EM-31.6

Category: Board & Management Operations
Topic: Business Continuity
Published: 11/18/2020

Overview

The *Business Continuity* topic provides guidance on evaluating a Farm Credit System (System) institution's enterprise-wide business continuity program. Business continuity refers to the activities necessary to continue, resume, and recover an institution's business processes when operations are interrupted. 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. In addition, pandemics and other similar health events present unique operational challenges that could impact an institution's delivery of financial services. An institution can avoid, or at least mitigate, the serious consequences of business interruptions by implementing and maintaining an effective business continuity management program. The Federal Financial Institutions Examination Council (FFIEC) defines business continuity management as the process to oversee and implement resilience, continuity, and response capabilities to safeguard employees, customers, and products and services.

A sound program considers the business operations, personnel, technology, and resources that are critical to the continuity and resilience of the entire institution, not just the information technology (IT) department. As such, it is important for the 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 program. The board should communicate its expectations on business continuity and the resilience of operations. Management should develop, maintain, and test the necessary plans and processes to ensure the institution can:

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

The Farm Credit Administration's (FCA) procedures and processes for examining business continuity are based on guidance published by the FFIEC. It maintains an IT Examination Handbook InfoBase (IT Handbook) that is made up of a series of booklets covering IT subject areas, including business continuity management. FFIEC revises the individual booklets periodically to reflect changes in federal regulatory and industry guidance. FCA's guidance below includes references and links to the Business Continuity Management booklet and other FFIEC IT booklets, as applicable.

Examination Procedures and Guidance

General

1. Policy & Procedures:

Evaluate the adequacy of business continuity policies and procedures.

Guidance:

The board and senior management are responsible for overseeing the business continuity program through effective policies and procedures that accomplish the following goals:

- Align business continuity management practices with the institution's risk appetite and strategic goals and objectives.
- Mitigate the risk of an unexpected business disruption occurring.
- Prepare for a business disruption.
- Respond to a disruptive event in a timely and effective manner.
- Recover, restore, and resume business processes, resources, and services impacted by a business disruption.
- Assess and report on the ability to meet business continuity objectives.

Refer to the FFIEC Business Continuity Management booklet for additional background and examination guidance on business continuity management governance, board and senior management responsibilities, and board reporting. In addition, the FFIEC Management booklet provides general information about governance and risk management, plus specific business continuity-related guidance about IT responsibilities and functions and risk mitigation.

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

- ***Board Policy:*** **Does the board provide adequate guidance and establish expectations for the business continuity program?** FCA Regulation 609.930(e) requires boards and management to adopt policy and procedures addressing business resumption. The policy should address the board's expectations for developing, reviewing, and maintaining the business continuity plan and program. An effective board policy should assign responsibility and accountability for business continuity management and establish expectations for management to assess, prioritize, and control risks to align with the institution's business strategy and risk appetite. 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, completion of training, the results of exercises and tests, and actions to address audit and examination findings. As part of addressing the institution's overall operations, the policy should also specifically address continuity of board operations (e.g., board meetings and board approvals).

- ***Procedures:*** **Does management have adequate procedures to establish and maintain effective business continuity management?** In accordance with FCA Regulation 609.930(e), management must establish procedures to implement the board's business continuity policies. Refer to the FFIEC Management booklet for additional examination guidance on senior management's role in the risk management of the business continuity program.

Refer to the National Institute of Standards and Technology's Special Publication 800-34 Rev. 1 - Contingency Planning Guide for Federal Information Systems for additional information and guidance.

2. Business Impact Analysis & Risk Assessment:

Evaluate the business impact analysis and risk assessment elements of the business continuity program 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 develop a business impact analysis (BIA) to identify and prioritize business functions and processes and to gauge the potential impact of business disruptions on those functions and processes. It is important to consider all business functions and processes, not just those directly dependent on IT systems. Next, management should complete a risk assessment to identify potential threats and events that could result in a business disruption, assess the likelihood of occurrence, and determine the impact on the institution. The types of threats or events could involve natural, technical, and human sources. This includes the unique risks and challenges associated with pandemics. Refer to the FFIEC Business Continuity Management booklet for additional information and examination guidance on risk management, which encompasses business impact analysis and risk assessment. Refer to the FFIEC Statement on Pandemic Planning (March 6, 2020) for examination guidance about incorporating pandemic risk into the BIA and business continuity risk assessment.

