Federal Housing Finance Agency
Office of Inspector General

Enterprise Business Resiliency: Risk Mitigation and Plan Development

White Paper • WPR-2021-003 • March 22, 2021

WPR-2021-003

March 22, 2021

Executive Summary

Under their charters, Fannie Mae and Freddie Mac (the Enterprises) are tasked with performing 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. The Federal Housing Finance Agency (FHFA or Agency) defines business resiliency management to mean the Enterprises' "ability to minimize the impact of disruptions and maintain business operations at predefined levels."

FHFA and the Enterprises identify business resiliency as a key risk. Ineffective business resiliency management can expose the Enterprises to operational, financial, legal, compliance, and reputational risks, according to FHFA. 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.

We recently published a white paper entitled *Enterprise Business Resiliency: Risk Assessment and Business Impact Analysis*, which described how the Enterprises' business resiliency programs identify and prioritize risks. In this white paper we describe the Enterprises' written procedures for how they then mitigate those risks and develop written resiliency plans to address them. For this report, we did not evaluate the adequacy of their written procedures, nor did we determine whether the procedures have been implemented and tested.

TABLE OF CONTENTS .....

ABBREVIATIONS

AB 2019-01	Advisory Bulletin AB 2019-01, *Business Resiliency Management*
Enterprises	Fannie Mae and Freddie Mac
FHFA or Agency	Federal Housing Finance Agency
HERA	Housing and Economic Recovery Act of 2008
PMOS	Prudential management and operations standards

BACKGROUND

Under their charters, Fannie Mae and Freddie Mac are tasked with performing 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 a 2013 Presidential Policy Directive, resilience is "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions."[1] That definition is widely accepted.[2] The policy directive further explains that business resiliency "includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents." The ongoing pandemic and a recent wide-ranging cyber-attack illustrate the need for business resiliency.[3] 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. FHFA defines business resiliency management to mean the Enterprises' "ability to minimize the impact of disruptions and maintain business operations at predefined levels." FHFA and the Enterprises identify business resiliency as a key risk.

Business Resiliency Risk

The Housing and Economic Recovery Act of 2008 (HERA) amended the Federal Housing Enterprises Financial Safety and Soundness Act of 1992 to require FHFA to establish prudential standards that address 10 specific areas relating to the management and operations of the regulated entities.[4] Pursuant to Section 1108 of HERA, FHFA issued its prudential management and operations standards (PMOS) in June 2012, effective August 7, 2012. The PMOS communicate FHFA's expectations for minimum risk management practices by the

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

[2] For more information, see Federal Financial Institutions Examination Council, *Information Technology Examination Handbook, Business Continuity Management Booklet* (online at ithandbook.ffiec.gov/it-booklets/business-continuity-management.aspx).

[3] For more information, see Cybersecurity & Infrastructure Security Agency, *Supply Chain Compromise* (online at www.cisa.gov/supply-chain-compromise).

[4] 12 U.S.C. § 4513b(a)(1)–(10); the 10 areas are: (1) adequacy of internal controls and information systems; (2) independence and adequacy of internal audit systems; (3) management of interest rate risk exposure; (4) management of market risk; (5) adequacy and maintenance of liquidity and reserves; (6) management of asset and investment portfolio growth; (7) investments and acquisitions of assets; (8) overall risk management processes; (9) management of credit and counterparty risk; and (10) maintenance of adequate records.

regulated entities, including managing risk from disasters and other disruptions to their operations. FHFA's PMOS 8, Principle 11 is applicable to business resiliency and disaster recovery. That PMOS Principle directs that "a regulated entity should have adequate and well-tested disaster recovery and business resumption plans for all major systems and have remote facilitates [sic] to limit the impact of disruptive events."[5]

In its 2020 annual 10-K filing with the Securities and Exchange Commission, Fannie Mae said "Shortcomings or failures in our internal processes, people, data management or systems could disrupt our business or have a material adverse effect on our risk management, liquidity, financial statement reliability, financial condition and results of operations." The Enterprise went on to say that as a result of the concentration of employees and operations in two metropolitan areas, "a major disruptive event . . . could impact our ability to operate notwithstanding the business continuity plans and facilities . . . including our out-of-region data center for disaster recovery."

