Federal Housing Finance Agency
Office of Inspector General

Enterprise Business Resiliency: Risk Assessment and Business Impact Analysis

White Paper • WPR-2020-006 • August 31, 2020

WPR-2020-006

August 31, 2020

Executive Summary

According to the Federal Financial Institutions Examinations Council, resilience is "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents."

The Federal Housing Finance Agency (FHFA or Agency), Fannie Mae, and Freddie Mac identify Enterprise business resiliency as a key risk. According to FHFA, ineffective business resiliency management can expose the Enterprises to operational, financial, legal, compliance, and reputational risks. FHFA, Fannie Mae, and Freddie Mac separately stressed to us the importance of strong business resiliency processes, given the Enterprises' critical mission and importance to the financial markets.

In light of the risks related to business resiliency, we have commenced a white paper series focused on business resiliency risk management at the Enterprises. In this white paper we describe the Enterprises' business resiliency risk management programs for the first component of the business resiliency cycle: risk assessment and business impact analysis.

TABLE OF CONTENTS

ABBREVIATIONS

AB 2019-01	Advisory Bulletin AB 2019-01, *Business Resiliency Management*
BIA	Business Impact Analysis
Enterprises	Fannie Mae and Freddie Mac
FHFA	Federal Housing Finance Agency
SOP	Standard Operating Procedure

BACKGROUND

Under their charters, Fannie Mae and Freddie Mac (the Enterprises) perform important roles in providing a stable source of housing finance that supports access to mortgage credit. Numerous events, such as a power outage, natural disaster, or cyber-attack, can jeopardize the Enterprises' ability to perform their mission critical operations.

According to the Federal Financial Institutions Examinations Council, resilience is "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents."[1] Resilience extends beyond recovery capabilities to incorporate proactive measures for mitigating the risk of a disruptive event in the overall design of operations and processes. Resilience strategies should extend across the entire business, including outsourced activities.

The Enterprises' business resiliency management programs include three core components:

- Business continuity plan, comprised of the written procedures for the Enterprise to recover, resume, and maintain business functions, including the underlying processes, at an acceptable predefined level following a disruption;
- Disaster recovery plan, comprised of the documented process to recover and resume the Enterprise's information technology infrastructure, business applications, and data services in the event of a major disruption; and
- Crisis management plan, comprised of the documented, coordinated responses to Enterprise-wide disruptions, including overseeing the activation of business continuity and disaster recovery plans.

Recent events underscore the role of business resiliency at the Enterprises when a disruption occurs. A Fannie Mae official told us that in light of the COVID-19 pandemic, in late February the Enterprise activated its crisis management plan and implemented its resiliency plans with respect to remote working. The official said that Fannie Mae's implementation of its resiliency plans enabled Fannie Mae to continue its normal business operations seamlessly. According to Fannie Mae's 10-Q for the second quarter of 2020, the Enterprise's business resiliency plans and technology systems have effectively supported the company-wide telework arrangement. Similarly, following earlier incident response actions, Freddie Mac

[1] For more information, see The White House, Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience* (Feb. 12, 2013) (online at https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil).

implemented invocation of its crisis management plan in March 2020, including remote work for all staff. A Freddie Mac official told us that prompt implementation of the crisis management plan facilitated continuation of Freddie Mac's operations without any adverse impact. Freddie Mac's 10-Q for the second quarter of 2020 stated that its business continuity plans have enabled it to continue fulfilling its mission while protecting staff and the community.

Business Resiliency Risk

FHFA, Fannie Mae, and Freddie Mac identify Enterprise business resiliency as a key risk. According to FHFA, ineffective business resiliency management can expose the Enterprises to operational, financial, legal, compliance, and reputational risks. The Enterprises are large, complex organizations and resiliency requires them to plan responses for disruptions related to people, operations and processes, equipment and facilities, and information technology and data across a wide array of hazards and risk scenarios in multiple geographic locations. Further, those resiliency efforts must constantly adapt and evolve in response to emerging circumstances to stay ahead of the risks.

FHFA, Fannie Mae, and Freddie Mac separately stressed to us the importance of strong business resiliency processes, given the Enterprises' critical mission and importance to the financial markets. As FHFA officials explained, should the Enterprises be unable to play their role, there could be a huge immediate impact on the mortgage finance industry and mortgage liquidity gridlock, with disruptions having widespread impacts on the financial services industry, homeowners, and investors.

According to FHFA, the Enterprises have a higher degree of business resiliency risk because of their reliance on thousands of third parties, including for key components of their business operations. Were a key Enterprise third party to suffer a disruption, that disruption could cause the Enterprise business disruptions, financial losses, legal issues, and compliance issues. As a consequence, the Enterprises' business resiliency programs must also assess and ensure the resiliency of critical third parties. Both Enterprises recognize cyber related risks as critical risks to manage through business resiliency programs.

In light of the risks related to business resiliency, we have commenced a white paper series focused on business resiliency risk management. In this white paper we describe the Enterprises' business resiliency risk management programs for the first component of the business resiliency cycle: risk assessment and business impact analysis. We did not evaluate the adequacy of their processes.

