Business Continuity Planning

Version 1.0
August 2013

Introduction

Business continuity planning (BCP) is an organization's preparation process to ensure that critical business functions will be available to customers, suppliers, regulators, and other entities that must have access to those functions even under extraordinary circumstances. These activities include many daily tasks such as customer/member correspondence, trading activities, project management, system backups, change control, and help desk operations. Effective BCP develops a roadmap for maintaining service levels, consistency and recoverability for these daily activities. BCP can sometimes be conflated with disaster recovery; however, disaster recovery is a subset of BCP as not all business disruptions would be categorized as disasters. This module is applicable in the examinations of Fannie Mae, Freddie Mac, the Federal Home Loan Banks (FHLBanks) (collectively, the regulated entities); and the Office of Finance.

BCP involves determining the strategy and methodology by which desired continuity will be achieved. The blueprint developed through the BCP process is the organization's business continuity plan (the plan). Because financial institutions play a crucial role in the overall economy, each regulated entity and the Office of Finance must have a planning process that is appropriate for the institution's size and complexity to ensure any disruptions in service will be minimized in order to help maintain public trust and confidence.

Consequences from any number of planned or unplanned scenarios may threaten an institution's ability to perform operations on any particular day. Scenarios might include a cyber-attack or event, technology system upgrade, natural disaster, infrastructure failure, human error, or act of terrorism.

The objectives of an institution's planning process are to minimize financial loss, ensure the safety of employees, continue to serve members, customers, and counterparties and mitigate the negative effects disruptions can have on strategic plans, reputation, operations, earnings, liquidity, credit quality, market position, and the institution's ability to remain in compliance with applicable laws and regulations. The cost of recovery may be significantly higher due to ineffective recovery strategies. Since financial markets and the regulated entities are always evolving, continuity planning must occur on a continuous basis especially as material changes occur within an institution.

The board of directors (board) is responsible for designing and adopting a business continuity plan at the institutional level. From there, the board will likely charge executive management to establish appropriate business continuity programs (programs) to identify and control risk at the department and often business unit level. The board-approved plan is the framework upon and around which the entity's overall programs are built. These programs may vary by department or business unit as they should be tailored to those units' specific risks and recovery challenges. Each program will consist of a set of policies and procedures designed to transform the institution's high-level articulation of principles (the institution's plan) into operational-level practices and protocols. These policies and procedures facilitate the operation of critical business functions on a day-to-day basis as well as recovery in a timely and orderly fashion from any unexpected disruption. The programs and their resulting policies and procedures must set clear responsibilities, establish reporting, and have acceptable business continuity goals for the organization and relevant business units. Policies should also address the business and infrastructure needs of the organization. Changes in business processes and in personnel make it challenging to maintain a current plan. An outdated plan coinciding with an unplanned disruption will likely result in additional time to recover and may result in errors, costly mistakes, and damaged reputation. The board must require management to maintain a plan and programs that are current and effective.

While the board may delegate the implementation of various aspects of the plan, programs, policies and procedures, the board cannot delegate its responsibility to ensure that the institution and its various sub-units maintain adequate policies, procedures, and practices. As part of discharging its responsibilities under FHFA's Prudential Management and Operations Standards (PMOS)(12 CFR Part 1236), FHFA anticipates the board will review the business continuity plan and programs periodically, for example, when material changes to the business impact a program, or as part of its annual review of major strategies and policies.

An effective plan is a risk mitigant. It affirms that the board and management have evaluated risk scenarios and identified appropriate risk mitigation strategies. An inadequate plan on the other hand, exposes the regulated entity to unacceptable levels of operational risk. In the event of a disruption, an inability to fulfill obligations and provide continuous services may result in legal liability and tarnish the institution's reputation. Therefore, the board must actively support the execution of organization's plan.

Examiners need to evaluate the board's level of commitment to the plan and resulting programs. The board minutes should reflect an appropriate level of BCP-related discussions. Examiners should be mindful that the complexities of BCP might go unappreciated when income producing activities or the prevention of significant revenue losses from other activities is competing for the board's attention. Nonetheless, the board has the responsibility to ensure that the organization has effective programs and cannot ignore this operational risk.

The plan and programs must address how the institution will resume operations after a disruption, how financial and decision-making data will become available and verified to be complete and accurate, and how the functionality of an organization's infrastructure will be restored. The plan must clearly define the path for recovery when responding to a widespread disruption or a loss of critical computer system and service functions.

Boards will often establish an operations committee that is responsible for business continuity. The board then establishes a reporting requirement for when, or under what circumstances, it receives updates. In all cases, however, management should inform the board of any event that causes an unexplained disruption to services. The board, or board committee, must also annually review and approve the plan.

Effective programs must receive an appropriate level of attention from the board and executive management. In certain circumstances, board attention down to the policies and procedures level may be appropriate. Management must assign the day-to-day business continuity responsibilities to business-line management, and be ready to execute business recovery efforts, if necessary. Further, management must have a holistic view of the plan and programs. Some entities choose to assign an administrator to their plan to be able to provide this view. A business continuity recovery team will often assist the program administrator in the execution of the plan and programs across the institution. The plan administrator presents the plan to the board to ensure at least an annual conversation about the state of the plan and programs.

The primary responsibilities of the board's designee for the execution of the plan, often a plan administrator, may include:

1) Develop and maintain a formal plan that is responsive to the institution's current business needs and operating environment;
2) Ensure that a business continuity recovery team includes representatives from all business units;
3) Provide ongoing business continuity training to all employees, including executive management and the board;
4) Evaluate documentation and provide a process to test each business unit's adherence to entity standards;
5) Ensure that thorough, current business impact analysis and risk assessments are maintained;
6) Review and approve periodic testing strategies, including analyzing the results of tests and providing recommendations, where appropriate;
7) Ensure a centralized executive view of the business continuity plan and programs;
8) Report the organization's general business continuity readiness and results of the periodic tests to the board and executive management; and,
9) Coordinate business continuity activities.

The recovery team is responsible for determining the extent of a disabling event and working with senior management to formulate recovery efforts. Once the institution has developed the plan and programs, the recovery team coordinators communicate instructions to appropriate staff and may provide training to better ensure an effective recovery, when necessary. Individual recovery team coordinators provide information on the status of documentation, establishment of test scenarios, and overall readiness to the plan's administrator. The recovery team coordinators assist business unit managers in the day-to-day continuity efforts.

Business Continuity Program

One of the first things management does to develop a satisfactory plan and programs is to perform a business impact analysis (BIA). This analysis predicts the consequences of disruptions of business functions and processes and gathers information needed to develop recovery strategies. Potential loss scenarios should be identified during an ensuing risk assessment. Operations may also be interrupted by vendor failures or delays. There are many possible scenarios which should be considered. (See FEMA's Business Continuity Plan resource material on http://www.Ready.gov for additional information.) The purpose of a BIA is to gather quantifiable data to make informed decisions concerning the allocation of limited resources during a disruption. All business functions and departments must participate and be included in the BIA process to ensure a comprehensive result. Examiners should evaluate how the BIA supports the plan by reviewing management assumptions, reviewing the supporting documentation, and interviewing management.

