

Federal Housing Finance Agency
Office of Inspector General



An Overview of Enterprise Use of Cloud Computing

White Paper • WPR-2020-002 • March 11, 2020



WPR-2020-002

March 11, 2020

Executive Summary

Cloud computing is a technology service that provides on-demand access to a shared pool of computing resources over the internet. Fannie Mae and Freddie Mac (the Enterprises) are migrating business operations to a cloud environment provisioned by third-party public cloud providers.

In August 2018, the Federal Housing Finance Agency (FHFA) issued Advisory Bulletin 2018-04, *Cloud Computing Risk Management* (AB 2018-04). This AB provides guidance and expectations for the Enterprises to oversee enterprise-wide risk management, and to assess and manage financial, operational, legal, compliance, and reputational risks of cloud computing when using third-party cloud service providers.

Under its Infrastructure Transformation Program, Freddie Mac began migrating legacy applications to the cloud in February 2019. It expects the legacy migration phase to be completed by the end of March 2020 or very early in the second quarter of 2020. According to Freddie Mac, about 30 percent of its legacy applications were not suitable for the cloud in their current form, and so will remain on Freddie Mac-operated infrastructure for now. Freddie Mac is also exploring modern, cloud-based replacements for its legacy applications.

Fannie Mae also has a cloud migration initiative underway. Internal reports show that as of October 2019, about a quarter of Fannie Mae's business applications are in the cloud, with a year-end 2020 target of 36 percent. Enterprise officials told us that they expect a total of about three quarters of Fannie Mae's applications to migrate to the cloud over the next few years.

FHFA officials cited four primary potential benefits of cloud computing for the Enterprises: economies of scale, improvements to disaster recovery, elastic response, and proprietary functions.

While both Enterprises invoked benefits of efficiency and technological advancement from a move to the cloud, both recognized high operational risks from these moves. In addition to the operational risks in play during the migration process, use of the cloud environment presents its own set of risks. AB 2018-04 details a number of risk areas for the Enterprises, including third-party, information security, and business resiliency risks. FHFA has separately assessed each of these as high risk areas for both Enterprises. The Enterprises must also consider concentration risk with their cloud service provider and risks with the adequacy of cloud computing staff. The purpose of this white paper is to explain the status of the Enterprises' cloud computing efforts and the risks identified with cloud computing.

TABLE OF CONTENTS

EXECUTIVE SUMMARY	2
ABBREVIATIONS	4
BACKGROUND	5
FHFA Advisory Bulletin	5
ENTERPRISE USE OF CLOUD COMPUTING.....	6
Freddie Mac	6
Fannie Mae	7
ENTERPRISE BENEFITS AND RISK CONSIDERATIONS.....	7
Cloud Computing Benefits	7
Economies of Scale.....	7
Improvements to Disaster Recovery.....	8
Elastic Response	8
Proprietary Functions.....	8
Cloud Computing Risk Considerations	8
FHFA Recognizes Cloud Computing Requires Extensive Risk Management.....	8
Third-party Cloud Provider Risk.....	9
Concentration Risk	9
Information Security Risk.....	10
Inadequate Staffing Expertise	10
CONCLUSION.....	10
OBJECTIVE, SCOPE, AND METHODOLOGY	11
ADDITIONAL INFORMATION AND COPIES	12

ABBREVIATIONS

AB 2018-04	Advisory Bulletin 2018-04, Cloud Computing Risk Management
Enterprises	Fannie Mae and Freddie Mac
FHFA or Agency	Federal Housing Finance Agency
NIST	National Institute of Standards and Technology
OIG	Federal Housing Finance Agency Office of Inspector General

BACKGROUND.....

Cloud computing is a technology service that provides on-demand access to a shared pool of computing resources over the internet. Cloud computing enables flexible, scalable, and broadly available computing infrastructure that is owned and maintained, typically off-site, by a cloud service provider. By contrast, traditional Enterprise infrastructure is maintained by the Enterprise, either on-premises or at an off-site data center.

