FFIEC Information Technology Examination Handbook

Business Continuity Management

NOVEMBER 2019

Contents

Introduction

The "Business Continuity Management" (BCM) booklet is one in a series of booklets that comprise the *Federal Financial Institutions Examination Council (FFIEC)*[1] *Information Technology Examination Handbook (IT Handbook)*. The *IT Handbook* is prepared for use by examiners.[2] With the publication of this booklet, the FFIEC member agencies replace the "Business Continuity Planning" booklet issued in February 2015. The change from business continuity planning to business continuity management reflects the changes in customer and industry expectations for the resilience of operations.

The BCM booklet describes principles and practices for IT and operations for safety and soundness, consumer financial protection, and compliance with applicable laws and regulations. The BCM booklet also outlines BCM principles to help examiners evaluate how management addresses risk related to the availability of critical financial products and services. This booklet discusses BCM governance and its related components, including resilience strategies and plan development; training and awareness; exercises and tests; maintenance and improvement; and reporting for all levels of management, including the board of directors.

The focus of this revised booklet is on enterprise-wide, process-oriented approaches that consider technology, business operations, testing, and communication strategies critical to the continuity of the entire entity. However, business continuity should not be focused only on the planning process to recover operations after an event, but rather it should include the continued maintenance of systems and controls for the resilience of operations. Business continuity should be incorporated into the risk management life cycle of all systems, processes, and operations of an entity.

For *IT Handbook* purposes, the term "entities" includes depository financial institutions,[3] nonbank financial institutions,[4] bank holding companies,[5] and third-party service providers.[6]

[1] The FFIEC was established on March 10, 1979, pursuant to Title X of the Financial Institutions Regulatory and Interest Rate Control Act of 1978, Pub. L. 95-630. The FFIEC members include the Board of Governors of the Federal Reserve System (FRB), the Consumer Financial Protection Bureau (CFPB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the State Liaison Committee (SLC).

[2] Each FFIEC member agency may use the principles outlined in this booklet, consistent with the member agency's supervisory authority.

[3] The term "depository financial institution" includes national banks, federal savings associations, state savings associations, state member banks, state nonmember banks, and credit unions.

[4] The term "nonbank financial institution" includes non-depository financial institutions under CFPB's jurisdiction and subject to CFPB supervision and examination.

[5] The term "bank holding company" includes any company which has control over any bank or over any company that is or becomes a bank holding company as defined by the Bank Holding Company Act.

[6] The term "third-party service providers" includes those entities that provide banking services subject to examination under the Bank Service Company Act, the Home Owners Loan Act of 1933, the Dodd-Frank Wall Street Reform and Consumer Protection Act, or other relevant law.

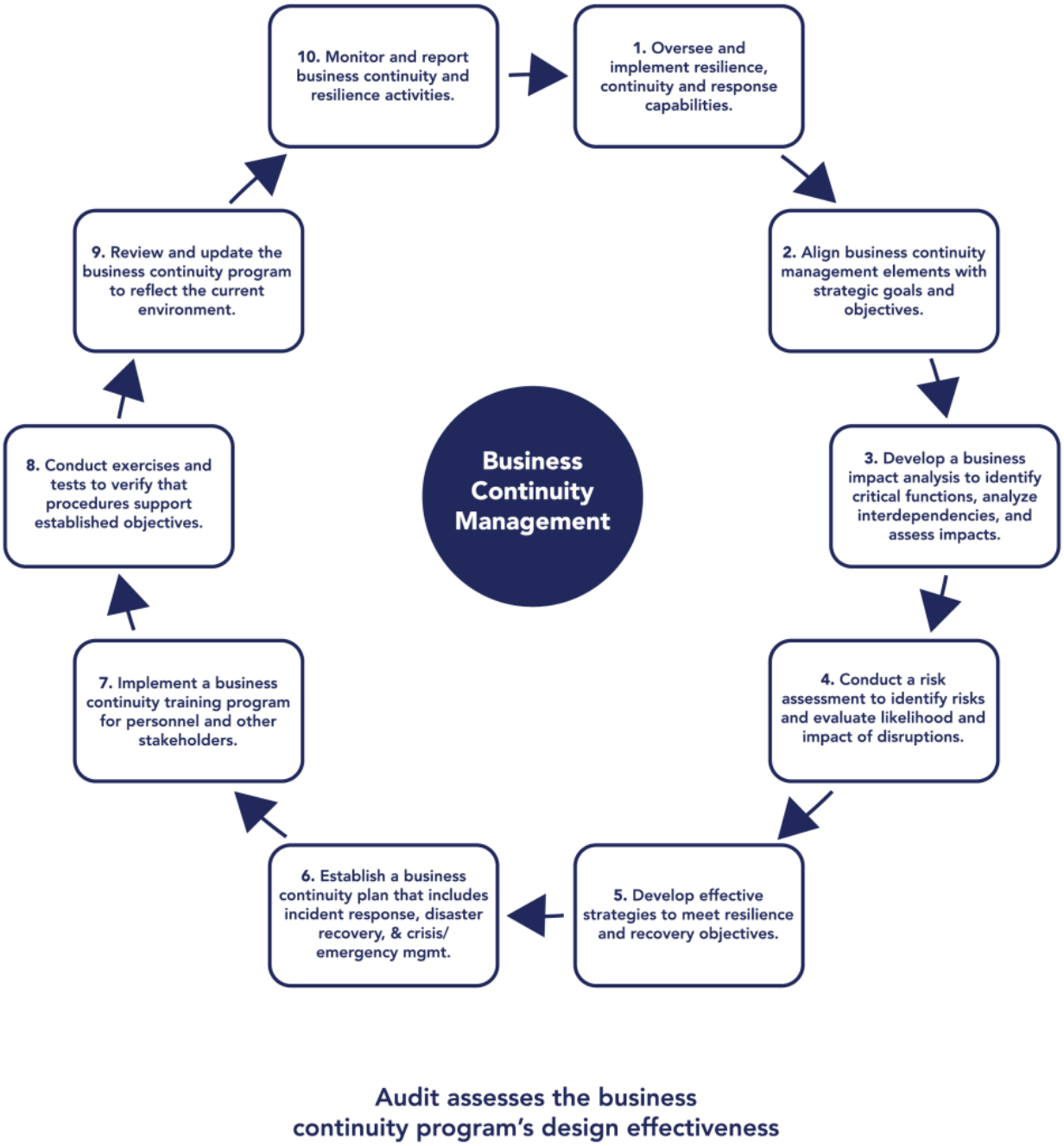
This booklet does not impose requirements on entities. Instead, this booklet describes practices that examiners may use to assess an entity's BCM function.

Appendix A of this booklet provides objectives-based examination procedures. The application of the principles and related examination procedures should vary according to an entity's complexity and risk profile. Examiners should evaluate entities in accordance with their agency's regulatory authority.

I Business Continuity Management

BCM is the process for management to oversee and implement resilience, continuity, and response capabilities to safeguard employees, customers, and products and services. Disruptions such as cyber events, natural disasters, or man-made events can interrupt an entity's operations and can have a broader impact on the financial sector. Resilience incorporates proactive measures to mitigate disruptive events and evaluate an entity's recovery capabilities. An entity's BCM program should align with its strategic goals and objectives. Management should consider an entity's role within and impact on the overall financial services sector when it develops a BCM program.

Figure 1: Business Continuity Management Cycle



II Business Continuity Management Governance

This section provides specific information about BCM governance, including board and senior management responsibilities. General information about governance and risk management is contained in the *IT Handbook's* "Management" booklet and the FFIEC members' examination handbooks.

BCM governance should include:

- Aligning BCM practices with the risk appetite.
- Identifying the continuity level needed, consistent with the operation's criticality.
- Establishing business continuity policy and plans.
- Allocating resources to BCM activities.
- Providing competent management to implement the program.
- Monitoring and assessing business continuity performance relative to these goals.

Figure 1 depicts a typical BCM cycle that entities may follow to manage business continuity risks on an ongoing basis. To manage these risks, the entity may develop a single encompassing BCM policy or individual policies and plans for different functions, depending on the size and complexity of the entity's operations. An effective practice for business continuity-related policies is to address, at a minimum, the following areas: scope and responsibilities within BCM, accountability, authority, and guidance to develop and maintain effective BCM.

II.A Board and Senior Management Responsibilities

Action Summary

The board and senior management govern business continuity through defining responsibilities and accountability, and by allocating adequate resources to business continuity.

Examiners should review for the following:

- Alignment of BCM elements with the entity's strategic goals and objectives.
- Board oversight.
- Management assignment of BCM-related responsibilities.
- Development of BCM strategies.

The board[7] and senior management should set the "tone at the top" and consider the entity's entire operations, including functions performed by affiliates and third-party service providers, when managing business continuity. Management should evaluate continuity risk, set short- and long-term continuity objectives, adopt policies and procedures to mitigate continuity risk, evaluate continuity performance, and adjust operations in response to test results and actual events.

Management can strengthen resilience by assessing risk, planning, testing the plans, and incorporating lessons learned from tests and events. Furthermore, management should consider resilience in business functions and the design of new products and services.

[7] Most financial institutions have boards of directors; however, not all third-party service providers do. When an entity does not have a board, the senior leaders may have the responsibilities of the board described in this booklet.

Board oversight should include:

- Assigning BCM responsibility and accountability.
- Allocating resources to BCM.
- Aligning BCM with the entity's business strategy and risk appetite.
- Understanding business continuity risks and adopting policies and plans to manage events.
- Reviewing business continuity operating results and performance through management reporting, testing, and auditing.
- Providing a credible challenge[8] to management responsible for the BCM process.

Management oversight should include:

- Defining BCM roles, responsibilities, and succession plans.
- Allocating knowledgeable personnel[9] and sufficient financial resources.
- Validating that personnel understand their business continuity roles and responsibilities.
- Establishing measurable goals against which business continuity performance is assessed, such as levels of preparedness and resilience targets.
- Designing and implementing a business continuity exercise strategy.
- Confirming that exercises, tests, and training are comprehensive and consistent with the BCM strategy.
- Resolving weaknesses identified in exercises, tests, and training that exceed the entity's risk appetite.
- Meeting regularly with a designated coordinator or a business continuity committee to discuss policy changes, exercises, tests, and training plans.
- Assessing and updating business continuity strategies and plans to reflect the current business conditions and operating environment for continuous improvement.
- Coordinating plans and responses with external groups (as described in IV.B, "Communications").

[8] A credible challenge involves being actively engaged, asking thoughtful questions, and exercising independent judgment.

[9] The term "personnel" includes both permanent and temporary staff.

II.B Audit

Action Summary

The board and senior management should engage internal audit or independent personnel to review and validate the design and operating effectiveness of the BCM program. Audit should report to the board and provide an assessment of management's ability to manage and control risks related to continuity and resilience.

Examiners should review the following:

- Scope of BCM-related audit activities.
- Audit reporting of BCM-related activities to the board.
- Board review of audit reports.
- Tracking and resolution of audit findings.
- Management's review of system and organization controls (SOC)[10] and third-party service provider audit reports.

The board and senior management should engage internal audit (or an independent review) to assess the BCM design effectiveness, including policies and procedures, and the effectiveness of controls. Audit should report to the board and provide an assessment of management's ability to oversee and control risks related to continuity and resilience. Auditors should be qualified and independent of BCM processes. Audit scope and frequency depend on the entity's complexity, risk profile, and changes the entity may be experiencing. Large, complex entities may have multiple audits, covering various departments or aspects of the BCM program. Less complex entities may have their business continuity activities included within an IT general controls audit.

The internal audit of the BCM program should provide an independent assessment of management's ability to oversee the entity's continuity and resilience risk. Auditors should:

- Evaluate the business impact analysis (BIA) and risk assessment for reasonableness, identification of critical functions, and the likelihood of different events and the potential impact on operations.
- Evaluate controls for reliability, adequacy, and effectiveness regarding continuity and resilience.
- Leverage SOC reports and other external artifacts from third-party service providers, as appropriate.

[10] "In 2017, the American Institute of Certified Public Accountants (AICPA) introduced the term "system and organization controls" (SOC) to refer to the suite of services practitioners may provide relating to system-level controls of a service organization and system- or entity-level controls of other organizations. Formerly, SOC referred to service organization controls. By redefining that acronym, the AICPA enables the introduction of new internal control examinations that may be performed (a) for other types of organizations, in addition to service organizations, and (b) on either system-level or entity-level controls of such organizations." (AICPA, *SOC 2 Examinations and SOC for Cybersecurity Examinations: Understanding the Key Distinctions.*)

- Compare the entity's inherent risk level and the effectiveness of risk mitigation against the entity's risk appetite.
- Verify whether test plans achieve the stated objectives.
- Monitor BCM testing to verify that issues (e.g., deviation from test plans and failed objectives) are appropriately identified and escalated.
- Assess the BCM program's effectiveness.

Refer to the *IT Handbook's* "Audit" booklet for additional information.

III Risk Management

Business continuity risk management focuses on a subset of operational risk factors, against which capital and reserves alone may not protect an entity, and involves managing the possibility of an event that jeopardizes critical systems.[11] The BIA and risk assessment represent the foundation of BCM. As illustrated in figure 2, BCM should integrate with an entity's enterprise risk management (ERM),[12] which allows for the identification and management of risk across the entire entity. BCM allows management to set strategy to effectively mitigate risks posed by disruptive events. The level and formality of BCM and ERM integration should be commensurate with the entity's complexity and risk profile.

Figure 2: Business Continuity Management Elements (Relative to Enterprise Risk Management)

[11] Refer to the U.S. Department of the Treasury and the Department of Homeland Security's (DHS) *Financial Services Sector-Specific Plan 2015*.

[12] ERM is "[a] process, effected by an entity's board of directors, management and other personnel, applied in strategy-setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within the risk appetite, to provide reasonable assurance regarding the achievement of entity objectives." (Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise Risk Management – Integrated Framework (Executive Summary)*, September 2004)

Management should use the BIA and risk management processes to identify and monitor continuity risks for an entity. Once management determines the risk, there are four common strategies to address that risk: risk acceptance, risk mitigation, risk transference, and risk avoidance. Risk transference, such as obtaining insurance, may allow management to recover financial losses or expenses resulting from an event and can be an effective capital management tool; however, insurance should not be a substitute for effective controls or continuity and resilience planning. Management's continuity and resilience planning efforts should focus on risk mitigation and avoidance strategies, and where appropriate, risk acceptance strategies. These strategies are covered more in depth throughout this booklet. Refer to the *IT Handbook's* "Management" booklet for additional information.

Management at large and systemically important entities whose failure could trigger a broader financial disruption should assess the likelihood and impact of a disruption, both to the entity and the entire financial sector. These entities are a critical component of the broader financial system and should incorporate scenarios of disruptions impacting the financial sector into the entity's BCM processes.

The *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System* (*Sound Practices Paper*)[13] outlines practices for financial industry participants that perform clearing and settlement activities for critical financial markets (core firms) and institutions that process a significant share of transactions in critical financial markets (significant firms). Regulators have notified all participants that meet the definition of a core or significant firm as set forth in the *Sound Practices Paper*. Because core and significant firms participate in one or more critical financial markets, and their failure to perform critical activities by the end of a business day could present systemic risk to financial systems, their role in financial markets should be addressed as part of the business continuity planning process.

[13] Refer to the *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System* issued by the SR Letter 03-9 (FRB), Bulletin 2003-14 (OCC), and Release No. 34-47638 (U.S. Securities and Exchange Commission (SEC)). Also refer to 68 Fed. Reg. 17809.

III.A Business Impact Analysis

Action Summary

Management should develop a BIA that identifies all business functions and prioritizes them in order of criticality, analyzes related interdependencies among business processes and systems, and assesses a disruption's impact through established metrics. The BIA should define recovery priorities and resource dependencies for critical processes.

Examiners should review the following as part of the BIA process:

- Identification of critical business functions.
- Identification of interdependencies across business units.
- Identification and analysis of disruptive events.
- Reasonableness of recovery objectives.
- Communication of BIA results throughout the entity.
- Comprehensiveness of management's BIA review.

A BIA is the process of identifying the potential impact of disruptive events to an entity's functions and processes. A BIA allows management to identify and analyze gaps in critical processes that would prevent the entity from meeting its business requirements. The BIA generally lists recovery priorities and resources on which critical processes depend (e.g., work flow analysis[14]). Through the BIA process, management should identify interdependencies among critical operations, departments, personnel, services, and the functions with the greatest exposure to interruption. Management should identify resources on which these functions and processes depend and exposures that would warrant further protective measures. Furthermore, the BIA should include financial and other resource costs (e.g., the loss of business, and exposure to legal and regulatory consequences) needed to recover and restore business functions and processes.

The time and resources to complete the BIA depends on the entity's size and complexity. Complex entities may have multiple BIAs for various business lines, subsidiaries, or other organizational separations. Information from the ERM, such as business processes and risk appetites, may facilitate the BIA development.

[14] The work flow analysis can assist in documenting interdependencies among critical operations, departments, personnel, and services.

III.A.1 Identification of Critical Business Functions

Completing the BIA generally involves gathering information regarding business functions, impacts from disruptions, and business interdependencies; analyzing this information; and establishing recovery objectives. Critical business functions,[15] including support activities (e.g., help desk, call center, human resources, and payroll), systems, and interrelationships may be analyzed in several ways. Work flows, interviews, organizational charts, network diagrams/topologies, data flow diagrams, succession plans, or delegations of authority for key personnel may help management identify business processes and hierarchies.

Management should inventory the entity's critical assets (e.g., people, hardware, software, data, information, and cash) and infrastructure (e.g., network connectivity, communication lines, facilities, and utilities), including those provided by third-party service providers. Furthermore, management should consider supporting activities (e.g., technology support, payroll, contracting) and software (e.g., email, office productivity suites), geographic locations, and unique aspects (e.g., proprietary hardware and software, documentation, or other specialized supplies). Management should also inventory third-party service providers, including specific services they provide. The methodology used should be repeatable, allowing management to reevaluate information after significant changes.

III.A.2 Interdependency Analysis

The BIA process allows management to identify, analyze, and prioritize interdependencies among business functions and systems for alignment with resilience and recovery objectives. The analysis allows management to evaluate interdependent business functions, systems, and shared resources.

During its analysis, management should identify single points of failure, which may include telecommunication lines, network connections between branches, backups that become corrupted, reliance on one power source, or data center locations in close geographic proximity. Personnel can be a single point of failure if there are no cross-trained personnel to back up their responsibilities. Important interdependencies that should be considered include the following:

- Internal systems and business functions, which could include customer services, production processes, hardware, software, application programming interfaces (i.e., code that allows two programs to communicate with each other), data, and documentation of vital records for legal/statutory or process documentation.
- Third-party service providers (e.g., core processing, online and mobile banking, settlement activities, and disaster recovery services), key suppliers (e.g., hardware, software, and utility providers), and business partners and their roles and responsibilities for resilience and recovery.