The scope of BIA analysis is broad and addresses the effect on the organization should any critical system not be available. While BIA analysis is not solely about technology, it is a tool by which management can estimate the cost of being without computer systems for different periods of time. The effect may be minor if it is only a few minutes, but even an otherwise small disruption, at the wrong time, can be devastating.

All BIAs are dependent on the quality of data and the ability of management to properly analyze recovery scenarios. They require that the regulated entity have a process to determine essential business requirements. Management must have a good way to prioritize recovery actions and individual business managers must understand and implement well-supported recovery point objectives (RPOs) and recovery time objectives (RTOs). The BIA also requires a good understanding of threats that may subject the organization or specific business units to disruptions.

Recovery Point and Time Objectives

RPOs reflect the maximum tolerable loss that is acceptable in a disruption situation. Loss may be measured in terms of time or data. RPOs identify the specific business processes that must be recovered after a disruption and to what degree they must be recovered, accepting that a certain amount of data may be unrecoverable, via automated systems, from the last backup to the point of the event. Business unit managers must determine their acceptable RPOs for each of their critical processes. Programs must address RPOs and have adequate policies and procedures in place to update systems once they become operational.

To provide acceptable RPOs, institutions must first consider infrastructure and business cost independently and then consider the quantifiable potential business costs resulting from a failure to make infrastructure upgrades. Some processes may be so critical that they demand virtually no downtime. In the case of the regulated entities and the Office of Finance, business processes and their automated systems that support liquidity in the marketplace might be such an example. Therefore, management should identify a backup system that can capture and retrieve data, to maintain real time accessibility for liquidity systems, even in the event of an incident.

RTOs represent the maximum acceptable amount of time for restoring a network or application or regaining access to data after a disruption. They may also be viewed as the maximum length of time allowable between a disruption and the resumption of normal operations. RTOs identify the time it takes to restore systems or processes that support a particular business function. They should consider any service agreements with external counterparties for the particular function and implications if the service provider suffers the same disruption. RTOs cover the span of time between the disruption and the point in time in which systems or processes are again available. Business unit managers must determine acceptable RTOs in the development of a BIA.

Threat Analysis

In addition to RPOs and RTOs, another component of the BIA is threat analysis. A threat analysis is a summary of potential disruptions and their probabilities of occurrence. This threat analysis informs BCP and often more specifically a subset of BCP – disaster recovery. Threat analysis will review the probability of severe disruptions of which earthquakes, floods, severe weather, fires, terrorism, theft, pandemics, cyber-attacks or events, and medical emergencies are common examples. Management should evaluate the likelihood of these events and consider them in the BIA process. This is a challenge, as these occurrences can range from being minor to devastating in nature. Management should use their best judgment given their geographical area and considering reasonable factors.

It may be reasonable to expect various downtimes for different processes. Institutions often choose to estimate the cost of being down in increments of 2, 4, 8, or 24 hours or even multiples of days. Typically, management allocates recovery resources when the cost of downtime to the business is greater than the cost of recovery. Management and examiners must keep in mind that the BIA is only a tool to assist in the decision making process. It may be prudent to establish a more robust system than the estimated business cost suggested by the BIA, depending on legal or regulatory requirements, risk to reputation, and other considerations.

Management Responsibilities

Management should diagram critical business functions to help ensure proper recovery priorities. A workflow diagram detailing all inputs and outputs, including system feeds, can sometimes reveal that a process believed to be non-critical feeds into the critical path of an essential business function. Workflow diagrams must be prepared from the perspective of the business unit, but readable by all interested parties, such as auditors, vendors, examiners, and executive management. The workflow diagram must consider external processes that provide support to that function, even if that process resides at a vendor.

Management should stress test business processes and BIA assumptions against various threat scenarios. Threat scenarios should range in severity from those with high probability of occurrence but low effect, such as brief power outages, to those with a low likelihood of occurrence but high effect, such as hurricanes or terrorist or cyber-attacks. Management's analysis should consider the effect of a broad range of possible business disruptions on the institution and its customers/members; the probability of occurrence; the loss effect on information services, technology, personnel, facilities, and service providers; and the security and retrievability of data and vital documents. Management should consider worst-case scenarios, such as destruction of facilities and loss of life.

Management sometimes hires consultants to assist with the development of the business continuity plan and programs, and assist in determining vulnerability to and likelihood of potential risks to the institution. The plan should include a risk assessment that identifies the specific potential risks to the institution. Risk assessments on the department or business unit level may also be appropriate as risk factors can impact unevenly across the institution. In addition, programs should develop a threat analysis, discussed above, which determines the likelihood that potential threats could occur. Obtaining such information is essential in developing programs that will effectively mitigate potential risks to the organization. Management and the board must determine how they will address any identified gaps, but the board is ultimately responsible for the quality of the plan and programs.

With information from the BIA and internal risk assessments as the foundation, management can then develop individual written programs with attendant policies and procedures. Individual business units may need discrete programs addressing their unique processes. The regulated entities and the Office of Finance also need to have programs to address executive processes, communications, and expectations during emergencies. Each business unit's program should focus upon the resumption of those business activities defined as critical during the BIA phase. The priority of business functions should determine the order of recovery. Programs should include detailed instructions to resume operations in manual mode when computer systems are inoperable. Programs must address the manner in which the institution will recover and process any backlog of activity and/or lost transactions at the recovery site. Programs should identify how the institution will bring transaction records current from the time of the disruption to the expected recovery timeframes. The organization's plan and business level programs should provide information about how to communicate with employees, customers/members, trade groups, and the press should a sudden disabling event occur. The organization's plan should address the effects of a recovery period lasting a longer duration than anticipated. Management should consider that before, during and/or after a severe disruption employees critical to the execution of the plan may choose to evacuate or tend to family instead of discharging their responsibilities under the plan. Management should plan accordingly for this potential and often likely outcome. Management may also consider the development of tertiary plans. Each regulated entity and the Office of Finance must communicate to the appropriate FHFA designee should it experience a disruption where it must implement steps detailed in its plan.

The tactical steps to ensure the infrastructure becomes available must be included in the programs and their attendant policies and procedures. Some institutions elect to have a separate disaster recovery plan that addresses the organization's infrastructure. Management must have proper plans to address infrastructure in case of a disruptive event. The business continuity plan or a separate disaster recovery plan must include the plans and tests for the recovery of infrastructure to conduct critical business processes. The chief technology officer (or equivalent) must incorporate the infrastructure recovery steps within the business continuity plan and programs.

Testing the Business Continuity Programs

A regulated entity must test its programs at least annually. Management should consider developing multi-year test strategies that progressively challenge recovery assumptions and making test exercises more complex and robust over time. Management must routinely assess the interdependencies between departments, functional areas, and third parties. Successful test strategies identify gaps or inadequacies in recovery facilities, personnel, and assumptions so that management can take corrective measures. The severity of gaps identified may warrant follow up testing within reasonable timeframes to ensure the risks associated with identified gaps are appropriately mitigated. If manual procedures are to be utilized for an extended period, tests should check to see that reliance on manual procedures is feasible and for what length of time. Although recovery tests should gradually increase in complexity, management should not unduly jeopardize normal business operations when testing programs. Based on test results, each department manager should be responsible for reviewing and, if appropriate, updating his/her area's program and communicating changes to the plan administrator or similar party.

