. Consider the following:

- Pre-examination planning memos;
- Prior regulatory reports of examination;
- Prior examination workpapers;
- Internal and external audit reports, including third-party reports;

- Business continuity test results; and
- The financial institution's overall risk assessment and profile.

2. Review management's response to audit recommendations noted since the last examination. Consider the following:

- Adequacy and timing of corrective action;
- Resolution of root causes rather than just specific audit deficiencies;
- Existence of any outstanding issues; and
- Monitoring systems used to track the implementation of recommendations on an on-going basis

3. Interview management and review the business continuity request information to identify:

- Any significant changes in management, business strategies or internal business processes that could affect the business recovery process;
- Any material changes in the audit program, scope, or schedule related to business continuity activities;
- IT environments and changes to configuration or components;
- Changes in key service providers (technology, communication, back-up/recovery, etc.) and software vendors; and
- Any other internal or external factors that could affect the business continuity process.

4. Determine management's consideration of newly identified threats and vulnerabilities to the organization's business continuity process. Consider the following:

- Technological and security vulnerabilities;
- Internally identified threats; and
- Externally identified threats (including security alerts, pandemic alerts, or emergency warnings published by information sharing organizations or local, state, and federal agencies).

5. Establish the scope of the examination by focusing on those factors that present the greatest degree of risk to the institution or service provider.

Board and Senior Management Oversight

Objective 2: Determine the quality of business continuity plan oversight and support provided by the board and senior management.

1. Determine whether the board has established an on-going, process-oriented approach to business continuity planning that is appropriate for the size and complexity of the organization. This process should include a business impact analysis (BIA), a risk assessment, risk management, and risk monitoring and testing. Overall, this planning process should encompass the organization's business continuity strategy, which is the ability to recover, resume, and maintain all critical business functions.

2. Determine whether a senior manager or committee has been assigned responsibility to oversee the development, implementation, and maintenance of the BCP and the testing program.

3. Determine whether the board and senior management has ensured that integral groups are involved in the business continuity process (e.g. business line management, risk management, IT, facilities management, and audit).

4. Determine whether the board and senior management have established an enterprise-wide BCP and testing program that addresses and validates the continuity of the institution's mission critical operations.

5. Determine whether the board and senior management review and approve the BIA, risk assessment, written BCP, testing program, and testing results at least annually and document these reviews in the board minutes.

6. Determine whether the board and senior management oversee the timely revision of the BCP and testing program based on problems noted during testing and changes in business operations.

Business Impact Analysis (BIA) and Risk Assessment

Objective 3: Determine whether an adequate BIA and risk assessment have been completed.

1. Determine whether the work flow analysis was performed to ensure that all departments and business processes, as well as their related interdependencies, were included in the BIA and risk assessment.

2. Review the BIA and risk assessment to determine whether the prioritization of business functions is adequate.

3. Determine whether the BIA identifies maximum allowable downtime for critical business functions, acceptable levels of data loss and backlogged transactions, recovery time objectives (RTOs), recovery point objectives (RPOs), recovery of the critical path (business processes or systems that should receive the highest priority), and the costs associated with downtime.

4. Review the risk assessment and determine whether the includes the impact and probability of disruptions of information services, technology, personnel, facilities, and

services provided by third-parties, including:

- Natural events such as fires, floods, severe weather, air contaminants, and hazardous spills;
- Technical events such as communication failure, power failure, equipment and software failure, transportation system disruptions, and water system disruptions;
- Malicious activity including fraud, theft or blackmail; sabotage; vandalism and looting; and terrorism; and
- Pandemics.

5. Verify that reputation, operational, compliance, and other risks that are relevant to the institution are considered in the BIA and risk assessment.

Risk Management

Objective 4: Determine whether appropriate risk management over the business continuity process is in place and if the financial institution's and TSP's risk management strategies consider wide-scale recovery scenarios designed to achieve industry-wide resilience.