The BIA will assist management in forming contract and service-level agreement (SLA) requirements for availability and reliability of each service. For pre-existing contracts and SLAs,

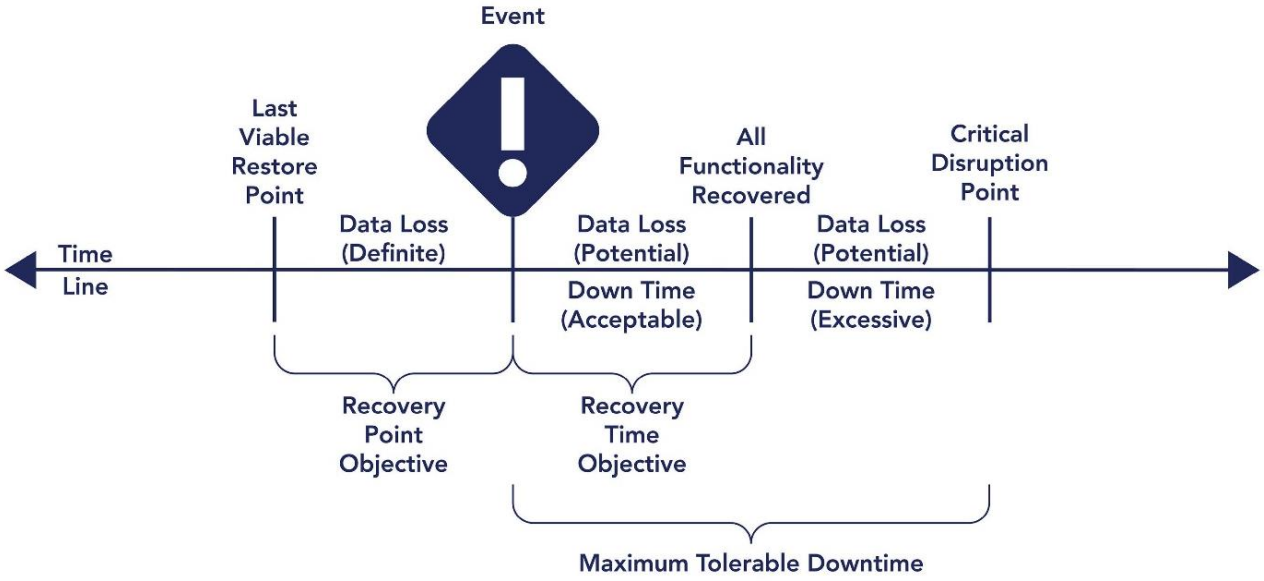
[15] The term "function" can consist of one or more processes.

management should confirm that the contract and SLA requirements align with management's and the customer's continuity and resilience expectations.

III.A.3 Impact of Disruption

Through the BIA process, management should evaluate the potential impact of disruptive events, including operational, financial, and reputational impacts. Management should establish recovery objectives after determining a disruption's impact. Common measurements include recovery point objective (RPO), recovery time objective (RTO), and maximum tolerable downtime (MTD). Where applicable, these measurements should be evaluated for alignment with third-party service providers' contracted recovery expectations.

Figure 3: Recovery Objectives (Relative to an Event)



As illustrated in figure 3, the RPO represents the point in time, before a disruption, to which data can be recovered (given the most recent backup copy of the data) after an outage. Refer to section IV.A.2, "Cyber Resilience," for additional information regarding backups.

As illustrated in figure 3, the RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources and business processes. Determining the RTO is important for selecting appropriate technologies and strategies. When it is not feasible to meet an RTO, management should verify whether the RTO is realistic, initiate an action plan and milestone(s) to document the situation, and, when appropriate, plan for its mitigation. Management should consider interrelated RTOs for each business function to determine the total downtime caused by a disruption. Establishing realistic RTOs assists management in determining a critical path and hierarchy for recovery. For example, a process with a shorter RTO that is dependent upon on a process with a longer RTO may indicate a gap that should be analyzed further.

Whether driven by customer expectations or technological advancement, previously established RTOs that were a few hours in duration may now require near real-time recovery. Therefore, it may be appropriate for management to reevaluate currently acceptable RTOs.

As illustrated in figure 3, the MTD represents the total amount of time the system owner or authorizing official is willing to accept for a business process disruption and includes all impact considerations. The MTD is important for contingency planners when selecting an appropriate recovery method and developing the scope and depth of recovery procedures. Examiners may encounter other terminology to describe MTD (e.g., maximum allowable downtime).

Failure to meet established metrics, such as RPO, RTO, and MTD, may have operational impacts, including discontinued or reduced service levels, inability to meet security requirements, workflow disruptions, supply chain disruptions, and delays of business initiatives. The financial impact could include the loss of revenue, increased costs, or fines and penalties.

III.B Risk Assessment

Action Summary

Management should evaluate the likelihood and impact of potential disruptions and events. As part of this evaluation, management should consider the geographical area where the entity operates. Additionally, management should consider the risks and threats that could affect the entity's third-party service providers. Once management identifies scenarios; evaluates specific threats to the controls, strategies, and plans; and understands the entity's risk exposure, management should develop risk treatment strategies (including risk acceptance or risk transfer) based on the entity's risk appetite.

Examiners should review the risk assessment and determine whether it addresses the impact and likelihood of disruptions of the entity's information services, technology, personnel, facilities, and services provided by third parties. Specifically, examiners should review whether the following types of events are included in the risk assessment:

- 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, blackmail, sabotage, cyber attacks, and terrorism.
- International events that may affect services (e.g., political instability and economic disruptions).
- Low likelihood and high impact events (e.g., terrorist attacks or pandemic events).

Risk assessment is the process of identifying risks to operations, organizational assets, individuals, and other organizations. Risk assessments incorporate threat and vulnerability

analyses and address the appropriate mitigations. As part of risk assessment processes, information from the ERM can be leveraged, such as business process documentation, critical risks, impacts, and tolerances. Management should use risk assessments to identify, measure, and mitigate risk exposures to critical functions and processes identified by the BIA. Furthermore, the risk assessment process may result in changes to the BIA. For example, management may prioritize business processes based on their importance to strategic goals and safe and sound practices; however, after developing threat models, results may necessitate prompt alteration of initial priorities or recovery plans.

III.B.1 Risk Identification

While management performs risk assessments, the focus of business continuity risk identification is on the resilience of the entity. While the causes of events can vary greatly, many of the effects do not. According to the Federal Emergency Management Agency (FEMA), threats and hazards can be categorized as natural, technological, and adversarial or human-caused.[16] Each of these threats and hazards can be subcategorized, for example as internal (e.g., malicious insider or human error) or external, systemic or non-systemic, deliberate or inadvertent, and with or without warning. Although the characteristics of each hazard and threat (e.g., speed of onset, size of the affected area) may be different, the general tasks for recovering operations are the same. Management should address common operational functions in the business continuity plan (BCP) instead of having unique plans for every type of hazard or threat. Planning for all threats and hazards ensures that, when addressing emergency functions, planners identify common tasks and the personnel responsible for accomplishing the tasks.

Management should evaluate potential risks that are in the entity's geographic area. For example, entities could be located in flood-prone areas, earthquake zones, terrorist targets, or areas affected by tornados or hurricanes. In addition to geographic areas, management should also assess geopolitical risk and the potential for retaliatory cyber attacks. For example, U.S. sanctions against a nation-state could increase the risk of cyber attacks against critical infrastructure(s).

Management should coordinate business continuity risk identification efforts throughout the entity. Individual business units within larger entities should coordinate risk identification activities to identify systemic threats to the overall entity. Management should identify and inventory the entity's internal and external assets, types of threats and hazards, and existing controls as an important part of effective risk identification. Refer to the *IT Handbook's* "Management" booklet for additional information.

Furthermore, management should identify cyber security risks (refer to the *IT Handbook's* "Information Security" booklet for additional information), which should be gathered as part of the risk assessment process. Cyber security can pose risk to customer information as discussed in

[16] Refer to FEMA's *Comprehensive Preparedness Guide (CPG) 101 Version 2.0*. Non-FFIEC agency documents are included for illustrative purposes of common risks and are not supervisory expectations.

the *Interagency Guidelines Establishing Information Security Standards*[17] that implement the Gramm-Leach-Bliley Act (GLBA).

Management should coordinate with external sources to obtain information about hazards and threats. External sources include industry information-sharing groups (e.g., Financial Services Information Sharing and Analysis Center (FS-ISAC)), and local, state, and federal authorities[18] that provide timely and actionable information about hazards and threats. In addition, sharing information about events at an entity may help others identify, evaluate, and mitigate cybersecurity threats and vulnerabilities. Information about hazards and threats should be considered in the BIA, risk assessment, and other BCM processes. Refer to the *IT Handbook's* "Information Security" booklet for additional information.

One component in the risk identification process is the gathering and assessment of threat intelligence, which National Institute of Standards and Technology (NIST) defines as "information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes." Management should integrate its threat-intelligence process with the BCM function.

Threats are potentially magnified when entities and their third-party service providers are tightly interconnected. An incident affecting one entity or third-party service provider can result in cascading impacts that quickly affect other service providers, institutions, or sectors. The term "supply chain risk" in BCM may be used to represent the risk related to the interconnectivity among the entity and others. A critical failure at a third-party service provider could have large-scale consequences. Management should identify interconnectivity points between the entity and its third-party service providers, as well as between other entities and third-party service providers. Documenting the flow of transactions, such as developing formal process diagrams, may help management identify interdependencies and end-to-end processes.

III.B.2 Likelihood and Impact

Management should evaluate the likelihood and impact of disruptive events. Risks may range from those with a high likelihood of occurrence and low impact, such as brief power interruptions, to those with a low probability of occurrence and high impact, such as pandemics. The most difficult risks to address are those that may have a high impact on the entity but a low probability of occurrence. The Department of Homeland Security's (DHS) *National Infrastructure Protection Plan*[19] provides examples of risk measurement processes and methodologies to help analyze risks.

[17] Refer to the *Interagency Guidelines Establishing Information Security Standards* issued by 12 CFR 364, Appendix B (FDIC); 12 CFR 208, Appendix D-2 and 12 CFR 225, Appendix F (FRB); and 12 CFR 30, Appendix B (OCC). Also refer to *Guidelines for Safeguarding Member Information*, 12 CFR 748, Appendix A (NCUA).

[18] Examples include ChicagoFIRST county and state government, the DHS's National Terrorism Advisory System, FEMA, and the World Health Organization.

[19] Refer to DHS's *National Infrastructure Protection Plan*.

As part of the assessment, management should quantify the impacts and define loss criteria as either quantitative (financial) or qualitative (e.g., impact to customers, reputational impact). The BCM risk assessment should be commensurate with the entity's risk and complexity and should include reasonably foreseeable events. Worst-case scenarios, such as destruction of the facilities and loss of life, should be addressed. State and local authorities may assist management with identifying specific risks or exposures for geographic locations, and special requirements for accessing emergency zones.

Management should also assess whether its third-party service providers consider the likelihood of a disruption based on the geographic location of facilities, their susceptibility to threats (e.g., location in a flood plain), and the proximity to critical infrastructure (e.g., power grids, telecommunications, nuclear power plants, airports, major highways, and railroads).

Management should determine the potential severity of threats and estimate the disruption's impact under various threat scenarios as it assesses the likelihood and impact of a disruption. The results may be scored quantitatively (e.g., based on a numerical ranking) or qualitatively (e.g., high, medium, and low) and then prioritized. Refer to the *IT Handbook's* "Management" booklet for additional information.

Once management identifies scenarios, it should evaluate specific threats to the entity's controls, strategies, and plans. The difference, or the gap, between the risks from likely foreseeable threats and the mitigation provided by current controls, represents the risk exposure. Management should develop strategies to manage risk, which could include risk mitigation, avoidance, acceptance, or risk transfer, based on the entity's risk appetite.

IV Business Continuity Strategies

Action Summary

The board and senior management should develop effective strategies to meet resilience and recovery objectives. Effective oversight generally includes guidelines to achieve defined business continuity objectives.

Examiners should review BCM strategies and determine whether the strategies:

- Address personnel, processes, technology, and facility issues.
- Address critical business risks in the operating environment (e.g., mitigate specific or unique threats, such as cyber threats or loss of critical third-party service providers).
- Outline a combination of backup, replication, and storage methods for data protection.
- Provide for high redundancy levels in the telecommunications infrastructure.
- Detail a consistent change management process throughout the entity.
- Include alternatives for any proprietary systems.
- Include provisions for appropriate international business activities, where applicable.

Business continuity strategies are developed after the BIA and risk assessment process. These strategies should be risk-based and address all foreseeable risks, including non-technology risks (e.g., transaction, liquidity, and reputation risks). Strategies should include allocation of resources to meet resilience and recovery objectives. Strategies should be validated to confirm that they are viable and sufficient for peak work volumes. For example, the increased reliance on and interconnectivity of technology makes it less feasible for many entities to operate manually for an extended period, if at all.

Strategies should include the potential impact to personnel, processes, technology, facilities, and data. Personnel-related strategies may include logistical arrangements to transport or house staff at alternate facilities. In addition, management may establish alternate methods for communicating with employees, customers, and external parties. Process-related strategies may include redundant work sites for business-line operations or manual processes. Technology-related strategies may include fully equipped backup data centers or cloud providers. Backup strategies should include data files, operating systems, and applications and utilities. Facilities-related strategies may include geographic diversity or multiple power sources to reduce single point of failure risk.

Data protection strategies typically include a combination of backup, replication, and storage to achieve different levels of continuity and resilience. For example, it may be appropriate to deploy more automated, scalable solutions, such as data replication to a cloud. Management should develop comprehensive strategies to protect data, such as:

- Integrating operational, continuity, and resilience strategies to protect data based on recovery objectives.
- Designing a process to preserve the integrity and availability of data from threats.
- Monitoring the effectiveness and efficiency of data protection solutions.

Strategies should address critical business risks in the operating environment. Management should consider strategies to mitigate specific or unique threats, such as cyber threats or loss of critical third-party service providers. The specific strategy in response to an event may be different based on the entity's capabilities. Management should determine what alternatives exist for proprietary systems given the significant, unique risks to an entity's business activities. For example, some entities use internally developed assets (e.g., spreadsheets or other tools) that are critical for certain calculations within a business unit, which are often overlooked, including where and how they are stored, during the risk assessment and BIA processes. Furthermore, management should also consider access capabilities for voice and data, mapping technology infrastructure to employee needs, and internal and external capacity (including remote capacity) to determine whether telecommuting strategies are sufficient.

Strategies could include cloud architectures, virtualization, and other technologies. Cloud solutions may provide a cost-effective and high-availability environment. Independent of the strategies selected for architecture and data protection, management should still be responsible for data integrity and overall resilience. Cloud-based disaster recovery services[20] may be considered as part of resilience programs. Refer to section V.C.1, "Data Center Recovery Alternatives," for additional information.

[20] Refer to the FFIEC's statement on *Outsourced Cloud Computing.*

IV.A Resilience

Action Summary

Management should evaluate whether there are appropriate resources to ensure resilience, including an accessible, off-site repository of software, configuration settings, and related documentation, appropriate backups of data, and off-site infrastructure to operate recovery systems.

Furthermore, management should discuss potential disaster scenarios with the entity's third-party service providers to prepare for an event. Subsequently, management should assess the entity's immediate or short-term space requirements, systems, and personnel capacity to assume or transfer failed operations. Additionally, management should assess critical third-party service providers' susceptibility to simultaneous attacks and verify their resilience capabilities.

Examiners should review the following:

- Appropriateness of resilience practices, including the adequacy of recovery infrastructure and backup processes.
- Integration with disaster recovery services to protect against data destruction.
- Assessment of alternate data communications infrastructure between the entity and critical third-party service providers.
- Evaluation of the entity's susceptibility to multiple threat scenarios in resilience planning, testing, and recovery strategies.
- Designation of emergency personnel, including for critical business process-level employees.

Resilience is "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents."[21] The business strategy, not technology solutions, should drive resilience. Resilience extends beyond recovery capabilities to incorporate proactive measures for mitigating the risk of a disruptive event in the overall design of operations and processes. Resilience strategies, including maintaining security standards, should extend across the entire business, including outsourced activities. Management should evaluate whether the entity has appropriate resources (e.g., human, financial, time) for resilience. When developing the entity's resilience strategies, management should consider lessons learned from previous events.

[21] Refer to the Presidential Policy Directive/PPD-21, *Presidential Policy Directive -- Critical Infrastructure Security and Resilience* February 12, 2013.

IV.A.1 Physical

Physical resilience is the traditional approach to business continuity and includes IT architecture, infrastructure, facilities, and communications. To avoid the potential for failures after a disruption, management, when possible, should diversify telecommunication lines, establish redundant connections between branches and data centers, create backups, identify multiple power sources, and verify geographic diversity of key entity locations.

IV.A.2 Cyber Resilience

A challenge for cyber resilience is maintaining operations despite ever-changing risks (e.g., malware, data or system destruction and corruption, and communications infrastructure disruption). The sophistication and frequency of cyber attacks increase the potential for disruption and destruction of data and systems. Given the broad and increasing spectrum of cyber threats, resilience measures should be flexible enough to adapt to a diverse range of events. For example, a cyber attack could impact both production and backup facilities simultaneously, potentially rendering both inoperable, whether hosted internally or by a third-party service provider.

In addition, adversaries may initiate a secondary disruption (e.g., the original disruption could be the impact of a hurricane with the secondary disruption being false transactions or accessing sensitive data). Alternatively, adversaries can launch simultaneous attacks (e.g., a distributed denial of service (DDoS) attack combined with a wire transfer compromise). Therefore, management should adhere to established security and privacy policies and processes to comply with applicable regulations, even during disruptive events.

IV.A.3 Data Backup and Replication

Management should maintain data confidentiality, integrity, and availability for all iterations of data, including data backup and replication, not just focused on the production environment. Data backup and re-creation are important to recovering critical business functions in the event of disruptions. Backup files are commonly created electronically and can be mirrored at an off-site location, backed up on removable media, stored temporarily on network servers until rotated off-site, or backed up to a cloud environment. Backups should be readily accessible and adhere to the entity's information security policy.

Management should reassess backup and recovery strategies as the technology and threat environments evolve. For real-time or high-volume systems, it may be appropriate to have advanced duplication and backup methods. These advanced methods, including cloud and mirroring, provide high availability and are detailed in section V.E.1, "Data Center Recovery Alternatives."

Management should maintain an accessible, off-site repository of software, configuration settings, and related documentation. Even standard software configurations can vary from one location to another. Differences could include parameter settings and modifications, security profiles, reporting options, account information, customized software changes, or other options.

Failure to back up software configurations could result in inoperability or could delay recovery. Therefore, a comprehensive backup of critical software is important. Software backups generally consist of the following components:

- Operating systems.
- Applications.
- Utility programs.
- Databases.
- Other critical software identified in the BIA.

Management should establish effective procedures to recover critical networks and systems. Procedures may address the following:

- Backup types (physical or virtual).
- Backup levels (full, incremental, or differential).
- Updates and retention cycle frequencies.
- Software and hardware compatibility reviews.
- Data transmission controls.
- Data repository maintenance.

Refer to the *IT Handbook's* "Operations" booklet for additional information.

Data replication (also referred to as data synchronization or mirroring) is the process of copying data, usually with the objective of maintaining identical data sets in separate locations. Replication is important in any environment for resilience. Furthermore, management should consider integrity controls during replication so that data changes in production, development, and quality assurance environments are applied throughout the network.

Two common data replication processes used for information systems are synchronous and asynchronous. Synchronous replication represents the direct application of the data by applying changes at the same time. In practice, synchronous replication allows data to be transmitted in a continuous stream and minimizes data loss; however, it requires significant communication bandwidth and has limitations on the distance data can be transported due to latency issues. Synchronous replication is typically used for critical business functions where little or no data loss can be tolerated. Conversely, asynchronous replication is the indirect application of data through applying changes to a log before transit. In practice, asynchronous replication allows data to be transmitted in intermittent batches. While asynchronous replication increases the potential for data loss related to the fractions of a second required to transmit the data, this process requires less communication bandwidth and is useful for data transport over longer distances, due to reduced latency issues.

Management should determine the appropriate retention periods for each iteration of data backup. Entities should safeguard against replicating malware and data corruption. This risk is heightened with the use of near real-time data replication systems, as malware can be replicated undetected. Even with diagnostic tools, management could be unaware of an event that causes data integrity issues until well after it happens, as data could appear uncorrupted but later

determined to be inaccurate. Management may determine that the backup of critical data files should be subject to longer retention periods to ensure the ability to recover a backup prior to a corruption event.