Entities should carefully evaluate whether cold or warm recovery sites will provide sufficient support for critical business functions. Hot-sites provide support in the event an organization's normal business location is not available. A cold-site has little or no infrastructure to support processing. It is simply a location that management may use to bring in equipment as need requires. A warm-site has some equipment and, in fact, may be close to a full production environment, but lacks key elements that would make it fully functional or able support all business units. FHFA expects the regulated entities and the Office of Finance to have full hot-sites that they can quickly employ to meet their business needs.

Recovery facilities may vary greatly. Some institutions may maintain designated recovery facilities while others may rely on third-party vendors to provide recovery services. A combination of the two methods may also provide a viable alternative. Management must test recovery facilities frequently, but no less than annually. Due to the complexity of the regulated entities and the Office of Finance, it may be more practical for institutions to complete some testing at least quarterly, with an integrated test that incorporates all critical processes at least annually.

An institution must test all new equipment or application software. Physical workspace and equipment for required personnel is as important as data processing capacity. Contingency planning for recovery facilities should take into account location, size, computer and telecommunications capacity, and required amenities needed to recover critical business functions and accommodate essential personnel.

Management should consider geographic distance and diversity when determining the physical location of recovery sites. Independent third-party assessments that specifically address distance issues and the institution's unique location can be valuable in analyzing alternatives and validating recovery assumptions. Recovery sites should be subject to a threat analysis that assesses the likelihood of widespread regional events. Locating business recovery centers (BRCs) too close to the primary site or in high-risk areas does not sufficiently insulate a regulated entity from regional events. In all cases, management should document and support, and the board should approve, all decisions about BRCs. The board is ultimately responsible for proximity decisions.

Institutions often place BRCs in or near the hot-site and a number of different approaches are acceptable. Employees must have adequate workstations, supplies, and availability of key processes. The organizational plan may address, at an executive level, the overall scheme, describe work locations, special needs, etc. FHFA would not consider it acceptable for a BRC to have work space or capacity that is not sufficient for all essential personnel.

Regulatory Environment

The primary regulations, standards, and guidance that pertain to business continuity planning are set forth below.

1) ***Rules and Regulations of the Federal Housing Finance Agency (FHFA) and its predecessors, the Federal Housing Finance Board (Finance Board) and the Office of Federal Housing Enterprise Oversight (OFHEO), which include the following parts and sections relevant to business continuity planning:***

   12 CFR Part 1236 of FHFA's regulations—Prudential Management and Operations Standards (PMOS). The PMOS rule establishes minimum prudential standards for safe and sound business practices of the regulated entities. Although other standards may apply depending upon the circumstances, the primary standards that should be considered when evaluating business continuity planning are:

   a) Standard 1 – Internal Controls and Information Systems
      i. Principle 8 – A regulated entity should have an effective risk assessment process that ensures that management recognizes and continually assesses all material risks, including credit risk, market risk, interest rate risk, liquidity risk, and operational risk.
      ii. Principle 12 – A regulated entity should have secure information systems that are supported by adequate contingency arrangements.
   b) Standard 8 – Overall Risk Management Processes
      Principle 11 – A regulated entity should have adequate and well-tested disaster recovery and business resumption plans for all major systems and have remote facilitates to limit the effect of disruptive events.
   c) Standard 10 – Maintenance of Adequate Records
      i. Principle 2 – A regulated entity should ensure that assets are safeguarded and financial and operational information is timely and reliable.

ii. Principle 5 – A regulated entity should ensure that reporting errors are detected and corrected in a timely manner.

Applicable to Fannie Mae and Freddie Mac:

12 CFR 1720.2 of OFHEO's regulations – Safety and soundness standards, and specifically, Appendix A to Part 1720 of OFHEO's regulations– Policy Guidance; Minimum Safety and Soundness Requirements. Each Enterprise should establish and implement policies and procedures to ensure that its computing resources, proprietary and nonpublic information, and data are reliable, accurate, and available at all times as needed for its business operations, including an ability to affect timely recovery and resume operations after a reasonably foreseeable adverse event.

Applicable to the Federal Home Loan Banks and the Office of Finance:

12 CFR Part 917 of the Finance Board's regulations – Powers and Responsibilities of Bank Boards of Directors and Senior Management. In particular, Section 917.3, Risk Management, and Section 917.6, Internal Control System, are pertinent. Among other requirements, these sections obligate the board to adopt a risk management policy that addresses business risk and establish an effective internal control system that addresses efficient and effective bank activities, safeguarding of assets, reliable and complete reporting, and compliance with laws and regulations, respectively.

2) ***Advisory Bulletins of the Federal Housing Finance Board that provide supervisory guidance relating to the topic of business continuity planning are the following:***

Advisory Bulletin 02-3, dated February 13, 2002, provides guidance on specific attributes to be considered by FHLBanks in the formulation of their business continuity plans.

Advisory Bulletin 03-2, dated February 10, 2003, provides guidance on the establishment of bilateral agreements with other FHLBanks.

Advisory Bulletin 05-05, dated May 18, 2005, provides guidance on the risk management responsibilities of the board of directors, senior management, and risk management.

3) ***Other industry resources pertaining to business continuity planning which offer guidance on best practices include:***

Federal Emergency Management Agency (FEMA) – The Business Continuity Plan website at http://www.Ready.gov provides resources for plan preparation, development and execution.

Federal Financial Institutions Examination Council (FFIEC) – The Information Technology Examination Handbooks for Business Continuity Planning and Operations addresses specific controls and procedures as to business continuity planning.

NIST Special Publication 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems, dated May 2010 provides instructions, recommendations, and considerations for federal information system contingency planning.

Additional Regulatory and Business Considerations

Each regulated entity and the Office of Finance has developed a specific approach to its plan. They each incorporate their different recovery philosophies, services offered, customer base, recovery needs, geographical areas, and technical infrastructures. Most have an enterprise plan that is translated into programs on the department or business unit level, and coordinate these programs using a centralized approach. This allows business units to establish recovery processes unique to their needs and allows the organization to be able to identify gaps and promote consistency.

Some of the institutions have structured the execution of the plan to fall under a specific business unit. For example, sometimes they place that responsibility within the Information Technology or Risk Management divisions. In other instances, they have the execution of the plan as a standalone function. While the standalone approach might be the strongest of all structures, the board must ensure that, regardless of where it is, the plan and resulting programs are effective. If disaster recovery planning is segregated from the overall business continuity plan, the board must also ensure that this structure is effective and that the communication and business processes linking the two components are also effective.

Processing environments vary greatly as well. Some institutions have elected to outsource the function, and some have chosen to outsource only certain processes, such as database management. Most institutions continue to have in-house environments where the institution owns and supports their infrastructure, and mixes vendor software with their own in-house developed applications. Some environments have been in operations for years and some environments are undergoing upgrades. All environments must have adequate cooling systems and be physically secured. Examiners must be familiar with the complexities of mainframe, mid-range, and wide-area network environments.