1. Determine whether management has engaged other firms in the discussion of scenarios, performed continuity planning using wide-scale or severely disruptive scenarios, and assessed capacity and feasibility of resuming normal operations.

2. Determine whether adequate risk mitigation strategies have been considered for:

- Alternate locations and capacity for:
  - Data centers and computer operations;
  - Back-room operations;
  - Work locations for business functions; and
  - Telecommunications and remote computing.
- Back-up of:
  - Data;
  - Operating systems;
  - Applications;
  - Utility programs; and
  - Telecommunications;
- Secure and up-to-date off-site storage of:

- Back-up media;
- Supplies;
- BCP; and
- System documentation (e.g. topologies; inventory listing; firewall, router, and network configurations; operating procedures).

- Alternate power supplies (e.g. uninterruptible power source, back-up generators);
- Recovery of data (e.g. backlogged transactions, reconciliation procedures); and
- Preparation for return to normal operations once the permanent facilities are available.

3. Determine whether satisfactory consideration has been given to geographic diversity for:

- Alternate facilities;
- Alternate processing locations;
- Alternate telecommunications;
- Alternate staff; and
- Off-site storage.

4. Determine whether management has considered the possibility of transferring critical aspects of the institution's operation to alternate backup providers or other industry participants to ensure continuity of operations in extreme situations.

5. Verify that appropriate policies, standards, and processes address business continuity planning issues including:

- Security;
- Project management;
- Change control process;
- Data synchronization, back-up, and recovery;
- Crisis management (responsibility for disaster declaration and dealing with outside parties);
- Incident response;

- Remote access;
- Employee training;
- Notification standards (employees, customers, regulators, vendors, service providers);
- Insurance; and
- Government and community coordination.

6. Determine whether personnel are regularly trained in their specific responsibilities under the plan(s) and whether current emergency procedures are posted in prominent locations throughout the facility.

7. Determine whether the continuity strategy addresses interdependent components, including:

- Utilities;
- Telecommunications;
- Third-party technology providers;
- Key suppliers/business partners; and
- Internal systems and business processes.

8. Determine whether management has reviewed all interrelated components of each mission critical application and the underlying continuity strategy to determine "single point of failure" exposure.

9. Determine whether there are adequate processes in place to ensure that a current BCP is maintained and disseminated appropriately. Consider the following:

- Designation of personnel who are responsible for maintaining changes in processes, personnel, and environment(s); and
- Timely distribution of revised plans to personnel.

10. Determine management's process for determining the scope of disaster recovery test scenarios, including whether management augments the tests with multiple concurrent or widespread interruptions to simulate the impact of "worst case" scenarios.

11. Determine whether audit involvement in the business continuity program is effective, including:

- Audit coverage of the business continuity program;
- Assessment of business continuity preparedness during line(s) of business reviews;
- Audit participation in testing as an observer and as a reviewer of test plans and results; and
- Documentation of audit findings

Business Continuity Planning (BCP) - General

Objective 5: Determine the existence of an appropriate enterprise-wide BCP.

1. Review and verify that the written BCP:

- Addresses the recovery of each business unit/department/function/application:
  - According to its priority ranking in the risk assessment;
  - Considering interdependencies among systems; and
  - Considering long-term recovery arrangements.
- Addresses the recovery of vendors and outsourcing arrangements.
- Take(s) into account:
  - Personnel;
  - Communication with employees, emergency personnel, regulators, vendors/ suppliers, customers, and the media;
  - Technology issues (hardware, software, network, data processing equipment, telecommunications, remote computing, vital records, electronic banking systems, telephone banking systems, utilities);
  - Vendor(s) ability to service contracted customer base in the event of a major disaster or regional event;
  - Facilities;
  - Liquidity;
  - Security;
  - Financial disbursement (purchase authorities and expense reimbursement for senior management during a disaster); and
  - Manual operating procedures.
- Include(s) emergency preparedness and crisis management plans that:
  - Include an accurate contact tree, as well as primary and emergency contact

information, for communicating with employees, service providers, vendors, regulators, municipal authorities, and emergency response personnel;

- Define responsibilities and decision-making authorities for designated teams or staff members;
- Explain actions to be taken in specific emergencies;
- Define the conditions under which the back-up site would be used;
- Include procedures for notifying the back-up site;
- Identify a current inventory of items needed for off-site processing;
- Designate a knowledgeable public relations spokesperson; and
- Identify sources of needed office space and equipment and a list of key vendors (hardware/software/telecommunications, etc.).