Even in situations when the primary and backup facilities are inoperable or corrupted, customers of the entities expect to be able to access their accounts. Entities should develop appropriate cyber resilience processes (e.g., recovery of data and business operations, rebuilding network capabilities and restoring data) that enable restoration of critical services if the institution or its critical service providers fall victim to a destructive cyber attack or similar event. BCM should include the ability to protect offline data backups from destructive malware or other threats that may corrupt production and online backup versions of data. An example of an industry initiative to assist in addressing the resilience of customer account information is Sheltered Harbor.[22]

IV.A.4 Personnel

Resilience is dependent upon personnel availability to maintain critical business processes. Personnel could be unavailable or distracted during such events as natural disasters, severe weather events, or pandemics.[23] While any one employee's role may not be designated as mission critical, management should plan for mass absenteeism during an event or disruption. Previous catastrophic events (e.g., Hurricane Katrina[24]) demonstrate that personnel availability affects timely recovery.

Management should plan for events during which personnel may not be able to access facilities and critical personnel may not be available immediately after the disruption. Public infrastructure and transportation systems may not be operating, and telecommunication systems may be overburdened and unavailable. Therefore, management should consider:

- Staffing and skills needed to operate critical functions related to business continuity.
- Lodging arrangements for displaced employees and their families.
- Basic necessities and services for displaced employees, including water, food, clothing, childcare, transportation, and cash.
- On-site medical support and mobile command centers.
- Secure telecommunication options if employees work from an alternate location.
- Designated emergency personnel, including critical business process-level employees.

[22] Sheltered Harbor is a voluntary industry initiative launched in 2015 following a series of cybersecurity simulation exercises between public and private sectors, known as the Hamilton Series. The purpose of the proposed Sheltered Harbor standard is to promote the stability and resiliency of the financial sector and to preserve public confidence in the financial system. The Sheltered Harbor standard proposes a combination of secure data vaulting of critical customer account information with a comprehensive resilience plan to provide customers timely access to their account information and underlying funds during a prolonged systems outage or destructive cyber attack. (Sheltered Harbor).

[23] Refer to the FFIEC's *FFIEC Releases Guidance on Pandemic Planning*.

[24] Refer to the FFIEC's *Lessons Learned From Hurricane Katrina: Preparing Your Institution for a Catastrophic Event*.

IV.A.5 Third-Party Service Providers

Many entities depend on third-party service providers to perform or support critical operations. A disruption in the delivery of those services can have a direct impact on entities' resilience. A critical failure at a widely used third-party service provider could have large-scale consequences. Management should assess critical third-party service providers' susceptibility to multiple event scenarios and verify such third parties' resilience capabilities. An entity's third-party service provider can be a single point of failure if management has not considered alternative providers or other contingency plans. If an alternative third-party service provider is not readily available, management should consider options to continue business operations and reevaluate resilience options periodically as conditions may change. Resilience planning should be closely coordinated with third-party service providers.

Establishing well-defined expectations with third-party service providers is important to business resilience. Contracts and SLAs with third-party service providers should detail roles and responsibilities of each party to promote resilience. Ongoing monitoring of the entity's third-party service providers helps management identify potential weaknesses in the third-party service provider's resilience that could affect the entity's operations.

Management's review of an entity's third-party service provider's BCM program may include independent audit reports or SOC reports. SOC reports can contain valuable information about the third-party service provider's products and processes. If management relies on SOC reports, it should verify whether business continuity activities are audited, including whether the scope and depth of review are sufficient to allow management to evaluate the third-party service provider's control environment.[25] Depending on the scope of the audit testing, additional inquiry and activities may be appropriate to understand the resilience of the third-party service provider.

Management should consider the same risks outlined in their entity's own internal BCP(s) in relation to third-party service providers, as well as:

- Capacity of third-party service provider to meet client recovery objectives in the agreements, relative to other clients' needs.
- Ability to participate in recovery testing with third-party service providers and access to testing results.
- Ability to move outsourced processes either in-house or to another third-party service provider.
- Alternative resource options (e.g., personnel and systems) for when primary services cannot be delivered.
- Data confidentiality, integrity, and availability (e.g., transportability and interoperability).

[25] SOC 1 reports cover controls at the third-party service provider that affect financial reporting. Business continuity activities are usually reported in unaudited sections of SOC 1 reports because they often do not have a direct correlation to the preparation of the financial statements, unless an event happened during the audit period. SOC 2 reports cover trust services criteria and include activities such as security, confidentiality, availability, privacy, and integrity. Audit firms typically do not opine on the quality of the business continuity activities, because it is difficult to predict what would happen during an actual event. Activities related to business continuity such as replication, plan development, and testing may be included in SOC 2 reports covering availability.

- Financial capacity to continue meeting contractual obligations.
- Services concentrated in a limited number of third-party service providers.

Business continuity-related provisions found in contracts and SLAs may include the following:

- Time parameter(s) for contracted service(s).
- Appropriate baseline metrics describing management's resilience and recovery expectations (e.g., an incident response metric to ensure timely response to events impacting business continuity and resilience).
- Periodic service reviews to ensure up-to-date agreements with all parties involved.

If operations at a third-party service provider cease, the length of time required to convert to an alternate system would, for most applications, exceed a reasonable RTO. To the extent possible, management should establish plans for the resilience of third-party service providers supporting critical operations.

IV.A.6 Telecommunications

Given the critical nature of telecommunications, management should ensure appropriate redundancy levels in the entity's telecommunications infrastructure. The entity's telecommunications infrastructure may contain single points of failure that are outside the control of a single entity. Management should understand the limitations of the entity's third-party telecommunications providers' infrastructure. For example, multiple carriers may rely on the same telecommunications backbone. Key aspects management should consider in establishing telecommunication redundancy include:

- Identifying and mitigating single points of failure across the entity's infrastructure.
- Developing and maintaining a plan to address an outage in the telecommunications lines with the entity's primary third-party service providers.
- Establishing redundant telecommunications links with each of the entity's third-party service providers through a contractual arrangement, which allows either party to switch its connection to an alternate communication path.
- Reviewing the entity's third-party service providers' plans and determining whether critical services can be restored within acceptable time frames.
- Developing guidelines, commensurate with the entity's size, complexity, and risk profile, to diversify connections to mitigate the risk of a telecommunications failure.
- Assessing the communications technology that bridges the transmission distance between the telecommunications service provider and the entity, sometimes referred to as the "last mile," for single points of failure.
- Monitoring relationships with telecommunications providers to manage risks.
- Inquiring about the physical paths used by telecommunications providers and verifying that system redundancies have been properly implemented.

Communication is critical to the financial services sector and other industries. Therefore, management should consider the following services provided by the federal government. These services give participants priority access to telecommunications during a wide-spread event.

- The Telecommunications Service Priority (TSP)[26] program.
- Government Emergency Telecommunications Service (GETS).[27]
- Wireless Priority Service (WPS),[28] which is the wireless complement to GETS.

IV.A.7 Power

The financial industry is dependent on power to run its technology infrastructure and to supply basic necessities to personnel and customers. A long-term power outage can negatively impact an entity's resilience. Management should implement measures to provide electricity in the event of a short-term power disruption. Furthermore, management should develop plans to provide electricity in the event of a long-term power disruption. As part of its short-term and long-term plans, management should consider the following:

- Alternate energy sources (e.g., generators, multiple power grids).
- Fuel requirements, both for fuel on-hand and contracts with suppliers for deliveries during events, and any potential impediments to obtaining fuel.
- Load capacity of generators (e.g., length of time, useful life, level of power supplied).
- Continued maintenance of generators.
- Testing of generators.

IV.A.8 Change Management

Management should implement and align a consistent change management process throughout the entity, making sure to include BCM. As changes are made to production systems and business processes during the normal course of business, recovery systems and documentation at alternate locations should similarly be updated to reflect production and primary system changes.

The change management process should allow for expedient implementation of emergency changes during an event, such as changing an access control list to provide rapid access for

[26] Refer to the DHS's "Telecommunications Service Priority" (TSP) webpage. The TSP program provides service vendors a Federal Communications Commission mandate to prioritize requests by identifying those services critical to national security and emergency preparedness. TSP-designated circuits are recovered first in an emergency. Management may contact the entity's primary federal regulator for information on the TSP program and whether the entity qualifies for a TSP designation. If the entity qualifies, management should integrate the TSP program into the entity's BCP.

[27] Refer to the DHS's "Government Emergency Telecommunications Service" (GETS) webpage. GETS provides "priority access and prioritized processing in the local and long distance segments of the landline networks, greatly increasing the probability of call completion." It is intended to be used in an emergency or crisis situation when the landline network is congested and the probability of completing a normal call is reduced. Management may request GETS cards by submitting an application to the entity's primary federal regulator.

[28] Refer to the DHS's "Wireless Priority Service" webpage.

troubleshooting and analysis. Change tickets and corresponding activity should be reviewed for appropriateness once the event has been resolved. Even during events, changes should still be properly authorized, monitored, and documented. Poorly administered emergency changes can result in further disruption. Additionally, the interrelated nature of systems can compound disruptions to previously unaffected systems. After an emergency event, systems documentation should be updated for any changes made. Change management elements are addressed in more detail in the *IT Handbook's* "Development and Acquisition" and "Operations" booklets.

IV.B Communications

Management should consider, plan for, and prepare multiple mechanisms to communicate with others. For example, when traditional voice communications and telecommunications are impaired or inoperable, management may consider alternative communications systems such as text messaging through employer-provided and personal mobile phones, personal email, and instant messaging. Other common solutions include an inbound hotline number, an informational webpage, or a two-way polling phone system. Regardless of the communication device used, appropriate controls to safeguard customer and other sensitive information should be maintained.

BCM should include communication protocols and contact lists to notify stakeholders. Management should consider the content and process for developing such protocols and templates. Communication protocols should incorporate strategic communications and crisis management approaches in concert with public affairs or external communications (e.g., prepared public/press statements, media response plans, managing social media, etc.). Communication protocols provide customers, third-party service providers, and other external groups a means to communicate when normal channels are inoperable. External groups could include the following:

- Regulatory agencies (federal and states).
- Emergency responders.
- Law enforcement.
- Financial sector trade associations.
- Customers, third-party service providers, and other third parties (e.g., counterparties, clearing and settlement partners, payment system operators).
- Information-sharing entities (e.g., FS-ISAC).

V Business Continuity Plan

Action Summary

Management should develop business continuity plan(s) (BCP) with sufficient detail in relation to the entity's size and complexity. The BCP should address key business needs and incorporate inputs from all business units.

Examiners should review the plan for the following:

- Authorities, responsibilities, and relocation strategies.
- Communications protocols, event management, business continuity, and disaster recovery.
- Liquidity concerns before and during an adverse event.[29]
- Alternatives for payment systems, facilities and infrastructure, data center(s), and branch relocation during a disaster.

As shown in figure 2, a BCP is an important component of BCM. The BCP documents the practices and procedures for continuing business operations during a disruption. The BCP focuses on critical business functions and varies according to the entity's size and complexity. The BCP includes specific elements, such as incident response, disaster recovery, and crisis management. Smaller entities may have a single BCP that includes these elements whereas large, complex entities may have multiple plans supported by subsidiary components for business functions, locations, or departments. Furthermore, the BCP should be a living document, regularly updated so that it remains current with system enhancements and organizational changes.[30]

A comprehensive plan describes the authorities, responsibilities, procedures, and relocation strategies. Components of the plan should include:

- Roles, responsibilities, and required skills for entity personnel and third-party service providers.
- Solutions to various types of foreseeable disruptions, including those emanating from cyber threats.
- Escalation thresholds.
- Immediate steps to protect personnel and customers and minimize damage.
- Prioritization and procedures to recover functions, services, and processes.
- Critical information protection (e.g., physical, electronic, hybrid, and use of off-site storage).

[29] Refer to NIST SP 800-61, *Computer Security Incident Handling Guide*.

[30] Refer to "BCP Strategy Concept," NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*. NOTE: While this document pertains to federal information systems, the principles are relevant for non-federal information systems.

- Logistical arrangements (e.g., housing, transportation, or food) for personnel at the recovery locations.
- Network equipment, connectivity, and communication needs, including entity-owned and personal mobile devices.
- Personnel at alternate sites, including arrangements for those permanently located at the alternate facility.
- Scope and frequency of testing.
- Resumption of a normalized state for business processes.

Representatives from all business units should contribute to BCP development and implementation. The BCP may be developed and maintained internally or outsourced. In either case, the entity's board and senior management should be responsible for the BCP. Management should verify the third-party service provider's qualifications and expertise when outsourcing BCP development. Management should work with the third-party service provider to design executable and viable strategies. Regardless of its development process, the BCP and supporting documentation should be stored so that it is readily accessible by personnel during adverse events.

V.A Event Management

The BCP may define various situations as events, disruptions, or triggers. An event is an occurrence or change in circumstances that may affect operations. An event can be physical, cyber, or a combination of both. A disruption is either an anticipated or unplanned event that causes operations to degrade or fail for an unacceptable length of time (e.g., a minor or extended power outage, an extended unavailable network, or equipment or facility damage or destruction). A trigger is an event that prompts management's response. Predefined threshold escalation triggers are a key element of a BCP, and responses should be designed to mitigate the impact from adverse events.

The BCP should include event management procedures that detail reasonably foreseeable event types and provide thresholds and responses. Procedures should describe how to report an event to management and the situations that warrant notification to those who address events. Management should consider establishing a team(s)[31] to address events. Individuals managing the event may change depending on the nature of the event and team member availability. While the team should manage the event and communicate with stakeholders, event monitoring is an entity-wide responsibility (e.g., board, senior management, and other personnel).

Responses may include activities, programs, or systems that protect life and property, meet basic human needs, and preserve the entity's operational capability. Examples of event responses include:

- Switching operations to a backup facility after a software upgrade and subsequent rollback fail.

[31] Depending on the entity's size and complexity, authority to respond to an event may fall to an individual, a team, or multiple teams. The term "team" is used for purposes of this booklet.

- Rerouting personnel to a safer location or authorizing telecommuting when the local area becomes unsafe.
- Authorizing telecommuting when an event causes disruptions to operations.
- Invoking disaster recovery procedures once management has identified a significant cyber attack.
- Activating emergency response procedures once a hurricane threatens the local region.

V.B Continuity and Recovery

Management should establish protocols for operations continuity and system recovery. The BCP may include:

- Addressing customer service requests during downtime.
- Tracking daily transactions.
- Reconciling general ledger accounts.
- Documenting operational tasks.
- Posting entries after system recovery.
- Maintaining backup records to provide customer account information (e.g., account numbers, customer names, addresses, account status, and account balances).
- Documenting steps for system hardware and software recovery and restart.

When appropriate, procedures should address manual steps for critical functions, such as back-office operations, loan operations, and customer support. Business continuity plans and procedures should be clear, concise, and easy to implement in an emergency,[32] such as checklists and step-by-step procedures.

Displaced customers may not have access to their normal identification and personal records. The BCP should include alternate identity verification methods, and management should be alert for fraud or other suspicious activities. Procedures should address fraud identification[33] and suspicious activity reporting[34] according to protocols and legal requirements.[35]

During the recovery phase, management should coordinate access and availability of power and telecommunications systems with various entities. Management should coordinate with the police and fire departments and local and state government agencies to facilitate timely, secure resilience strategies. Management may also coordinate with other federal agencies, such as the

[32] Refer to NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*. NOTE: While this document pertains to federal information systems, the principles are relevant for non-federal information systems.

[33] Refer to the Financial Crimes Enforcement Network's (FinCEN) FIN-2006-A001, *Guidance to Financial Institutions Regarding Hurricane-Related Benefit Fraud*.

[34] Refer to FinCEN's FIN-2013-G002, *Administrative Difficulties in Submitting Electronic Reports to FinCEN*.

[35] Refer to 31 CFR 1020.220, *Customer Identification Programs for Banks, Savings Associations, Credit Unions, and Certain Non-Federally Regulated Banks*.

Federal Emergency Management Agency, depending on the disaster severity. Refer to the *IT Handbook's* "Operations" booklet for additional information.

V.C Facilities and Infrastructure

The BCP should identify alternatives for core operations, facilities, infrastructure systems, suppliers, utilities, interdependent business partners, and key personnel. The backup site may mirror the operational functionality of the primary site. Management should consider site relocation for short-, medium-, and long-term scenarios. When selecting a facility, management should plan for scalability because an event may last for an extended period of time. In addition, management should consider the entity's proximity to police, fire, and medical facilities, and the expected response time frames should be factored into recovery strategies. Management should enlist the assistance of state and local agencies to expedite building permits and inspections for temporary facilities. Management should verify that recovery alternatives can accommodate the services and processing capabilities affecting critical operations, including:

- Core processing.
- Check processing and imaging.
- Commercial cash management.
- Payments.
- Mailing, faxing, and printing.
- Customer identification.

V.C.1 Data Center Recovery Alternatives

Data center recovery alternatives vary for infrastructure, configuration, operational state, and data migration. Management should document the reasons (e.g., cost and service level) for choosing an alternative and why it is appropriate based on the entity's risk profile and complexity. The level of intervention required to activate the alternate sites affects both the cost and duration to resume operations. Recovery alternatives may take several forms, such as fully redundant systems at alternate sites, cloud-based recovery solutions (either internally developed or outsourced), another data center, or a third-party service provider. Data center and alternate site development is complex, and management should consider constraints in the analysis and design process. The primary objectives are for data to be available and remotely accessible. Management should maintain appropriate controls, regardless of solution. Alternative recovery site examples may include:

- **Cold site:** A backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place. The facility is ready to receive computer equipment when personnel move from their main computing location to the backup facility. This facility is usually not considered as the primary recovery option within the financial services industry because of the significant time necessary to install and activate the infrastructure. Comprehensive testing cannot occur until the infrastructure is established.
- **Warm site:** An environmentally conditioned work space that is partially equipped with information systems and telecommunications equipment to support relocated operations in

the event of a significant disruption. The systems are not loaded with the software or data required to resume operations and typically require manual intervention for failover and system reboots to resume critical processes. Therefore, end users may experience some disruption.

- **Hot site:** A fully operational off-site data center equipped with hardware and software used in the event of an information system disruption. Hot site development is complex, and management should consider constraints in the analysis and design process.
- **Mirrored data recovery sites:** Two or more separate, active sites that back up one another with each site independently supporting critical business functions. These sites provide almost immediate resumption capacity and are seamless for end users. Physical distance and its related latency present limitations for data centers that use real-time, data mirroring backup technologies. Similar to a hot site, these sites contain all of the equipment and connectivity capabilities; however, they also have a duplicate copy of the data. This method of high availability is commonly referred to as "Active-Active."
- **Mobile site:** A site that possesses capabilities between what a warm and a cold site offer and has portable structures equipped with computing equipment available to customers or personnel. Completely activating a mobile site depends on how quickly it can be delivered and backups restored.
- **Colocation facility:** A facility that provides space, power, infrastructure, environmental controls, and telecommunications capabilities for multiple non-related tenants. If management relies on a colocation facility to deliver resources, there is a risk that the capacity at the colocation service provider may not be able to support the entity's operations during a regional or large-scale event.
- **Reciprocal agreement:** An agreement that allows two entities to back up each other. While these agreements may be cost-effective, they are viable only if there is adequate excess capacity at the reciprocal financial institution and both operate on the same version and configuration of core software. Consideration should be given to security and privacy, as sensitive customer information could be exposed to the staff at the reciprocal financial institution. While these arrangements may be acceptable as a short-term solution, management should not rely on them as a long-term recovery solution.
- **Disaster recovery as a service (DRaaS):** A cloud-computing solution for replicating and hosting infrastructure, applications, and data that provides failover and recovery services.