Regulated entities and the Office of Finance have also taken advantage of more recent innovations such as virtual computing, and consideration of cloud computing is ongoing. Cloud computing, which may hold differing meanings to various parties, typically refers to shared computing where applications and resources are accessed and run via the Internet rather than on local servers or devices. Examiners must be diligent to ensure that the organization is evaluating and documenting risk when it moves into a newer technology. On the other hand, examiners must also be aware of organizations that do not keep pace with technology. As vendors introduce new products, they offer less support for their older products and at some point no longer support those older products. Older products become obsolete and support eventually wanes or ceases altogether. Furthermore, using obsolete equipment or applications (or equipment or applications nearing obsolescence) also raises security concerns.

Examination Guidance

The workprogram for the Business Continuity Planning examination module is detailed below. If this module is included in the examination scope, the examiner must perform worksteps sufficient in coverage to document the basis for conclusions on the quantity of risk and quality of risk management pertaining to this area. Transaction testing is mandatory and the examiner must document sufficient worksteps from Section 4, *Testing,* to support the findings and conclusions from this examination module.

In determining the extent of review and testing he or she will conduct in completing each examination, the examiner should take into account any applicable FHFA off-site monitoring or analysis reports. Such reports might include analyses of the quality and effectiveness of corporate governance practices, financial condition and performance, economic and housing industry conditions, internal controls, and audit coverage relating to the institution's business continuity planning activities. In addition, where suggested worksteps overlap with other workprograms or analyses undertaken by FHFA economists, financial analysts, accountants, or examiners, the Examiner-in-Charge (EIC) should collaborate with those responsible for completing the corresponding workprograms or analyses to ensure adequate and consistent coverage.

NOTE: Text in (*italics*) referenced in a workstep represents illustrative guidance that serves as suggestions for specific inquiry.

1. Scope of Examination Work Performed

1) Review past reports of examination for outstanding issues or previous problems related to business continuity planning.

2) Review FHFA off-site monitoring or analysis reports, and workpapers produced as part of on-going monitoring, related to business continuity planning.

3) Assess the status of outstanding Matters Requiring Attention and violations pertaining to business continuity planning.

4) Review internal audit reports for outstanding issues relating to business continuity planning.

5) Review minutes of meetings of the board of directors and relevant board and management committees for any issues regarding business continuity planning.

6) Review the following prior examination documents and reports for outstanding issues or problems:

   a) Prior examination workpapers;
   b) Internal and external audit reports, including Statement on Standards for Attestation Engagement (SSAE) 16 reports;
   c) Business continuity test scenarios;
   d) Business continuity test schedules;
   e) Business continuity test results; and
   f) Risk assessments performed on the institution, department or business unit level.

   (What have been the historical issues/problems? What were the identified root causes for the historical issues/problems? Was management aware of the historical issues/problems before they appeared in internal reports?)

7) Review management's response to audit recommendations noted since the last examination. *(Was management's response adequate? Was the timing of corrective action appropriate? Did management resolve the root causes of the issue rather than just specific audit deficiencies? Are any issues still outstanding? How effective are monitoring systems used to track the implementation of recommendations on an on-going basis?)*

8) Interview management and review the business continuity request information to understand the institution's BCP process. *(Have there been any significant changes in management, business strategies or internal business processes that could affect the business recovery process? Have there been any significant changes outside of the institution (e.g., industry, regulatory environment) since the last examination? Have there been any material changes in the audit program, scope, or schedule related to business continuity activities? Have there been any significant changes in the information technology environment or changes to configurations or components? Have there been any changes in key service providers (e.g., technology, communication, backup/recovery) or software vendors? Have there been any other internal or external factors that could affect the business continuity process?)*

9) Determine and assess management's consideration of newly identified threats and vulnerabilities to the institution's business continuity process. *(Has management effectively identified and analyzed technological and security vulnerabilities; internally identified threats; and externally identified threats (including security alerts, pandemic alerts, cyber-security alerts or emergency warnings published by information sharing organizations or local, state, and federal agencies)?)*

10) Establish and document the scope of the examination by focusing on those factors that present the greatest degree of risk to the institution. *(What are the examination objectives?*

What are the details of what will be reviewed? What will not be reviewed in order to evaluate the institution's business continuity planning process?)

Summarize the work performed in the examination of the institution's business continuity planning area. To the extent there were modifications to the originally planned scope based on concerns identified during the examination, document those changes and the reasons for such changes.

2. Description of Risks

1) Determine if the institution has identified any new risks since the last examination and if the identification of potential risks is appropriate. *(How effective is the institution's process for identifying new risks? Are there any new risks that the institution failed to identify?)*

2) Evaluate the institution's analysis of trends in the risk(s) to the organization. *(How effective is the institution's process for identifying and assessing the effects of trends in the risks? Are there any trends in the risks that the institution failed to identify?)*

3) Determine if the institution has undergone any changes that would expose it to new risks, affect its exposure to existing risks, or change the trends of any risks. *(If yes, how effective was the institution's process to identify and assess the effect of the change?)*

4) Determine if there have been any changes in the industry that would expose the entity to any new risks, affect the entity's exposure to risks, or change the trends of any risks. *(If yes, how effective was the institution's process to identify and assess the effect of the change?)*

5) Determine whether a workflow analysis was performed to ensure that all departments and business processes, as well as their related interdependencies, were included in the BIA and any risk assessments. *(Is the analysis well-documented? Are the assumptions appropriate? Are there significant functions that the institution has failed to include in the analysis? Did the institution involve appropriate personnel from various departments in the analysis process?)*

6) Review the organization's risk assessments and determine whether they include the effect and probability of disruptions of information services, technology, personnel, facilities, and services provided by third-parties. *(Are the risk assessments complete? Do they take into consideration natural events such as fires, floods, severe weather, air contaminants, pandemics or hazardous spills? Do they consider technical events such as communication failure, power failure, equipment and software failure, transportation system disruptions, or water system disruptions? Do they consider malicious activity including fraud, theft, or blackmail; sabotage; vandalism and looting; terrorism; or cyber-attacks?)*

7) Determine whether the continuity strategy addresses interdependent components. *(Does the strategy appropriately address utilities, telecommunications, third-party technology providers, key suppliers/business partners, and internal systems and business processes?)*

8) Determine whether the plan incorporates management's analysis of the effect on operations if essential functions or services provided by outside parties are disrupted during a pandemic, cyber or similar event. *(Does management maintain an accurate, complete, and timely list of service providers or other outside parties that provide essential functions? Is management's analysis of the likely effects appropriate?)*

9) Determine whether the plan includes continuity plans and other mitigating controls (e.g., social distancing, teleworking, functional cross-training, and conducting operations from alternative sites) to sustain critical internal and outsourced operations in the event large numbers of staff are unavailable for long periods. *(Are the scenarios that the institution utilized appropriate? Are there scenarios that should have been considered but were not? Are the assumptions appropriate? Did the institution involve appropriate personnel from various departments during the planning process?)*

3. Risk Management

Risk Identification Process

1) Determine whether the BIA identifies maximum allowable downtime for critical business functions, acceptable levels of data loss and backlogged transactions, RTOs, RPOs, recovery of the critical path (i.e., business processes or systems that should receive the highest priority), and the costs associated with downtime. *(Are the approved thresholds appropriate? Are the assumptions appropriate? Have there been any actual events that caused any thresholds to be exceeded?)*

2) Verify that reputational, operational, compliance, and other risks relevant to the institution are considered in the BIA and risk assessments. *(Has the institution appropriately considered all relevant risks?)*

3) Review the BIA and risk assessments to determine whether the prioritization of business functions is adequate. *(Does the institution have an effective process to prioritize business functions? Are the assumptions appropriate? Are all relevant business functions included in the prioritization process?)*

4) Determine whether the board has established an on-going, process-oriented approach to business continuity planning that is appropriate for the size and complexity of the institution.

