EM-31.6

Category: **Board & Management Operations**

Topic: **Business Continuity**

Published: 4/20/2016

Overview

Business continuity refers to the activities necessary to continue, resume, and recover an organization's business processes when operations are interrupted unexpectedly. A business interruption can be caused by a natural disaster, such as a fire or flood, or by a technical or human-based disruption, such as a power failure or robbery. An organization can avoid, or at least mitigate, the serious consequences of business interruptions by implementing and maintaining an effective business continuity program.

The focus of this examination topic and related procedures is on an enterprise-wide business continuity program. A sound program considers the business operations, personnel, technology, and resources that are critical for continuing the entire organization, not just the information technology (IT) department. As such, it is important for an institution's business continuity program to include risk assessment, planning, training, testing, and maintenance processes.

The board and management are responsible to identify, assess, prioritize, manage, and control risks as part of the business continuity process. The board should communicate its expectations on business continuity, and management should develop, maintain, and test the necessary plans and processes to ensure the organization can:

- Minimize disruptions of service to the institution and its customers,
- Ensure timely resumption of operations, and
- Limit financial loss.

A current and comprehensive continuity plan will aid management in selecting reasonable cost solutions in highly stressful disaster situations.

Examination Procedures and Guidance

General

1. Policy & Procedures:

Evaluate the adequacy of business continuity policies and procedures.

Guidance:

An institution's board and senior management are responsible for overseeing the business continuity process through effective policies and procedures which accomplish the following goals:

- Prepare the institution to deal with a business disruption.
- Mitigate the risk of unexpected business disruption.
- Respond to a disaster situation in a timely and effective manner.
- Recover business processes, resources, and services impacted by a business disruption.
- Assess and report on the institution's ability to meet business continuity objectives.

Evaluative questions and items to consider when examining business continuity policies and procedures include:

- ***Board Policy:*** **Has the board provided adequate guidance and established expectations for the business continuity process?** FCA Regulation 609.930(e) requires institution boards and management to adopt policy and procedures addressing business resumption. In the policy, the board should establish expectations for management to assess, prioritize, and control risks as part of the business continuity planning process. When defining expectations for management, the board's policy should identify the frequency of management reports on items such as the status and readiness of the business continuity plan, lessons learned from business continuity testing, and audit and examination results. The policy should also address the board's expectations for the development and review of the business continuity plan.

- ***Procedures:*** **Does the institution have adequate procedures or other documentation (e.g., a business continuity manual) that establishes and maintains the following:**

    - Business continuity steering committee that includes an executive sponsor and a program manager?
    - Business continuity risk assessment process?
    - Business Continuity Plan development, approval, and maintenance processes?
    - Business continuity training and awareness program?
    - Reporting expectations to board, employees, customers, and other interested parties?

Refer to the following documents from the Federal Financial Institutions Examination Council (FFIEC) and the National Institute of Standards and Technology (NIST) for additional guidance and information:

- FFIEC Business Continuity Planning Booklet - Board and Senior Management Responsibilities
- FFIEC Business Continuity Planning Booklet - Business Continuity Planning Process
- FFIEC Management Booklet - Section I.B.4: Business Continuity
- NIST Special Publication 800-34 Rev. 1 - Contingency Planning Guide for Federal Information Systems

2. Risk Assessment & Business Impact:

Review the institution's business continuity risk assessment to determine whether management appropriately identified potential threats, related consequences, and the resulting impact to the institution.

Guidance:

Before developing the business continuity plan (BCP), management should complete a risk assessment to identify potential threats and the impact of those threats on the institution. As part of the risk assessment, a business impact analysis (BIA) should be completed to identify and

prioritize the institution's business functions and processes and to gauge the potential impact of business disruptions on those functions and processes. The risk assessment should identify natural, technical, and human threats that may disrupt operations, determine the potential consequences or impact, and assess the likelihood of the threats. The risk assessment should also address the institution's dependency on major service providers and potential exposure to service disruption. Management should update the BIA and risk assessment as needed when internal or external changes occur.