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

***Business Impact Analysis*:**

- **Does management appropriately complete a BIA that identifies all critical business functions and processes, including those that are not directly dependent on IT systems?** The BIA should identify the critical business functions and processes, the interdependencies across business units, and the recovery priorities and objectives. Typically, timely recovery of business functions and processes is critical to continuity and resilience of operations. Management should review organizational charts, observe daily workflows, 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. Refer to the FFIEC Business Continuity Management booklet for additional information and examination guidance on the identification of critical business functions.

- **Does the BIA include reasonable recovery priorities for business units and systems?** As management gathers information and identifies critical operations, they should review business operations and interdependencies to establish processing priorities between departments. The analysis should result in a prioritized list of business units and systems. This assessment may be expressed in qualitative terms (such as low, medium, or high) or in monetary terms. Refer to the FFIEC Business Continuity Management booklet for additional information and examination guidance on interdependency analysis.

- **Does the BIA include reasonable recovery objectives and workaround procedures?** The BIA should establish recovery objectives that align with the disruption's impact and the risk management strategy. Recovery objectives are necessary to limit the consequences of disruptive events and to ensure the timely resumption of critical operations and processes. Workaround procedures allow business processes to continue through alternative methods if resources are unavailable. Refer to the FFIEC Business Continuity Management booklet for additional information and examination guidance on the impact of disruption, including an illustration of the following common measurements for recovery objectives:

    - *Recovery point objective (RPO)* – The point in time, prior to a disruption or system outage, to which mission or business process data can be recovered (given the most recent backup copy of the data) after an outage. RPO is a factor of how much data loss the mission or business process can tolerate during the recovery process.

    - *Recovery time objective (RTO)* – The length of time required to recover disrupted systems and resources before negatively impacting the institution's mission or business processes; the length of time between the disruption and the resumption of normal operations.

    - *Maximum tolerable downtime (MTD)* – The amount of time the business process can be disrupted without causing significant harm or irreversible consequences to operations, finances, and reputation; the total amount of time the system owner or authorizing official is willing to accept for business process disruption, including all impact considerations. The RTO makes up the first segment of the MTD. The second segment is the time needed to get critical business functions up and running after the systems are restored.

Risk Assessment:

- **Does management sufficiently consider potential internal and external threats?** Threat scenarios should consider the event's potential severity, which is based upon the impact and the likelihood of business disruptions resulting from identified threats. Refer to the FFIEC Business Continuity Management booklet for additional information and examination guidance on risk assessment. The following list provides examples of internal and external threats, but it should not be considered all-inclusive:

    - *Natural* – earthquake, fire, snow or ice storm, flood, tornado, illness (pandemic)
    - *Technical* – power failure, network failure, server failure, water leaks
    - *Human* – fraud, cyber-attack, vandalism, theft, terrorism, disgruntled employee

- **For each threat identified, does management appropriately identify the consequences if the threat were to materialize?** When assessing the likelihood of a disruption, management should consider the geographic location of all institution facilities, their susceptibility to threats (e.g., location in a flood plain, earthquake zone, or tornado region), and the proximity to critical infrastructures (e.g., power sources, nuclear power plants, airports, major highways, railroads). Management should also consider worst-case scenarios, such as destruction of the facilities and loss of life. For example, when assessing the consequences of an ice storm, management should identify that a power outage caused by the storm may shut down 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. Refer to the

FFIEC Business Continuity Management booklet for additional information and examination guidance on risk identification.

- **Does management appropriately 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 threat may not warrant further review; however, every threat that poses a high adverse impact usually warrants further consideration, regardless of its likelihood (probability) of occurrence. Management should consider the impact of the threats to the institution's facilities, people, and IT systems. Threats may range from those with a high probability of occurrence and a low impact, such as brief power interruptions, to those with a low probability of occurrence and a high impact, such as pandemics, 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. Using good risk management and planning, however, management can develop business continuity strategies that are flexible and adaptable to all types of disruptions. Refer to the FFIEC Business Continuity Management booklet for additional information and examination guidance on assessing the likelihood and impact of disruptive events.

- **Does the risk assessment adequately address the institution's dependency on third-party service providers and their potential exposure to service disruption?** If the institution depends on third-party service providers to perform or support critical business functions and processes, this interconnection could increase the severity of potential threats. Management should consider the risks and threats that could affect third-party service providers and other entities interconnected to those providers. An incident or critical failure that affects the third-party service provider could adversely impact the institution's operations. Refer to the FFIEC Business Continuity Management booklet for additional information and examination guidance related to this aspect of risk identification.