(Does the process include a BIA, risk assessments, risk management, and risk monitoring and testing? Does the planning process encompass the institution's business continuity strategy, which is the ability to recover, resume, and maintain all critical business functions?)

5) Assess the board's knowledge of and commitment to the plan and resulting programs. *(Do the minutes of the board reflect that board members ask relevant questions? Has the board approved the organization's plan? Has the board approved the organization's programs? Has it designated a board committee to support related activities? Do the members demonstrate a satisfactory understanding of attendant risks? Is any board member trained in relevant issues? Does the board receive, at least annually, plan updates? Does the board require that management report all significant unplanned disruptions?)*

6) Assess executive management's involvement and commitment to the plan and resulting programs. *(Has executive management assigned a qualified plan administrator to promote an effective plan? Has executive management provided the proper level of authority for the plan administrator to do an effective job? Does executive management track related activities? Does executive management set expectations for managers to maintain an appropriate program within their business units and encourage them to support related efforts? Has management implemented adequate metrics to promote an effective plan?)*

7) Determine whether adequate risk mitigation strategies have been considered. *(Has the institution appropriately considered alternate locations and capacity for: data centers and computer operations; back-room operations; work locations for business functions; timing and logistics of getting key personnel to the alternate location; and telecommunications and remote computing? Has the institution appropriately considered backup of: data; operating systems; applications; utility programs; and telecommunications? Has the institution appropriately considered secure and up-to-date off-site storage of: backup media; supplies; and system documentation (e.g., topologies; inventory listing; firewall, router, and network configurations; operating procedures)? Has the institution appropriately considered alternate power supplies (e.g., uninterruptible power source, backup generators)? Has the institution appropriately considered recovery of data (e.g., backlogged transactions, reconciliation procedures)? Has the institution appropriately considered preparation for return to normal operations once the permanent facilities are available?)*

8) Determine whether satisfactory consideration has been given to geographic diversity. *(Has the institution appropriately considered alternate facilities; alternate processing locations; alternate telecommunications; alternate staff; and off-site storage? Do temporary or recovery sites operate from the same critical infrastructure as the entity, including electricity, water, telecommunications, transportation or data? See FFIEC Business Continuity Planning Booklet, Appendix G for additional information.)*

9) Review and assess the completeness of the plan.

   a) *(Does the plan appropriately address the recovery of critical business units/departments/functions/applications according to the priority ranking in risk assessments? Does the plan consider interdependencies among systems; and consider long-term recovery arrangements? Does the plan appropriately address the recovery of vendors and outsourcing arrangements?*
   b) *Does the plan appropriately take into account: personnel; communication with employees, emergency personnel, FHFA, vendors/suppliers, customers, and the media; technology issues (e.g., hardware, software, network, data processing equipment, telecommunications, remote computing, vital records, utilities); vendor(s') ability to service contracted customer base in the event of a major disaster or regional event; facilities; liquidity; security; financial disbursement (e.g., purchase authorities and expense reimbursement for senior management during a disaster); and manual operating procedures?*
   c) *Does the plan appropriately include emergency preparedness and crisis management plans that include an accurate contact tree, as well as primary and emergency contact information, for communicating with employees, service providers, vendors, FHFA, municipal authorities, and emergency response personnel; define responsibilities and decision-making authorities for designated teams or staff members; explain actions to be taken in specific emergencies; define the conditions under which the backup site would be used; include procedures for notifying the backup site; identify a current inventory of items needed for off-site processing; designate a knowledgeable public relations spokesperson; and identify sources of needed office space and equipment and a list of key vendors (e.g., hardware, software, telecommunications.)?)*

10) Determine whether personnel are regularly trained in their specific responsibilities under the plan and whether current emergency procedures are posted in prominent locations throughout the facility. *(When was the last time personnel were trained regarding the plan? Does the institution have an appropriate process to ensure that new employees are trained regarding the plan in a timely manner? Does the institution have an appropriate process to ensure that personnel are trained in a timely manner after significant changes to the plan? Does the institution have appropriate emergency procedures posted? Are the postings in prominent locations throughout all of the institution's facilities? Does the institution have an appropriate process to ensure that the postings are current and complete at each of its facilities?)*

11) Determine whether there are adequate processes in place to ensure that the current plan is maintained and disseminated appropriately. *(Has the institution appropriately designated personnel who are responsible for maintaining changes in processes, personnel, and environment(s)? Does the institution have an appropriate process to ensure timely distribution of revised plans to personnel?)*

12) Determine whether there is a comprehensive, written agreement or contract for alternative processing or facility recovery. *(Does the institution have an appropriate process to periodically review the written agreement or contract to assess if it is still acceptable? Have there been any occasions where the institution has had to rely upon alternative processing or facility recovery? If so, did the institution analyze the scenario to identify any "lessons learned" that were subsequently addressed, or should have been addressed, through a change to the written agreement or contract?)*

13) Determine whether the plan appropriately includes pandemic related elements, and is appropriately scaled for the size, activities, and complexities of the institution. (*Does the plan appropriately include a documented strategy that provides for scaling the institution's pandemic efforts so they are consistent with the effects of a particular stage of a pandemic outbreak, such as first cases of humans contracting the disease overseas, first cases within the United States, and first cases within the institution? Does the plan include a comprehensive framework of facilities, systems, or procedures that provide the institution the capability to continue its critical operations in the event that a large number of the institution's staff is unavailable for prolonged periods (e.g., social distancing to minimize staff contact, telecommuting, or conducting operations from alternative sites)? Does the plan appropriately include testing pandemic planning practices and an oversight program to ensure ongoing reviews and updates to the pandemic plan? Does the plan appropriately include the assignment of responsibility for pandemic planning, preparing, testing, responding, and recovering? Does the plan appropriately address communication and coordination with institution employees and the following outside parties regarding pandemic issues: critical service providers; key financial correspondents; customers; media representatives; local, state, and federal agencies; and FHFA?)*

14) Determine whether the board, or a committee thereof, and senior management provide appropriate oversight of the institution's pandemic preparedness program. *(Do the minutes of the board or designated committee reflect that it appropriately discusses the institution's pandemic preparedness program? Are there aspects of the institution's pandemic preparedness program that should be enhanced that the board or designated committee or senior management failed to recognize?)*