Evaluative questions and items to consider when examining a BIA and business continuity risk assessment include:

***Business Impact Analysis*:**

- **Did management complete a BIA that includes an assessment of the criticality of each business unit and system?** The purpose of a BIA is to determine what impact a disruptive event would have on the institution. Typically, timely recovery of business functions and processes is critical to the institution's continuity of operations. The business continuity committee or project manager should review organizational charts, observe daily work flow, and interview department managers and employees to identify critical functions and significant interdependencies on an enterprise-wide basis. Information can also be gathered using surveys, questionnaires, and team meetings.

- **Did the BIA include recovery priorities for business units and systems?** As information is gathered and critical operations are identified, business operations and interdependencies should be reviewed to establish processing priorities between departments. The analysis should result in a prioritized list of the institution's business units and systems. This assessment may be in qualitative terms (such as low, medium, or high), or in monetary terms.

- **Did the BIA include recovery time frames and workaround procedures?** The BIA should also estimate the maximum allowable downtime for critical business functions and processes, and the acceptable levels of loss (data, operations, financial, reputation, and market share) associated with this estimated downtime. Frequently, alternate operating procedures are identified that can be used during a recovery. Workaround procedures allow business processes to continue through alternative methods if resources are unavailable. These often involve manual operations and tend to be temporary, less efficient, or more expensive than those that are normally used.

Risk Assessment:

- **Did management sufficiently consider potential internal and external threats?** Threat scenarios should consider the potential severity of the disaster, which is based upon the impact and the probability of business disruptions resulting from identified threats. The following list provides examples of various types of threats, but should not be considered all-inclusive:

    - Natural - earthquake, fire, snow/ice storm, flood, tornado, illness (pandemic)
    - Technical - power failure, network failure, server failure, water leaks
    - Human - hacker, vandalism, robbery, terrorism, disgruntled employee

- **For each threat identified, did management identify the consequences to the business if the threat were to materialize?** When assessing the probability of a disruption, institutions

should consider the geographic location of all facilities, their susceptibility to threats (e.g., location in a flood plain), and the proximity to critical infrastructures (e.g., power sources, nuclear power plants, airports, major highways, railroads, etc.). Worst-case scenarios, such as destruction of the facilities and loss of life, should be considered. For example, when assessing the consequences of an ice storm, management should identify that a power outage caused by an ice storm may lead to a shutdown of the institution's operating systems. Additionally, an ice storm could also impact staff if road conditions were unsafe and prevented staff from traveling to work.

- **Did management evaluate the impact and likelihood of the threats identified in the risk assessment?** The impact of the threat, rather than the source, should guide the development of business continuity programs. For example, a low impact may not warrant further review; however, every threat that poses a high adverse impact usually warrants further consideration, regardless of its probability of occurrence. Management should consider the impact of the threats to their facilities, people, and IT systems. Threats may range from those with a high probability of occurrence and a low impact to the institution, such as brief power interruptions, to those with a low probability of occurrence and a high impact to the institution, such as hurricanes or terrorist attacks. The most difficult threats to address are those that have a high impact on the institution, but a low probability of occurrence. Through good planning, however, the BCP may be more flexible and adaptable to all types of disruptions.

The following references contain further information on BIAs and business continuity risk assessments:

- FFIEC Business Continuity Planning Booklet - Business Impact Analysis
- FFIEC Business Continuity Planning Booklet - Appendix F: Business Impact Analysis Process
- FFIEC Business Continuity Planning Booklet - Risk Assessment
- FFIEC Business Continuity Planning Booklet - Appendix C: Internal and External Threats
- FFIEC Business Continuity Planning Booklet - Appendix J: Strengthening the Resilience of Outsourced Technology Services
- FCA Informational Memorandum on Threats to Information Management Systems (August 30, 1999)
- FCA Informational Memorandum on Guidance on Preparing Your Institution for a Catastrophic Event (June 22, 2006)
- NIST Special Publication 800-34 Rev. 1 - Contingency Planning Guide for Federal Information Systems

3. Business Continuity Plan:

Review the institution's business continuity plan (BCP) to verify that the plan contains the components necessary to continue, resume, and recover the institution's business processes when operations are interrupted unexpectedly.