The Enterprises are migrating business operations to a public cloud¹ environment provisioned by third-party service providers.² As described by the National Institute of Standards and Technology (NIST), a public cloud is a multi-tenant platform in which infrastructure and computational resources are owned and operated by an outside party for use by the general public. NIST reported in 2011 that public cloud computing is an emerging technology that represents a “significant” shift from conventional methods.

While both Enterprises invoked benefits of efficiency and technological advancement from a move to the cloud, both recognized high operational risks from these moves. In their 2019 10-Ks, both Enterprises stated that if they do not transition to the cloud in a “well-managed, secure,” and “effective manner,” they may “experience unplanned service disruption or unforeseen costs.” Further, when in the cloud environment, the Enterprises must consider the new risk landscape that cloud computing presents. Cloud computing is a vast and complex subject that touches on matters intersecting numerous areas of the Enterprises’ business. This white paper will provide a high-level overview of cloud computing at the Enterprises.

FHFA Advisory Bulletin

In August 2018, FHFA issued AB 2018-04 on cloud computing.³ This AB provides guidance and expectations for the Enterprises’ boards and senior management to oversee enterprise-wide risk management, and assess and manage financial, operational, legal, compliance, and

¹ There are four types of cloud “deployment models,” primarily differentiated by the user and the owner/operator: private cloud, community cloud, public cloud, and hybrid cloud. For more information, see National Institute of Standards and Technology, *The NIST Definition of Cloud Computing* (Sept. 2011) (online at <https://csrc.nist.gov/publications/detail/sp/800-145/final>).

² Freddie Mac informed us that although it is utilizing a public cloud, it is running software “on top” of that public cloud environment, which would constitute a hybrid cloud solution. Fannie Mae is also using this software within its public cloud environment.

³ The advisory bulletin was issued to Fannie Mae, Freddie Mac, 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, *Cloud Computing Risk Management* (Aug. 14, 2018) (AB 2018-04) (online at www.fhfa.gov/SupervisionRegulation/AdvisoryBulletins/Pages/Cloud-Computing-Risk-Management.aspx).

reputational risks of cloud computing when using third-party cloud service providers. An FHFA official told us that the Agency issued AB 2018-04 to articulate its supervisory expectations for the use of cloud computing and explained that the AB was not meant to be prescriptive on whether to use the cloud or the type of cloud infrastructure to choose.

ENTERPRISE USE OF CLOUD COMPUTING

Freddie Mac

During 2018, Freddie Mac launched an Infrastructure Transformation Program, which it intends to execute in two phases: (1) migrate legacy applications to the cloud in their current form and (2) modernize applications for the cloud environment.

In November 2018, FHFA, as conservator, approved Freddie Mac's plan to migrate its legacy applications to the cloud, and Freddie Mac began the migration effort in February 2019. Freddie Mac expects the legacy migration phase to be completed by the end of March 2020 or very early in the second quarter of 2020. Freddie Mac is moving roughly 70 percent of its legacy applications, in their current form, from on-premises infrastructure into the cloud environment operated by a third-party public cloud provider. According to Freddie Mac, the remaining 30 percent of its legacy applications were not suitable for the cloud in their current form, and so, as part of the legacy migration phase, it will migrate these applications to data centers where the computing infrastructure will continue to be maintained by Freddie Mac. In the second phase, Freddie Mac is exploring modern, cloud-based options for the legacy applications—for both the applications that it did not move to the cloud and the applications that moved to the cloud in their legacy form.

An FHFA risk assessment noted that Freddie Mac is vulnerable to disruptions during the migration of legacy applications. During 2019, Freddie Mac internally reported that the transitional state of its technology infrastructure was one of the four drivers of its high operational risk profile, with technology related incidents reaching a record high in September 2019. An Enterprise official told us that a task force was created to identify the causes of the technology related incidents and address them. The official told us in January 2020 that the number of those incidents has dropped significantly.

Upon completion of its cloud migration, Freddie Mac expects a decrease in its overall operational risk because its technology infrastructure would no longer be in a transitional state.