BCP - Hardware, Back-up and Recovery Issues

Objective 6: Determine whether the BCP includes appropriate hardware back-up and recovery.

1. Determine whether there is a comprehensive, written agreement or contract for alternative processing or facility recovery.

2. If the organization is relying on in-house systems at separate physical locations for recovery, verify that the equipment is capable of independently processing all critical applications.

3. If the organization is relying on outside facilities for recovery, determine whether the recovery site:

- Has the ability to process the required volume;
- Provides sufficient processing time for the anticipated workload based on emergency priorities; and
- Is available for use until the institution achieves full recovery from the disaster and resumes activity at the institution's own facilities.

4. Determine how the recovery facility's customers would be accommodated if simultaneous disaster conditions were to occur to several customers during the same period of time.

5. Determine whether the organization ensures that when any changes (e.g. hardware or software upgrades or modifications) in the production environment occur that a process is in place to make or verify a similar change in each alternate recovery location.

6. Determine whether the organization is kept informed of any changes at the recovery

site that might require adjustments to the organization's software or its recovery plan(s).

BCP - Security Issues

Objective 7: Determine that the BCP includes appropriate security procedures.

1. Determine whether adequate physical security and access controls exist over data back-ups and program libraries throughout their life cycle, including when they are created, transmitted/delivered, stored, retrieved, loaded, and destroyed.

2. Determine whether appropriate physical and logical access controls have been considered and planned for the inactive production system when processing is temporarily transferred to an alternate facility.

3. Determine whether the intrusion detection and incident response plan considers facility and systems changes that may exist when alternate facilities are used.

4. Determine whether the methods by which personnel are granted temporary access (physical and logical), during continuity planning implementation periods, are reasonable.

5. Evaluate the extent to which back-up personnel have been reassigned different responsibilities and tasks when business continuity planning scenarios are in effect and if these changes require a revision to systems, data, and facilities access.

6. Review the assignment of authentication and authorization credentials to determine whether they are based upon primary job responsibilities and if they also include business continuity planning responsibilities.

BCP - Pandemic Issues

Objective 8: Determine whether the BCP effectively addresses pandemic issues.

1. Determine whether the Board or a committee thereof and senior management provide appropriate oversight of the institution's pandemic preparedness program.

2. Determine whether the BCP addresses the assignment of responsibility for pandemic planning, preparing, testing, responding, and recovering.

3. Determine whether the BCP includes the following elements, appropriately scaled for the size, activities and complexities of the organization:

- A preventive program to reduce the likelihood that an institution's operations will be significantly affected by a pandemic event, including: monitoring of potential outbreaks, educating employees, communicating and coordinating with critical service providers and suppliers, and providing appropriate hygiene training and tools to employees.
- A documented strategy that provides for scaling the institution's pandemic efforts so they are consistent with the effects of a particular stage of a pandemic outbreak, such as first cases of humans contracting the disease overseas, first cases within the United States, and first cases within the organization itself.
- A comprehensive framework of facilities, systems, or procedures that provide the

organization the capability to continue its critical operations in the event that a large number of the institution's staff are unavailable for prolonged periods. Such procedures could include social distancing to minimize staff contact, telecommuting, or conducting operations from alternative sites.

- A testing program to better ensure that the institution's pandemic planning practices and capabilities are effective and will allow critical operations to continue.
- An oversight program to ensure ongoing reviews and updates to the pandemic plan, so that policies, standards, and procedures include up-to-date, relevant information provided by governmental sources or by the institution's monitoring program.