Guidance:

A BCP is a comprehensive, written plan that contains an organized set of procedures and guidelines to recover and restore an organization's critical services and restore full business operations with minimum delay after a disaster or disruptive event. The BCP addresses the recovery capability for the organization's technology (which is often referred to as *disaster recovery*) and business units. All institutions should establish a BCP regardless of whether they process their work internally or

outsource their processing to a service provider. If an institution uses a service provider to process its daily transactions, management should ensure that it has incorporated applicable guidelines from the vendor's BCP into the institution's plan. ***If an institution activates the BCP, management must notify FCA's Office of the Chief Examiner at 1-888-244-3365.***

Evaluative questions and items to consider when examining an institution's business continuity plan include:

- ***BCP Components:*** **Does the BCP contain the information needed to guide business continuity activities?** The following is a list of recommended BCP components, but this is not the only way to structure a BCP. Plans can vary in form and content from one institution to another because of differing business needs. It is important for any plan to be both comprehensive and feasible. These plan components may be included in the enterprise-wide plan or the individual business unit plans.

    - **Objective and Scope –** State the purpose of the plan, and identify the operational and technical areas that it covers (locations, business units, off-site storage facilities, alternate recovery sites or work areas, etc.).

    - **Disaster Definition and Declaration –** Provide a clear and concise definition of a disaster, and identify who has the authority to declare a disaster and activate the plan.

    - **Assessments & Strategy –** Summarize the risk assessment and BIA report.

    - **Business Continuity Teams –** Include roles and responsibilities of each team and member. Identify dependencies between individuals or business units.

    - **Communication –** Establish predetermined guidelines to provide consistent, timely, and accurate information during the crisis. The plan should identify the authorized communication coordinator, define the communication authorization process, indicate who is to be contacted, specify what is communicated, and establish the frequency of communication. Include up-to-date contact information (call trees, contact lists, vendor lists, etc.). If this information is included in a separate document or plan, such as a *Crisis Communications Plan*, the BCP should reference it.

    - **Plan Implementation Processes –** Document the steps to take in a business disruption. The purpose of this plan is to bring the crisis under control. Establish predetermined procedures to carry out a managed, coordinated, effective, and immediate response to an emergency – protect life, environment, and organizational assets. If this information is included in a separate document or plan, such as an *Emergency Response Plan* or *Emergency Preparation Plan*, the BCP should reference it.

    - **Service Provider Information –** Document and incorporate all relevant service provider business continuity requirements and agreements.

    - **BCP Change Controls –** Establish a process to update the plan as changes occur (people, processes, or resources).

    - **Appendices –** Provide any supplemental information or references.

- ***Coverage of Business Units:*** **Does the BCP cover each department, business unit, branch office, and business function?** Institutions should conduct business continuity planning on an enterprise-wide basis. Planning should not be limited to restoring IT systems and services or data maintained in electronic form. Such actions, by themselves, cannot always put an institution back in business. Typically each department, business unit, or business function will complete a plan to address its recovery needs and processes. These plans are part of the institution's enterprise-wide BCP and should be accessible to staff in either hard copy or electronic form.

- ***BCP Maintenance:*** **Are processes for maintaining the BCP sufficient?** As part of the maintenance process, the BCP should be reviewed by management, the program manager, team members, and the board at least annually. The team or coordinator should contact business unit managers at least annually to assess the nature and scope of any changes to the institution's business, structure, systems, software, hardware, personnel, or facilities. The board and management should also ensure that business continuity maintenance processes are built into the organization's change management process (e.g., system development, building maintenance programs, corporate planning, etc.). Change, both internal and external, is a common occurrence for organizations and can potentially invalidate the BCP unless the plan is properly adjusted and modified to reflect these changes. Internal change can involve processes, people, and resources, while external change can involve business partners, vendors, alternate recovery facilities, and off-site storage facilities. If significant changes have occurred, or if audit findings warrant changes to the BCP or test program, management should update the BCP and related processes accordingly.