Management should update the BIA and risk assessment as needed when internal or external changes occur. Refer to the following for additional information and guidance on BIAs and business continuity risk assessments:

- FCA Informational Memorandum on Guidance on Preparing Your Institution for a Catastrophic Event (June 22, 2006)
- FCA Informational Memorandum on Threats to Information Management Systems (August 30, 1999)
- NIST Special Publication 800-184 – Guide for Cybersecurity Event Recovery
- NIST Special Publication 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems
- NIST Special Publication 800-30 Rev. 1 – Guide for Conducting Risk Assessments

3. Business Continuity Plan:

Examine the business continuity plan (BCP) to determine if it contains the components necessary to continue, resume, and recover the institution's business processes when operations are interrupted.

Guidance:

A BCP is a comprehensive, written plan that contains an organized set of procedures and guidelines to recover, restore, and continue critical services and business operations during and after a disruptive event. It includes specific elements that address incident response, disaster recovery, and crisis management, and should specifically address how internal controls will be maintained during an event. The BCP format could vary, but it should be commensurate with the institution's business model, risk profile, and complexity. Some institutions may have a single BCP that includes all the elements, while others may incorporate subsidiary plans to address different business functions, locations, or departments. 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. Refer to the FFIEC Business Continuity Management booklet for additional information and examination guidance on business continuity plans and strategies.

As noted in FCA's Informational Memorandum on Reporting Security Incidents and Business Continuity Events to FCA dated June 27, 2017, if an institution activates the BCP, management should notify FCA's Office of the Chief Examiner at 1-888-244-3365. Within 24 hours of BCP activation, the institution should also provide FCA with a written summary of the actions it has taken and submit the summary through the centralized email address COOPReport@fca.gov.

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

- ***BCP Components:*** **Does the BCP contain the information needed to guide business continuity activities?** It is important for the BCP to be both comprehensive and feasible. The plan should address the authorities, responsibilities, procedures, and relocation strategies for continuing operations and maintaining internal controls during a disruption. Plans may vary in form and content at each institution due to differing business needs. Plan components may be included in the enterprise-wide plan or the individual business unit plans. As noted in the FFIEC Statement on Pandemic Planning (March 6, 2020), the BCP should also address the threat of a pandemic outbreak and its potential impact on the delivery of critical financial services. This pandemic segment should be sufficiently flexible to address a wide range of possible effects that could result from such a threat. Refer to the FFIEC Business Continuity Management booklet for additional information and examination guidance. Please note this is not the only way to structure a BCP. The following are recommended BCP components:

    - *Event Management* – Establish procedures to identify plausible event types and include the corresponding thresholds and responses. An *event* is defined as an occurrence or change in circumstances that may affect operations. Its origin may be physical, cyber, or a combination of both. Procedures should describe how to report an event to management and the situations that warrant notification to those who address events.

    - *Continuity and Recovery* – Establish protocols for operations continuity and system recovery. Refer to the *Operations* procedure in the *Information Technology & Security* Examination Manual topic and the FFIEC Operations booklet for additional information and examination guidance.

    - *Facilities and Infrastructure* – Identify alternatives for core operations, facilities, infrastructure systems, suppliers, utilities, interdependent business partners, and key personnel. Refer to the FFIEC Business Continuity Management booklet for

additional information and examination guidance on data center recovery alternatives and branch relocation.

- *Incident Response* – Align incident response procedures with other related processes (e.g., cybersecurity, network operations, physical security, and internal controls) and outsourced services. Verify that the procedures and related controls are considered during planning and BCP development. Refer to the *Security* procedure in the *Information Technology & Security* Examination Manual topic and the FFIEC Information Security booklet for additional information and examination guidance about evaluating incident response.

- *Disaster Recovery* – Identify key business processes and activities to be maintained while IT systems and applications are unavailable. Prioritize the order in which these systems are restored and reflect this information in the BIA.

- *Crisis or Emergency Management* – Establish protocols and procedures to identify a crisis event, activate the BCP, and manage emergencies. This involves predefined leadership and communication protocols and should consider the impact of business continuity decisions on the institution's system of internal controls. Examiners should ensure the board and management clearly define events that constitute partial or full BCP activation. If offices are shut down to public access and most essential and non-essential employees are working remotely, as in the case of a pandemic, management should activate the BCP given the unique impact a pandemic can have on employees, customers, and business partners. Protocols and procedures should also address decision-making responsibilities for unforeseen events or event outcomes that require deviation from established plans. As noted in FCA's Informational Memorandum on Reporting Security Incidents and Business Continuity Events to FCA dated June 27, 2017, BCPs should include directions to notify FCA's Office of the Chief Examiner at 1-888-244-3365 if the plan is activated. BCPs should also include directions to provide FCA with a written summary of actions taken and to complete the submission through the centralized email address COOPReport@fca.gov within 24 hours of BCP activation.