4. Determine whether pandemic risks have been incorporated into the business impact analysis and whether continuity plans and strategies reflect the results of the analysis.

5. Determine whether the BCP addresses management monitoring of alert systems that provide information regarding the threat and progression of a pandemic. Further, determine if the plan provides for escalating responses to the progress or particular stages of an outbreak.

6. Determine whether the BCP addresses communication and coordination with financial institution employees and the following outside parties regarding pandemic issues:

- Critical service providers;
- Key financial correspondents;
- Customers;
- Media representatives;
- Local, state, and federal agencies; and
- Regulators.

7. Determine whether the BCP incorporates management's analysis of the impact on operations if essential functions or services provided by outside parties are disrupted during a pandemic.

8. Determine whether the BCP includes continuity plans and other mitigating controls (e.g. social distancing, teleworking, functional cross-training, and conducting operations from alternative sites) to sustain critical internal and outsourced operations in the event large numbers of staff are unavailable for long periods.

9. Determine whether the BCP addresses modifications to normal compensation and absenteeism polices to be enacted during a pandemic.

10. Determine whether management has analyzed remote access requirements, including the infrastructure capabilities and capacity that may be necessary during a pandemic.

11. Determine whether the BCP provides for an appropriate testing program to ensure that continuity plans will be effective and allow the organization to continue its critical operations. Such a testing program may include:

- Stress testing online banking, telephone banking, ATMs, and call centers capacities to handle increased customer volumes;
- Telecommuting to simulate and test remote access;
- Internal and external communications processes and links;
- Table top operations exercises; and
- Local, regional, or national testing/exercises.

BCP - Third-Party Management and Outsourced Activities

Objective 9: Determine whether management and the BCP addresses critical third parties and outsourced activities and whether there is appropriate oversight in place.

1. Determine if management has taken sufficient steps to ensure third-party technology service providers (TSPs) employ the most recent techniques and technologies (or identify where gaps exist) to mitigate against:

- Large scale disruptive events that could affect the ability to service clients;
- Cyber events that could impact the ability to service clients; and
- Significant downtime that would threaten the financial institution's business resiliency.

2. Determine if the financial institution's due diligence processes considered its service provider's business continuity program. Consider whether management assessed:

- Recovery capabilities and capacity of the service provider;
- Cyber resilience and preparedness;
- Significant downtime that would threaten the financial institution's business resilience; and
- Service provider's oversight of subcontractors.

3. Assess whether the third-party TSP's contract provides for the following elements to ensure business resiliency:

- DR/BCP test results for RTOs that provide evidence the TSP can recover from large scale disruptions and cyber events;
- Independent audit reports that support the RTOs;
- Inclusion of reasonable performance standards (e.g., SLAs, RTOs);
- Right to terminate language (if the TSP defaults on SLAs and RTOs);
- TSP accountability for actions/inactions of subcontractors should the subcontractor fail to provide necessary service(s) for business recovery capabilities;
- Adherence to U.S. data confidentiality and security standards at a minimum by foreign-based service providers/subcontractors;
- Testing requirements with the TSP; and
- Data governance expectations.

4. Evaluate the financial institution's third-party ongoing monitoring program, including the adequacy of information reviewed to determine that the service provider can continue to meet its obligations to provide financial services and support the institution's business resilience. Consider:

- Full-scope, end-to-end testing with a frequency commensurate with complexity and risk;
- Review of independent third-party assessments and regulatory reports;
- Regular review of MIS reporting (e.g., adherence to RTOs);
- Participation in third-party testing;
- Third-party testing results;
- Periodic reporting to an appropriate oversight committee; and
- Awareness and oversight of service provider's use of subcontractors.

5. Evaluate data governance standards and expectations with third-party providers. Consider:

- Data protection, classification, accuracy, availability and back-up; and
- Data volume and growth.

6. Determine whether the BCP addresses communications and connectivity with TSPs in

the event of a disruption at the institution.