Business Resiliency Cycle

FHFA issued Advisory Bulletin AB 2019-01, *Business Resiliency Management* (AB 2019-01) to Fannie Mae and Freddie Mac in May 2019.[2] Prior to the issuance of AB 2019-01, FHFA did not have any guidance in place for the Enterprises that addressed disaster recovery or business resiliency as the sole focus. Instead, elements of resiliency were addressed on a piecemeal basis. An Agency official explained to us that FHFA issued AB 2019-01 to draw more attention to and focus on business resiliency or business continuity programs at the Enterprises. Recognizing that there needed to be more maturity in both Enterprises' business resiliency and disaster recovery programs, the Agency decided to create a more robust and comprehensive advisory bulletin that would cover disaster recovery. FHFA also took the opportunity to discuss what key elements it wanted to see in the Enterprises' business resiliency programs.

AB 2019-01 states that FHFA expects the Enterprises to establish and maintain a business resiliency risk management program that includes four components of the business resiliency cycle: risk assessment and business impact analysis; risk mitigation and plan development; testing and analysis; and risk monitoring and program sustainability.

RISK ASSESSMENT AND BUSINESS IMPACT ANALYSIS IN BUSINESS RESILIENCY

In May 2019, FHFA issued AB 2019-01 to provide the Enterprises guidance on business resiliency management. FHFA advised that each Enterprise should establish its business resiliency risk management program to align with its Enterprise-wide risk management program.

According to AB 2019-01, the first step in a cyclic, process-oriented approach should cover risk assessment and business impact analysis. The risk assessment determines potential threats to an Enterprise's business operations and considers a broad range of scenarios. The risk assessment should factor in disruptions involving information services, equipment, personnel, facilities, and services by third-party providers, as well as threats related to location.

[2] AB 2019-01 was also issued to the Federal Home Loan Banks and the Office of Finance. This white paper discusses only Fannie Mae and Freddie Mac. For more information, see Federal Housing Finance Agency, Advisory Bulletin 2019-01, *Business Resiliency Management* (May 7, 2019) (online at www.fhfa.gov/SupervisionRegulation/AdvisoryBulletins/Pages/Business-Resiliency-Management.aspx).

The business impact analysis (BIA) assesses and prioritizes an Enterprise's business functions and processes that must be recovered after a disruption. After identifying business functions and processes, the Enterprise evaluates and compares business function requirements. The BIA should also identify interdependencies between critical systems, departments, personnel, and services that could be affected during a disruption.

FHFA, Fannie Mae, and Freddie Mac separately reported to us that the risk assessments and BIAs are critical to a successful business resiliency management program.

Fannie Mae

The Fannie Mae Business Resiliency Standard details the requirements for business resiliency. It provides a guideline and mandate for Fannie Mae to secure continuity of operations following a business disruption.

Fannie Mae's Business Resiliency Team monitors compliance with the resiliency model steps contained in the Fannie Mae Business Resiliency Standard as well as emerging resiliency risks across the Enterprise. There are three parties involved in resiliency plan operations: (1) the plan owner, (2) the process owner (who leads the process/function), and (3) the plan manager (who updates and coordinates the plan itself). Each of the three parties must finalize and sign off on the plan. Because Fannie Mae's Business Resiliency Team has the subject matter expertise, the team is also required to sign off on the plan.

Risk Assessment

Under the Fannie Mae Business Resiliency Standard, Fannie Mae Enterprise Resiliency assesses the probability and severity of impacts associated with possible threats and hazards to Fannie Mae's operations on an annual basis or following an occurrence of significant disruption.[3] Recently, Fannie Mae completed a procedure formalizing how it will perform resiliency risk assessments. This procedure details what criteria will be assessed, how it will look at the Enterprise's physical locations in proximity to known risks in the area, and how it will assess the risk and work with partners in risk management to understand the possibility of those risks affecting Fannie Mae's operations.

According to the Fannie Mae Business Resiliency Standard, planning is conducted around "loss of" scenarios, such as loss of personnel, facilities, technology, or third parties. First, Fannie Mae identifies threats that could impact Enterprise operations. Fannie Mae looks at risk assessments from an all-hazards approach and considers widescale disruptions that it can anticipate, such as hurricanes, tornadoes, winter weather, civil unrest, or terrorist attacks.

[3] Fannie Mae Enterprise Resiliency includes the Business Resiliency Team, along with the Technical Resiliency Team and Crisis Management Team.

Next, the Enterprise analyzes the likelihood and impact of threats and measures the risk. When assessing risk, Fannie Mae applies a 50-year historical risk value that forecasts the frequency, severity, and likelihood of such risks based on data collected over the past 50 years. Fannie Mae then evaluates the controls and plans that the Enterprise has in place to assess low/medium/high risk. The worst-case scenarios are presented to the management committee.

Business Impact Analysis

Under the Fannie Mae Business Resiliency Standard, BIAs examine business processes and the effect of a disruption. BIAs are facilitated by the Business Resiliency Team with the process owners in coordination with the plan managers. They are conducted once annually or when material changes are made within a business unit that necessitate higher frequency, such as when a business unit consolidates or changes its business model. Fannie Mae looks at the BIA in place and then performs the entire process again to identify changes.