15) Determine whether the plan addresses modifications to normal compensation and absenteeism policies to be enacted during a pandemic. The nature of an organization's compensation and absenteeism policies can support or hinder their plan. For example, compensation policies can be designed to provide incentives for employees to properly staff recovery sites in the event of a natural disaster, which would support the plan. Conversely, in the event of a disruption like a pandemic, the organization may want to provide incentives to personnel to not work from an office but rather telecommute therefore reducing opportunities for transmission. Well-crafted compensation and absenteeism policies would support this aim. *(Does the institution address compensation and absenteeism policies separately for a pandemic from other business continuity planning events? If so, is it appropriate?)*

16) Determine whether pandemic risks have been incorporated into the BIA. *(Do the institution's continuity plans and strategies appropriately reflect the results of the analysis?)*

17) Determine whether the plan provides for an appropriate testing program to ensure that continuity plans will be effective and allow the institution to continue its critical operations. *(Does the testing program appropriately incorporate telecommuting to simulate and test remote access; internal and external communications processes and links; table top operations exercises; and local, regional, or national testing/exercises?)*

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

19) Determine whether test results are appropriately analyzed and addressed. *(Does the institution compare test results against stated objectives? Are test issues assigned ownership? Does the institution have an appropriate mechanism to prioritize test issues? Are test problems tracked until resolution? Does the institution prepare and document recommendations for future tests? Does the institution have an appropriate process to ensure that the plan and programs are adjusted, as needed, based upon test results?)*

20) Determine whether the test processes and results have been subject to independent observation and assessment by a qualified third-party (e.g., internal or external audit). *(What are the third-party's qualifications? Does the third- party's written report demonstrate that the party effectively reviewed the institution's test processes and results?)*

21) Determine whether an appropriate level of re-testing is conducted in a timely fashion to address test problems or failures. *(How much time was between the original test and the re-test? Was the time difference warranted? Does the institution have appropriate guidelines to ensure timely re-testing? Does the institution have appropriate guidelines to ensure that the appropriate test problems or failures are re-tested?)*

Organizational Structure

1) Determine whether a senior manager or committee has been assigned responsibility to oversee the development, implementation, and maintenance of the plan. *(Is the assigned oversight responsibility appropriate?)*

2) Determine whether the board and senior management have ensured that integral groups are involved in the business continuity process. *(Does the institution's business continuity process appropriately include business line management, risk management, information*

technology, facilities management, and audit? Are there any groups that should be included, but are not?)

3) If the organization has designated a plan administrator, assess their qualifications for and success in preparation and execution of the plan. *(Has the plan administrator received appropriate training? Does the plan administrator have appropriate certifications and/or experience? Does the plan administrator have sufficient time to do a satisfactory job? Does the plan administrator ensure that the components of an effective plan are in place? Does the plan administrator verify information obtained from any recovery team members? Does the plan administrator have good channels of communication and support with all essential areas of the organization, including the board?)*

Policy and Procedure Development

1) Determine whether the board and senior management have established entity-wide written programs that address and validate the continuity of the institution's mission critical operations. *(Are the written programs complete, timely, consistent, and relevant?)*

2) Determine whether the board and senior management oversee the timely revision of programs based on problems noted during testing and changes in business operations. Determine how any revisions to programs are rolled up or integrated in to the entity's plan. *(When was the last time a change was made to the programs? Why was the change made? Was the change appropriate? Was the change timely? Are there changes that should be made that the board or senior management failed to recognize or fully implement?)*

3) Determine whether the board and senior management review and approve the BIA, risk assessments, written plan, policies and procedures, testing program, and testing results. *(Are the reviews conducted at least annually? Are the reviews and approvals appropriately documented in the board minutes?)*

4) Verify that appropriate policies, standards, and processes address BCP issues. *(Does the institution's policies, standards, and processes effectively address: security; project management; change control process; data synchronization, backup, and recovery; crisis management (e.g., responsibility for disaster declaration and dealing with outside parties); incident response; remote access; employee training; notification standards (e.g., to employees, customers, FHFA, vendors, service providers); insurance; and government and community coordination?)*

5) Determine whether the institution has an appropriate business continuity testing policy. *(Does the policy sets testing expectations for entity-wide continuity functions, business lines, support functions, and crisis management? Does the testing policy identify key roles and responsibilities of the participants in the testing program? Does the testing policy establish a testing cycle with increasing levels of scope and complexity?)*

6) Determine whether the institution has a business continuity testing strategy that includes documented test plans and related testing scenarios, testing methods, and testing schedules; and also addresses expectations for mission critical business lines and support functions. *(How appropriate is the scope and level of detail of the testing program? How appropriate is the institution's involvement of staff, technology, and facilities in the development of the business continuity testing strategy? Has the institution effectively communicated expectations for testing internal and external interdependencies? Does the institution conduct an evaluation of the reasonableness of assumptions used in developing the testing strategy?)*

7) Determine whether the testing strategy describes management's assumptions and whether the assumptions appear reasonable. *(Do the assumptions appropriately address available resources and services, length of disruption, testing methods, capacity and scalability issues, and data integrity? Are the assumptions reasonable, based on a cost/benefit analysis and recovery and resumption objectives?)*

8) Determine whether the testing strategy addresses the need for entity-wide testing and testing with significant third parties. *(Does the institution have an appropriate process to ensure that any new, significant third parties are incorporated into the testing strategy on a timely basis?)*

9) Determine whether the testing strategy includes guidelines for the frequency of testing that are consistent with the criticality of business functions, RTOs, RPOs, and recovery of the critical path, as defined in the BIA and risk assessments, and corporate policy. *(Does the institution routinely comply with the established guidelines for the frequency of testing?)*

10) Determine whether the testing strategy addresses the documentation requirements for all facets of the continuity testing program, including test scenarios, plans, scripts, results, and reporting. *(Does the institution comply with the established documentation requirements? Do the documentation requirements address timeliness, completeness, accuracy, relevancy, and consistency?)*

11) Determine whether the testing strategy includes testing the effectiveness of a institution's crisis management process for responding to emergencies. *(Does the testing strategy include testing the effectiveness of the institution's: roles and responsibilities of crisis management group members; risk assumptions; crisis management decision process; coordination with business lines, information technology, internal audit, and facilities management; communication with internal and external parties through the use of diverse methods and devices (e.g., calling trees, toll-free telephone numbers, instant messaging, websites); and notification procedures to follow for internal and external contacts?)*

12) Determine whether the testing strategy appropriately addresses physical and logical security. *(Does the testing strategy consider the facility, vital records and data, telecommunications, and personnel?)*

13) Determine whether the testing strategy addresses staffing considerations. *(Does the testing strategy consider the ability to perform transaction processing and settlement? Does the testing strategy consider the ability to communicate with key internal and external stakeholders? Does the testing strategy consider the ability to reconcile transaction data? Does the testing strategy consider the accessibility, rotation, and cross training of staff necessary to support critical business operations? Does the testing strategy consider the ability to relocate or engage staff from alternate sites? Does the testing strategy consider staff and management succession plans? Does the testing strategy consider staff access to key documentation (e.g., plans, procedures, and forms)? Does the testing strategy consider the ability to handle increased workloads supporting critical operations for extended periods?)*