7. Determine whether the BCP addresses communications and connectivity with TSPs in the event of a disruption at any of the TSP's facilities.

8. Determine whether there are documented procedures in place for accessing, downloading, and uploading information with TSPs, correspondents, affiliates and other service providers, from primary and recovery locations, in the event of a disruption.

9. Determine whether the institution has a copy of the TSPs' BCP and incorporates it, as appropriate, into their plans.

10. Determine whether management has received and reviewed testing results of their TSPs.

11. Determine whether institution management has assessed the adequacy of the TSPs' business continuity program through their vendor management program (e.g. contract requirements, third-party reviews).

12. For foreign-based third-party service providers determine if management has adequately addressed production and back-up data that remains offshore. Consider:

- Evidence of management's evaluation of whether storage of data offshore (production or back-up) meets the financial institution's risk appetite and profile; and
- Management's assessment of the foreign-based provider's resilience architecture and strategy.

Cyber Resilience

Objective 10: Determine whether the financial institution's and TSP's risk management 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.

1. Determine whether the financial institution and service provider have developed specific procedures for the investigation and resolution of data corruption in response and recovery strategies, including data integrity controls.

2. Determine whether the use of cloud-based disaster recovery services integrate with and protect against data destruction with the same level of assurance as existing (internal) disaster recovery solutions.

3. Determine whether the financial institution and service provider manage the underlying virtualization platform upon which cloud disaster recovery services are based to minimize the impact of attacks designed to cause data destruction and corruption.

4. Determine whether the financial institution and service provider are considering alternate data communications infrastructure to achieve resilience. Consider the efficacy of managing the following risks:

- Reliance upon a single communications provider;
- Disruption of telephony and electronic messaging due to the convergence of voice and data services on the same network; and
- Disruption of data and voice communications between facilities and service providers.

5. Determine whether the financial institution and service provider use a layered anti-malware strategy, including integrity checks, anomaly detection, system behavior monitoring and employee security awareness training, in addition to traditional signature-based anti-malware systems.

6. Determine whether the financial institution and service provider consider their susceptibility to simultaneous attacks in their business resilience planning, testing, and recovery strategies.

7. Determine whether the financial institution and service provider consider their susceptibility to an insider threat and what impact this may have on business continuity and broader resilience.

8. Determine whether the financial institution and service provider have made advance arrangements for both third-party computer forensics and incident management services in advance of a wide-scale cyber security event.

9. Determine whether the incident response program includes a cyber component and assess whether it is appropriate for the size and complexity of the financial institution or service provider. Review the incident response plan to ensure that it addresses the following:

- Teams and responsibilities;
- Procedures for determining the nature and scope of the incident;
- Steps to be taken to contain the problem;
- Details about what is required for contacting affected customers;
- Details about contacting the appropriate regulator;
- Details about filing Suspicious Activity Reports (SARs);
- Details about addressing zero-day attacks;
- A requirement for periodic testing of the incident response plan in the real-world threat landscape; and
- Data destruction and corruption.

Risk Monitoring and Testing

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

Testing Policy

1. Determine whether the institution has a business continuity testing policy that sets testing expectations for the enterprise-wide continuity functions, business lines, support functions, and crisis management.

2. Determine whether the testing policy identifies key roles and responsibilities of the participants in the testing program.

3. Determine whether the testing policy establishes a testing cycle with increasing levels of test scope and complexity.

Testing Strategy

1. Determine whether the institution has a business continuity testing strategy that includes documented test plans and related testing scenarios, testing methods, and testing schedules and also addresses expectations for mission critical business lines and support functions, including:

- The scope and level of detail of the testing program;
- The involvement of staff, technology, and facilities;
- Expectations for testing internal and external interdependencies; and
- An evaluation of the reasonableness of assumptions used in developing the testing strategy.