V.C.2 Branch Relocation

An adverse event may lead management to temporarily limit or cease branch operations or temporarily transfer a branch's operations to alternate locations. An important BCP component is establishing a physical location where personnel and customers can go to conduct business. For financial institutions, approval by the appropriate regulator may be required to close, relocate, or establish additional branch facilities.[36]

[36] Refer to 12 U.S.C. 1831r-1, "Notice of Branch Closure"; 64 Fed. Reg. 34844, "Policy Statement of the Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of Thrift Supervision Concerning Branch Closing"; 12 CFR 303, Subpart C, "Establishment and Relocation of Domestic Branches and Offices" (FDIC); 12 CFR 208.6, "Establishment and Maintenance of Branches" (FRB); 12 CFR 5.30, "Establishment, Acquisition, and Relocation of a Branch of a National Bank"

V.D Payment Systems

The BCP should address alternate arrangements if payment systems fail (e.g., automated teller machines (ATM), funds transfers, electronic banking, remote deposit capture, or mobile capabilities). Alternate solutions may include manual procedures for calling in or faxing wire or automated clearing house requests to correspondent financial institutions. In addition, web-based systems or third-party software may be used to perform transactions. Management should verify that redundant electronic payment systems and equipment (e.g., tokens and routers) are included at recovery sites for activation and that documentation is maintained for timely posting of entries when systems are recovered.

The BCP should also address increased cash demands and moving funds through electronic systems, including internet and mobile banking. Management may consider developing procedures for pre-established withdrawal limits based on the financial institution's relationships with customers. In addition, management should prepare for a potential increase in branch traffic when ATMs are unavailable. Pre-established agreements with various cash delivery services within and outside of the local area should also be considered so that ATMs can meet customer demand when service returns.

V.E Liquidity Considerations

The BCP should detail processes to address potential cash and liquidity needs during adverse events. During a disaster, power and communications systems may fail (e.g., inoperable ATMs or debit and credit card systems), requiring cash to fulfill customer and business needs. Arrangements to help meet liquidity needs may include:

- Emergency borrowing access.
- Alternative cash delivery.
- Procedures to secure, deliver, and distribute cash.
- Temporary purchase authority guidelines.
- Expense reimbursement options for personnel.
- Higher-limit credit cards or separate checking accounts, with designated individuals who can sign checks in emergency situations.

V.F Other Components

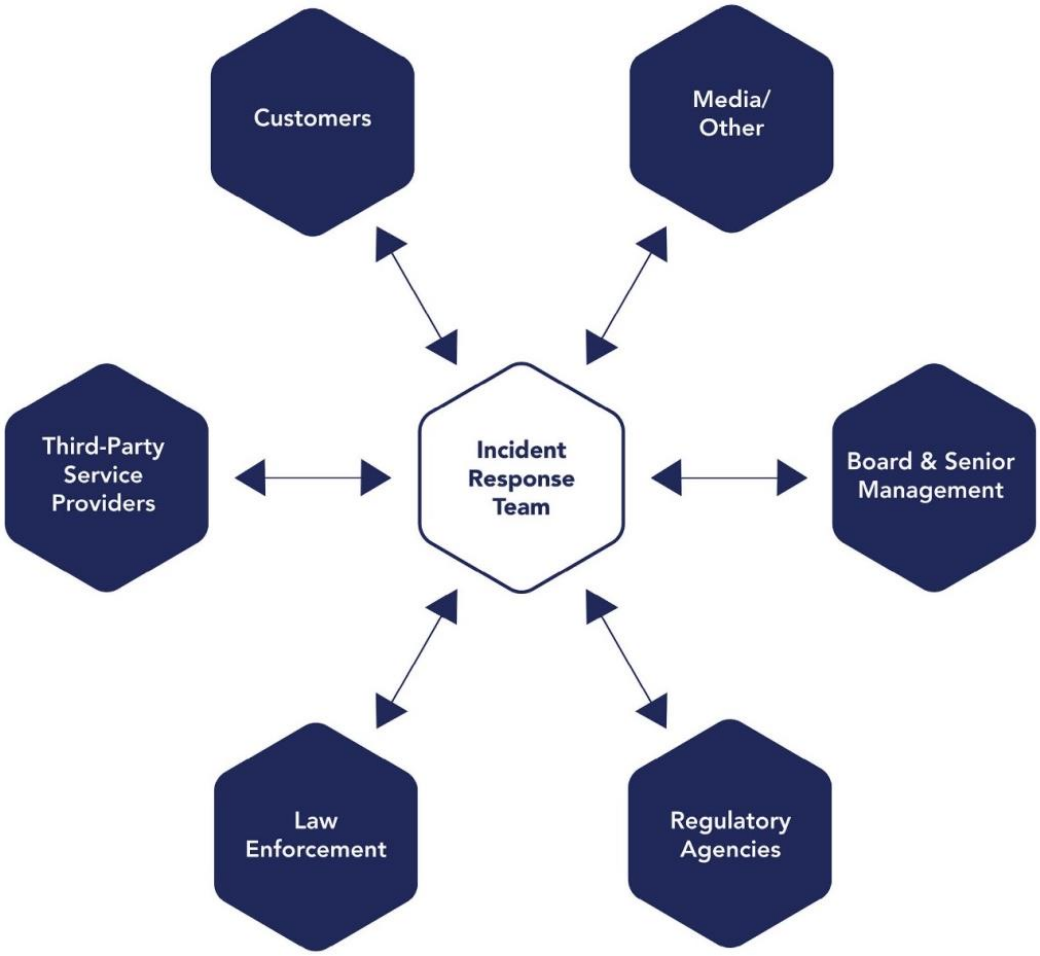
The BCP focuses on sustaining business processes during and after an event. The BCP may incorporate other plans and procedures to minimize a disruption's impact. Components may include incident response, disaster recovery, and crisis or emergency management.

(OCC); and 12 CFR 5.31, "Establishment, Acquisition, and Relocation of a Branch and Establishment of an Agency Office of a Federal Savings Association" (OCC).

V.F.1 Incident Response

Incident response helps management minimize the disruption of services or loss of information from an adverse event. Incident response priorities include preservation of life, preservation of property, incident stabilization, and communicating with stakeholders (e.g., impacted personnel, third-party service providers, customers, regulators, law enforcement). As shown in figure 4, the incident response team should coordinate communication with the noted stakeholders. Management should align incident response procedures with other related processes (e.g., cybersecurity, network operations, and physical security), outsourced services (e.g., contracted incident response obligations), and verify that the procedures are considered during planning and BCP development.

Figure 4: Incident Response Team (Adapted From NIST SP 800-61, Rev. 2)



Management should designate a spokesperson(s) to communicate with the news media. Management should consider various, pre-planned response scenarios approved by the board and senior management. Communication with the news media and via social media may be important for disseminating accurate information. Social media monitoring during an event can help management resolve conflicting messages and proactively respond to issues and concerns.

Management should train personnel to adhere to the plan when approached by the news media or communicating via social media.

Furthermore, management should leverage routine processes (e.g., vulnerability management and network monitoring) to anticipate potential incidents, including cyber incidents, and coordinate incident response planning with any third-party service provider plans. Furthermore, management should consider prearranging third-party forensic and incident response services. Management should periodically update and test the entity's incident response program to verify that it functions as intended, given rapidly changing threats. Refer to the *IT Handbook's* "Information Security" booklet for additional information.

V.F.2 Disaster Recovery

Disaster recovery is the restoring of IT infrastructure, data, and systems. Management should identify key business processes and activities to be maintained while IT systems and applications are unavailable and prioritize the order in which these systems are restored, which should be reflected in the BIA. In addition, management should develop a coordinated strategy for the recovery of data centers, networks, servers, storage, service monitoring, user support, and related software.

Recovery plans should address a broad range of adverse events (e.g., natural disasters, infrastructure failures, technology failures, unavailability of staff, or cyber attacks). Disaster recovery should address guidelines for returning operations back to a normalized state with minimum disruption.

Disaster recovery should also address the following:

- Security controls and protocols, including physical and logical, for implementation and operation of recovery systems.
- Procedures for restoring backlogged activity or lost transactions to identify how transaction records will be brought current within expected recovery time frames.
- Instructions to access critical information repositories and other resources when the primary facility is unavailable.

When developing disaster recovery plans, management should exercise caution when identifying critical and non-critical systems. For example, telephone banking, internet banking, or ATMs may not seem critical when systems are operating normally; however, these systems play a critical role in delivering services to customers during a disruption. Similarly, an email system may not appear critical but may be the primary system available for communication during an adverse event.

V.F.3 Crisis or Emergency Management

Crisis or emergency management[37] is the process that allows the recognition of a crisis, activation of a BCP, and management of emergencies. Crisis or emergency management includes the ability to recover from a major event through predefined leadership and communication. Not every event warrants a crisis or emergency management response. Management should consider the impact of a crisis or emergency on the entity's reputation and personnel. For example, management may invoke crisis or emergency response procedures during a natural disaster, cyber attack, or other high-profile event.

The crisis or emergency management portion of the BCP should address coordination with regulatory agencies, local and state officials, law enforcement, and first responders. Scenarios should detail disruptions, and not be confined to a single event, facility, or geographic area. Also, crisis or emergency management plans should address simultaneous disruptions of telecommunications and electronic messaging, including between the entity and third-party service providers.

Management should designate key personnel from applicable departments to act during a crisis or emergency situation, commensurate with the entity's size and complexity. Designated personnel should be authorized to make decisions in a timely manner. Key personnel may include:

- Senior management for leadership.
- Facilities management for safety and physical security.
- Human resources for personnel issues, travel, and relocation.
- Media relations for managing communications.
- Finance and accounting for funds disbursement and financial decisions, including unanticipated expenses.
- Legal and compliance for legal and regulatory concerns.
- IT, including information security, and operations for specific tactical responses.

Communication protocols for a crisis or emergency event should include contact lists and other viable methods to reach personnel and other stakeholders who may be called upon during a crisis. The contact list should be distributed and accessible to key personnel and should be verified and updated regularly. Management should be able to communicate with personnel located in isolated areas or dispersed across multiple locations. Procedures should enable employees to report their status in a centralized manner and obtain current information. Crisis or emergency management communication protocols should include provisions to contact the entity when normal communication channels are inoperable.

Notification systems can be manual or automated. In less complex environments, manual communication techniques, such as call trees, are often used; however, information gathering can

[37] The financial services industry uses the terms "crisis management" and "emergency management" interchangeably.

be time consuming, and responses can be unreliable in a crisis. Maintaining contact information can become unwieldy for large entities; therefore, automated solutions may be used.

VI Training

Action Summary

Management should implement a business continuity training program for all stakeholders.

Examiners should review for the following:

- Objectives of business continuity training.
- Alignment of business continuity training with strategies.
- Extent of targeted business continuity training provided to stakeholders, such as personnel, business continuity program staff, and the board.
- Format of the business continuity training program.
- Process for reviewing and updating the business continuity training program.

Management should include training as part of an effective business continuity program to educate stakeholders on resilience, business continuity goals, corporate-wide objectives, policies, and individual personnel roles and responsibilities. The board or senior management delegates a committee or individual to oversee the training program; however, the board should be responsible for the training program's effectiveness. Refer to the *IT Handbook's* "Management" booklet for additional information.

The training program should align with the entity's strategy and use a comprehensive, risk-based, multi-year approach, including interrelated programs (e.g., disaster recovery and third-party risk management). The frequency of exercises should depend on the size and complexity of the entity and the elements of the training program, risks, and testing program iteration, with all elements covered in a timely manner. Management should take inventory of the current skill sets for business continuity and identify and address any gaps. When appropriate, management should establish goals and objectives for supporting the entity's business continuity program as part of the performance management process. Some elements of the training program may include:

- Exercises.
- Current risks.
- Future risks.
- Recent failures.
- New programs/technologies.
- Organizational changes.
- Previous (exercise) lessons learned.

Training generally involves a conceptual understanding of business continuity, including testing methods, test results, and critical business functions. The training program should include conditions for activating the BCP and what to do when key personnel are unavailable. Training should selectively and purposely seek to validate plans and assumptions by testing the interactions of people, processes, and technology risks and vulnerabilities in a consequence-free exercise environment.

Training should be tailored to the target audience, addressing the needs of specific groups. Training participants should include the board, senior management, business process owners, and frontline personnel. For example, training for personnel who manage the business continuity program should be different than training for personnel not directly involved in recovery operations. Training should include significant business continuity concepts, interdependencies, disruption impacts, and operational resilience. When applicable, contractors involved with the business continuity program should also receive appropriate training.

The board should understand the business continuity program, testing initiatives, and key business continuity-related reports. Board training should occur regularly, or more frequently, based on significant changes to business processes, risks, BIA results, or lessons learned from incidents that have impacted the entity. Training methods may involve instructional classes, computer-based training, hands-on experience, lessons learned, and collaborating with other organizations. Role-based training includes cross-training personnel to compensate for significant absenteeism or operational disruptions, which may occur during an event. Training should reflect changes to the business continuity program as they occur.

VII Exercises and Tests

Action Summary

The board and senior management should provide for appropriate exercises and tests to verify that business continuity procedures support business continuity objectives. Exercises and tests should be used to validate one or more aspects of the entity's BCP.

Examiners should review for the following in exercise and testing plans:

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

Exercises and tests[38] help ensure that business continuity procedures support business continuity objectives. An exercise is a task or activity involving people and processes that is designed to validate one or more aspects of the BCP or related procedures. There are many different types of exercises, depending on the intended goals and objectives. Exercises may include scenario-driven simulations of BCP elements. For example, exercises may include performing duties in a simulated environment (i.e., functional) or be discussion based (i.e., tabletop).

A test is a type of exercise intended to verify the quality, performance, or reliability of system resilience in an operational environment. Tests are evaluation tools that use quantifiable metrics to validate the operability of an IT system or system component in an operational environment

[38] For purposes of this booklet, the term "exercise" represents both exercises and tests, unless the term "test" is specifically mentioned.

(e.g., what happens as a result of removing power from a system or system component). Tests may focus on backup and recovery options of systems. The degree of testing can vary, from individual system components up to comprehensive tests of all system components that support business operations. Effectively, the distinction between the two is that exercises address people, processes, and systems whereas tests address specific aspects of a system.

VII.A Exercise and Test Program

Management should develop a comprehensive exercise and testing program including objectives, and plans to validate the entity's ability to restore critical business functions. The entity's risk profile should influence the frequency, objectives, and documentation of the overall exercise schedule. The entity's consolidated exercise and test schedule should be reflective of exercise and test objectives and the overall exercise and test universe.[39]

Management should designate personnel with the authority to control the exercise or test and confirm milestones are met. Business line management should retain ownership and accountability for testing resilience of business operations, including applications and processes (both internal and external). While business line management should be responsible for testing its specific business processes and related interdependencies, managers should coordinate with personnel involved in the enterprise-wide business continuity process and support areas, such as IT and facilities management. Results should be reported to the board and senior management for inclusion in the enterprise-wide business continuity process.

Exercises and tests should occur either at appropriate intervals, when new risks are identified, or when significant changes affect the entity's operating environment. Significant changes can render existing test plans obsolete, so BCP(s) should be retested soon after the change. A comprehensive program allows management to evaluate business interdependencies and improve continuity and resilience.

A key objective for management should be to develop a testing process that validates the effectiveness of the entity's business continuity program, and identifies any deficiencies that may exist. Therefore, the exercise and test program should incorporate the following:

- A policy that includes strategies and expectations for exercise and test planning.
- Roles and responsibilities for implementation.
- Sufficient personnel to perform the exercise or test, provide oversight, and document the results.
- Precautions to safeguard production data, such as performing a backup before performing a test in a test environment, or testing during non-peak hours.
- Provisions for emergency stops (i.e., management's authority to stop an exercise if a real-life event occurs) and concluding exercises and tests.

[39] Similar to an audit universe, an entity's exercise and test universe is composed of an inventory of all business processes and system components that are compiled and maintained to identify areas for the exercise and test planning process.

- Verification of continuity and resilience process assumptions and the ability to process a sufficient volume of work during adverse operating conditions.
- Activities commensurate with the importance of the business process, as well as to critical financial markets.
- Result comparison against the BCP to identify gaps between the exercise or test process and recovery guidelines, with revisions incorporated where appropriate.
- Independent review of business continuity program and exercises and tests (internal and external).

VII.B Exercise and Test Policy

The entity's policies should define exercise and testing expectations and strategies. The policies should:

- Identify key roles and responsibilities.
- Establish minimum frequency, scope, and reporting requirements.
- Define documentation expectations that are consistent across business processes.
- Include a process for correcting deficiencies identified during exercises or tests.
- Address testing of communication and connectivity between the entity and third-party service providers.
- Detail participation with critical third-party service providers to confirm that entity personnel understand integration with recovery processes.

VII.C Exercise and Test Strategies

Management should develop exercise and testing strategies that demonstrate the entity's ability to support connectivity, functionality, volume, and capacity using alternate facilities. The strategies should include expectations for individual business lines and use of exercise and testing methodologies and scenarios. Testing strategies should encompass internal and external dependencies, including activities outsourced to domestic and foreign-based third-party service providers. Management should test all aspects of the entity's BCP. Strategies may include:

- A multi-year plan to execute the specific depth and breadth of exercises and tests to identify gaps in the program by using different methodologies and scenarios over time.
- Expectations for testing internal and external recovery dependencies.
- Assumptions, methodologies, and exercises used to develop the test strategies.

Lessons learned from natural disasters and other events show that for critical business functions, testing strategies should include transaction processing and functional testing to assess the recoverability of infrastructure, capacity, and data integrity. Regardless of the recovery strategy used, management should regularly test recovery provisions commensurate with the risk to the entity and, where applicable, the overall financial service sector.

VII.D Exercise and Test Objectives

The exercise and testing objectives should include resilience, system monitoring, and the recovery of business processes and critical system components. Tests can range from recovering a single file to a full-scale failover to another data center. Tests should include physical security, critical systems, multiple departments, and third-party relationships. Exercises should be sufficiently thorough to test dependencies and interrelationships among systems and third-party service providers. As the exercise and test process matures, it should become increasingly complex up to and including full-scale recovery exercises. Exercises and any associated tests should accomplish the following objectives:

- Build confidence that resilience and recovery strategies meet business requirements.
- Demonstrate that critical services can be recovered within agreed upon recovery objectives (RTOs and RPOs), including customer SLAs, and within MTDs.
- Establish that critical services can be restored in the event of an incident at the recovery location.
- Familiarize staff with recovery processes.
- Verify that personnel are adequately trained and knowledgeable of recovery plans and procedures.
- Confirm exercise and test plans remain compatible with the BCP and the entity's infrastructure.
- Identify gaps and deficiencies.

VII.E Exercise and Test Plans

Plans address the objectives and expectations of the exercise or test and outline the scenario and any assumptions or constraints that may exist. Exercises and test plans should include metrics to assess whether objectives are met. Plans should identify roles and responsibilities for participants, support personnel, and observers.[40] Exercise and test plans should be commensurate with the nature, scale, and complexity of the recovery objectives.

Management should receive and review third-party service provider exercise results, regardless of the entity's extent of participation. Management should consider the scope and results of these exercises in the entity's BCP. Management should evaluate third-party service providers' resilience and ability to recover critical services used by the entity if an event occurs. Refer to the *IT Handbook's* "Outsourcing Technology Services" booklet for additional information.

Test plans generally include the following:

- Roles and responsibilities for all test participants, including support personnel.
- A consolidated exercise and test schedule that encompasses all objectives.
- A specific description of objectives and methods.
- Identification of decision makers and succession plans.

[40] For the purposes of this booklet, the term "observers" does not constitute an independent review or audit function.