- *Payment Systems* – Identify alternate arrangements or solutions if payment systems fail (e.g., funds transfers, wire and automated clearing house transactions, electronic banking, automated teller machines, mobile capabilities). Although System institutions, due to their non-depository nature, may not have much risk exposure to some payment systems, a regional disruption could impact their customers.

- *Liquidity Considerations* – Identify processes to address potential cash and liquidity needs during adverse events.

- ***Business Unit Coverage:*** **Does the BCP sufficiently cover each department, business unit, branch office, and business function?** The board and management 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 continue or restore normal business operations. Typically, each department, business unit, or business function will complete a plan to address its resilience and recovery needs, processes, and controls. These plans are part of the enterprise-wide BCP and should be accessible to staff in either hard copy or electronic form.

- ***Third-Party Service Providers:*** **Does the BCP adequately address the institution's dependency on third-party service providers for any critical services or operations?** If an institution uses a third-party service provider for any critical services or operations, management should consider the service provider's business continuity program in the institution's BCP and incorporate the specific responsibilities of all parties. Management should also verify the service provider's resilience capabilities, which involve its ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents. Refer to the FFIEC Business Continuity Management booklet for additional information and examination guidance on third-party service providers. In addition, the FFIEC Outsourcing Technology Services booklet provides business continuity planning guidance related more specifically to technology service providers.

- ***BCP Maintenance:*** **Are processes for maintaining the BCP sufficient?** As part of the maintenance process, management, the program manager, team members, and the board should review the BCP at least annually. The business continuity 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 business continuity maintenance processes are built into the change management process (e.g., systems development, building maintenance programs, strategic planning). Change, both internal and external, is a common occurrence and can potentially invalidate the BCP unless the plan is properly adjusted and modified to reflect these changes. Internal change can involve processes, people, or resources, while external change can involve legal or regulatory requirements, third-party service providers and vendors, or alternate recovery 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. Refer to the FFIEC Business Continuity Management booklet for additional information and examination guidance about maintenance and improvement.

Refer to the following for additional information and guidance:

- FCA Informational Memorandum on Guidance on Preparing Your Institution for a Catastrophic Event (June 22, 2006)

- FCA Informational Memorandum on Threats to Information Management Systems (August 30, 1999)

- NIST Special Publication 800-184 – Guide for Cybersecurity Event Recovery

- NIST Special Publication 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems

4. Disaster Recovery Plan:

Evaluate the disaster recovery plan to determine if it supports the institution's recovery goals and provides the necessary guidance to restore IT infrastructure, data, and systems.

Guidance:

Disaster recovery is a subset of business continuity. The disaster recovery plan (DRP) focuses on the recovery of IT systems and resources if 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 *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, it might not have a separate DRP. In that situation, the extent of disaster recovery planning should be commensurate with the institution's business model, risk profile, and complexity. Refer to the FFIEC Business Continuity Management booklet for additional information and examination guidance about disaster recovery.

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 adequately prioritized a list of systems and applications to restore, and did they sufficiently document procedures necessary for the restoration process?** Management should use the BIA and risk assessment results when developing procedures to recover systems and applications. In developing the DRP, management should exercise caution when identifying non-critical systems and applications. For example, the electronic mail system may not appear to be mission critical, but it may be the only system available for employee or external communication during a disruption.

- ***Recovery Area:*** **Has management identified sufficient recovery site options?** Management should have a comprehensive, written agreement or contract for alternate processing capability in the event its data processing site becomes inoperable or inaccessible. Management should carefully consider the distance and travel time between the recovery site and the primary site. 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 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. Refer to the FFIEC Business Continuity Management booklet for additional information and examination guidance about data center recovery alternatives. 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:

    - Data center(s) and related facilities.
    - Hardware – servers, networks, storage, 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:*** **Has management established sufficient IT technical recovery teams?** Management should establish technical recovery teams to focus on the recovery of specific technical areas (operating systems, networking and communications, database systems, etc.). Team members should have appropriate knowledge of, and experience in, the activities and procedures assigned to the team. Ideally, management should staff the teams 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?** Data backup and re-creation are important components in the recovery of critical business functions after a disruption. Management should ensure backups are readily available and adhere to the institution's information security policy. Management should also maintain a comprehensive backup of critical software and configuration settings. Refer to the FFIEC Business Continuity Management booklet for additional information and examination guidance about data backup and replication.