Similarly, in its 2020 10-K filing, Freddie Mac said, "Shortcomings or failures in our internal processes, people, or systems, or those of third parties with which we interact, could lead to impairment of our liquidity, disruption of our business . . . , incorrect payments to investors in our securities, errors in our financial statements, liability to customers or investors, further legislative or regulatory intervention, reputational damage, and financial and economic loss." The Enterprise further noted that the key business activities and people in its Virginia office "represent a concentrated risk of people, technology, and facilities. As a result, an infrastructure disruption . . . could significantly adversely affect our ability to conduct normal business operations. Any measures we take to mitigate this risk may not be sufficient to respond to the full range of events that may occur or allow us to resume normal business operations in a timely manner."

Ineffective business resiliency management can expose the Enterprises to operational, financial, legal, compliance, and reputational risks, according to FHFA. 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. Additionally, the Enterprises' business resiliency programs must assess and ensure

[5] At the time FHFA adopted its PMOS, the importance of business resiliency, out-of-region centers (geographically dispersed resources), and testing of back-up sites was well-established. The Securities and Exchange Commission, the Board of Governors of the Federal Reserve System, and the Office of the Comptroller of the Currency issued a 2003 Interagency Paper (Interagency Paper) to advise financial institutions on necessary steps to protect the financial system. The Interagency Paper identified four key practices built upon long-standing principles of business continuity planning to strengthen the overall resilience of the financial system: (1) Identifying critical activities that support its critical financial markets; (2) Determining appropriate recovery and resumption objectives; (3) Maintaining sufficient geographically dispersed resources; and (4) Routinely using or testing recovery and resumption arrangements.

the resiliency of critical third parties because Fannie Mae and Freddie Mac rely on thousands of third parties, including for key components of their business operations.

Enterprise Business Resiliency White Paper Series

In light of these risks, we have commenced a white paper series focused on Enterprise business resiliency risk management. We recently published a white paper entitled *Enterprise Business Resiliency: Risk Assessment and Business Impact Analysis*, which described how the Enterprises' business resiliency programs identify and prioritize risks.[6] In this white paper we describe the Enterprises' written procedures for how they then mitigate those risks and develop written resiliency plans to address them. For this report, we did not evaluate the adequacy of their written procedures, nor did we determine whether the procedures have been implemented and tested.

RISK MITIGATION AND PLAN DEVELOPMENT IN BUSINESS RESILIENCY

FHFA issued Advisory Bulletin AB 2019-01, *Business Resiliency Management* (AB 2019-01), to Fannie Mae and Freddie Mac in May 2019 to provide the Enterprises with guidance on business resiliency management.[7] AB 2019-01 states that FHFA expects the Enterprises to establish and maintain business resiliency risk management programs that include 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.

In the second component, risk mitigation and plan development, the Enterprises are expected to use results from the first component to identify solutions and plan business recovery.

---

[6] For more information, see OIG, *Enterprise Business Resiliency: Risk Assessment and Business Impact Analysis* (August 31, 2020) (WPR-2020-006) (online at www.fhfaoig.gov/sites/default/files/WPR-2020-006.pdf).

[7] 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).

According to AB 2019-01, risk mitigation should include appropriate insurance and may also include solutions such as redundant vendor support, additional reserves of critical supplies, or a geographically distinct data center.

In turn, resiliency plans are then to be developed and documented by each Enterprise to implement the risk mitigation strategies and recovery solutions. Among other things, plans are required to include the criteria to trigger activation and escalation in response to incidents, along with assigned roles and responsibilities for activation and execution. AB 2019-01 advises that resiliency plans should include short-term and long-term recovery operations, as well as steps to transition back to normal business. AB 2019-01 adds that plans should account for internal and external dependencies and should avoid single points of failure.

Fannie Mae

Fannie Mae's written procedures state that its Enterprise Resiliency program is intended to coordinate resiliency planning at the Enterprise. In this white paper, we did not assess whether this program has been implemented nor did we test whether it works as implemented.[8]

Risk Mitigation

Fannie Mae's business processes carry out day-to-day operations at the Enterprise. Fannie Mae reported to us that the Enterprise has hundreds of business processes, and risk mitigation strategies are developed at the process level. Fannie Mae standards direct the development of cost-effective business resiliency strategies to validate recovery and continuity of business processes during a business disruption. The Enterprise maintains that its risk-based approach directs Fannie Mae to focus on and properly invest in critical business processes, including associated technology and other dependencies.[9]

For strategy development, Fannie Mae considers recovery strategies for four "loss of" scenarios, including loss of personnel, facility, technology, or a third-party supplier. According to a Fannie Mae official, Fannie Mae's approach does not focus on the cause of the problems, but rather the end result, the loss, and how to recover from it. Critical business processes must integrate at least two recovery strategies.