During the second quarter of 2019, Freddie Mac began its effort to modernize applications as part of its second phase of the Infrastructure Transformation Program. There is no set

timeframe to complete this effort. Freddie Mac officials advised that some legacy applications may not be modernized for the cloud environment.

Fannie Mae

Fannie Mae also has a cloud migration initiative underway. The initiative, according to Fannie Mae officials, has three concurrent “streams”: (1) preparing the cloud environment; (2) migration of applications; and (3) data migration.

Fannie Mae recognizes that operational risk is elevated during migration of applications and data to the cloud. Specifically, Fannie Mae identified the risk of creating multiple copies of data, which can cause confusion and conflicts, during the migration process. Fannie Mae officials told us the Enterprise is actively monitoring the risk and exercising a high level of rigor as they migrate the data.

Fannie Mae expects its on-premises warehouse data migration, under stream three, to be complete and fully adopted by year-end 2020. Nonetheless, Fannie Mae anticipates that it will be in a transitional state for several years as it migrates applications to the cloud under stream two. Internal reports show that as of October 2019, about a quarter of its business applications were in the cloud, with a year-end 2020 target of 36 percent. Enterprise officials told us that they expect a total of about three quarters of Fannie Mae’s applications to migrate to the cloud over the next few years. These officials reported that Fannie Mae sought to move all applications into the cloud, but also that some legacy applications may not be suitable.

ENTERPRISE BENEFITS AND RISK CONSIDERATIONS

Cloud Computing Benefits

FHFA officials cited four primary potential benefits of cloud computing for the Enterprises: economies of scale, improvements to disaster recovery, elastic response, and proprietary functions.

Economies of Scale

An FHFA official described cloud computing as the outsourcing of computing infrastructure to take advantage of enormous economies of scale. The 2011 Federal Cloud Computing Strategy notes that cloud providers can centralize infrastructure costs and lower costs to individual users when servicing a wide-area network. According to the Enterprises, the cloud provides a more cost-efficient and simplified infrastructure alternative to managing their own hardware.

Improvements to Disaster Recovery

FHFA and Freddie Mac officials told us that a critical consideration for Freddie Mac’s migration to the cloud is improvement of its disaster recovery posture, a core component of business resiliency. According to NIST, cloud computing has built-in resiliency features such as redundancy, the duplication of critical functions spanning different geographic regions. Redundancy increases reliability and reduces the time it will take for a business to recover computing assets and continue business operations in the event of a disruption.

Elastic Response

With cloud services, storage and computing power can be scaled up or down as required and on-demand. An FHFA official described this as elastic response. By contrast, traditional on-premises infrastructure operates under static computing resources. Periods of peak computing requirements take up only a fraction of the Enterprises’ operations. FHFA and Freddie Mac told us that it is more costly and inefficient to provide for peak computing requirements all the time.

Proprietary Functions

An FHFA official told us that in recent years, cloud providers have added proprietary functions to allow users to perform advanced processes more efficiently. Fannie Mae officials referred to the cloud’s added performance and capabilities as “the wisdom of the cloud” and affirmed this as the Enterprise’s primary benefit in cloud adoption. Both Enterprises articulated that those capabilities will allow them to more quickly deliver innovative solutions to the market.

Cloud Computing Risk Considerations

In addition to the operational risks in play during the migration process, use of the cloud environment presents its own set of risks. Below is a summary of risks we identified.

FHFA Recognizes Cloud Computing Requires Extensive Risk Management

As detailed in FHFA’s AB 2018-04, cloud computing raises a number of risks for the Enterprises, including third-party, information security, and business resiliency risks. FHFA has separately assessed each of these as high risk areas for both Enterprises. Fannie Mae publicly reported in its 2019 10-K that its information-sharing activities, including on cloud-based systems, expose it to ongoing threats that “may result in unauthorized access, loss or destruction of data or other cybersecurity incidents.” Freddie Mac publicly reported in its 2019 10-K that its plans to outsource infrastructure to the cloud or other third-parties may increase its risk exposure.

