Sources Concerning: Business Continuity Management As of 12/17/19.

DISCLAIMER: *While we attempt to assert that this document includes all information available on the ffiec.gov website as of the date listed above, we offer this as an aid to audit and consulting Clients, and in no way warrant this as being all-inclusive, complete, or thorough. Please use at your own risk.*

Resources:

FFIEC IT Examination Handbook

Business Continuity Management Booklet

I: Business Continuity Management

https://ithandbook.ffiec.gov/it-booklets/business-continuity-management/i-business-continuity-management.aspx (Accessed 12/17/19)

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.

FFIEC IT Examination Handbook

Business Continuity Management Booklet

II: Business Continuity Management Governance

https://ithandbook.ffiec.gov/it-booklets/business-continuity-management/ii-business-continuity-management-governance.aspx (Accessed 12/17/19)

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.

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.

FFIEC IT Examination Handbook
Business Continuity Management Booklet
II. A: Board and Senior Management Responsibilities
https://ithandbook.ffiec.gov/it-booklets/business-continuity-management/ii-business-continuity-management-governance/iia-board-and-senior-management-responsibilities.aspx (Accessed 12/17/19)

The board 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.

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 to management responsible for the BCM process.

Management oversight should include:

- Defining BCM roles, responsibilities, and succession plans.
- Allocating knowledgeable personnel 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.

FFIEC IT Examination Handbook
Business Continuity Management Booklet
II. B: Audit
https://ithandbook.ffiec.gov/it-booklets/business-continuity-management/ii-business-continuity-management-governance/iib-audit.aspx (Accessed 12/17/19)

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.
- 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.

FFIEC IT Examination Handbook
Business Continuity Management Booklet
III: Risk Management
https://ithandbook.ffiec.gov/it-booklets/business-continuity-management/iii-risk-management.aspx (Accessed 12/17/19)

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. The BIA and risk assessment represent the foundation of BCM. BCM should integrate with an entity's enterprise risk management (ERM), 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.

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.

FFIEC IT Examination Handbook
Business Continuity Management Booklet
III. A: Business Impact Analysis
https://ithandbook.ffiec.gov/it-booklets/business-continuity-management/iii-risk-management/iiia-business-impact-analysis.aspx (Accessed 12/17/19)

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). 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.

FFIEC IT Examination Handbook
Business Continuity Management Booklet
III. A1: Identification of Critical Business Functions
https://ithandbook.ffiec.gov/it-booklets/business-continuity-management/iii-risk-management/iiia-business-impact-analysis/iiia1-identification-of-critical-business-functions.aspx (Accessed 12/17/19)

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, 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.

FFIEC IT Examination Handbook
Business Continuity Management Booklet
III. A2: Interdependency Analysis
https://ithandbook.ffiec.gov/it-booklets/business-continuity-management/iii-risk-management/iiia-business-impact-analysis/iiia2-interdependency-analysis.aspx (Accessed 12/17/19)

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

FFIEC IT Examination Handbook
Business Continuity Management Booklet
III. A3: Impact of Disruption
https://ithandbook.ffiec.gov/it-booklets/business-continuity-management/iii-risk-management/iiia-business-impact-analysis/iiia3-impact-of-disruption.aspx (Accessed 12/17/19)

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.

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. 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.

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.

FFIEC IT Examination Handbook
Business Continuity Management Booklet
III. B: Risk Assessment
https://ithandbook.ffiec.gov/it-booklets/business-continuity-management/iii-risk-management/iiib-risk-assessment.aspx (Accessed 12/17/19)

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.

FFIEC IT Examination Handbook
Business Continuity Management Booklet
III. B.1: Risk Identification
https://ithandbook.ffiec.gov/it-booklets/business-continuity-management/iii-risk-management/iiib-risk-assessment/iiib1-risk-identification.aspx (Accessed 12/17/19)

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. 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 the Interagency Guidelines Establishing Information Security Standards[2] 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[3] 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.

FFIEC IT Examination Handbook
Business Continuity Management Booklet
III. B.2: Likelihood and Impact
https://ithandbook.ffiec.gov/it-booklets/business-continuity-management/iii-risk-management/iiib-risk-assessment/iiib2-likelihood-and-impact.aspx (Accessed 12/17/19)

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 provides examples of risk measurement processes and methodologies to help analyze risks.

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.