FEDERAL HOUSING FINANCE AGENCY

ADVISORY BULLETIN

AB 2019-01: BUSINESS RESILIENCY MANAGEMENT

Purpose

This advisory bulletin (AB) provides Federal Housing Finance Agency (FHFA) guidance on business resiliency management at Fannie Mae, Freddie Mac, the Federal Home Loan Banks (FHLBanks), and the Office of Finance (OF) (collectively, the regulated entities).[1] This AB rescinds and replaces Federal Housing Finance Board Advisory Bulletin 02-3 Disaster Recovery Planning, February 13, 2002.

For purposes of this AB, business resiliency management refers to the regulated entity's ability to minimize the impact of disruptions and maintain business operations at predefined levels. Disruptions can expose the regulated entities to operational, financial, legal, compliance, and reputational risks. An effective business resiliency management program (program) helps to ensure safe and sound operations at each regulated entity.

Background

Uncontrolled events, such as natural disasters, pandemics, and cyberattacks, can threaten the regulated entities' ability to perform mission critical operations, such as providing liquidity and access to credit in the mortgage market. Disruptions in service can expose the regulated entities to a variety of risks and potentially lead to adverse economic consequences in the financial sector. A program establishes documented strategic processes and procedures that a regulated entity should follow to mitigate and respond to risks in order to continue its business operations.

The core components of a program include the business continuity plan (BCP), disaster recovery plan (DRP) and crisis management plan (CMP) (collectively, plans). The BCP is the written set of procedures a regulated entity follows to recover, resume, and maintain business functions and their underlying processes at acceptable predefined levels following a disruption. The BCP accounts for disruptions affecting personnel, equipment, facilities, data, third-party providers,

[1] The OF is not a "regulated entity" as the term is defined by statute (*see* 12 U.S.C. 4502(20)). However, for convenience, references to the "regulated entities" in this AB should be read to also apply to the OF.

and the technical assets associated with business functions and processes. The DRP is the documented process to recover and resume the regulated entity's IT infrastructure, business applications, and data services in the event of a major disruption. The CMP provides documented, coordinated responses to enterprise-wide disruptions, including overseeing the activation of the DRP and BCPs.

FHFA's general standards for safe and sound operations are set forth in the Prudential Management and Operations Standards (PMOS) at 12 CFR Part 1236 Appendix. Three relevant PMOS articulate guidelines for a regulated entity's board of directors and senior management to evaluate when establishing internal controls and information systems (Standard 1), overall risk management processes (Standard 8, especially Standard 8.11), and maintenance of adequate records (Standard 10). A business resiliency program that is aligned with this AB will meet FHFA's supervisory expectations on the points that the AB addresses, with respect to those standards. A business resiliency program that is not aligned with this AB may not meet those standards and may not be safe and sound.[2]

Guidance

FHFA expects the regulated entities to establish and maintain a program that includes the following:

I. Governance
II. Business Resiliency Cycle
    A. Risk Assessment and Business Impact Analysis
    B. Risk Mitigation and Plan Development
    C. Testing and Analysis
    D. Risk Monitoring and Program Sustainability

Each regulated entity should establish its program in alignment with its enterprise-wide risk management program,[3] and in accordance with all relevant FHFA guidance. The regulated entity should develop strategies, policies, procedures, and internal standards that apply to the program. The program should guide the regulated entity to respond appropriately to disruptions affecting business operations, personnel, equipment, facilities, IT systems, and information assets. In order to remain current and effective, the program should adopt a cyclical, process-oriented approach that incorporates the following steps: (1) risk assessment and business impact analysis, (2) risk mitigation and plan development, (3) testing and analysis, and (4) risk monitoring and program sustainability.

[2] 12 CFR 1236.4
[3] 12 CFR 1239.11(a).

I. Governance

The board of directors or a committee thereof (board) is responsible for maintaining a strong business resiliency culture and overseeing the program. The board provides oversight of senior management's implementation of the program and maintenance of plans that reflect the regulated entity's current operating environment and risk appetite. The board should review and approve the enterprise-wide business resiliency strategic objectives of the program on an annual basis.