Third-party Cloud Provider Risk

According to FHFA, the Enterprises are exposed to third-party risks when outsourcing their technology infrastructure. An internal Fannie Mae document reported that its increasing use of cloud computing exposes the Enterprise to additional operational and reputational risks because the operating environment is extended off-premises. When using a third-party cloud provider, the Enterprises must share responsibility for safeguarding information and systems in the cloud environment. An FHFA official told us, however, that the Enterprises cannot outsource accountability and must make sure all the “protections” are in place. Fannie Mae and Freddie Mac must also configure how systems will be switched over efficiently for disaster recovery plans.

FHFA and the Enterprises confirmed to us that third-party cloud providers also present fourth party risk. Fourth parties are sub-contractors to the third-party provider and, according to internal Fannie Mae reporting, they pose additional risk that must be managed.

Concentration Risk

The Enterprises and Common Securitization Solutions⁴ all utilize at least one of the same third-party cloud providers. Cloud provider concentration, according to an internal FHFA presentation, presents the risk that technology failure, cyberattack, disaster, or corporate failure at the cloud provider may have a wide-ranging impact on the secondary mortgage market. The presentation summarized controls in place by a cloud provider to minimize risk. For example, the cloud provider separates the user’s operations from the cloud provider’s operations so that the user’s information is not compromised in the event of a successful external cyberattack on the cloud provider’s operations.

An FHFA official told us that the cloud provider discussed in the above referenced presentation has many independent data centers. Operations are distributed and duplicated between these data centers in such a way that they can operate independently if one portion fails; given this redundancy capability, the cloud provider is not a single point of failure. Another FHFA official told us that if an Enterprise were to use a different cloud provider as a back-up to its primary cloud provider for a particular function, this would increase risk. Designing for and testing changes in two different cloud environments for the same function increases costs and complexity, according to the FHFA presentation.

⁴ Common Securitization Solutions is a joint venture owned by Fannie Mae and Freddie Mac charged with developing, building, and operating the Common Securitization Platform. For more information, see OIG, *Special Report on the Common Securitization Platform* (Mar. 29, 2019) (OIG-2019-005) (online at www.fhfa.oig.gov/Content/Files/OIG-2019-005%20Special%20Report%20on%20the%20Common%20Securitization%20Platform_Redacted.pdf).

Information Security Risk

Cloud computing presents new security challenges for the Enterprises. According to an internal FHFA assessment, “from a security perspective, a number of new risks and challenges have been introduced from the relocation to a cloud environment, deteriorating much of the effectiveness of traditional protection mechanisms.” FHFA and Enterprise officials told us, however, that certain security risks may be lower with the cloud than with on-premises infrastructure. An FHFA official explained to us, for example, that the Enterprises will benefit from the high security standards of a large company providing cloud services.

Nonetheless, security and privacy risks in the cloud are continuously evolving, according to NIST. As noted in a 2019 FHFA internal assessment, the shifting cybersecurity landscape and the complexity of Enterprise technology infrastructure contribute to a high-risk security environment for the Enterprises.

Inadequate Staffing Expertise

Because cloud computing is a rapidly evolving field, there is a risk to the Enterprises of inadequate staffing expertise. According to internal reports and interviews with Enterprise officials, both Enterprises advise that they have developed risk mitigation strategies for hiring, training, and retaining cloud personnel.

CONCLUSION.....

Cloud computing touches on matters intersecting numerous areas of the Enterprises’ business. While both Enterprises invoked benefits of efficiency and technological advancement from a move to the cloud, both recognized high operational risks from these moves. In addition to the operational risks in play during the migration process, use of the public cloud environment presents its own set of risks. FHFA’s AB 2018-04 details a number of cloud computing risk areas for the Enterprises, including third-party, information security, and business resiliency risks. Additional risks include concentration risks with a cloud service provider and risks with inadequate cloud computing staff.

OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of this white paper was to provide a high-level overview of cloud computing at the Enterprises and discuss benefits and risks, particularly with third-party public cloud services. To achieve this objective, we reviewed internal and publicly available FHFA and Enterprise documents, as well as publicly available documents from other institutions. 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