2. Determine whether the testing strategy articulates management's assumptions and whether the assumptions (e.g. available resources and services, length of disruption, testing methods, capacity and scalability issues, and data integrity) appear reasonable based on a cost/benefit analysis and recovery and resumption objectives.

3. Determine whether the testing strategy addresses the need for enterprise-wide testing and testing with significant third-parties.

4. Determine whether the testing strategy includes guidelines for the frequency of testing that are consistent with the criticality of business functions, RTOs, RPOs, and recovery of the critical path, as defined in the BIA and risk assessment, corporate policy, and regulatory guidelines.

5. Determine whether the testing strategy addresses the documentation requirements for all facets of the continuity testing program, including test scenarios, plans, scripts, results, and reporting.

6. Determine whether the testing strategy includes testing the effectiveness of an institution's crisis management process for responding to emergencies, including:

- Roles and responsibilities of crisis management group members;
- Risk assumptions;
- Crisis management decision process;
- Coordination with business lines, IT, internal audit, and facilities management;
- Communication with internal and external parties through the use of diverse methods and devices (e.g., calling trees, toll-free telephone numbers, instant messaging, websites); and
- Notification procedures to follow for internal and external contacts.

7. Determine whether the testing strategy addresses physical and logical security considerations for the facility, vital records and data, telecommunications, and personnel.

Execution, Evaluation, and Re-Testing

1. Determine whether the institution has coordinated the execution of its testing program to fully exercise its business continuity planning process, and whether the test results demonstrate the readiness of employees to achieve the institution's recovery and resumption objectives (e.g. sustainability of operations and staffing levels, full production recovery, achievement of operational priorities, timely recovery of data).

2. Determine whether test results are analyzed and compared against stated objectives; test issues are assigned ownership; a mechanism is developed to prioritize test issues; test problems are tracked until resolution; and recommendations for future tests are documented.

3. Determine whether the test processes and results have been subject to independent observation and assessment by a qualified third party (e.g., internal or external auditor).

4. Determine whether an appropriate level of re-testing is conducted in a timely fashion to address test problems or failures.

Testing With Third-Party Service Providers

Objective 12: Determine whether the financial institution's testing program enhances resilience through demonstrated ability to recover, resume, and maintain operations after disruptions, ranging from minor outages to wide-scale disasters consistent with the BIA and risk assessment.

1. Determine whether testing with third-party providers is included in the institution's enterprise BCP testing program. When testing with the critical service providers, determine whether management considered testing:

- From the institution's primary location to the TSPs' alternative location;
- From the institution's alternative location to the TSPs' primary location; and
- From the institution's alternative location to the TSPs' alternative location.

2. Determine whether a process exists to rank third parties based on criticality, risk, and testing scope.

3. Determine whether the financial institution has a process to ensure they are included in their critical third-party providers' testing program(s) at reasonable intervals. Consider whether:

- Testing is full-scale and end-to-end;
- Testing includes network connectivity and identifies interdependencies; and
- Testing includes critical subcontractors.

4. Evaluate how the financial institution ensures timeliness, thoroughness, and completeness of periodic testing with their critical providers.

5. Determine whether testing scenarios with critical third-parties considers:

- An outage or disruption of the service provider;
- An outage or disruption at the financial institution;
- An incident response plan;
- Crisis management;
- Cyber events; and
- Return to normal operations.

6. Assess documented process/transaction flow charts to evaluate the thoroughness of the testing scope, plans and strategy.

7. Determine whether the client institution has received assurance, via testing documentation, that the third party can restore services to client institution and support typical volumes during a recovery event.

8. Determine whether the institution relies on proxy testing.

9. Determine whether the institution receives adequate testing information which validates and demonstrates the recovery capability and capacity of their critical service providers.

Testing Expectations for Core Firms and Significant Firms

Note: The following testing expectations only apply to core and significant firms as defined by interagency guidelines.

Core firms are defined as organizations that perform core clearing and settlement

activities in critical financial markets. Significant firms are defined as organizations that process a significant share of transactions in critical financial markets.