As delegated by the board, senior management[4] is responsible for executing the program. Senior management ensures that:

- Each step of the program is carried out by assigned personnel with clear roles and responsibilities;
- There are designated resources and qualified personnel from across the regulated entity's business units and operations to develop and implement plans;
- Employees are adequately trained and participate in testing exercises, as necessary, to demonstrate understanding of their role when plans are activated in the event of a disruption;
- There is sufficient communication and coordination to properly execute plans and maintain enterprise-wide business resiliency;
- Effective reporting and metric requirements are in place, such as reviewing internal audit reports and providing reports to the board;
- The review and approval of plans involving critical business functions are conducted on an annual basis or when there are material changes in the operating environment that affect critical business functions; and
- The board is informed of significant issues involving the strategies, plans, or testing of critical business functions.

II. Business Resiliency Cycle

A. Risk Assessment and Business Impact Analysis

Developing an effective plan begins with a risk assessment that determines the potential threats to a regulated entity's business operations. A risk assessment considers the full spectrum of scenarios that could affect operations, ranging from low impact, high probability occurrences (such as power or telecommunication disruptions) to low probability, high impact occurrences (such as pandemics or natural disasters). As part of the risk assessment process, the regulated entity should take into account disruptions involving information services, equipment, personnel,

[4] The term "senior management" refers to those employees who plan, direct, and formulate policies, and provide the overall direction of the regulated entity for the development and delivery of products or services, within the parameters approved by the board.

facilities, and services by third-party providers. The regulated entities should also consider their proximity to infrastructure in conjunction with their susceptibility to threats.

The business impact analysis (BIA) assesses and prioritizes those business functions and processes, including their associated technical assets, that must be recovered after a disruption. The BIA should identify the potential impact of uncontrolled events on the regulated entity's ability to execute its business functions and processes. The regulated entity should also consider the impact of disruptions on its ability to perform its role in the financial marketplace, satisfy legal and regulatory requirements, follow safe and sound practices, maintain public confidence, and achieve its strategic goals.

Conducting a thorough and accurate BIA is the basis for developing effective plans and a comprehensive program for the regulated entity. As part of the BIA, the regulated entities should identify business functions and processes, evaluate and compare business function requirements, and identify interdependencies between critical systems, departments, personnel, and services that may be compromised during a disruption. The BIA should be risk-focused, taking into consideration the priority of certain business functions and processes. The BIA should be conducted at least annually.

Recovery point objectives (RPOs) and recovery time objectives (RTOs) are calculated results informed by the BIA. An RPO defines the maximum level of data loss (in terms of time) that can be afforded during a failure. An RTO estimates the maximum allowable downtime for business processes and associated technical assets that should be recovered after a disruption. The regulated entity should additionally consider how RTOs and RPOs affect data recovery and reconciliation, especially when business and IT interdependencies are involved. RTOs inform the regulated entity on how it should categorize and group business processes and technical assets from the most critical functions to the least critical.

B. Risk Mitigation and Plan Development

Risk Mitigation

The regulated entity should use the results from the risk assessment and BIA to determine appropriate recovery solutions that mitigate the risk of a disruption to a level that is acceptable for its business functions and processes. The recovery solutions may include data synchronization, redundant vendor support, alternative power sources, high-availability technologies for critical business functions, fire detection and suppression systems, and additional reserves of critical equipment and supplies. The regulated entity should also consider the appropriate insurance coverage for its business, taking into consideration the BIA findings and its risk profile.

Some business functions have high availability requirements where even minimal downtime presents risk. The regulated entities should have an alternate, geographically distinct data center as an enterprise-wide disaster recovery solution that maintains availability within pre-determined RTOs and RPOs. Alternatively, the regulated entity can rely on its cloud service provider.[5] A geographically distinct data center should be at an appropriate distance from the regulated entity's primary operations and should not be subject to the same inherent risks as the primary site during a disaster. Pursuant to the DRP, the alternate site would be activated to recover, by priority, the technical assets of the primary location. The facility should be capable of operating at the regulated entity's normal volume and be available for use until the regulated entity achieves full recovery from the disaster. For any FHLBank, partnering with another FHLBank is a useful strategy for short-term resumption of certain business processes, but by itself should not be considered an adequate disaster recovery solution.