- Exercise and test locations.
- Exercise and test escalation procedures and the ability to adjust for simulated scenarios.
- Contact information.
- Metrics to measure the success or failure of the exercise or test.

Management should review the exercise and test results, update the BCP where appropriate, and report the results to the board or board-designated committee. Suggestions for improving test scenarios, plans, or scripts provided by test participants should be incorporated into the testing cycle, where appropriate.

VII.F Exercise and Test Scenarios

Management should develop realistic exercise and test scenarios, based on risks, which simulate disruptions in business functions and help management determine the ability to meet both business requirements and customer expectations. The goal should not be to execute "perfect" exercises without issues; instead, it should be to continuously strengthen the business continuity program and validate the BCP(s). Management should identify and document assumptions used in developing each scenario. The scenarios should include threats that could affect third-party service providers and others, such as significant business partners. Exercises and tests should include communication processes with applicable stakeholders. Exercises demonstrate not only the ability to failover to an alternate site but also validate recovery objectives. Management should consider all reasonably foreseeable risks to connectivity and service-level agreements between the entity's facility(ies), third-party service provider facilities, and with any applicable counterparties (i.e., entities on the other side of a financial transaction) with whom they transact significant or critical business.

Scenarios may include:

- Simultaneous attacks affecting both the entity and a third-party service provider.
- Cyber-related events (e.g., isolated malware attack, DDoS attack, data corruption, or a full-scale data center outage).
- Use of mirrored sites to demonstrate that alternate sites can effectively support customer-specific requirements, work volumes, and site-specific business processes.
- Processing a full day's work at peak volumes.

To the extent possible, scenarios should include only resources that would be available during an event (e.g., backup files or equipment at the alternate site). Considering data and systems helps management verify the integrity of data backups (including access to encrypted data) and the adequacy of off-site systems and supplies, such as workstations and procedure manuals.

Management should develop exercise and test scripts to guide participants and meet objectives. Each script should document the procedures, which may include:

- Applications, business processes, systems, or facilities reviewed.
- Sequential steps for employees or external parties to perform.

- Procedures to guide manual work-around processes.
- A detailed schedule for completion.
- Methods for participants to record results, quantifiable metrics, and any issues.

VII.G Exercise and Test Methods

Exercises and tests help management validate continuity and resilience of technology components, including systems, networks, applications, and data, that support critical business functions. The type or combination of methods should be determined by the entity's size and complexity and the nature of its business. The DHS offers assistance and examples of testing methods,[41] which are available to all entities and may be helpful when developing exercises and tests. Rigorous exercise methods and increased frequency help provide greater confidence in the continuity and resilience of business functions. While comprehensive exercises involve greater investments of time, resources, and coordination, the benefit is a more accurate assessment of recovery capabilities if a disaster occurs. This assists management in assessing the resilience of systems and responsiveness of the individuals involved in the recovery process. Comprehensive testing of all critical functions and applications allows management to identify potential problems; therefore, management should use one of the more thorough testing methods discussed in this section to verify the BCP's viability

While names for exercises and tests may be different, or used interchangeably, this booklet lists the most commonly encountered elements in the following subsections.

VII.G.1 Full-Scale Exercise

Full-scale exercises (sometimes called a full interruption or comprehensive exercise) help management validate internal and external interdependencies between critical business functions, information systems, and networks (e.g., for critical functions, exercises should include transaction processing and functional testing). Integrated exercises move beyond comprehensive exercises to include testing with internal and external parties and the supporting systems, processes, and resources. Management should periodically reassess and update exercise and test plans to reflect changes in the business and operating environment.

A full-scale exercise simulates full use of available resources (personnel and systems) prompting a full recovery of business processes. The goal of a full-scale exercise is to determine whether all critical systems can be recovered at the alternate processing site and whether personnel can implement the procedures defined in the BCP. For example, a full-recovery exercise might simulate the complete loss of primary facilities. Features of a full-scale exercise may include the following:

[41] As members of an established sector of critical infrastructure, financial institutions can leverage testing constructs implemented by the DHS. The Homeland Security Exercise and Evaluation Program is the DHS policy and guidance for designing, developing, conducting, and evaluating exercises. The program provides a threat- and performance-based exercise process that includes a mix and range of exercise activities through a series of four reference manuals to establish exercise programs and design, develop, conduct, and evaluate exercises.

- Engaging personnel from all business units to participate and interact with internal and external management response teams.
- Validating the crisis or emergency management process is operating as designed.
- Verifying personnel knowledge and skills.
- Validating management response and decision-making capability.
- Coordinating participants and decision makers.
- Validating communication protocols.
- Conducting activities at alternate locations or facilities.
- Processing data using backup media or alternative methods.
- Completing actual transactional volumes or an illustrative subset.
- Performing recovery exercises over a sufficient length of time to allow issues to unfold as they would in a crisis.

VII.G.2 Limited-Scale Exercise

A limited-scale exercise is a simulation involving applicable resources (personnel and systems) to recover targeted business processes. The goal of a limited-scale exercise is to determine whether targeted systems can be recovered and whether personnel understand their responsibilities as defined in the plan. Features of a limited-scale exercise may include the following:

- Implementing a plan appropriate to the scenario.
- Verifying personnel knowledge and skills.
- Validating management response and decision-making capability.
- Executing on-the-scene coordination and decision-making roles.
- Verifying whether participants can connect to alternate system(s).
- Conducting activities at alternate locations or facilities.
- Testing communication and remote access capability (e.g., switching to alternate equipment or telecommuting).

While limited-scope exercises are important, they often have limited participation (e.g., departmental personnel only) or scope and do not necessarily allow management to gauge interconnectivity and how systems and capacity would support daily activities and workloads.

VII.G.3 Tabletop Exercise

A tabletop exercise (sometimes referred to as a walk-through) is a discussion during which personnel review their BCP-defined roles and discuss their responses during an adverse event simulation. The goal of a tabletop exercise is to determine whether targeted plans and procedures are reasonable, personnel understand their responsibilities, and different departmental or business unit plans are compatible with each other. By themselves, tabletop exercises are likely insufficient to validate recovery capabilities, because they are limited to a discussion-based analysis of policies and procedures.

Features of a tabletop exercise may include the following:

- Engaging operational and support personnel who are responsible for implementing the BCP.
- Practicing and validating specific functional response capabilities.
- Demonstrating knowledge, skills, team interaction, and decision-making capabilities.
- Role playing with simulated responses, critical steps, recognizing difficulties, and resolving problems.
- Clarifying critical plan elements, as well as problems noted during exercises.
- Creating action plans to correct issues.

VII.G.4 Tests

Management uses tests to verify the quantifiable performance and reliability of system resilience. The goal of testing is to determine whether system resilience conforms to the BCP and stated recovery objectives. Test methodologies and frequencies should align with the risk associated with the business function as well as the entity's testing strategies and objectives. Management should clearly define the characteristics of a successful test, which may include the following:

- Validating RPOs, RTOs, and MTDs.
- Demonstrating recoverability at peak volumes.
- Confirming that systems can support critical business processes (e.g., transfer to alternate sites, increased workloads, manual workarounds, and communication).
- Integrating technologies that support critical business activities, including data replication, recovery, and off-site storage.
- Testing backup data to assess integrity and availability.
- Certifying facility controls (e.g., environmental, backup power, and physical security).
- Verifying workspace restoration (e.g., network connectivity and communications).

VII.H Industry Exercises and Resilience

Given the potential for and nature of widespread and systemic disruptive events, public and private sector groups[42] conduct exercises with their members to verify resilience across the financial industry. These exercises simulate significant regional or industry-wide emergencies, and members are encouraged to use backup sites and test their recovery capabilities. In addition to financial institutions, these coordinated tests often include participation by third-party service providers and government agencies. There are several methods for entities of all sizes to participate, such as through third-party service provider user groups or industry initiatives. For example, industry initiatives include the U.S. Department of the Treasury's Hamilton Series (national and regional series) and the FS-ISAC's Cyber-Attack Against Payment Systems (CAPS). The results of these exercises are usually available to members of industry and regulatory groups, and summaries may be available to the public.

[42] Public and private groups include the FS-ISAC, Financial Services Sector Coordinating Council (FSSCC), Financial Systemic Analysis & Resilience Center (FSARC), Financial and Banking Information Infrastructure Committee (FBIIC), and some regional coalitions.

Examiners should understand that opportunities to participate in such exercises may be limited. The *Financial Sector Cyber Exercise Template*[43] is publicly available from the U.S. Department of the Treasury, and management can use it to help verify the entity's own response capabilities and evaluate how it would respond during similar situations. Additionally, the template and results may be used as resources to validate exercise and testing assumptions and scenarios.

VII.I Third-Party Service Provider Testing

Third-party service providers deliver critical services to many entities and should be included in the enterprise-wide exercise and testing program. The extent of inclusion in the entity's program should be based on the criticality of the third-party service provider and the business function. Management should obtain assurance that third-party service providers are resilient and have adequate infrastructure and personnel to restore critical services consistent with business and contractual requirements. The right to perform or participate in testing with third-party service providers should be included in the contract governing the entity's relationship with the third party.

Management should actively participate in the entity's third-party service providers' testing programs and should verify that testing strategies include likely significant disruptive events. Third-party service providers should be transparent about testing parameters and results because not all clients can participate in every testing activity (e.g., when there is a large client volume) and some exercises and tests may not be relevant to the services provided to a specific customer. Management should request and receive test results and reports, remediation action plans and status reports upon their completion, and related analysis or modeling. Management should track and resolve any issues identified during the exercise in a timely manner, according to the severity of the issues. Any test results that affect the entity should be presented to its board. In most instances, equating one entity's recovery experience with another's does not guarantee similar results; therefore, management should perform its own analysis. Refer to the *IT Handbook's* "Outsourcing Technology Services" booklet for additional information.

VII.J Testing for Core and Significant Firms

Management at core and significant firms should develop verification strategies and execute exercise and testing activities to validate that the entity implemented sound recovery practices consistent with the entity's role in the industry. Additionally, management should consider the impact of an event at its entity on the entire financial sector. The elements discussed in the *Sound Practices Paper* supplement the agencies' respective policies and other guidance on business continuity planning. Entities not designated as core and significant firms may also consider guidance from the *Sound Practices Paper* as a model for enhancing their testing processes.

Identification of external interdependencies is important given the sector's reliance on core and significant firms. Internal testing activities should include systems that support critical market activities in which these firms are core or significant. Exercise and testing activities should confirm that such critical clearing and settlement activities could be recovered within RTOs.

[43] Refer to the U.S. Department of the Treasury's *Financial Sector Cyber Exercise Template*.

Industry standard time frames are continually adjusted based on available technology, pertinent risks, and industry initiatives. Management should adjust its RTOs to be in line with industry standard time frames. Furthermore, management should design testing activities to demonstrate the ability to perform the following activities if a wide-scale disruption affects the accessibility of key personnel:

- Complete pending material payments and transactions.
- Access funding.
- Manage material open risk positions.
- Make related entries to books and records.
- Validate internal and external communication protocols.
- Ensure connectivity, functionality, and volume capacity.

Management should test with the relevant core firms from their alternate sites and meet testing standards the core firms establish specifically for significant firms and for participants more generally. Management at core and significant firms should perform testing to assess the effectiveness of their recovery strategies. Management is also encouraged, to the extent practical, to participate in pertinent market-wide and cross-market tests[44] that validate connectivity from alternate sites and include transaction, settlement, and payment processes.

Examination and supervisory activities may include evaluations of verification strategies and testing plans to assess whether core and significant firms, which are the focus of the *Sound Practices Paper*, have achieved the resilience to protect the financial system from a wide-scale disruption.

VII.K Post-Exercise and Post-Test Actions

Management should document issues identified during exercises and tests and create action plans with target dates for resolving issues. Exercise and test results should be analyzed and compared with the objectives and success criteria in the exercise and test plans, and reported to appropriate levels of management. For those items not remediated, management should document decisions to accept risks identified during the exercises.

Additionally, management should test corrective actions implemented as a result of a failed recovery objective or to address major issues encountered. Management may choose to retest during or before the next regularly scheduled exercise depending on an issue's severity. Business line management should update the BCP based on test results and adjust the BCM process, including the exercise and testing program. Finally, management should submit regular reports to the board on the exercise and testing activities and whether the BCP meets the entity's recovery and resilience objectives.

Exercise and test results may include the following documentation:

[44] Industry and cross-market tests are often conducted by associations such as the Securities Industry Association, Bond Market Association, and Futures Industry Association. These associations are mentioned for illustrative purposes only; this note is not an endorsement of any of these associations.

- Dates and locations.
- An executive summary comparing objectives and results.
- Material deviations from the plans, including whether intended participation was achieved.
- Problems identified and lessons learned.
- Assignment of responsibility for timely resolution of issues identified.

Management should periodically analyze results and issues to determine whether problems can be traced to a common source, such as inadequate change control procedures. Fixing the root cause of the problem may help resolve many underlying issues.

VIII Maintenance and Improvement

Because risks and technology often change, management should regularly review and update the business continuity program to reflect the current environment. Periodic reviews allow management to align the business continuity processes with business objectives. Management should use this information to prioritize and focus on system and process corrections and enhancements. Triggers that prompt maintenance and improvement of the business continuity program may include the following:

- Changes in enterprise strategies.
- New or reconfigured products, services, or infrastructure.
- Changes in products and services offered by third-party service providers.
- Deficiencies identified in third-party service provider business continuity processes.
- New legislation, regulatory requirements, or resilience practices.
- Results of operational metric analysis (e.g., key risk indications, key performance indicators).
- Early warning indicators that may identify potential continuity events, crises, or incidents (e.g., frequency and severity of storms, increased cyber attacks, or increases in customer service calls).
- Variances between budgeted and actual business continuity expenses.
- Results from exercises and tests, and lessons learned.
- Changes in the threat landscape (e.g., new capabilities, intent of threat actors).
- Recommendations (e.g., from audits, vulnerability assessments, and penetration tests).

To determine the extent of changes to the business continuity program, BCM program personnel should contact business unit managers regularly to assess the nature of any changes to the business, structure, systems, software, hardware, personnel, or facilities. Management at smaller, less complex entities may perform this function informally; however, the maintenance and improvement concepts remain valid for those entities.

The business continuity program should be reviewed for accuracy and completeness at periodic intervals. Likely areas[45] that should be adjusted within the BCP may include:

[45] The concept of business continuity program review elements aligns with NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*. While this document pertains to federal information systems, the principles are relevant for non-federal information systems.

- Operational requirements.
- Security requirements.
- Technical procedures.
- Hardware, software, and other equipment.
- Team member contact information.
- Vendor contact information.
- Alternate and off-site facility requirements.
- Vital records.

When updating the business continuity program, management should document, track, and resolve any changes. Management should document, analyze, and review lessons learned from adverse events. Understanding these lessons allows management to prepare for future adverse events. Documented procedures for incorporating lessons learned should include:

- Identifying the failure(s).
- Determining the cause(s).
- Evaluating potential solutions.
- Implementing timely corrective actions as appropriate.
- Recording and reviewing corrective actions taken.

As part of the maintenance and improvement process, management should maintain version control of key business continuity documents and ensure that the latest versions are readily available to appropriate personnel. The level of detail in documentation should be commensurate with the nature of the entity's operations. This information should be accessible during an event and can be maintained by BCM program management and personnel. The BCM documentation should include evidence substantiating periodic updates of the BIA, risk assessment, and BCP(s).

Business continuity document management processes may include the following:

- Roles and responsibilities.
- Document control.
- Version control.
- Storage and disposal.

Management should follow the entity's information security standards for confidential or sensitive information contained within business continuity documentation. Additionally, management should maintain backup copies of relevant business continuity documentation in the event that the primary repository becomes inaccessible.

IX Board Reporting

Action Summary

The board should establish expectations for management's business continuity reporting, regularly monitor business continuity and resilience activities, and provide credible challenges to management.

Examiners should review reports and meeting minutes and conduct discussions with management on the following:

- BIA.
- Risk assessment.
- BCP.
- Resilience.
- Exercise and test results.
- Identified issues.
- Strategy updates.
- Audit results.
- Metrics, including key risk indicators and key performance indicators for BCM and resilience.

As illustrated in figure 1, management should report on the status of business continuity to the board, completing the BCM cycle. Reports should include a written presentation providing the BIA, risk assessment, BCP, exercise and test results, and identified issues. Additionally, reports should include regular strategy updates based on changes in personnel, roles and responsibilities, and business operations. The board should monitor business continuity and resilience activities regularly to verify that they are implemented as envisioned and reviewed periodically or as changes dictate. The board should be updated in a timely manner based on lessons learned. Board minutes should reflect business continuity discussion (including credible challenges) and approvals.

Appendix A: Examination Procedures

Examination Objective

These examination procedures (also known as the work program) are intended to assist examiners in determining the quality and effectiveness of the business continuity process on an enterprise-wide basis or across a particular line of business. Additionally, these procedures assist examiners in evaluating whether business continuity testing demonstrates the entity's ability to meet its business continuity objectives including management's ability to recover, resume, and maintain operations after disruptions, ranging from minor outages to full-scale disasters. Examiners are not limited by the examination procedures presented here and may choose to use only certain components of the work program based on the size, complexity, and nature of the entity's business. Depending on the examination objectives, a line of business can be selected to sample how the entity's continuity planning or testing processes work individually or for a particular business function or process.

Objective 1: Determine the appropriate scope and objectives for the examination.

1. Review past reports for outstanding issues or previous problems. Consider the following:

    a. Regulatory reports of examination.
    b. Internal and external audit reports.
    c. Reports by independent risk management.
    d. Business continuity tests.
    e. Regulatory, audit, and business continuity reports on third-party service providers.

2. Review management's response to issues identified during or subsequent to the last examination. Consider the following:

    a. Adequacy and timing of corrective action.
    b. Resolution of root causes rather than symptoms.
    c. Status of uncorrected issues.
    d. Retesting to validate corrective action.

3. Interview management and review responses to pre-examination information requests to identify changes to technology infrastructure or new products and services that could affect business resilience. Consider the following:

    a. Products or services delivered to either internal or external users.
    b. Network topology or diagram, including changes to configuration or components and all internal and external connections.
    c. Hardware and software inventories.
    d. Loss, addition, or change in duties of key personnel.
    e. Third-party service providers and software vendor listings.
    f. Changes to internal business processes.
    g. Changes based on industry changes or threat intelligence.

4. Review newly identified threats and vulnerabilities to the continuity of operations. Consider the following:

    a. Technology and security vulnerabilities.
    b. Internally identified threats.
    c. Externally identified threats (e.g., cybersecurity alerts, pandemic alerts, or emergency warnings published by information-sharing organizations and government agencies).

Objective 2: Determine whether the board and senior management promote effective governance of business continuity through defined responsibilities, accountability, and adequate resources to support the program. (II.A, "Board and Senior Management Responsibilities")

1. Determine whether business continuity policies and critical business procedures are:

    a. Up-to-date and reflective of the current business environment.
    b. Communicated effectively throughout the entity.
    c. Available during adverse events.
    d. Securely maintained.

2. Determine whether the board and senior management provide leadership when overseeing business continuity, including:

    a. Evaluating continuity risk.
    b. Setting short- and long-term continuity objectives.
    c. Adopting appropriate policies and procedures.
    d. Evaluating continuity performance.
    e. Adjusting programs and operations in response to test results and actual events.

3. Determine whether management strengthens resilience through the following:

    a. Assessing continuity risk.
    b. Resilience planning.
    c. Testing business continuity plans.
    d. Incorporating lessons learned from testing and events.
    e. Considering resilience in business functions and the design of existing operations and new products and services.