---

[8] FHFA has found that Fannie Mae's program fails to meet PMOS 8, Principle 11. For more information, see OIG, *For Nine Years, FHFA Has Failed to Take Timely and Decisive Supervisory Action to Bring Fannie Mae into Compliance with its Prudential Standard to Ensure Business Resiliency* (March 22, 2021)(EVL-2021-002)(online at www.fhfaoig.gov/sites/default/files/EVL-2021-002_(Redacted).pdf).

[9] Fannie Mae internal guidance describes critical business processes as the strategically core Enterprise activities. Unavailability of critical business processes would cause consequences unacceptable to the Enterprise.

Fannie Mae guidance also requires that risk mitigation strategies be sustainable for at least 30 days, which an Enterprise official explained is consistent with the industry standard. These strategies must also consider interdependencies with other business processes, third-party processes, and technology. Pursuant to PMOS 8, Principle 11, its disaster recovery and business resumption plans for all major systems must be "well-tested."

In addition to mitigating the impact of a business disruption, a Fannie Mae official told us that Fannie Mae has sought to develop and incorporate strategies to decrease the likelihood of a disruption occurring. For example, the Enterprise works to identify and eliminate single points of failure and maintains multiple options to perform a certain task.

Plan Development

After development, Fannie Mae's resiliency risk mitigation strategies are then required to be documented in resiliency plans. The core resiliency plans in Fannie Mae's program include business continuity plans, disaster recovery plans, technical contingency plans, and a crisis management plan, all of which are interrelated and are supposed to work in conjunction with one another. Fannie Mae officials explained to us that, in order to address the impacts of a disruption, the Enterprise develops plans that detail the relationships between people, business processes, technology assets, and key deliverables. Fannie Mae standards also describe third-party dependencies that are incorporated in its plans. According to PMOS 8, Principle 11, these plans, as they apply to major Enterprise systems, must be "well-tested."

Business Continuity Plans

Fannie Mae standards require business continuity plans to include strategies to handle the "loss of" scenarios specific to business processes. A process owner is expected to be assigned to each documented process and multiple processes can roll up into a business continuity plan.

Disaster Recovery Plans

A Fannie Mae official explained to us that disaster recovery plans function as technology plans. However, unlike technical contingency plans, which account for specific technology assets,[10] disaster recovery plans document recovery strategies at a site level. For example, a disaster recovery plan addresses events requiring Fannie Mae to move operations to a secondary location.

[10] The Enterprise's Technical Resiliency Standard directs that any technology asset that Fannie Mae uses must have a technical resiliency plan documenting recovery procedures.

Crisis Management Plan

Fannie Mae's crisis management team maintains a crisis management plan to manage disruptive events.[11] Enterprise standards require the crisis management plan to detail criteria for activating the appropriate response to a variety of incidents. Fannie Mae's Crisis Management Standard describes incidents as events ranging from those that may cause "interruption" to those that may cause a "catastrophe." When an incident of high or potentially high severity occurs, Fannie Mae's crisis management plan is activated and, according to Fannie Mae officials, the crisis management team assesses the situation and decides whether to invoke a business continuity plan or a technical contingency plan.[12] According to the Crisis Management Standard, executive leadership oversees the Enterprise's response to the most severe incidents as defined in the crisis management plan. For smaller scale incidents, based on impact, that standard permits crisis management coordinators to invoke a resiliency plan without assembling executive leaders. According to Enterprise officials, Fannie Mae resiliency plans include criteria and procedures for returning to normal operations after crisis conditions have abated.

Fannie Mae's resiliency plans are required to be reviewed and approved annually or after material changes, such as a major disruption or a significant change to a process or asset. Various levels of review are required to verify that all appropriate personnel, contact information, and recovery strategies and solutions have been identified and validated. According to Fannie Mae's Business Resiliency Standard, disruptions are reviewed to identify and improve plan and process weaknesses.

Fannie Mae also reviews resiliency plans for certain third-parties. An Enterprise official explained that Fannie Mae performs in-depth reviews of critical third-party resiliency plans both when the third-party is onboarded and as part of the Enterprise's annual review cycle.

Freddie Mac

Freddie Mac's Enterprise Business Resiliency Risk Policy establishes the framework for managing business resiliency risk enterprise-wide.

---

[11] Fannie Mae reports that its crisis management plan also includes embedded plans, considered subsets of the crisis management plan, that detail Enterprise responses to specific hazards. For example, Enterprise standards describe that the crisis management team maintains an infectious disease plan to provide additional guidance to manage health incidents. According to Fannie Mae, its infectious disease plan has been active since February 2020.