If a third-party provider is used to mitigate business resiliency risk, the regulated entity should evaluate, according to the risk assessment or BIA, whether its business resiliency objectives are met within its third-party provider risk management framework.[6] Commensurate with the risk involved, the regulated entity should consider the strength of a third-party provider's business resiliency program.

The regulated entities should also consider risk mitigation strategies in addition to those addressing RPOs and RTOs. For instance, a senior management-approved response plan to handle media inquiries can reduce the risk of reputational harm after a disruptive event. FHFA also encourages the regulated entities to contact federal, state, and local authorities as needed to determine specific risks or exposures for their geographic location and requirements for accessing emergency zones. The regulated entities should consider taking advantage of government-sponsored emergency programs and coordinating with agencies, emergency personnel, and service providers during the recovery and resumption of operations.

Plan Development

The regulated entity should document how to implement the risk mitigation strategies and recovery solutions in its plans. Plans should include short-term and long-term recovery operations with steps to transition back to normal business based on the criticality of the business functions and processes affected. Plans should also account for internal and external dependencies in the event that third-party providers,[7] personnel, or certain equipment are unavailable or inefficient. Plans should avoid single points of failure as the strength of a plan can be diminished by weak components. If the regulated entity outsources the development of

[5] *See Cloud Computing Risk Management*, AB 2018-04.
[6] *See Oversight of Third-Party Provider Relationships*, AB 2018-08.
[7] Ibid.

its plans, it is responsible for choosing a service provider that has the requisite expertise appropriate for the entity's size, complexity, and risk environment.

The regulated entity's plans should include the following:

- The assumptions used to develop each plan, understanding that certain assumptions may not be met when a plan is activated;
- Criteria to trigger activation of the plan and escalate incidents, if appropriate;
- Assigned roles and responsibilities for personnel to activate and execute the plans;
- Contingency plans for technical assets, where appropriate;
- Incident response measures to protect the availability, confidentiality, and integrity of information;
- Current contact information for employees, customers, service providers, municipal authorities, and emergency response personnel that is readily accessible at off-site locations;
- Internal and external communication protocols, including notifying FHFA, the board, and customers, and call trees and employee notification procedures;
- Relocation strategies to other facilities and remote access policies and standards if personnel are working from a remote location in the event of a disaster; and
- References to emergency response measures to prevent loss of life and minimize injury and property damage.

The regulated entity should prioritize the recovery of its business functions and processes according to the RTOs and RPOs as stated in each plan. Each business function, process, and associated technical asset should map to a BCP. Technical assets should also be accounted for in the DRP as they relate to the prioritized recovery and protection of the regulated entity's IT infrastructure, business applications, and data. The regulated entity should determine the enterprise-wide risk thresholds that trigger activating the CMP and the corresponding steps to respond to such incidents at an enterprise level. The regulated entity should consider the operational, legal, compliance, financial, and reputational risks involved when determining the thresholds to trigger the CMP. The CMP should include the coordinated responses to implement the DRP and BCPs, handle media inquiries, and oversee emergency response measures.

C. Testing and Analysis

Testing demonstrates how well each plan achieves the business resiliency objectives defined by the regulated entity. Each regulated entity should develop a testing program that includes policies, standards, and procedures that address test planning, execution, reporting of test results, and test revisions, as necessary.

Senior management should designate personnel to oversee the testing of plans and allocate adequate time and resources for test exercises. Senior management is also responsible for ensuring that employees are aware of their roles (i.e., administrator or participant) in executing tests regularly. Test plans should periodically rotate employee roles, as appropriate, to reduce reliance on specific individuals who may not be available during a disruptive event. Testing of plans involving critical business functions should be completed at least annually, and when material changes occur to the business operating environment. The frequency of testing should be consistent with the criticality of the business function, but should not jeopardize normal business operations.