4. Determine whether board oversight includes the following:

    a. Assigning business continuity responsibility and accountability.
    b. Allocating resources to business continuity (e.g., personnel, time, budget, and training).
    c. Aligning BCM with business strategy and risk appetite.
    d. Understanding business continuity risks and adopting appropriate policies and plans to manage events.
    e. Understanding business continuity operating results and performance.

f. Providing a credible challenge to management responsible for the business continuity process (e.g., the board minutes provide evidence of active discussions).
g. Establishing a provision for management intervention if timeliness for corrective action is not met.

5. Determine whether management oversight of business continuity includes the following:

a. Defining business continuity roles, responsibilities, and succession plans.
b. Allocating knowledgeable personnel and sufficient financial resources.
c. Validating that personnel understand their business continuity roles.
d. Establishing measurable goals against which business continuity performance is assessed.
e. Designing and implementing a business continuity exercise strategy.
f. Confirming that exercises, tests, and training are comprehensive and consistent with the exercise strategy.
g. Resolving weaknesses identified in exercises, tests, and training.
h. Meeting regularly to discuss policy changes, testing plans, and training.
i. Assessing and updating business continuity strategies and plans to reflect the current business conditions and operating environment for continuous improvement.
j. Aligning plans between business units across the enterprise.
k. Coordinating plans and responses with external entities.

Objective 3: Determine whether the board and senior management engage audit or other independent review functions to review and validate the design and operating effectiveness of the BCM program. (II.B, "Audit")

1. Determine whether the board and senior management have engaged audit (or an independent review) to validate the design effectiveness of the business continuity program and whether controls are operating effectively.

2. Determine whether audit reports to the board and provides an assessment of management's ability to manage and control risks related to continuity and resilience.

3. Determine whether audit leverages SOC reports and other external artifacts from third-party service providers, as appropriate.

4. Determine whether the board or management validates that the auditor is qualified to carry out the review and is independent of the business continuity or related functions.

5. Evaluate the audit coverage of business continuity, whether through a general controls audit, during audits of business lines, or as a stand-alone business continuity audit. Audit coverage should include the following:

a. The reasonableness and comprehensiveness of the BIA and business continuity risk assessment(s).
b. The reliability, adequacy, and effectiveness of continuity and resilience controls.

c. The effectiveness of risk mitigation efforts.
d. Whether test plans achieve their stated objectives based on reasonable assumptions.
e. Audit monitoring of exercises and tests, reviewing test plans and results, and verifying that any issues are identified and appropriately escalated.
f. Assessment of the business continuity program effectiveness.

Objective 4: Determine whether management developed an appropriate and repeatable BIA process that identifies all business functions and prioritizes them in order of criticality, analyzes related interdependencies, and assesses a disruption's impact. (III.A, "Business Impact Analysis")

1. Determine the process through which management inventories business functions. Management may use the following artifacts to identify the functions:

   a. Organizational charts.
   b. Work flows (also called process maps).
   c. Interview notes.
   d. Network diagrams/topologies.
   e. Data flow diagrams.

2. Determine whether management inventoried the critical assets and infrastructure upon which business functions depend, including the identification of single points of failure. Critical assets and infrastructure may include the following:

   a. People.
   b. Hardware.
   c. Software.
   d. Cash reserves.
   e. Supporting activities (e.g., technology support, payroll, contracting).
   f. Supporting software (e.g., email, office productivity suites).
   g. Network connectivity.
   h. Communication lines.
   i. Facilities.
   j. Utilities.
   k. Infrastructure and services provided by third-party service providers.

3. Determine whether the interdependency analysis includes the following:

   a. Internal systems and business functions, including services, production processes, hardware, software, and application programming interfaces, data, and vital records.
   b. Third-party service providers, key suppliers, and business partners.
   c. Telecommunications single points of failure.
   d. Power single points of failure.

4. Review the BIA to determine whether the prioritization of business functions is reasonable. Consider management's ability to do the following:

a. Determine the operational and financial impacts of a disruption.
b. Aggregate loss impacts and determine a rating scale to indicate impact severity.
c. Reconcile BIA and risk assessment results with prioritization and document whether the reconcilement is adequate.

5. Determine whether the BIA produces sufficient information to estimate the following:

a. Recovery point objectives (RPO).
b. Recovery time objectives (RTO).
c. Maximum tolerable downtime (MTD).

Objective 5: Determine whether management conducts a risk assessment sufficient to evaluate the likelihood and impact of potential disruptions and events. (III.B, "Risk Assessment")

1. Review risk assessment(s) to determine whether management has identified all reasonably foreseeable hazards and threats to the continuity and resilience of the entity. Examples of risks can include:

a. Natural:
   - Flood, earthquake, hurricane, tornado, and other weather events.
b. Technological:
   - Technological: Malware, cyberattack, and hardware and software failure.
   - Operational: Critical infrastructure disruption (e.g., transportation and water systems).
c. Adversarial or human-caused:
   - Personnel: Strike, pandemic, and malicious insider.
   - Social: Terrorism, vandalism, looting, riots, and protests.
d. Combination:
   - Facility: Fire, power outage, and loss of access.
   - Geographic-related: Proximity to railroad or highways used for transport of hazardous materials, proximity to airports, traffic difficulties, and other issues.
   - Third-party: Services concentrated in a limited number of third-party service providers.

2. Determine whether management identifies BCM risks and coordinates risk identification efforts throughout the entity to identify systemic threats.

a. Determine whether management identifies and inventories the following:
   - Internal and external assets.
   - Types of threats and hazards.
   - Existing controls.
b. Verify that the risk assessment includes the identification of cybersecurity risks and results of information security risk assessments.
c. Assess whether management obtains information about hazards and threats from external sources.
d. Determine whether management considers threat intelligence in risk identification efforts.

3. Ascertain whether management identifies interconnectivity points between the entity and its third-party service providers, as well as interconnectivity between other entities and their third-party service providers (i.e., supply chain).

4. Determine whether the risk assessment includes the impact and likelihood of potential disruptive events, including worst-case scenarios.

5. Determine whether management identifies and analyzes gaps between the entity's risk exposure and the risk appetite, and documents any controls implemented to mitigate the residual risk.

Objective 6: Determine whether the entity's risk management strategies are designed to achieve resilience. (IV.A, "Resilience")

1. Verify that management has evaluated strategies and resource needs and allocates appropriate resources to achieve resilience:

    a. Appropriate personnel and skillsets to carry out the functions.
    b. Time to identify and implement solutions.
    c. Budget to accomplish resilience goals and objectives.

2. Determine whether management has implemented physical resilience measures that:

    a. Establish redundant communications between branches and data centers.
    b. Identify multiple power sources.
    c. Geographically diversify key entity locations.

3. Determine whether management has implemented data and cyber resilience measures that:

    a. Maintain confidentiality, integrity, and availability for backup, replication, and production environments.
    b. Implement appropriate backups and sufficient documentation and retention periods for each iteration of data backup.
    c. Periodically reassess backup and recovery strategies as technology and threats change.
    d. Maintain an accessible, off-site repository of software, configuration settings, and related documentation.
    e. Establish procedures to recover critical networks and systems, including:
        - Backup types (physical or virtual).
        - Backup levels (full, incremental, or differential).
        - Update and retention cycle frequencies.
        - Software and hardware compatibility reviews.
        - Data transmission controls.
        - Data repository maintenance.
    f. Protect offline data backups from destructive malware that may corrupt production and online backup versions of data.

4. Determine whether management documented and implemented, as appropriate, the following resilience measures for personnel:

    a. Staffing and skills needed to operate critical functions related to business continuity.
    b. Lodging arrangements for displaced employees and their families.
    c. Basic necessities and services for displaced employees, including water, food, clothing, childcare, and transportation.
    d. On-site medical support and mobile command centers.
    e. Secure telecommunication options if employees work from an alternate location.
    f. Designated emergency personnel, including critical business process-level employees (i.e., those necessary to ensure all critical business operations function appropriately).

5. Determine whether management documented and implemented, as appropriate, the following resilience measures for third-party service providers:

    a. Considered disruptive events that threaten the operational resilience and viability of the entity's third-party service provider.
    b. Assessed the entity's immediate or short-term space, systems, and personnel capacity to assume or transfer failed operations.
    c. Assessed critical third-party service providers' susceptibility to multiple event scenarios.
    d. Reviewed third-party service provider's resilience capabilities, including available test and SOC reports.
    e. Verified that SLAs with third-party service providers align with the entity's recovery objectives.
    f. Established plans for the resilience of third-party service providers supporting critical operations.

6. Determine whether management documented and implemented, as appropriate, the following resilience measures for telecommunications:

    a. Identifying and mitigating single points of failure across the entity's infrastructure.
    b. Developing and maintaining a plan to address an outage in the telecommunications lines with its primary third-party service providers.
    c. Establishing redundant telecommunications links with each of the entity's third-party service providers through a contractual arrangement that allows either party to switch its connection to an alternate communication path.
    d. Reviewing the entity's third-party service providers' plans and determining whether critical services can be restored within time frames acceptable to the entity.
    e. Developing guidelines, commensurate with the entity's size, complexity, and risk profile, to diversify connections to mitigate the risk of a telecommunications failure.
    f. Assessing the communications technology that bridges the transmission distance between the telecommunications service provider and the entity for single points of failure.
    g. Monitoring relationships with telecommunications providers to manage risks.
    h. Evaluating communications and resilience needs to ensure branch communications.

i. Inquiring about the physical paths used by telecommunications providers and verifying that system redundancies have been properly implemented.

7. Determine whether management considers the following as part of the entity's power resilience strategies:

   a. Alternate energy sources (e.g., generators and multiple power grids).
   b. Fuel requirements, both for fuel on-hand and contracts with suppliers for deliveries during events.
   c. Continued maintenance of generators.
   d. Testing of generators.

8. Verify that BCM activities align with the entity's change management process.

Objective 7: Determine whether the entity's BCM includes communication protocols. (IV.B, "Communications")

1. Determine whether management considers, plans for, and prepares multiple mechanisms to communicate with personnel and other stakeholders while maintaining appropriate controls to safeguard customer information. Other stakeholders could include:

   a. Regulatory agencies (federal and state).
   b. Emergency responders.
   c. Law enforcement.
   d. Financial sector trade associations.
   e. Information-sharing entities (e.g., FS-ISAC).

Objective 8: Assess the appropriateness of the entity's enterprise-wide BCP. (V, "Business Continuity Plan")

1. Verify that management implemented a comprehensive BCP that is reflective of the entity's risk environment. The BCP should outline the following:

   a. Roles, responsibilities, and required skills for entity personnel and third-party service providers.
   b. Solutions to various types of foreseeable disruptions, including those emanating from cyber threats.
   c. Escalation thresholds.
   d. Immediate steps to protect personnel and customers and minimize damage.
   e. Prioritization and procedures to recover functions, services, and processes.
   f. Critical information protection (e.g., physical, electronic, hybrid, and use of off-site storage).
   g. Logistical arrangements (e.g., housing, transportation, or food) for personnel at the recovery locations.
   h. Network equipment, connectivity, and communication needs, including entity-owned and personal mobile devices.

i. Personnel at alternate sites, including arrangements for those permanently located at the alternate facility.
j. Scope and frequency of testing.
k. Resumption of a normalized state for business processes.

2. If management outsources the BCP's development, verify that management maintains oversight and ownership of the BCP.

   a. Determine whether management verified the third-party service provider's qualifications and expertise.
   b. Verify that entity management worked with the third-party service provider to design executable and viable strategies.
   c. Verify that the plan reflects the entity's current products, business processes, and third-party service providers.
   d. Determine whether roles and responsibilities reflect the entity's current organizational structure.

3. Determine whether the BCP includes event management procedures that detail reasonably foreseeable event types, and those procedures include threshold metrics and response methods.

   a. Verify that procedures explain how to report an event to management and the situations that warrant notification.
   b. Determine whether management (either an individual or team) has implemented procedures to communicate with both internal and external stakeholders.
   c. Verify that event management processes include event response procedures that are appropriate to the event.

4. Assess management's protocols for operations continuity and system recovery. Verify that procedures are clear, concise, accessible, and can be implemented in an emergency. Verify the BCP includes procedures for the following:

   a. Manual steps for critical functions, as applicable.
   b. Alternate identity verification methods.
   c. Fraud identification and suspicious activity reporting.
   d. Other procedures as applicable. Examples may include:
      - Addressing customer service requests during downtime.
      - Tracking daily transactions.
      - Reconciling general ledger accounts.
      - Documenting operational tasks.
      - Posting entries after system recovery.
      - Maintaining backup records to provide customer account information (account numbers, customer names, addresses, account status, and account balances).

5. Verify that the BCP lists alternatives for core operations, facilities, infrastructure systems, suppliers, utilities, interdependent business partners, and key personnel.

a. Verify that the BCP includes site relocation for short-, medium-, and long-term scenarios.
b. Determine whether management considers scalability.
c. Verify that recovery alternatives can accommodate the services and processing capabilities affecting critical operations, including:
   - Core processing.
   - Check processing and imaging.
   - Commercial cash management.
   - Mailing, faxing, and printing.
   - Customer identification.
   - Data center activities.

6. Verify that the BCP includes procedures for coordination with the first responders and local and state government agencies, when appropriate.

7. Verify that the BCP includes procedures to establish an alternate physical location(s) where personnel and customers can go to conduct business, if appropriate.

8. Determine whether the BCP addresses alternate arrangements in the event payment systems fail (e.g., ATMs, funds transfers, electronic banking, remote deposit capture, mobile capabilities).

   a. Determine whether the BCP addresses processes for retrieving and transmitting transactions when payment systems are disrupted (e.g., manual procedures for calling in or faxing wire or automated clearing house requests to correspondent banks; mitigating strategies for web-based systems; or third-party software used to perform transactions).
   b. Determine whether management verifies that redundant electronic payment systems and equipment (e.g., tokens and routers) are included at recovery sites for activation and that documentation is maintained for timely posting of entries when systems are recovered.
   c. Determine whether instant issue cards are utilized and card company security procedures are implemented to limit potential fraud.

9. Verify that the BCP addresses the entity's cash management requirements. Procedures may include:

   a. Pre-established cash delivery arrangements.
   b. Plans for increases in branch traffic when ATMs are unavailable.
   c. Plans for the entity’s operational cash needs.
   d. Temporary purchase authority guidelines.
   e. Expense reimbursement options for personnel.
   f. Higher-limit credit cards or separate checking accounts with designated individuals who can sign checks in emergency situations.

10. Determine whether management established an incident response process. As part of incident management planning, determine whether management does the following:

a. Aligns incident response procedures with other related processes (e.g., cybersecurity, network operations, and physical security).
b. Considers incident response procedures during the development of the business continuity strategy.
c. Leverages routine processes (e.g., vulnerability management and network monitoring) to anticipate potential incidents, including cyber incidents.

11. Verify that management developed a coordinated disaster recovery strategy for data centers, networks, servers, storage, service monitoring, user support, and related software. Verify that procedures address the following:

a. Security controls and protocols, including physical and logical.
b. Procedures for restoring backlogged activity or lost transactions to identify how transaction records will be brought current within expected recovery time frames.
c. Instructions to access the repository of critical information when the primary facility is unavailable.

12. Verify whether management designates key personnel from applicable departments to act during a crisis or emergency situation. Key personnel may include:

a. Senior management for leadership.
b. Facilities management for safety and physical security.
c. Human resources for personnel issues and travel.
d. Media relations for managing communications.
e. Finance and accounting for funds disbursement and financial decisions, including unanticipated expenses.
f. Legal and compliance for legal and regulatory concerns.
g. IT, including information security, and operations for specific tactical responses.

13. Determine whether management established a crisis or emergency management process. Verify whether the BCP addresses the following:

a. Coordination with regulatory agencies, local and state officials, law enforcement, and first responders.
b. Disruptions not confined to a single event, facility, or geographic area.
c. Simultaneous disruptions of telecommunications and electronic messaging, including between the entity and third-party service providers.
d. Crisis or emergency management communication protocols, including the designation of a spokesperson(s) to communicate with the news media, as appropriate.

Objective 9: Determine whether the BCM program includes training and awareness to educate stakeholders about the entity's continuity objectives and BCM goals. (VI, "Training")

1. Verify that the training program aligns with the entity's BCM strategy. Determine whether management does the following:
   a. Inventories the current skillsets for BCM and identifies and addresses any training gaps.

b. Establishes goals and objectives for supporting the BCM program as part of the entity's performance management process.
c. Implements a training program to educate stakeholders about the BCM goals and objectives. Elements may include:
   - Exercises.
   - Current risks.
   - Future risks.
   - Recent failures.
   - New programs/technologies.
   - Organizational changes.
   - Previous (exercise) lessons learned.

2. Assess whether management tailors training to the target audience, based on the audience's needs. The target audience could include:

   a. Board members.
   b. Senior management.
   c. Business process owners.
   d. Frontline personnel.
   e. Contract personnel, as applicable.

3. Validate that management incorporates significant business continuity concepts, interdependencies, disruption impacts, and operations resilience into the training program.

4. Verify that the BCM training program, including board training, is updated as significant changes occur.

Objective 10: Determine whether the exercise and testing program is sufficient to allow management to assess the entity's ability to meet its continuity objectives. (VII, "Exercises and Tests")

1. Determine whether management implemented a comprehensive exercise and testing program, objectives, and plans to validate the entity's ability to restore critical business functions.

2. Verify that the program is appropriate for the entity's risk profile. Assess whether the entity's consolidated exercise and test schedule is reflective of exercise and test objectives and the overall exercise and test universe.

3. Determine whether management covers all of the functions in the exercise and test universe according to its established timeframes (e.g., all processes are covered annually or every three years).

4. Determine whether management has designated personnel with the authority to control the exercise or test and confirm exercise and test milestones are met.

5. Verify that business line management retains ownership for testing its specific business processes and coordinates with personnel involved in the enterprise-wide BCM process and support areas.

6. Verify that exercises and tests occur at appropriate intervals, or when significant changes affect the entity's operating environment.

7. Verify that management developed a process that is sufficiently robust to confirm the effectiveness of the entity's business continuity program. Therefore, the exercise program should incorporate the following:

    a. A policy that includes strategies and expectations for exercise and test planning.
    b. Roles and responsibilities for implementation.
    c. Sufficient personnel to perform the exercise or test, provide oversight, and document the results.
    d. Precautions to safeguard production data, such as performing a backup before performing a test in a test environment, or testing during non-peak hours.
    e. Provisions for emergency stops and concluding exercises and tests.
    f. Verification of continuity and resilience process assumptions and the ability to process a sufficient volume of work during adverse operating conditions.
    g. Activities commensurate with the importance of the business process.
    h. Entity's processes commensurate with their significance to critical financial markets.
    i. Comparison of exercise and test results against the BCP to identify gaps between the exercise or test process and recovery guidelines, with revisions incorporated where appropriate.
    j. Independent review of business continuity program and exercises and tests (internal and external).

8. Determine whether the exercise and test policy is appropriate and includes the following:

    a. Key roles and responsibilities.
    b. Minimum frequency, scope, and reporting.
    c. Documentation expectations.
    d. Processes for correcting deficiencies identified during exercises or tests.
    e. Communication and connectivity between the entity and third-party service providers.
    f. Participation with critical third-party service providers to confirm that entity personnel understand integration with all related recovery processes.

9. Determine whether the exercise and test strategies allow management to demonstrate the entity's ability to support connectivity, functionality, volume, and capacity using alternate facilities. Strategies may include the following:

    a. Expectations for individual business lines and use of exercise and testing methodologies and scenarios.
    b. Internal and external dependencies, including activities outsourced to domestic and foreign-based third-party service providers.

c. Multi-year plan(s) to execute the specific depth and breadth of exercises and tests, which use different methodologies and scenarios over time.
d. Expectations for testing internal and external recovery dependencies.
e. Assumptions, methodologies, and exercises used to develop the test strategies.
f. Transaction processing and functional testing to assess the recoverability of infrastructure, capacity, and data integrity.