For core and significant firms:

1. Determine whether core and significant firms have established a testing program that addresses their critical market activities and assesses the progress and status of the implementation of the testing program to address BCP guidelines and applicable industry standards.

2. Determine the extent to which core and significant firms have demonstrated through testing or routine use that they have the ability to recover and, if relevant, resume operations within the specified time frames addressed in the BCP guidelines and applicable industry standards.

3. Determine whether core and significant firm's strategies and plans address wide-scale disruption scenarios for critical clearance and settlement activities in support of critical financial markets. Determine whether test plans demonstrate their ability to recover and resume operations, based on guidelines defined by the BCP and applicable industry standards, from geographically dispersed data centers and operations facilities.

4. Determine that back-up sites are able to support typical payment and settlement volumes for an extended period.

5. Determine that back-up sites are fully independent of the critical infrastructure components that support the primary sites.

6. Determine whether the tests validate the core and significant firm's back-up arrangements to ensure that: :

- Trained employees are located at the back-up site at the time of disruption;
- Back-up site employees are independent of the staff located at the primary site, at the time of disruption; and
- Back-up site employees are able to recover clearing and settlement of open transactions within the timeframes addressed in the BCP and applicable industry guidance.

7. Determine that the test assumptions are appropriate for core and significant firms and consider:

- Primary data centers and operations facilities that are completely inoperable without notice;
- Staff members at primary sites, who are located at both data centers and operations facilities, are unavailable for an extended period;
- Other organizations in the immediate area that are also affected;
- Infrastructure (power, telecommunications, transportation) that is disrupted;

- Whether data recovery or reconstruction necessary to restart payment and settlement functions can be completed within the timeframes defined by the BCP and applicable industry standards; and
- Whether continuity arrangements continue to operate until all pending transactions are closed.

For core firms:

8. Determine whether the core firm's testing strategy includes plans to test the ability of significant firms, which clear or settle transactions, to recover critical clearing and settlement activities from geographically dispersed back-up sites within a reasonable time frame.

For significant firms:

9. Determine whether the significant firm has an external testing strategy that addresses key interdependencies, such as testing with third-party market providers and key customers.

10. Determine whether the significant firm's external testing strategy includes testing from the significant firm's back-up sites to the core firms' back-up sites.

11. Determine whether the significant firm meets the testing requirements of applicable core firms.

12. Determine whether the significant firm participates in "street" or market-wide tests sponsored by core firms, markets, or trade associations that tests the connectivity from alternate sites and includes transaction, settlement, and payment processes, to the extent practical.

Conclusions

Objective 13: Discuss corrective action and communicate findings.

1. From the procedures performed:

- Determine the need to proceed to Tier II objectives and procedures for additional validation to support conclusions related to any of the Tier I objectives and procedures.
- Document conclusions related to the quality and effectiveness of the business continuity process.
- Determine and document to what extent, if any, you may rely upon the procedures performed by the internal and external auditors in determining the scope of the business continuity procedures.
- Document conclusions regarding the testing program and whether it is appropriate for the size, complexity, and risk profile of the institution.
- Document whether the institution has demonstrated, through an effective testing

program, that it can meet its testing objectives, including those defined by management, the FFIEC, and applicable regulatory authorities.

2. Review your preliminary conclusions with the examiner-in-charge (EIC) regarding:

- Violations of law, rulings, regulations;
- Significant issues warranting inclusion as matters requiring board attention or recommendations in the report of examination; and
- The potential impact of your conclusions on composite and component ratings.

3. Discuss your findings with management and obtain proposed corrective action and deadlines for remedying significant deficiencies.

4. Document your conclusions in a memo to the EIC that provides report ready comments for all relevant sections of the report of examination.

5. Organize and document your work papers to ensure clear support for significant findings and conclusions.

Tier II Objectives and Procedures

Tier II objectives and examination procedures may be used to provide additional verification of the effectiveness of business continuity planning or identify potential root causes for weaknesses in the business continuity program. These procedures may be used in their entirety or selectively, depending on the scope of the examination and the need for additional verification. Examiners should coordinate this coverage with other examiners to avoid duplication of effort while reviewing various issues found in other work programs.