The following references contain further guidance and information on BCPs:

- FCA Informational Memorandum on Guidance on Preparing Your Institution for a Catastrophic Event (June 22, 2006)
- FFIEC Business Continuity Planning Booklet - Appendix G: Business Continuity Plan Components
- FFIEC Business Continuity Planning Booklet - Appendix D: Pandemic Planning
- FFIEC Business Continuity Planning Booklet - Appendix J: Strengthening the Resilience of Outsourced Technology Services
- FFIEC Business Continuity Planning Booklet - Board and Senior Management Responsibilities
- FFIEC Outsourcing Technology Services Booklet - Related Topics: Business Continuity Planning
- NIST Special Publication 800-34 Rev. 1 - Contingency Planning Guide for Federal Information Systems

4. Disaster Recovery Plan:

Review the institution's disaster recovery plan to determine if the institution is prepared to restore IT systems to support the institution's recovery goals.

Guidance:

The disaster recovery plan (DRP) focuses on the recovery of IT systems and resources in the event that they are disrupted. The DRP is part of the BCP, but is focused on the recovery of the *technology,* as opposed to the recovery of the institution's business operations. Technology service providers (TSPs) and institutions that provide part, or all, of their own technology infrastructure

often maintain a separate DRP to address IT systems recovery as part of enterprise-wide business continuity planning. Some of these institutions might include DRP items in the enterprise-wide business continuity plan, which is acceptable if these items are sufficiently covered. The following guidance is directed to examinations of those institutions. If an institution does not provide its own technology services (typically, the smaller ACAs), it would not be expected to have a DRP. In those situations, this procedure is not applicable.

Evaluative questions and items to consider when examining a DRP include:

- ***Systems Recovery Priority:*** **Based on the list of critical systems developed in the BIA, has IT management prioritized a list of systems and applications to restore, with procedures developed for the restoration process?** Management should ensure that the results of the BIA and risk assessment are used when developing procedures to recover systems and applications. In developing the DRP, institutions should exercise caution when identifying non-critical systems and applications. For example, an institution's electronic mail system may not appear to be mission critical, but it may be the only system available for employee or external communication in the event of a disruption.

- ***Recovery Area:*** **Has management identified recovery site options?** The institution should make formal arrangements for alternate processing capability in the event its data processing site becomes inoperable or inaccessible. Careful consideration of the distance between the recovery site and the primary site is necessary. Management should ensure the recovery site is unlikely to be affected by the same disaster, has the ability to provide sufficient processing time for the institution's anticipated workload, and will be available for recovery efforts until the institution has fully recovered from the disaster and resumes operations at its own facilities. In addition, management should ensure appropriate technical support is available during recovery and should consider the time needed to travel to the recovery site. Recovery facility options typically include:

    - Using an existing facility at another location
    - Establishing reciprocal arrangements with other organizations
    - Maintaining a company-owned hot, warm, or cold site
    - Contracting a commercial hot, warm, or cold site

- ***DRP Components:*** **Does the DRP sufficiently address the key technology components that could be impacted by a disaster?** An effective DRP would address the following items:

    - Hardware – mainframe, mid-range, servers, network, end user
    - Software – applications, operating systems, utilities
    - Communications (network and telecommunications)
    - Power Supply – backup generators (including sufficient fuel) or uninterruptible power source (UPS) devices
    - Data files and vital records
    - Operations processing equipment
    - Office equipment

- ***IT Recovery Teams:*** **Have IT technical recovery teams been established?** Technical recovery teams are needed to focus on the recovery of specific technical areas (operating systems, networking and communications, database systems, etc.). Members of a team should be chosen based on their knowledge of, and experience in, the activities and procedures assigned to the team. Ideally, teams are staffed with the personnel who

perform similar tasks under normal operations.