10. Verify that exercise and test objectives include resilience, system monitoring, and the recovery of business processes and critical system components.

11. Verify that exercises and associated tests accomplish the following objectives:

a. Build confidence that resilience and recovery strategies meet business requirements.
b. Demonstrate that critical services can be recovered within agreed upon recovery objectives (RTOs, RPOs, and MTDs) and customer SLAs.
c. Establish that critical services can be restored in the event of an incident at the recovery location.
d. Familiarize staff with recovery processes.
e. Verify that personnel are adequately trained and knowledgeable of recovery plans and procedures.
f. Confirm that exercise and test plans remain compatible with the BCP and the entity's infrastructure.
g. Identify any gaps between business continuity procedures and objectives.

12. Determine whether management established exercise and test plans, commensurate with the nature, scale, and complexity of the recovery objectives that address the objectives and expectations of the exercise or test and outline the scenario and any assumptions or constraints that may exist. Verify whether exercise and test plans include the following:

a. Identification of roles and responsibilities for participants, support personnel, and observers.
b. Metrics to assess whether objectives are met.
c. A consolidated exercise and test schedule that encompasses all objectives.
d. Specific descriptions of objectives and methods.
e. Roles and responsibilities for all test participants, including support personnel.
f. Identification of decision makers and succession plans.
g. Exercise and test locations to be utilized.
h. Escalation procedures and the ability to adjust for simulated scenarios.
i. Contact information.

13. Determine whether management developed reasonably foreseeable threat scenarios that simulate disruptions in business functions and the ability to meet both business requirements and customer expectations. Management should:

a. Identify and document assumptions used in developing each scenario.

b. Develop scenarios that include threats that could affect third-party service providers, including communication processes with applicable stakeholders.
c. Develop exercises that demonstrate not only the ability to failover to an alternate site but also validate recovery objectives.
d. Create scenarios that include only the data and systems that would be available for recovery.

14. Verify that exercise and test scripts document the procedures for executing the exercise or test, which may include:

    a. Applications, business processes, systems, or facilities reviewed.
    b. Sequential steps for employees or external parties to perform.
    c. Procedures to guide manual work-around processes.
    d. A detailed schedule for completion.
    e. Methods for participants to record results, quantifiable metrics, and any issues.

15. Assess whether exercise and test methods are commensurate with the size and complexity of the entity and the criticality of the function to the entity. Verify that exercises and tests are designed to do following:

    a. Validate personnel knowledge and skills, including backup responsibilities.
    b. Operate and perform duties (e.g., daily, quarterly, annually) from an alternate site.
    c. Process transactions and assess system functionality.
    d. Test the viability of both full and incremental backups.
    e. Test network connectivity and interdependencies, including those with critical third-party service providers.

16. If management performs full-scale exercises, verify whether the exercise includes the following, where appropriate:

    a. Engaging personnel from all business units to participate and interact with internal and external management response teams.
    b. Validating that the crisis/emergency management process is operating as designed.
    c. Verifying personnel knowledge and skills.
    d. Validating management response and decision-making capability.
    e. Demonstrating coordination among participants and decision makers.
    f. Validating communication protocols.
    g. Conducting activities at alternate locations or facilities.
    h. Processing data using backup media or alternative methods.
    i. Completing actual transactional volumes or an illustrative subset.
    j. Performing recovery exercises over a sufficient length of time to allow issues to unfold as they would in a crisis.

17. If management performs limited-scale exercises, verify whether the exercise includes the following, where appropriate:

a. Implementing a plan appropriate to the scenario.
b. Verifying personnel knowledge and skills.
c. Validating management response and decision-making capability.
d. Executing on-the-scene coordination and decision-making roles.
e. Verifying whether participants can connect to alternate system(s).
f. Conducting activities at alternate locations or facilities.
g. Testing communication and remote access capability (e.g., switching to alternate equipment or telecommuting).

18. If management performs tabletop exercises, determine whether targeted plans and procedures are reasonable, personnel understand their responsibilities, and different departmental or business unit plans are compatible with each other. (By themselves, tabletop exercises are likely insufficient to validate recovery capabilities because they are limited to a discussion-based analysis of policies and procedures.) Tabletop exercises may include the following:

    a. Engaging operational and support personnel who are responsible for implementing the BCP.
    b. Practicing and validating specific functional response capabilities.
    c. Demonstrating knowledge and skills, as well as team interaction and decision-making capabilities.
    d. Role playing with simulated responses, evaluating critical steps, recognizing difficulties, and resolving problems.
    e. Clarifying critical plan elements, as well as problems noted during exercises.
    f. Creating action plans to correct issues.

19. Verify that management clearly defines the characteristics of a successful test, which may include the following:

    a. Validating RPOs, RTOs, and MTDs.
    b. Demonstrating recoverability at peak volumes.
    c. Confirming that systems can support critical business processes (e.g., transfer to alternate sites, increased workloads, manual workarounds, and communication).
    d. Integrating technologies that support critical business activities, including data replication, recovery, and off-site storage.
    e. Testing backup data to assess integrity and availability.
    f. Certifying facility controls (e.g., environmental, backup power, and physical security).
    g. Verifying workspace restoration (e.g., network connectivity and communications).
    h. Ensuring that personnel are familiar with and are able to execute their responsibilities.

20. Determine whether the right to perform testing or participate in exercises and tests with third parties is described in the contract governing the entity’s relationship with the third-party service provider.

21. Determine whether exercises and tests with third-party service providers are included in the entity’s enterprise exercise and test program based on the risk prioritization of the third-party

service provider and the criticality of the services provided to the entity. Assess the following:

a. The process to rank third-party service providers based on criticality, risk, and testing scope.
b. Coordinated exercises and tests that reasonably validate the abilities of both the entity and the third-party service provider to recover, restore, resume, and maintain operations after disruptions consistent with business and contractual requirements.
c. Evidence that exercises and tests of critical service providers include reasonably foreseeable significant disruptive events.
d. Documentation of the scope, execution, and results of exercises and tests in which the entity is unable to directly participate.

22. Determine whether the entity participates in its critical third-party service providers' exercise and test program(s) at reasonable intervals. Assess the execution of the exercises and tests and whether they included the following:

a. End-to-end and, when appropriate, full-scale exercises.
b. Transaction processing and functional testing.
c. Network connectivity and interdependencies to include those with critical fourth parties.
d. Bidirectional operations between the entity's and its third-party service provider's primary and alternate locations and systems.
e. Supply chain considerations.

23. Determine whether testing scenarios with critical third-party service providers consider the following:

a. An outage or disruption of the service provider.
b. An outage or disruption at the entity.
c. Incident response plans.
d. Crisis management plans.
e. Communication processes with third-party service providers and other stakeholders.
f. Cyber events.
g. Returning to normal operations.

24. Determine whether the tests validate the core or significant firm's backup arrangements to confirm the following:

a. Backup sites are able to support typical payment and settlement volumes for an extended period.
b. Backup sites are fully independent of the critical infrastructure components that support the primary sites.
c. Trained employees are located at the backup sites at the time of disruption.
d. Backup site employees are independent of the staff located at the primary site at the time of disruption.

e. Backup site employees are able to recover clearing and settlement of open transactions within the time frames addressed in the BCM processes and applicable industry standards.

25. Determine whether the exercise and test assumptions are appropriate for core and significant firms and consider the following:

    a. Primary data centers and operations facilities that are completely inoperable without notice.
    b. Whether personnel at primary sites, who are located at both data centers and operations facilities, are unavailable for an extended period.
    c. Whether other organizations are also affected, causing effects that have the potential to cascade from one organization across to the entire financial services sector.
    d. Infrastructure (e.g., power, telecommunications, transportation) that is disrupted.
    e. Whether data recovery or reconstruction to restart payment and settlement functions can be completed within the time frames defined by the BCM process and applicable industry standards.
    f. Whether continuity arrangements continue to operate until all pending transactions are closed.

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

27. Determine whether the significant firm has an external exercise and test strategy that addresses key interdependencies, such as exercises and tests with third-party market providers and key customers, and determine the following:

    a. Whether external exercise and test strategies include the significant firm's backup sites to the core firm's backup sites.
    b. Whether the significant firm participates in industry (e.g., U.S. Department of the Treasury's Hamilton Series and FS-ISAC's CAPS exercises) or cross-market tests sponsored by core firms, markets, or trade associations. Tests should incorporate verifying the connectivity from alternate sites and include transaction, settlement, and payment processes, to the extent practical.

28. Determine whether the exercise and test program is sufficient to demonstrate the entity's ability to meet its continuity objectives and whether the results demonstrate the readiness of personnel to achieve the entity's recovery and resumption objectives. Determine whether management accomplishes the following:

    a. Coordinate the execution of its exercise and test program to fully exercise its business continuity planning process.
    b. Analyze and compare results against stated objectives.
    c. Raise issues with appropriate personnel and assign responsibility for resolution.

d. Escalate issues that cannot be resolved in a timely manner to the appropriate level of management.
e. Prioritize and track issues through final resolution.
f. Analyze results and issues to determine whether problems can be traced to a common source.
g. Document recommendations for future exercise and tests.

29. Verify that corrective actions have been implemented and that retesting occurs in a timely fashion to address deficiencies in meeting the entity's objectives.

30. Verify that test results are used to update the business continuity processes, enhance future testing, and evaluate whether risk mitigation strategies should be adjusted.

Objective 11: Determine whether management continuously measures the progress and assesses the effectiveness of BCM and uses the information to improve the BCM process. (VIII, "Maintenance and Improvement")

1. Determine whether management reviews and updates the business continuity program to reflect the current environment. Triggers that prompt maintenance and improvement of the BCM may include the following:

   a. Changes in enterprise strategies.
   b. New or reconfigured products, services, or infrastructure.
   c. Changes in products and services offered by third-party service providers.
   d. Deficiencies identified in third-party service provider BCM processes.
   e. New legislation, regulatory requirements, or resilience practices.
   f. Results of operational metric analysis (e.g., key risk indications, key performance indicators).
   g. Early warning indicators that may identify potential continuity events, crises, or incidents (e.g., frequency and severity of storms, heightened cyber attack activity, or increases in customer service calls).
   h. Variances between budgeted and actual BCM expenses.
   i. Results from exercises and tests and lessons learned.
   j. Changes in the threat landscape (e.g., new capabilities, intent of threat actors).
   k. Recommendations (e.g., from audits, vulnerability assessments, and penetration tests, including those involving the use of advanced cybersecurity analysis and assessments).

2. Determine whether management has documented, analyzed, and reviewed lessons learned from adverse events. Documented procedures for incorporating lessons learned may include:

   a. Identifying the failure(s).
   b. Determining the cause(s).
   c. Evaluating potential solutions.
   d. Implementing corrective actions as appropriate.
   e. Recording and reviewing corrective actions taken.

3. Verify that management documents, tracks, and resolves any changes when updating the BCP and the exercise and testing program(s). Furthermore, verify that management maintains appropriate version control of key BCM documents.

4. Determine whether management maintains backup copies of relevant BCM documentation in the event that the primary repository becomes inaccessible.

Objective 12: Determine whether the board has established expectations for BCM reporting. (IX, "Board Reporting")

1. Review board minutes to determine whether management periodically reports to the board on the status of BCM.

    a. Determine whether reports include a written BCM presentation, including the BIA, risk assessment, BCP, exercise and test results, and identified issues.
    b. Determine whether management provides the board with regular strategy updates based on changes in personnel, roles and responsibilities, and business operations.
    c. Verify that management documents the reasons (e.g., cost and service level) for choosing recovery alternatives and why they are appropriate based on the entity's risk profile and complexity.
    d. Assess whether the board provides a credible challenge to management, when appropriate.

Objective 13: Discuss corrective action and communicate findings.

1. Review preliminary conclusions with the examiner-in-charge regarding the following:

    a. Apparent violations of laws and regulations.
    b. Significant issues warranting inclusion in the report of examination.
    c. Proposed Uniform Rating System for IT (URSIT) management component rating and the potential impact of the examiner's conclusions on composite or other URSIT component ratings.
    d. Potential impact of the examiner's conclusions on the entity's risk assessment(s).

2. Discuss findings with management and obtain proposed corrective action for significant deficiencies.

3. Document conclusions in a memorandum to the examiner-in-charge that provides report-ready comments for all relevant sections of the report of examination and clarifying guidance to future examiners.

4. Organize work papers to show clear support for significant findings by examination objective.

Appendix B: Glossary

The purpose of the glossary is to define technical terms used in the *FFIEC IT Examination Handbook* booklets in the context of supervisory activities for the entities over which FFIEC members have supervisory authority. The FFIEC members strive to align terminology in the glossary with appropriate authoritative standards, including the *NIST Computer Security Resource Center Glossary* (NIST Glossary) as the primary source for cyber-related definitions, as appropriate. FFIEC members employed the following process to select, modify, or develop definitions.

When a NIST definition existed:

- If NIST had a defined term and modifications to the definition were unnecessary, the FFIEC members included the NIST definition in this glossary. When multiple NIST definitions were available for the same term, the FFIEC members selected a definition for supervisory purposes.
- If NIST had a defined term, but the definition needed additional clarity for supervisory purposes to assist with the identification of safety and soundness and enterprise risks related to IT, the FFIEC members included both the NIST definition and the FFIEC-adapted definition. Definitions of this nature are labeled "FFIEC Adapted for Supervisory Purposes" in this glossary's source column.

When a NIST definition did not exist or the definition was not appropriate for supervisory purposes:

- If NIST did not have a defined term, but there was an appropriate authoritative third-party source (e.g., the International Organization for Standardization (ISO) Glossary), the FFIEC members included that authoritative definition.
- If NIST did not have a defined term and there was not an appropriate authoritative third-party source, the FFIEC members developed a definition for supervisory purposes. Definitions of this nature are labeled "FFIEC Developed for Supervisory Purposes" in this glossary's source column.

Note: Due to the constantly evolving nature of IT and its associated risks, the FFIEC members may update definitions to maintain alignment with other government agencies and the financial services industry.

Term	Definition	Source
A		
Application programming interface (API)	A system access point or library function that has a well-defined syntax and is accessible from application programs or user code to provide well-defined functionality.	NIST Glossary
	Software code that allows two or more programs to communicate with each other.	FFIEC Adapted for Supervisory Purposes

Asynchronous replication	Data is first written to the primary storage area (store) and then copied to the secondary storage area (forward) at predefined intervals, which is useful over smaller bandwidth connections and longer distances where latency could occur.	FFIEC Developed for Supervisory Purposes
B		
Business continuity	The capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruption.	ISO 22300:2018(en)
Business continuity management (BCM)	The process for management to oversee and implement resilience, continuity, and response capabilities to safeguard employees, customers, and products and services.	FFIEC Developed for Supervisory Purposes
Business continuity plan (BCP)	The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption.	NIST Glossary
	A comprehensive written plan(s) to maintain or resume business in the event of a disruption.	FFIEC Adapted for Supervisory Purposes
Business impact analysis (BIA)	An analysis of an information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.	NIST Glossary
	Management's analysis of an entity's requirements, functions, and interdependencies used to characterize contingency needs and priorities in the event of a disruption.	FFIEC Adapted for Supervisory Purposes
C		
Cold site	A backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment in the event that the user has to move from their main computing location to an alternate site.	NIST Glossary
Contingency plan	A plan that is maintained for disaster response, backup operations, and post-disaster recovery to ensure the availability of critical resources and to facilitate the continuity of operations in an emergency situation.	NIST Glossary
Crisis	Abnormal and unstable situation that threatens the organization's strategic objectives, reputation or viability.	Business Continuity Institute Disaster Recovery Journal Glossary
Crisis management	The process of managing an entity's preparedness, mitigation response, continuity, or recovery in the event of an unexpected significant disruption, incident, or emergency.	FFIEC Developed for Supervisory Purposes
Critical financial markets	Financial markets whose operations are critical to the economy. Critical financial markets provide the means for financial institutions to adjust their cash and securities positions and those of their customers in order to manage liquidity, market, and other risks to their organizations. Critical financial markets also provide support for the provision of a wide range of financial services to businesses and consumers in the United States and support the implementation of monetary policy. Examples of critical financial markets include federal funds, foreign	FFIEC Developed for Supervisory Purposes

	exchange, and commercial paper; U.S. government and agency securities; and corporate debt and equity securities.	
D		
Data	A representation of information as stored or transmitted.	NIST Glossary
	A physical or digital representation of information processed, stored (at rest), or transmitted (in transit).	FFIEC Adapted for Supervisory Purposes
Data center	A facility that houses virtual and/or physical information technology infrastructure(s) (e.g., computer, server, and networking systems and components) designed to store, process, and serve large amounts of data in support of an entity's strategic and business objectives. A data center may be a dedicated facility or an area or room, that contains computer, server and networking systems and components, and may be private or shared (e.g., a co-location facility).	FFIEC Developed for Supervisory Purposes
Data mirroring	The act of copying data from a database at a primary location to a database at a secondary location in or near real time.	FFIEC Developed for Supervisory Purposes
Data replication	The process of copying data, usually with the objective of maintaining identical sets of data in separate locations.	FFIEC Developed for Supervisory Purposes
Data synchronization	The simultaneous comparison and reconciliation of interdependent data files, to ensure that the files contain the same information.	FFIEC Developed for Supervisory Purposes
Database	A repository of information or data, which may or may not be a traditional relational database system.	NIST Glossary
	A repository of information or data organized to be accessed, managed, and updated.	FFIEC Adapted for Supervisory Purposes
Disaster	Situation where widespread human, material, economic, or environmental losses have occurred, which exceeded the ability of the affected organization, community, or society to respond and recover using its own resources.	ISO 22300:2018(en)
Disaster recovery	The process, policies, and procedures related to preparing for recovery or continuation of technology infrastructure, systems, and applications, which are vital to an organization after a disaster or outage. Disaster recovery focuses on the information or technology systems that support business functions, as opposed to business continuity, which involves planning for keeping all aspects of a business functioning in the midst of disruptive events. Disaster recovery is a subset of business continuity.	Business Continuity Institute Disaster Recovery Journal Glossary
Disruption	An unplanned event that causes the general system or major application to be inoperable for an unacceptable length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction).	NIST Glossary
	An anticipated or unplanned event that causes operations to degrade or fail for an unacceptable length of time	FFIEC Adapted for Supervisory Purposes

E		
Emergency management	See crisis management.	
Emergency response	Actions taken in response to a disaster warning or alert to minimize or contain the eventual negative effects, and those taken to save and preserve lives and provide basic services in the immediate aftermath of a disaster impact, for as long as an emergency situation prevails.	Business Continuity Institute Disaster Recovery Journal Glossary
Event	Occurrence or change of a particular set of circumstances.	NIST Glossary
	An occurrence or change in circumstances that may affect operations. An event can be physical, cyber, or a combination of both	FFIEC Developed for Supervisory Purposes
Exercise	A simulation of an emergency designed to validate the viability of one or more aspects of an IT plan.	NIST Glossary
	A task or activity done to practice or test a procedure. There are many different types of exercises, depending on the intended goals and objectives. An exercise may involve performing duties in a simulated environment and can be discussion-based or simulation-based.	FFIEC Adapted for Supervisory Purposes
F		
Failover	The capability to switch over automatically (typically without human intervention or warning) to a redundant or standby information system upon the failure or abnormal termination of the previously active system.	NIST Glossary
Full-scale exercise	A simulation involving a full use of available resources (e.g., hardware, software, personnel, communications, utilities, and processing from an alternate site) at the same time.	FFIEC Developed for Supervisory Purposes
Functional testing	Testing that verifies that an implementation of some function operates correctly.	NIST Glossary
H		
High availability	A failover feature to ensure availability during device or component interruptions.	NIST Glossary
	Ability of a system to be continuously operational for a desirably long length of time and to maintain a minimum amount of downtime during device or component interruptions. Availability can be measured relative to "100% uptime" or "never failing."	FFIEC Adapted for Supervisory Purposes
Hot site	A fully operational off-site data processing facility equipped with hardware and software, to be used in the event of an information system disruption.	NIST Glossary
I		
Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of a system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.	NIST Glossary