The procedures provided in this section should not be construed as requirements for control implementation. The selection of controls and control implementation should be guided by the risk profile of the institution. Therefore, the controls necessary for any single institution or any given area may differ from those noted in the following procedures.

Testing Strategy

Objective 1: Determine whether the testing strategy addresses various event scenarios, including potential issues encountered during a wide-scale disruption:

Event Scenarios

1. Determine whether the strategy addresses staffing considerations, including:

- The ability to perform transaction processing and settlement;
- The ability to communicate with key internal and external stakeholders;

- The ability to reconcile transaction data;
- The accessibility, rotation, and cross training of staff necessary to support critical business operations;
- The ability to relocate or engage staff from alternate sites;
- Staff and management succession plans;
- Staff access to key documentation (plans, procedures, and forms); and
- The ability to handle increased workloads supporting critical operations for extended periods.

2. Determine whether the strategy addresses technology considerations, including:

- Testing the data, systems, applications, and telecommunications links necessary for supporting critical financial markets;
- Testing critical applications, recovery of data, failover of the network, and resilience of telecommunications links;
- Incorporating the results of telecommunications diversity assessments and confirming telecommunications circuit diversity;
- Testing disruption events affecting connectivity, capacity, and integrity of data transmission; and
- Testing recovery of data lost when switching to out-of-region, asynchronous back-up facilities.

3. Determine whether the business line testing strategy addresses the facilities supporting the critical business functions and technology infrastructure, including:

- Environmental controls - the adequacy of back-up power generators; heating, ventilation, and air conditioning (HVAC) systems; mechanical systems; and electrical systems;
- Workspace recovery - the adequacy of floor space, desk top computers, network connectivity, e-mail access, and telephone service; and
- Physical security facilities - the adequacy of physical perimeter security, physical access controls, protection services, and video monitoring.

Test Planning

Objective 2: Determine if test plans adequately complement testing strategies.

Scenarios - Test Content

1. Determine whether the test scenarios include a variety of threats and event types, a range of scenarios that reflect the full scope of the institution's testing strategy, an increase in the complexity and scope of the tests, and tests of wide-scale disruptions over time.

2. Determine whether the scenarios include detailed steps that demonstrate the viability of continuity plans, including:

- Deviation from established test scripts to include unplanned events, such as the loss of key individuals or services; and
- Tests of the ability to support peak transaction volumes from back-up facilities for extended periods.

3. Determine that test scenarios reflect key interdependencies. Consider the following:

- Whether plans include clients and counterparties that pose significant risks to the institution, and periodic connectivity tests are performed from their primary and contingency sites to the institution's primary and contingency sites;
- Whether plans test capacity and data integrity capabilities through the use of simulated transaction data; and
- Whether plans include testing or modeling of back-up telecommunications facilities and devices to ensure availability to key internal and external parties.

Plans: How the institution conducts Testing

1. Determine that the test plans and test scripts are documented and clearly reflect the testing strategy, that they encompass all critical business and supporting systems, and that they provide test participants with the information necessary to conduct tests of the institution's continuity plans, including:

- Participants' roles and responsibilities, defined decision makers, and rotation of test participants;
- Assigned command center and assembly locations;
- Test event dates and time stamps;
- Test scope and objectives, including RTOs, RPOs, recovery of the critical path,

duration of tests, and extent of testing (e.g. connectivity, interoperability, transaction, capacity);

- Sequential, step-by-step procedures for staff and external parties, including instructions regarding transaction data and references to manual work-around processes, as needed;
- Detailed information regarding the critical platforms, applications and business processes to be recovered;
- Detailed schedules to complete each test; and
- A summary of test results (e.g. based on goals and objectives, successes and failures, and deviations from test plans or test scripts) using quantifiable measurement criteria.