14) Determine whether the testing strategy addresses technology considerations. *(Does the testing strategy address testing the data, systems, applications, and telecommunication links necessary for supporting critical financial markets? Does the testing strategy address critical applications, recovery of data, failure of the network, and resilience of telecommunication links? Does the testing strategy address incorporating the results of telecommunication diversity assessments and confirming telecommunications circuit diversity? Does the testing strategy address testing disruption events affecting connectivity, capacity, and integrity of data transmission? Does the testing strategy address testing recovery of data lost when switching to out-of-region, asynchronous backup facilities?)*

15) Determine whether the business line testing strategy addresses the facilities supporting the critical business functions and technology infrastructure. *(Does the testing strategy address environmental controls such as the adequacy of backup power generators; heating, ventilation, and air conditioning [HVAC] systems; mechanical systems; and electrical systems? Does the testing strategy address workspace recovery such as the adequacy of floor space, desktop computers, network connectivity, e-mail access, and telephone service? Does the testing strategy address remote access such as the adequacy of connectivity and availability of critical systems? Does the testing strategy address physical security facilities such as the adequacy of physical perimeter security, physical access controls, protection services, and video monitoring?)*

16) Determine whether the test scenarios are appropriate. *(Do the scenarios include a variety of threats and event types? Has the institution included a range of scenarios that reflect the full scope of the institution's testing strategy, an increase in the complexity and scope of the tests, and tests of wide-scale disruptions over time?)*

17) Determine whether the test scenarios include detailed steps that demonstrate the viability of continuity plans. *(Do the scenarios include a deviation from established test scripts to include unplanned events, such as the loss of key individuals or services? Do the scenarios test the ability to support peak transaction volumes from backup facilities for extended periods?)*

18) Determine that test scenarios reflect key interdependencies. *(Do the scenarios include customers and counterparties that pose significant risks to the institution? Are periodic connectivity tests performed from their primary and contingency sites to the institution's primary and contingency sites? Do the scenarios test capacity and data integrity capabilities through the use of simulated transaction data? Do the scenarios include testing or modeling of backup telecommunications facilities and devices to ensure availability to key internal and external parties?)*

19) Determine that the test plans and test scripts are documented and clearly reflect the testing strategy, that they encompass all critical business and supporting systems, and that they provide test participants with the information necessary to conduct tests of the institution's continuity plans. *(Does the documentation clearly reflect participants' roles and responsibilities, define decision makers, and establish rotation of test participants? Does the documentation communicate the assigned command center and assembly locations? Does the documentation clearly state the test event dates; and test scope and objectives, including RTOs, RPOs, recovery of the critical path, duration of tests, and extent of testing (e.g., connectivity, interoperability, transaction, and capacity)? Does the documentation include sequential, step-by-step procedures for staff and external parties, including instructions regarding transaction data and references to manual work-around processes, as needed? Is there detailed information regarding the critical platforms, applications, and business processes to be recovered? Are there detailed schedules to complete each test? Does the documentation provide for a summary of test results (e.g., based on goals and objectives, successes and failures, and deviations from test plans or test scripts) using quantifiable measurement criteria?)*

Risk Metrics

Evaluate and conclude on the effectiveness of any metrics pertaining to BCP that the institution may monitor. *(Are the metrics appropriate? Are there any metrics the institution should be monitoring that it is not? Does the institution have an appropriate process in place to routinely review the metrics to assess if they continue to be relevant?)*

Reporting

1) Assess and conclude on the adequacy of the institution's business continuity reporting. *(Are reports pertaining to business continuity appropriate? Are they produced in a timely manner? Are they delivered to the appropriate audience? Do they present an accurate assessment of the institution's business continuity status? Is there any information that should be included that is not? Is the information consistent within each report and across different reports?)*

2) Determine whether the plan appropriately addresses pandemic reporting. *(Does it address management's monitoring of alert systems that provide information regarding the threat and*

progression of a pandemic? Does it provide for escalating responses to the progress or particular stages of an outbreak?)

Internal/External Audit

Determine whether audit involvement in the plan and resulting programs is effective. *(Is there appropriate audit coverage of the plan? Does audit perform an assessment of business continuity preparedness during reviews of business line? Does audit participate in testing as an observer or as a reviewer of test plans and results? Is there appropriate documentation of audit findings?)*

Information Technology

1) If the institution is relying on in-house systems at separate physical locations for recovery, verify that the equipment is capable of independently processing all critical applications. *(Has the institution effectively planned for a scenario where separate physical locations may become partially and wholly unavailable?)*

2) If the institution is relying on outside facilities for recovery, assess and conclude on the institution's business continuity planning with regard to the recovery site. *(Does the recovery site have the ability to process the required volume? Does the recovery site provide sufficient processing time for the anticipated workload based on emergency priorities? Is the recovery site available for use until the institution achieves full recovery from the disaster and resumes activity at the institution's own facilities?)*

3) Determine how the recovery facility's customers would be accommodated if simultaneous disruptions were to occur to several customers during the same period of time. *(Is this acceptable? Does the institution have an appropriate process in place to routinely review this issue with the recovery facility to ensure the planned actions remain acceptable?)*

4) Determine whether the institution ensures that when any changes (e.g., hardware or software upgrades or modifications) in the production environment occur that a process is in place to make or verify a similar change in each alternate recovery location. *(Does the institution have an appropriate process in place to ensure that alternate recovery locations are tested within a reasonable time period after each significant change?)*

5) Determine whether the institution is kept informed of any changes at the recovery site that might require adjustments to the institution's software or its recovery plan(s). *(How effective is the communication process? Have there been any instances where changes were made but the institution was not informed? If so, what steps has the institution taken to ensure that this does not occur again?)*

6) Determine whether adequate physical security and access controls exist over data backups and program libraries throughout their life cycle. *(Do the controls encompass when the data*

backups and program libraries are created, transmitted/delivered, stored, retrieved, loaded, and destroyed?)

7) Determine whether appropriate physical and logical access controls have been considered and established for the inactive production system when processing is temporarily transferred to an alternate facility. *(Does the institution test these controls on a regular basis?)*

8) Determine whether the intrusion detection and incident response plan considers facility and systems changes that may exist when alternate facilities are used. *(Does the institution conduct intrusion detection testing at all alternate facilities? Has the institution developed an appropriate incident response plan for all alternate facilities?)*

9) Determine whether the methods by which personnel are granted temporary access (physical and logical) during continuity planning implementation periods are reasonable. Conclude on the appropriateness of steps in this area. *(Does the institution have an appropriate process to ensure that all temporary access rights are revoked as soon as they are no longer necessary?)*

10) Evaluate the extent to which backup personnel have been reassigned different responsibilities and tasks when business continuity planning scenarios are in effect and if these changes require a revision to systems, data, and facilities access. *(Has the regulated entity appropriately incorporated the use of backup personnel in relevant testing scenarios?)*

11) Review the assignment of authentication and authorization credentials to determine whether they are based upon primary job responsibilities and if they also include BCP responsibilities. *(Are the assignment of credentials appropriate?)*

12) Determine whether management has analyzed remote access requirements, including the infrastructure capabilities and capacity that may be necessary during a pandemic. *(Has the institution appropriately incorporated remote access during a pandemic in relevant testing scenarios?)*