Incident management	The process of identifying, analyzing, and correcting disruptions to operations and preventing future recurrences. The goal of incident management is to limit the disruption and restore operations as quickly as possible.	FFIEC Developed for Supervisory Purposes
Incident response	The response of an organization to a disaster or other significant event that may significantly impact the organization, its people, or its ability to function productively. An incident response may include evacuation of a facility, initiating a disaster recovery plan, performing damage assessment, and any other measures necessary to bring an organization to a more stable status.	Business Continuity Institute Disaster Recovery Journal Glossary
Infrastructure	System of facilities, equipment, and services needed for the operation of an organization.	ISO 22300:2018(en)
Integrated exercise	A simulation to test the effectiveness of the continuity plans for a business line or major function that incorporates more than one component or module, including external dependencies.	FFIEC Developed for Supervisory Purposes
Interdependencies	When two or more departments, processes, functions, or third-party providers interact to successfully complete a task, business function, or process.	FFIEC Developed for Supervisory Purposes
L		
Last mile	Communications technology that bridges the transmission distance between the telecommunication service provider and the entity.	FFIEC Developed for Supervisory Purposes
Latency	Time delay in processing voice packets.	NIST Glossary
	Time delay in processing voice and data packets.	FFIEC Adapted for Supervisory Purposes
Limited-scale exercise	A simulation involving applicable resources (personnel and systems) to recover targeted business processes.	FFIEC Developed for Supervisory Purposes
M		
Maximum tolerable downtime (MTD)	The amount of time mission/business process can be disrupted without causing significant harm to the organization's mission.	NIST Glossary
	The total amount of time the system owner or authorizing official is willing to accept for a business process disruption, including all impact considerations.	FFIEC Adapted for Supervisory Purposes
N		
Network backbone	The main communication channel of a network that interconnects one or more network segments and provides a path for the exchange of data between devices. A backbone can span any geographic area.	FFIEC Developed for Supervisory Purposes
O		
Operational resilience	The ability of systems to resist, absorb, and recover from or adapt to an adverse occurrence during operation that may cause harm, destruction, or loss of ability to perform mission-related functions.	NIST Glossary
	The ability of an entity's personnel, systems, telecommunications networks, activities, or processes to resist, absorb, and recover from or	FFIEC Adapted for Supervisory Purposes

	adapt to an incident that may cause harm, destruction, or loss of ability to perform mission-related functions.	
Outage	The interruption of systems, infrastructure, support services, or essential business functions, which may result in the entity's inability to provide services for some period of time. The amount of time lost from an outage may result in downtime. Conversely, downtime may cause an outage.	FFIEC Developed for Supervisory Purposes
Outsourcing	The practice of contracting through a formal agreement with a third party(ies) to perform services, functions, or support that might otherwise be conducted in-house.	FFIEC Developed for Supervisory Purposes
R		
Reciprocal agreement	An agreement that allows two organizations to back up each other.	NIST Glossary
	An agreement that allows two entities (or two internal business groups) with compatible systems and functionality that allows each one to recover at the other's location.	FFIEC Adapted for Supervisory Purposes
Recovery point objective (RPO)	The point in time to which data must be recovered after an outage.	NIST Glossary
	The point in time to which data used by an activity is restored to enable the resumption of business functions. The RPO is expressed backward in time from the point of disruption and can be specified in increments of time (e.g., minutes, hours, or days).	FFIEC Adapted for Supervisory Purposes
Recovery time objective (RTO)	The overall length of time an information system's components can be in the recovery phase before negatively impacting the organization's mission or mission/business processes.	NIST Glossary
Remote access	Access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet).	NIST Glossary
Resilience	The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.	NIST Glossary
S		
Scenario	A sequential, narrative account of a hypothetical incident that provides the catalyst for the exercise and is intended to introduce situations that will inspire responses and thus allow demonstration of the exercise objectives.	NIST Glossary
Service level agreement	Defines the specific responsibilities of the service provider and sets the customer expectations.	NIST Glossary
	A formal agreement between two parties that records: a common understanding about products or services to be delivered, priorities, responsibilities, guarantees, and warranties between the parties. In addition, the agreement describes the nature, quality, security, availability, scope, and timeliness of delivery and response of the parties, the point(s) of contact for end-user problems, and the metrics by which the effectiveness of the process is monitored and approved, and may include other measurable objectives. The agreement should cover not only expected day-to-day situations, but also unexpected or adverse events, as the need for the service may vary.	FFIEC Adapted for Supervisory Purposes

Supply chain risk management	The implementation of processes, tools, or techniques to minimize the adverse impact of attacks that allow the adversary to utilize implants or other vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (information technology products) or services at any point during the life cycle.	NIST Glossary
	The implementation of processes, tools, or techniques to minimize the adverse impact of attacks that allow the adversary to exploit vulnerabilities inserted prior to installation. This is done in order to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (information technology products) or services at any point during the supply chain (e.g., initial production, packaging, handling, storage, transport, mission operation, and disposal).	FFIEC Adapted for Supervisory Purposes
Synchronous replication	Data is written to both primary and secondary storage areas at the same time to ensure that multiple copies of the data are current and identical. This method is used for critical business functions where latency is unacceptable, and little or no data loss can be tolerated.	FFIEC Developed for Supervisory Purposes
T		
Tabletop exercise	A discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles during an emergency and their responses to a particular emergency situation. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario.	NIST Glossary
	A discussion-based exercise where personnel meet in a classroom setting or in breakout groups to validate a component(s) of the business continuity plan(s) by discussing their roles and responsibilities. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario.	FFIEC Adapted for Supervisory Purposes
Test	An evaluation tool that uses quantifiable metrics to validate the operability of a system or system component in an operational environment specified in an IT plan.	NIST Glossary
	A type of exercise intended to verify the quality, performance, or reliability of system resilience in an operational environment.	FFIEC Adapted for Supervisory Purposes
Threat intelligence	Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes.	NIST Glossary
Trigger	An event that causes the system to initiate a response. Note: Also known as a triggering event.	NIST Glossary
	An event that prompts a response from management or an automated system. Also known as a triggering event.	FFIEC Adapted for Supervisory Purposes
W		
Warm site	An environmentally conditioned work space that is partially equipped with information systems and telecommunications equipment to support relocated operations in the event of a significant disruption.	NIST Glossary

Appendix C: Abbreviations

ATM	automated teller machine
BCM	business continuity management
BCP	business continuity plan
BIA	business impact analysis
CA Letter	Consumer Affairs Letter
CAPS	Cyber-Attack Against Payment Systems
CDC	Centers for Disease Control and Prevention
CFPB	Consumer Financial Protection Bureau
CFR	Code of Federal Regulations
COSO	Committee of Sponsoring Organizations of the Treadway Commission
DDoS	distributed denial of service
DHS	U.S. Department of Homeland Security
DRaaS	disaster recovery as a service
ERM	enterprise risk management
FBIIC	Financial and Banking Information Infrastructure Committee
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FIL	Financial Institution Letter
FRB	Board of Governors of the Federal Reserve System
FS-ISAC	Financial Services Information Sharing and Analysis Center
FSARC	Financial Systemic Analysis & Resilience Center
FSSCC	Financial Services Sector Coordinating Council
GETS	Government Emergency Telecommunications Service
IIA	Institute of Internal Auditors
ISO	International Organization for Standards
IT	information technology
IT Handbook	*FFIEC Information Technology Examination Handbook*
MTD	maximum tolerable downtime
NCUA	National Credit Union Administration
NIST	National Institute of Standards and Technology
OCC	Office of the Comptroller of the Currency
ODNI	Office of the Director of National Intelligence
RPO	recovery point objective
RTO	recovery time objective
SLA	service-level agreement
SLC	State Liaison Committee
SOC	systems and organization control
SR Letter	Supervision and Regulation Letter
SSAE	Statement on Standards for Attestation Engagement
TSP	Telecommunications Service Priority
URSIT	Uniform Rating System for Information Technology
USC	United States Code
WPS	Wireless Priority Service Program

Appendix D: References

Laws

12 U.S.C. 95(b) / 1463(a) / 3102(b), "Comptroller Authority to Declare a Legal Holiday"
12 U.S.C. 1464, "Home Owners' Loan Act"
12 U.S.C. 1831r-1, "Notice of Branch Closure"
12 U.S.C. 1861–1867, "Bank Service Company Act"
12 U.S.C. 1882, "Bank Protection Act"
12 U.S.C. 3352, "Emergency Exceptions for Disaster Areas"
15 U.S.C. 6801 and 6805(b), "Gramm–Leach–Bliley Act"
18 U.S.C. 1030, "Fraud and Related Activity in Connection With Computers"

Consumer Financial Protection Bureau

Guidance

CFPB Statement on Supervisory Practices Regarding Financial Institutions and Consumers Affected by a Major Disaster or Emergency (September 2018)
CFPB Compliance Bulletin and Policy Guidance; 2016-02, Service Providers (October 2016)

Federal Reserve

Regulations

12 CFR 208, Appendix D-1, "Interagency Guidelines Establishing Standards for Safety and Soundness"
12 CFR 208, Appendix D-2, "Interagency Guidelines Establishing Information Security Standards (State Member Banks)"
12 CFR 225, Appendix F, "Interagency Guidelines Establishing Information Security Standards"

Guidance

SR Letter 16-11, "Supervisory Guidance for Assessing Risk Management at Supervised Institutions with Total Consolidated Assets Less than $50 Billion" (June 2016)
SR Letter 15-10 / CA Letter 15-8, "Expansion of the Federal Reserve's Emergency Communications System" (October 2015)
SR Letter 15-9, "FFIEC Cybersecurity Assessment Tool for Chief Executive Officers and Boards of Directors" (July 2, 2015)
SR Letter 13-16, "End of Microsoft Support for Windows XP Operating System" (October 2013)
SR Letter 13-19 / CA Letter 13-21, "Guidance on Managing Outsourcing Risk" (April 2013)
SR Letter 13-6 / CA Letter 13-3, "Supervisory Practices Regarding Banking Organizations and Their Borrowers and Other Customers Affected by a Major Disaster or Emergency" (March 2013)

SR Letter 12-14, "Revised Guidance on Supervision of Technology Service Providers" (October 2012)
SR Letter 10-13, "Interagency Supervisory Guidance for Institutions Affected by the Deepwater Horizon Oil Spill" (October 2010)
SR Letter 07-18, "FFIEC Guidance on Pandemic Planning" (December 12, 2007)
SR Letter 06-5, "Influenza Pandemic Preparedness" (March 15, 2006)
SR Letter 06-3, "Interagency Supervisory Guidance for Institutions Affected by Hurricane Katrina" (February 3, 2006)
SR Letter 05-24, "Interagency Questions and Answers for Financial Institutions in Response to Hurricanes Katrina and Rita" (December 2, 2005)
SR Letter 05-17, "Katrina Related Marketing Practices Invoking the Name of the Federal Reserve" (September 22, 2005)
SR Letter 05-16, "Supervisory Practices Regarding Banking Organizations and Consumers Affected by Hurricane Katrina" (September 15, 2005)
SR Letter 03-9, "Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System" (May 28, 2003)

Federal Deposit Insurance Corporation

Regulations

12 CFR 304.3(d), "Notification of Performance of Bank Services, Form FDIC 6120/06"
12 CFR 364, Appendix A "Interagency Guidelines Establishing Standards for Safety and Soundness"
12 CFR 364, Appendix B "Interagency Guidelines Establishing Information Security Standards"
12 CFR 364, Supplement A to Appendix B "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice"

Guidance

FIL-19-2019, "Technology Service Provider Contracts" (April 2, 2019)
FIL-63-2018, "Cybersecurity Preparedness Resource" (October 19, 2018)
FIL-62-2017, "Major Disaster Examiner Guidance" (December 15, 2017)
FIL-68-2016, "FFIEC Cybersecurity Assessment Tool: Frequently Asked Questions" (October 18, 2016)
FIL-43-2016, "Information Technology Risk Examination (InTREx) Program" (June 30, 2016)
FIL-37-2016, "FFIEC Joint Statement on Cybersecurity of Interbank Messaging and Wholesale Payment Networks" (June 7, 2016)
FIL-55-2015, "Cybersecurity Awareness Resources" (November 23, 2015)
FIL-28-2015, "Cybersecurity Assessment Tool" (July 2, 2015)
FIL-13-2015, "FFIEC Joint Statements on Destructive Malware and Compromised Credentials" (March 30, 2015)
FIL-13-2014, "Technology Outsourcing: Informational Tools for Community Bankers" (April 7, 2014)

FIL-11-2014, "Distributed Denial of Service (DDoS) Attacks" (April 2, 2014)
FIL-44-2008, "Third-Party Risk: Guidance for Managing Third-Party Risk" (June 6, 2008)
FIL-6-2008, "Interagency Statement on Pandemic Planning: Guidance for Minimizing a Pandemic's Potential Adverse Effects" (February 6, 2008)
FIL-49-2006, "Lessons Learned from Hurricane Katrina: Preparing Your Institution for a Catastrophic Event" (June 15, 2006)
FIL-25-2006, "Influenza Pandemic Preparedness Interagency Advisory" (March 15, 2006)
FIL-27-2005, "Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice" (April 1, 2005)
FIL-84-2002, "Financial and Banking Information Infrastructure Committee's Interim Policy on the Sponsorship of Private Sector Financial Institutions in the GETS Card Program" (August 6, 2002)
FIL-50-2001, "Bank Technology Bulletin on Outsourcing" (June 4, 2001)

National Credit Union Administration

Regulations

12 CFR 748, Appendix A, "Guidelines for Safeguarding Member Information"
12 CFR 749, Appendix A, "Record Preservation Program and Record Retention"
12 CFR 749, Appendix B, "Catastrophic Act Preparedness Guidelines"

Guidance

NCUA Letter to Credit Unions 08-CU-01, "Guidance on Pandemic" (January 2008)
NCUA Letter to Credit Unions 07-CU-13, "Evaluating Third-Party Relationships" (December 2007)
NCUA Risk Alert 06-Risk-01, "Disaster Planning and Response" (April 2006)
NCUA Letter to Credit Unions 06-CU-06, "Influenza Pandemic Preparedness" (March 2006)
NCUA Letter to Credit Unions 02-CU-17, "e-Commerce Guide for Credit Unions" (December 2002)
NCUA Letter to Credit Unions 01-CU-21, "Disaster Recovery and Business Resumption Contingency Plans" (December 2001)
NCUA Letter to Credit Unions 01-CU-20, "Due Diligence Over Third-Party Service Providers" (November 2001)
NCUA Letter to Credit Unions 98-CU-12, "Business Resumption Contingency Planning" (June 1998)

Office of the Comptroller of the Currency

Regulations

12 CFR 5.30, "Establishment, Acquisition, and Relocation of a Branch of a National Bank"
12 CFR 5.31, "Establishment, Acquisition, and Relocation of a Branch and Establishment of an Agency Office of a Federal Savings Association"

12 CFR 30, Appendix A, "Interagency Guidelines Establishing Standards for Safety and Soundness"
12 CFR 30, Appendix B, "Interagency Guidelines Establishing Information Security Standards"
12 CFR 30, Appendix D, "OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches"
12 CFR 30, Appendix E, "OCC Guidelines Establishing Standards for Recovery Planning by Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches"

Guidance

OCC Bulletin 2019-13, "Recovery Planning"
OCC Bulletin 2019-8, "Loans in Areas Having Special Flood Hazards – Private Flood Insurance: Final Rule"
OCC Bulletin 2018-47, "Recovery Planning Guideline: Final Revised Guidelines"
OCC Bulletin 2018-14, "Installment Lending: Core Lending Principles for Short-Term, Small-Dollar Installment Lending"
OCC Bulletin 2018-8, "Cyber Insurance: FFIEC Joint Statement on Cyber Insurance and Its Potential Role in Risk Management Programs"
OCC Bulletin 2017-61, "Major Disasters: Interagency Examiner Guidance for Institutions Affected by Major Disasters"
OCC Bulletin 2017-54, "Branches and Relocations: Revised Comptroller's Licensing Manual Booklet"
OCC Bulletin 2017-35, "Flood Disaster Protection Act: Revised Comptroller's Handbook Booklet"
OCC Bulletin 2017-24, "Branch Closings: Revised Comptroller's Licensing Manual Booklet"
OCC Bulletin 2017-21, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29"
OCC Bulletin 2017-7, "Third-Party Relationships: Supplemental Examination Procedures"
OCC Bulletin 2016-34, "Cybersecurity: Frequently Asked Questions on the FFIEC Cybersecurity Assessment Tool"
OCC Bulletin 2016-30, "Enforceable Guidelines for Recovery Planning: Final Guidelines"
OCC Bulletin 2015-31, "Cybersecurity: FFIEC Cybersecurity Assessment Tool"
OCC Bulletin 2015-9, "FFIEC Information Technology Examination Handbook: Strengthening the Resilience of Outsourced Technology Services, New Appendix for Business Continuity Planning Booklet"
OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance"
OCC Bulletin 2012-28, "Supervisory Guidance on Natural Disasters and Other Emergency Conditions"
OCC Bulletin 2006-26, "Disaster Planning: Hurricane Katrina – Lessons Learned"
OCC Bulletin 2006-12, "Influenza Pandemic Preparedness: Interagency Advisory"
OCC Bulletin 2006-6, "Community Reinvestment Act: Hurricanes Katrina and Rita"

OCC Bulletin 2003-14, "Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System"
OCC Bulletin 2003-13, "Telecommunications Service Priority (TSP) Program: Policy on Sponsorship of TSP for Private Sector Entities"
OCC Bulletin 2002-33, "Government Emergency Telecommunications Service (GETS): FBIIC Policy on Sponsorship of GETS Cards for Private Sector Entities"
OCC Bulletin 2002-16, "Bank Use of Foreign-Based Third-Party Service Providers: Risk Management Guidance"
OCC Bulletin 1998-3, "Technology Risk Management: Guidance for Bankers and Examiners"

Other References

U.S. Department of Health & Human Services, Centers for Disease Control and Prevention, *Pandemic Influenza* (January 2019)
Communications, Security, Reliability, and Interoperability Council, *Infrastructure Sharing During Emergencies* (December 2014)
National Infrastructure Protection Plan, *NIPP 2013: Partnering for Critical Infrastructure and Resilience* (November 2013)
NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Information Technology Systems* (May 2010)
BITS Financial Services Roundtable, *BITS Framework for Managing Technology Risk for Service Provider Relationships* (May 2008)
Basel Committee on Banking Supervision, *The Joint Forum: High-level Principles for Business Continuity* (August 2006)
U.S. Department of Homeland Security, *Pandemic Influenza Preparedness, Response, and Recovery Guide for Critical Infrastructure and Key Resources* (September 2006)
Department of Health and Human Services, Centers for Disease Control and Prevention *Business Pandemic Influenza Planning Checklist* (December 2005)
Homeland Security Council *National Strategy for Pandemic Influenza* (November 2005)
Federal Reserve Bank of New York, *Best Practices to Assure Telecommunications Continuity for Financial Institutions and the Payment and Settlement Utilities: Report by the Assuring Telecommunications Continuity Task Force* (September 2004)
The President's National Security Telecommunications Advisory Committee, *Financial Services Task Report* (April 2004)