- ***Offsite Storage Facilities:*** **Does the offsite storage location for data and vital records have appropriate controls?** The offsite storage location should be environmentally controlled, fire resistant, and secure. The offsite 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. Management should include a copy of the BCP and documentation supporting the current network environment in the data and vital records stored at the offsite location. Management should not allow employees to store backup data files at their residences due to potential security concerns. Cloud storage is another option for offsite storage. Like physical storage facilities, management should ensure the cloud storage service provider has appropriate security controls.

Refer to the following for additional information and guidance:

- FCA Informational Memorandum on Guidance on Preparing Your Institution for a Catastrophic Event (June 22, 2006)

- FCA Informational Memorandum on Threats to Information Management Systems (August 30, 1999)

- NIST Special Publication 800-184 – Guide for Cybersecurity Event Recovery

- NIST Special Publication 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems

- FFIEC Statement on Pandemic Planning (March 6, 2020)

5. Training Program:

Determine if the institution provides adequate training for all personnel (board, management, and staff) to address a business disruption or disaster event.

Guidance:

Management should provide business continuity training for all personnel on a regular basis, and at least annually. The training should ensure everyone is aware of, and prepared to perform, their primary and backup responsibilities if a business disruption or disaster occurs. The training program

should align with business continuity goals and strategies. It 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 people responsible for its execution and maintenance do not have adequate training and awareness. Management should document the training plan and activities, ensure issues are resolved, and expand training where needed. Refer to the FFIEC Business Continuity Management booklet for additional information and examination guidance about training.

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

- ***Training Frequency and Participation:*** **Does management appropriately provide regular training for all personnel, which includes the board, management, and staff?** It is important to provide training programs and materials to all personnel on a regular basis (at least annual) and more frequently when significant changes impact organizational processes, risks, or personnel. It is equally important to tailor the training to the target audience and address each group's specific needs, roles, and responsibilities. During a disruption or emergency, well-trained personnel will more likely remain calm, realize the potential threats, adapt to changing conditions, and safely implement required procedures without endangering their lives or the lives of others.

- ***Cross-Training:*** **Does the training plan adequately address employee cross-training?** Cross-training of personnel is an important element of business continuity training. Management should cross-train employees throughout the institution and assign backup personnel for key operational positions. This practice will help ensure vital functions continue to be performed if key personnel are unavailable at the time of a disruption or during the recovery stage.

- ***Program Maintenance and Improvement:*** **Does management adequately monitor and evaluate training progress and reassess training needs?** Management should have an established process for reviewing and updating the business continuity training program. An effective training program should be comprehensive and periodically reevaluated and updated to ensure everyone understands their primary and backup roles in the operational resilience process. Management should incorporate changes in organizational structure, technology, business operations, and business continuity strategies into the training program.

Refer to the following for additional information and guidance:

- FCA Informational Memorandum on Guidance on Preparing Your Institution for a Catastrophic Event (June 22, 2006)
- FCA Informational Memorandum on Threats to Information Management Systems (August 30, 1999)
- NIST Special Publication 800-184 – Guide for Cybersecurity Event Recovery
- NIST Special Publication 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems
- FFIEC Statement on Pandemic Planning (March 6, 2020)

6. Exercise & Test Program:

Evaluate the adequacy of the business continuity exercise and test program.

Guidance:

Management should develop and document a comprehensive exercise and test program that includes plans and strategies to validate the BCP and the ability to restore critical business functions. Management is responsible for ensuring exercises and tests are consistent with the board's business continuity management strategy. Exercises and tests are tools used to validate the BCP's effectiveness and to verify that business continuity procedures support objectives to restore critical business functions. The FFIEC Business Continuity Management booklet defines an *exercise* as a task or activity involving people and processes that is designed to validate one or more aspects of the BCP or related procedures. It defines *test* as a type of exercise intended to verify the quality, performance, or reliability of system resilience in an operational environment. The distinction between the two is that exercises address people, processes, and systems whereas tests address specific aspects of a system. The objective of exercises and tests is to ensure the BCP remains accurate, relevant, and operable under adverse conditions. Management should ensure exercises and tests are performed at regular intervals based on the institution's exercise and test universe, when new risks are identified, and after significant changes to technology systems, business operations, facilities, or organizational structure. This would include the unique risks associated with pandemics. Refer to the FFIEC Business Continuity Management booklet for additional information and examination guidance about exercise and test programs and the related board and senior management responsibilities.