13) Determine whether the plan addresses communications and connectivity with any technology service providers (TSPs) in the event of a disruption at the institution. *(Has the institution appropriately tested the communication process and connectivity with all TSPs?)*

14) Determine whether the plan and programs address communications and connectivity with any TSPs in the event of a disruption at any of the service provider’s facilities. *(Has the institution participated in tests with all TSPs in the scenario where the TSPs experience a disruption? Have there been any instances where a TSP has experienced a disruption? If so, how well did the institution execute its plan?)*

15) Determine whether there are documented procedures in place for accessing, downloading, and uploading information with TSPs, correspondents, affiliates, and other service providers

from primary and recovery locations in the event of a disruption. *(Have the procedures been tested? Does the institution have an appropriate process in place to ensure that the procedures are updated as necessary in a timely manner?)*

16) Determine whether the institution has a copy of the TSPs' business continuity plan and incorporates it, as appropriate, into their plan. *(Does the institution have an appropriate process in place to ensure that it receives all updates to any TSP's business continuity plans in a timely manner?)*

17) Determine whether management has received and reviewed testing results of their TSPs. *(When was the last time testing was conducted? Is the timeframe appropriate? How quickly after the testing did the institution receive the test results? Is the timeframe appropriate? How quickly after receiving the test results did the institution review the results? Is the timeframe appropriate?)*

18) Assess the effectiveness of the institution's testing with the critical service providers. *(Did the test scenarios include testing from the institution's primary location to the TSPs' alternative location? Did the test scenarios include testing from the institution's alternative location to the TSPs' primary location? Did the test scenarios include testing from the institution's alternative location to the TSPs' alternative location?)*

19) Determine whether the regulated entity's management has assessed the adequacy of the TSPs' plan through their vendor management program. *(Does the plan address contract requirements and SSAE 16 reviews?)*

Compliance

1) Determine if the institution is in compliance with applicable laws, regulations, and any pertinent regulatory guidance. *(Are there any instances of violations? If so, what are the root causes of the violations? How should internal controls be strengthened to ensure there are no future regulatory violations?)*

2) Assess compliance with 12 CFR Part 1236, FHFA's Prudential Management and Operations Standards. In particular:

   a) Standard 1 – Internal Controls and Information Systems

      i) Principle 8 - A regulated entity should have an effective risk assessment process that ensures that management recognizes and continually assesses all material risks, including credit risk, market risk, interest rate risk, liquidity risk, and operational risk. *(Based upon the findings from this examination, does the regulated entity comply with the requirements of this Principle?)*
      ii) Principle 12 – A regulated entity should have secure information systems that are supported by adequate contingency arrangements. *(Based upon the findings from this*

examination, does the regulated entity comply with the requirements of this Principle?)

b) Standard 8 – Overall Risk Management Processes

Principle 11 - A regulated entity should have adequate and well-tested disaster recovery and business resumption plans for all major systems and have remote facilities to limit the effect of disruptive events. *(Based upon the findings from this examination, does the regulated entity comply with the requirements of this Principle?)*

c) Standard 10 – Maintenance of Adequate Records

i) Principle 2 - A regulated entity should ensure that assets are safeguarded and financial and operational information is timely and reliable. *(Based upon the findings from this examination, does the regulated entity comply with the requirements of this Principle?)*

ii) Principle 5 - A regulated entity should ensure that reporting errors are detected and corrected in a timely manner. *(Based upon the findings from this examination, does the regulated entity comply with the requirements of this Principle?)*

3) Determine if the regulated entity is in compliance with all applicable board-approved policies and procedures. *(Does the regulated entity have an appropriate process to ensure effective monitoring and enforcement of policy compliance?)*

4. Testing

1) Complete testing, as appropriate, to assess adherence with the institution's plan, programs, and policies and procedures.

2) Consider evaluating results from internal testing.

3) If possible, consider observing the institution's testing of the plan.

4) Visit a disaster recovery site to evaluate compliance with sound business continuity standards.

5) Based on testing completed, identify any potential problems with the institution's approach to ensuring business continuity.

5. Conclusions

1) Summarize conclusions for all examination work performed, including work performed by other FHFA staff as it relates to the institution's business continuity planning function. Develop a memorandum articulating the risks to the institution resulting from its BCP practices and management of those risks. The memorandum should clearly and articulately describe the basis of conclusions reached and summarize the analysis completed. Within the memorandum, discuss the types of risk the institution is exposed to (e.g., market, credit, operational); the level of risk exposure; the direction of risk (stable, decreasing, increasing); and the quality of risk management practices (strong, adequate, weak). A memorandum must be prepared irrespective of whether the examiner's assessment is positive or negative.

2) Conclude on the responsiveness to previous examination findings. Evaluate the adequacy of the institution's response to previous examination findings and concerns.

3) Develop findings and prepare findings memoranda, as appropriate. Based on examination work performed, develop findings communicating concerns identified during the examination. Findings should identify the most significant risks to the institution and the potential effect to the institution resulting from the concerns identified. Such documents should describe a remediation plan specifying the appropriate corrective action to address examination concerns and establish a reasonable deadline for the institution to remediate the finding. Communicate preliminary findings to the EIC, other interested examiners, and senior FHFA staff, as appropriate. Discuss findings with institution personnel to ensure the findings and analysis are free of factual errors.

4) Develop a list of follow-up items to evaluate during the next annual examination. In addition to findings developed in the steps above, include concerns noted during the examination that do not rise to the level of a finding. Potential concerns include issues the institution is in the process of addressing, but require follow-up work to ensure actions are completed appropriately. In addition, potential concerns should include anticipated changes to the institution's practices or anticipated external changes that could affect the institution's business continuity practices.

Workprogram

1. Scope of Examination Work Performed

Workpapers must document the examination activities undertaken to evaluate potential risks related to business continuity planning.

2. Description of Risks

- Identify areas of concern related to business continuity planning
- Assess current risks and trends in the risk to the organization emanating from the area being examined
- Evaluate changes within the organization or industry affecting risk
- Evaluate the organization's own risk-identification practices and conclude on its adequacy

3. Risk Management

- Assess and conclude on the adequacy of the organization's risk identification process
- Assess and conclude on the overall adequacy of internal controls, including an evaluation of:
    - The institution's organizational structure
    - Policy and procedure development for this area
    - Appropriateness of risk metrics established in this area
    - Reporting by management and the board
- Assess and conclude on the internal and external audit of risks
- Assess and conclude on the adequacy of information technology and controls related to business continuity planning
- Assess and conclude on the adequacy of the organization's efforts to ensure:
    - Compliance with laws, regulations and other supervisory guidance
    - Compliance with the organization's policies and procedures

4. Testing

- Complete testing, as appropriate, to assess adherence with applicable standards

5. Conclusions

- Summarize conclusions for all examination work performed related to business continuity planning
    - Conclude on the level of risk to the organization
    - Include an assessment of the adequacy of an organization's monitoring of risk and establishment of internal controls to mitigate risk
- Conclude on responsiveness to examination findings from previous examinations
- Develop findings and Matters Requiring Attention, violations, and recommendations, as appropriate
- Identify areas requiring follow-up examination activities or monitoring