- ***Backup and Storage Strategies:*** **Does the institution have appropriate backup and storage strategies to ensure data is available for recovery purposes after a disruption?** Management should base software and data file backup decisions on the criticality of the software and data files to the institution's operations. Various options for data backups exist, including:

    - **Electronic vaulting –** electronically transferring copies of data to an off-site backup location periodically.

    - **Backup tape storage –** making tapes and physically taking them to an off-site backup location periodically. (Note: If an institution uses this type of media for its primary backup storage, management should ensure that backup tapes are sent to the off-site storage facility as soon as possible, do not reside at the originating location overnight, are not returned to the originating location until replaced with the current day's backup tapes, and are properly secured to prevent damage or unauthorized access.)

    - **Storage Area Network (SAN) –** a dedicated network for connected storage systems.

    - **Disk Mirroring –** a technique that allows a system to automatically maintain multiple copies of data so in the event of a disk hardware failure, the system can continue to process or recover data quickly.

- ***Off-site Storage Facilities:*** **Does the off-site storage location for data and vital records have appropriate controls?** The off-site storage location should be environmentally controlled, fire resistant, and secure. The off-site premises should be an adequate distance from the computer operations location to ensure that both locations will not be affected by the same disruptive event. As part of the data and vital records stored at the off-site location, management should include a copy of the BCP and documentation supporting the current network environment. Institutions should not allow employees to store backup data files at their residences due to potential security concerns.

See the following references for further guidance and information:

- FFIEC Business Continuity Planning Booklet - Appendix G: Business Continuity Plan Components
- FFIEC Business Continuity Planning Booklet - Appendix E: Interdependencies
- FFIEC Business Continuity Planning Booklet - Appendix J: Strengthening the Resilience of Outsourced Technology Services
- NIST Special Publication 800-34 Rev. 1 - Contingency Planning Guide for Federal Information Systems

5. Staff Training Program:

Determine if the institution provides adequate staff training to address a business disruption or disaster event.

Guidance:

Management should provide business continuity training for all personnel at least annually to ensure everyone is aware of their responsibilities if a business disruption or disaster occurs. The training

program should incorporate enterprise-wide training as well as specific training for individual business units. A valid and up-to-date business continuity plan (BCP) is of little value if the employees responsible for its improvement and execution do not have adequate training and awareness. Management should document the training plan and activities, ensure issues are resolved, and expand training where needed.

Evaluative questions and items to consider when examining business continuity training programs include:

- **Did management provide regular (at least annual) training for all staff?** It is important to provide training programs and materials to all staff. During a disaster or emergency, a well-trained staff will more likely remain calm, realize the potential threats that may affect the institution, and be able to safely implement required procedures without endangering their lives or the lives of others.

- **Does the training plan address cross-training of employees?** Cross-training of personnel and succession planning is an important element of business continuity training. Management should cross-train employees throughout the organization and assign backup personnel for key operational positions to ensure that vital functions are performed if key personnel are unavailable at the time of a disruption or during the recovery stage.

- **Did management involve a variety of business unit staff in the testing of the BCP?** Employee participation in testing can offer important training opportunities and can also increase individual awareness, buy-in, and ownership to achieve successful BCP implementation. An effective training program should ensure that non-IT staff and managers are involved in the testing.

- **Does management monitor and evaluate training progress, and reassess training needs?** A comprehensive training program should be periodically reevaluated and kept up-to-date to ensure everyone understands their current role in the overall recovery process.

The following references contain additional information on business continuity training programs:

- FFIEC Business Continuity Planning Booklet - Other Policies, Standards, and Processes: Employee Training
- FFIEC Business Continuity Planning Booklet - Appendix G: Business Continuity Plan Components
- FFIEC Business Continuity Planning Booklet - Board and Senior Management Responsibilities
- FCA Informational Memorandum on Guidance on Preparing Your Institution for a Catastrophic Event (June 22, 2006)
- NIST Special Publication 800-34 Rev. 1 - Contingency Planning Guide for Federal Information Systems

6. Testing Program:

Evaluate the adequacy of the institution's annual Business Continuity Plan (BCP) testing process.