Prior to each test, management should validate the testing methods to identify potential problems. Test plans or exercises should be evaluated to assess whether test objectives are feasible and whether assumptions used in developing the test strategy are reasonable. Testing of plans should align with the risk assessments and the BIAs to validate pre-determined RPOs and RTOs. Additionally, priority-based testing should:

- Incorporate a variety of threats, event types, and crisis management scenarios that range from isolated system failures to full-scale disruptions;
- Evaluate identified internal and external interdependencies, including the testing of primary and alternate facilities with key third-party providers;
- Progressively increase in scope and complexity, functions, physical locations, and participants; testing should ultimately process at least a full day's work at the regulated entity's normal levels;
- Include a full-scale DRP test to confirm the entity's ability to conduct and sustain normal business in an alternate data center and the ability to return to pre-defined levels of operations in the primary data center; and
- Over time, adapt to changes in the regulated entity's business activities and risk profile.

Internal audit or a qualified independent third party should review the testing program and conduct an independent assessment of selected tests, including the underlying assumptions and methodology. Management should have oversight of key tests that are observed, verified, and evaluated by the independent party in order to validate the testing process and accuracy of test results. Test results, deviations from test plans, problems identified during testing, and any specified remediation steps should be properly documented.

Test results should be periodically analyzed to determine if problems identified during testing can be traced to a common source, remediated, and resolved through revisions to the testing program. Problems encountered during testing should be corrected and retested in a timely manner. Test participants or test owners can also provide suggestions to the test scenarios, plans or scripts to improve the test program. Once tests are completed and assessed, the test program

should be updated to address any gaps identified during tests and retested, as necessary, for robustness and effective remediation within a reasonable timeframe.

D. Risk Monitoring and Program Sustainability

The regulated entity should also implement risk monitoring to track how changes to the business operating environment, including personnel, technologies, equipment, or third-party providers, may affect business resiliency strategies and plans.

Regular reports of test results and risk monitoring inform senior management of the effectiveness of the regulated entity's program. Senior management should use this information to determine if gaps exist between the risk assessment or BIA and the existing plans in place. Based on this gap analysis, RPOs and RTOs may need to be reassessed and risk mitigation strategies may need to be evaluated for particular plans. Management or plan administrators should revise plans based on test results or when material changes occur to the current business operating environment—including changes to personnel and internal and external dependencies, such as reliance on other business units or outsourced activities. Relevant business line managers and stakeholders should also be informed of test results so they can address material business resiliency problems identified during testing. The test and/or audit reports of third-party providers, lessons learned from an actual event, and any emerging risks identified should also be used in a gap analysis for each step of the program. Updates to plans should be completed in a timely manner and revised plans should be communicated and made available to appropriate managers and employees.

Related Guidance

12 CFR Part 1236 Prudential Management and Operations Standards, Appendix.

Oversight of Third-Party Provider Relationships, Federal Housing Finance Agency Advisory Bulletin 2018-08, September 28, 2018.

Cloud Computing Risk Management, Federal Housing Finance Agency Advisory Bulletin 2018-04, August 14, 2018.

Information Security Management, Federal Housing Finance Agency Advisory Bulletin 2017-02, September 28, 2017.

Internal Audit Governance and Function, Federal Housing Finance Agency Advisory Bulletin 2016-05, October 7, 2016.

Data Management and Usage, Federal Housing Finance Agency Advisory Bulletin 2016-04, September 29, 2016.

Operational Risk Management, Federal Housing Finance Agency Advisory Bulletin 2014-02, February 18, 2014.

Contingency Planning for High-Risk or High-Volume Counterparties, Federal Housing Finance Agency Advisory Bulletin 2013-01, April 1, 2013.

Business Continuation Contingency Planning, Federal Housing Finance Board Advisory Bulletin 03-2, February 10, 2003.

Disaster Recovery Planning, Federal Housing Finance Board Advisory Bulletin 02-3, February 13, 2002 (rescinded by this advisory bulletin).

FHFA has statutory responsibility to ensure the safe and sound operations of the regulated entities and the Office of Finance. Advisory bulletins describe FHFA supervisory expectations for safe and sound operations in particular areas and are used in FHFA examinations of the regulated entities and the Office of Finance. Questions about this advisory bulletin should be directed to: SupervisionPolicy@fhfa.gov.