[12] A Fannie Mae official explained that incidents are generally either business or technology incidents, not both. As discussed earlier, the disaster recovery plan functions as a technology plan.

Risk Mitigation

Freddie Mac's Business Resiliency team informed us that it uses the outputs from business impact analyses to determine recovery strategies. An Enterprise official explained that Business Resiliency partners with the Enterprise Risk Management Division to determine risk appetite and to develop strategies that include risk acceptance, transfer, management, and reduction.

Freddie Mac describes its recovery strategies as impact-based. Similar to Fannie Mae, Freddie Mac standards require the development of strategies to recover from four loss scenarios, including loss of technology, facility, personnel, and third-party. All recovery solutions are required to be sustainable for a minimum of 30 days. In addition, Freddie Mac reported to us that its Enterprise risk mitigation strategies prioritize mission critical and foundational processes. Enterprise officials explained that mission critical processes cover core business functions and foundational processes impact infrastructure. Enterprise officials also explained to us that migration to cloud infrastructure is part of the Enterprise's resiliency risk mitigation efforts.[13]

Freddie Mac also reported to us that its strategies include incorporating lessons learned from live incidents and monitoring infrastructure and network systems to decrease the likelihood of a disruption.

Plan Development

Divisional risk officers are responsible for developing plans that align with Freddie Mac's business resiliency strategy and risk appetite. According to Enterprise standards, Freddie Mac develops and maintains resiliency plans including business continuity plans, disaster recovery plans, and a crisis management plan. An Enterprise official explained that Freddie Mac resiliency plans identify critical and foundational processes and are developed to incorporate strategies for how to recover from a disruption. Under Enterprise policy and standards, a disruption is an "interruption or degradation of normal business, functions, operations, or processes, whether anticipated (e.g., hurricane) or unanticipated (e.g., blackout, terror attack, technology failure, or earthquake)."

Business Continuity Plans

Freddie Mac standards state that business continuity plans document strategies and procedures for recovering business processes and resuming operations "at acceptable level of service." The plans must be directly informed by the business impact analysis. The plans must also

[13] For more information on Freddie Mac's migration to the cloud, see OIG, *An Overview of Enterprise Use of Cloud Computing* (March 11, 2020) (WPR-2020-002) (online at www.fhfaoig.gov/sites/default/files/WPR-2020-002.pdf).

link to the Enterprise's crisis management plan with notification and escalation information for when the business continuity plan is invoked.

Disaster Recovery Plans

Freddie Mac disaster recovery policies and procedures address the recovery and continuation of technology infrastructure and capabilities. Enterprise standards require that disaster recovery plans document the approved resources, actions, tasks, and data for managing technology recovery.

Crisis Management Plan

Freddie Mac's standards describe that its crisis management plan documents the procedures, communication protocols, and governance structure that guide the Enterprise's crisis response. Freddie Mac defines a crisis as an event causing significant business disruption, such as necessitating personnel relocation or causing the potential loss or misuse of critical technology. According to the Enterprise, the crisis management plan is supported by an incident management framework to respond to lower-level incidents that may be activated without activating the overarching crisis management plan. An Enterprise official explained that the crisis management plan also includes de-escalation criteria, specifying thresholds that need to be met to return to standard business operations.

Freddie Mac standards require resiliency plans to be reviewed and updated annually, at a minimum. More frequent reviews and updates are required if there are significant changes, such as changes in personnel, facilities, or technology. Plans are also required to be reviewed and updated to address any issues identified during the testing component of the resiliency lifecycle.

In plan development, Freddie Mac incorporates third-party dependencies into its business continuity plans, according to an Enterprise official. Freddie Mac expects third-parties to have business continuity plans and does oversight and monitoring through its third-party risk management program.

CONCLUSION

Ineffective business resiliency management can expose the Enterprises to operational, financial, legal, compliance, and reputational risks, according to FHFA. 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. In this white paper we describe the Enterprises' written procedures for how they

mitigate risks and develop written resiliency plans to address them. For this report, we did not evaluate the adequacy of their written procedures, nor did we determine whether the procedures have been implemented and tested.

OBJECTIVE, SCOPE, AND METHODOLOGY .....

The objective of this paper was to provide an overview of the second stage of the business resiliency cycle, risk mitigation and plan development. To achieve this objective, we reviewed internal and publicly available FHFA and Enterprise documents. We also interviewed FHFA and Enterprise officials. For this white paper, we did not evaluate the adequacy of the Enterprises' written procedures, nor did we determine whether the procedures have been implemented and tested.

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