Guidance:

Testing validates the effectiveness of a BCP by determining how well the plan works or which portions of the plan need improvement. The objective of testing is to ensure the BCP remains accurate, relevant, and operable under adverse conditions. Testing should be completed at least

annually and after significant changes to technology systems, business operations, facilities, or organizational structure.

Evaluative questions and items to consider when examining BCP testing processes include:

- ***Testing Methodologies:*** **Has the institution used sufficient testing methodologies to evaluate the effectiveness of the BCP?** Testing should validate the institution's plan to continue and recover business operations on an enterprise-wide basis. Tests are most effective when they simulate realistic disasters and include some improvisation to meet unexpected events. Institutions should consider different methodologies to accomplish these tests, such as:

    - Desk reviews
    - Simulations
    - Technical recovery of systems
    - Call tree tests
    - Alternate site business tests
    - Building emergency and evacuation drills
    - Crisis management team activities
    - Comprehensive tests of all critical functional areas

- ***Testing Scope & Staff Involvement:*** **Does testing evaluate the effectiveness of the enterprise-wide BCP, and not just the technology recovery plan(s) (e.g., the DRP)? Is the appropriate staff involved in the testing process?** While testing should include reestablishing technology systems, it should not be limited to those activities or involve only IT personnel. Tests also serve to evaluate and train staff in emergency, backup, and recovery procedures. Therefore, business continuity tests should use the maximum number of personnel that will be involved in implementing the BCP. Independent staff, such as auditors, should be involved to help ensure the validity of the testing process and the accuracy of the reporting.

- ***Test Documentation*****: Did management appropriately summarize and document the BCP test results?** After the tests are executed, management should properly document test results, which would typically include:

    - Test dates and locations
    - An executive summary detailing a comparison between the test objectives and test results
    - Material deviations from the test plans, including whether intended participation levels were achieved
    - Problems identified during testing
    - An evaluation by a qualified independent party

- ***Test Results*****: Did management analyze and report the results of the BCP test to the board and senior management?** After tests have been executed and documented, management should evaluate test results to ensure that test objectives are achieved and that business continuity successes, failures, and lessons learned are thoroughly analyzed. The business continuity executive sponsor or program manager should assess the institution's ability to meet its business continuity objectives and testing program requirements, and report the following to the board and senior management:

- Test results
- Gaps between the BCP and the actual test results
- The resolution of any problems
- The need for additional testing or training

- ***Coordination with a TSP:*** **If the institution contracts with a TSP for technology services, does management evaluate the TSP's BCP test results?** When an institution relies on a TSP for technology services, management should review the TSP's BCP, test results, and related audits to determine the adequacy of the TSP's plans and the effectiveness of its testing processes. In addition, management should ensure that critical institution services can be restored (either by the institution or the TSP) within acceptable time frames as established by the institution. (Note: A TSP could be a district bank.)

The following references contain additional information on business continuity testing programs:

- FFIEC Business Continuity Planning Booklet - Risk Monitoring and Testing: Principles of the Business Continuity Testing Program
- FFIEC Business Continuity Planning Booklet - Appendix H: Testing Program – Governance and Attributes
- FFIEC Business Continuity Planning Booklet - Appendix J: Strengthening the Resilience of Outsourced Technology Services
- FFIEC Supervision of Technology Service Providers (TSP) Booklet - Introduction
- FCA Informational Memorandum on Guidance on Preparing Your Institution for a Catastrophic Event (June 22, 2006)
- NIST Special Publication 800-34 Rev. 1 - Contingency Planning Guide for Federal Information Systems

7. Audit:

Determine if the institution conducts an effective audit (scope, reporting, and followup) of the business continuity program.

Guidance:

The internal audit and review program is a key mechanism for ensuring business continuity processes are functioning effectively and in compliance with regulations and policies. The internal auditor or other qualified, independent party should review the adequacy of business continuity processes to ensure compliance with applicable criteria. The business continuity plan and testing results, in particular, should be subject to periodic independent audit. The audit risk assessment and scope should address business continuity topics, and audit frequency should be commensurate with the complexity of the institution's operations and risk profile. A reliable audit program provides the board reasonable assurance that business continuity processes are sound and that related reporting is complete and accurate.