First, the Enterprise considers worst-case scenarios where the result would be that the business unit cannot operate. The analysis focuses on the time it takes for the scenario to impact financial, operational, reputational, and client considerations. Fannie Mae looks at that analysis and measures in time against the risk assessment methodology that is used across Fannie Mae's operational units to ensure an apples-to-apples comparison. Fannie Mae applies formulas and weighting factors enterprise-wide to determine what is the most and least critical of every process at the Enterprise. That provides the information Fannie Mae will need for the next stage of the resiliency cycle, in which it determines recovery strategies to minimize impacts.

Freddie Mac

Freddie Mac's Enterprise Business Resiliency Risk Policy establishes the framework for managing business resiliency risk enterprise-wide. Freddie Mac's Business Resiliency Standard Operating Procedure (SOP) provides guidance regarding the required steps for conducting and maintaining BIAs and business continuity plans in alignment with the Freddie Mac Enterprise Business Resiliency Risk Policy.

Enterprise Operations and the divisions work together to complete the steps required by the Freddie Mac Business Resiliency SOP. Enterprise Operations collaborates with division risk officers to identify impacts of disruptive event scenarios on mission-critical and foundational processes. The division risk officers are responsible for identifying, evaluating, and, as appropriate, mitigating divisional business resiliency risks consistent with the Enterprise's and division's risk appetite. Enterprise Operations ensures that the requirements of the Freddie Mac Business Resiliency SOP are satisfied.

Risk Assessment

Under Freddie Mac's risk assessment process, Enterprise Operations holds a formal quarterly resiliency risk committee meeting to assess and discuss the risks associated with Freddie Mac's resiliency risk profile. Every division participating in the meeting assesses the resiliency risk of their organization and analyzes attributes that are governed by Freddie Mac's risk assessment standards and methodologies. The results are reported to the Operational Risk Committee and the Enterprise Risk Committee.

Freddie Mac uses two core standards to assess business resiliency risk: the risk control self-assessment standard and the 25-block risk assessment standard. Applying the risk control self-assessment standard, all mission-critical divisions assess their processes for resiliency risk within their organizations; Information Technology also assesses risk in each division. The 25-block risk assessment standard is a consistent methodology for evaluating the level of exposure to a risk based on inherent risk assessment of impact and likelihood of a risk before controls and mitigants (inherent risk) and after the application of controls and mitigants (residual risk). The 25-blocks are the intersection of the parameters for impact (5 parameters) and likelihood (5 parameters).

Business Impact Analysis

Under Freddie Mac's Business Resiliency SOP, BIAs identify the impacts of disruptive event scenarios on mission-critical and foundational processes. Evaluating the worst-case scenario, the BIAs analyze critical process needs across people, process, technology, information, third-party, and facilities dependencies, and the impact to the business processes, if they become unavailable. Freddie Mac uses the BIAs to prioritize business processes that must be recovered during a disruption. Each division completes BIAs for mission-critical and foundational processes, which are reviewed by division risk officers. Enterprise Operations then reviews the BIAs for consistency to ensure they are aligned with the business resiliency standards and requirements.

Freddie Mac's BIAs are updated, reviewed, and approved on a rolling 12-month cycle or as material changes occur. When performing its annual review of a BIA, Freddie Mac updates the analysis from the existing BIA. The results of a BIA directly inform the next step of Freddie Mac's resiliency cycle, the business continuity plan, which provides the strategies and procedures to enable the recovery of processes from a disruption and the resumption of operations.

CONCLUSION

Ineffective business resiliency management can expose the Enterprises to operational, financial, legal, compliance, and reputational risks. Strong business resiliency processes are critical, given the Enterprises' critical mission and importance to the financial markets. This white paper describes the Enterprises' business resiliency risk management programs for the first component of the business resiliency cycle: risk assessment and business impact analysis.

OBJECTIVE, SCOPE, AND METHODOLOGY .....

The objective of this paper was to provide an overview of the first stage of the business resiliency cycle, risk assessment and business impact analysis. To achieve this objective, we reviewed internal and publicly available FHFA and Enterprise documents. We also interviewed FHFA and Enterprise officials.

We provided FHFA with the opportunity to respond to a draft of this white paper. We appreciate the cooperation of FHFA staff, as well as the assistance of all those who contributed to the preparation of this white paper.

ADDITIONAL INFORMATION AND COPIES.....

For additional copies of this report:

- Call: 202-730-0880
- Fax: 202-318-0239
- Visit: www.fhfaoig.gov

To report potential fraud, waste, abuse, mismanagement, or any other kind of criminal or noncriminal misconduct relative to FHFA's programs or operations:

- Call: 1-800-793-7724
- Fax: 202-318-0358
- Visit: www.fhfaoig.gov/ReportFraud
- Write:

  FHFA Office of Inspector General
  Attn: Office of Investigations – Hotline
  400 Seventh Street SW
  Washington, DC 20219