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

- ***Plans:*** **Has management developed and documented appropriate exercise and test plans that identify objectives and expectations, outline scenarios, and provide assessment metrics?** Management should ensure exercise and test plans contain the necessary information to guide participants in validating the institution's ability to restore critical business functions. Plans should identify the objectives and expectations of the specific exercise or test. They should describe the event scenarios, including any assumptions or constraints, and identify the roles and responsibilities of all participants. Plans should provide metrics to assess whether the exercise and test objectives were met. Refer to the FFIEC Business Continuity Management booklet for additional information and examination guidance about exercise and test plans.
- ***Methods:*** **Does the institution use sufficient exercise and test methods to evaluate the effectiveness of the BCP and to validate the continuity and resilience of business functions?** Exercises and tests should validate the plan to continue and recover business operations on an enterprise-wide basis. Management may use or combine different exercise and test methods based on the criticality and complexity of business operations. Refer to the FFIEC Business Continuity Management booklet for additional information and examination guidance about exercise and test methods, including the following sections that provide more detailed descriptions:
    - Full-scale exercise
    - Limited-scale exercise

- Tabletop exercise
- Tests

- ***Third-Party Service Providers:*** **If the institution contracts with a third-party service provider to perform or support critical operations, does management sufficiently address the third-party service provider in the enterprise-wide exercise and test program?** When relying on a third-party service provider for critical technology services or business functions, management should ensure the provider can restore the services or functions within the acceptable time frames established by business and contractual requirements. Management should ensure the contractual relationship with the third-party service provider includes the institution's right to perform or participate in testing with third-party service providers. Management should review the third-party service provider's exercise and test results, related audit reports, and remediation plans to determine the adequacy and effectiveness of the provider's testing and remediation processes. *[Note: A third-party service provider could be the institution's funding bank.]* Refer to the FFIEC Business Continuity Management booklet for additional information and examination guidance about third-party service provider testing. In addition, refer to the FFIEC Outsourcing Technology Services booklet for guidance on evaluating the outsourcing processes and controls that govern TSP relationships.

- ***Documentation and Reporting*****: Did management appropriately document, analyze, summarize, and report business continuity exercise and test results to the board?** After the exercises and tests are executed, management should properly document the results and issues identified. They should develop action plans and establish target dates to resolve or remediate any issues, which might involve retesting. Management should evaluate the results to ensure exercise and test objectives were achieved, and that business continuity successes, failures, and lessons learned are thoroughly analyzed. Finally, management should report this information to the board. Refer to the FFIEC Business Continuity Management booklet for additional information and examination guidance about post-exercise and post-test actions and board reporting.

Refer to the following for additional information and guidance:

- FCA Informational Memorandum on Critical Infrastructure Designation (March 27, 2020)
- FCA Informational Memorandum on Guidance on Preparing Your Institution for a Catastrophic Event (June 22, 2006)
- FCA Informational Memorandum on Threats to Information Management Systems (August 30, 1999)
- NIST Special Publication 800-184 – Guide for Cybersecurity Event Recovery
- NIST Special Publication 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems
- FFIEC Statement on Pandemic Planning (March 6, 2020)

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 the business continuity program to ensure compliance with applicable criteria. In particular, business continuity plans and the exercise and testing activities and results 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. Refer to the FFIEC Audit booklet for additional information and examination guidance about the IT audit function, and to the FFIEC Business Continuity Management booklet about the audit function in relation to the business continuity program.

Note: This procedure focuses on evaluating the reliability and effectiveness of internal audits and reviews in this topical area. Refer to the *Audit & Review Programs* topic in the Examination Manual for guidance on examining the overall internal audit and review program.

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

- ***Audit Coverage:*** **Is there periodic audit or review coverage of the business continuity program?** 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 the primary 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:

    - Business continuity policies and procedures.
    - Business impact analysis (BIA) and risk assessment.
    - The enterprise-wide BCP and subsidiary plans (e.g., individual department continuity plans and disaster recovery plans).
    - Business continuity training programs.
    - Exercise and test programs, including related plans, scenarios, and schedules.
    - Independent audit reports and Service Organization Controls reports from third-party service providers.

- Management's communications and reporting to the board about the business continuity program (e.g., BIA, risk assessment, BCP, exercise and test results, identified issues, corrective action resolution).

- 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, 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.