Evaluative questions and items to consider when examining the audit and review function regarding business continuity processes include:

- ***Audit Coverage:*** **Is there periodic audit or review coverage of business continuity processes?** Audit or review coverage and frequency should be appropriate relative to risks, changes in the operating environment, regulatory requirements, and periodic testing needs. Coverage should also be consistent with the institution's risk assessment results and annual

audit plan.

- ***Scope and Depth:*** **Are audit or review scope and depth sufficient to conclude on the adequacy, completeness, and timeliness of business continuity processes?** The scope should cover key processes and controls within the area being audited or reviewed. The depth of work should be sufficient to determine if internal controls are functioning as intended and regulatory requirements are met. The scope and depth of coverage should be consistent with the approved audit or review plan and engagement contract (if applicable). If audit or review work deviated materially from the original planned scope, the board (or Audit Committee, if so delegated) should be notified of the reasons for the change. Specific items that should be considered in the audit or review scope include:

    - Management's risk assessment and business impact analysis.
    - The enterprise-wide business continuity plan.
    - Individual department plans, including the IT department's Disaster Recovery Plan.
    - Business continuity training programs.
    - Testing plans, scenarios, and schedules.
    - Communication of plans, test results, and recommendations to the board.
    - Fraud-related threats and vulnerabilities, as well as anti-fraud controls.

- ***Reliability of Results:*** **Did FCA identify any concerns with audit and review reliability?** Evaluate the reliability of internal audit or review work by comparing the results to FCA's examination results in this area. This comparison often includes FCA testing of transactions that were covered in the internal audit or review (transactions are often loans or loan applications, but may include other types of transactional activity, as well). In addition to the audit or review report, examiners should request and review the workpapers and hold discussions with the auditor to obtain a more thorough understanding of work completed. Often, auditors and reviewers will complete line sheets, flowcharts, control matrices, standard work programs, workpaper forms, or other relevant documents when conducting work. Workpapers should adequately document the work performed and support the final report. In addition, any proforma work programs, workpapers, or other tools should be accurate and sufficiently thorough. If there are material weaknesses identified by examiners that are not identified by internal audits or reviews, examiners should assess the underlying reasons.

- ***Reports:*** **Do internal audit reports sufficiently communicate business continuity review results and recommendations, if applicable?** Examiners should consider the following when evaluating the audit or review report:

    - Is the report prepared in accordance with the institution's guidelines?

    - Is an executive summary or overview included to provide the board with a general conclusion on audit or review results?

    - Is the report accurate, concise, supported, and timely in communicating the audit or review objectives, scope, results, conclusions, and recommendations?

    - Are conclusions and recommendations realistic and reasonable given the institution's size and complexity, with material and higher risk issues clearly identified and prioritized?

- Are conclusions and recommendations supported by convincing evidence and persuasive arguments (condition, criteria, cause, and effect)?
- Does the report conclude whether the institution adheres to policies, procedures, and applicable laws or regulations, and whether operating processes and internal controls are effective?
- Does the report address potential vulnerabilities to fraud, if applicable?

- ***Corrective Action:*** **Are management responses to audit findings in this area reasonable, complete, and timely? Have corrective actions been effective?** Audits and reviews are only effective if corrective action is taken to remedy the weaknesses identified. As such, there should be a reasonable, complete, and timely management response to the audit or review report. In some cases, management commitments and agreements or any areas of disagreement are documented in the report or in a separate memo or tracking system. If corrective actions are not resolving the issues or concerns (based on repetitive audit findings, FCA findings, etc.), examiners should further investigate the reasons. For example, this could indicate the audit or review did not sufficiently identify the underlying causes or materiality of weaknesses, sufficient resources are not being directed toward corrective actions, or weaknesses exist in the institution's corrective action process, including board oversight of the process.

Refer to the FFIEC Business Continuity Planning Booklet - Board and Senior Management Responsibilities for additional information on business continuity auditing.