Federal Housing Finance Agency
Office of Inspector General

Compliance Review of DBR's Examinations of Critical Cybersecurity Controls at the Federal Home Loan Banks

Compliance Review • COM-2019-004 • May 7, 2019

COM-2019-004

May 7, 2019

Executive Summary

The Federal Housing Finance Agency (FHFA or Agency), established by the Housing and Economic Recovery Act of 2008, is responsible for the supervision, regulation, and housing mission oversight of Fannie Mae, Freddie Mac, and the Federal Home Loan Bank System. The Federal Home Loan Bank System consists of the 11 Federal Home Loan Banks (FHLBanks) and the Office of Finance.

With an increasing number of cybersecurity incidents, including large-scale data breaches, affecting financial institutions of all sizes, it is important for institutions to have preventive and detective controls in place to mitigate the threat. Two such controls are vulnerability scans and penetration tests, which are applied to identify information security deficiencies and determine if existing security measures in an entity's technology environment could be circumvented.

In February 2016, we issued an audit report in which we found FHFA's Division of Federal Home Loan Bank Regulation (DBR) examinations generally did not assess the design of the FHLBanks' vulnerability scans and penetration tests when evaluating the operational effectiveness of those controls. We made two recommendations to address this shortcoming, which FHFA accepted—we recommended that the Agency (1) update its guidance to direct examiners to assess the design of the Banks' vulnerability scans and penetration tests when assessing the operational effectiveness of such controls, and (2) require examiners to document their assessments of the design of those scans and tests. In early 2017, the Agency updated its guidance to implement our recommendations and clarified that existing examiner documentation standards applied. We closed the recommendations in February 2017 based upon those actions.

We initiated this compliance review to evaluate DBR's compliance with its January 2017 guidance and existing standards for examiners to conduct and document design assessments of the FHLBanks' and Office of Finance's vulnerability scans and penetration tests when evaluating the operational effectiveness of those controls. We reviewed documentation for examinations for which work plans were approved between February 18, 2017, and December 31, 2018. For 11 of the 18 examinations (approximately two-thirds) in which DBR evaluated the operational effectiveness of vulnerability scans and penetration tests, we found that DBR did not fully comply with its revised guidance. Upon inquiry, DBR acknowledged with regard to the 11 previously cited examinations that it did not "seek to assess the design" of the vulnerability scans and penetration tests. Our recommendation that DBR require examiners to document their assessments of the design of vulnerability

COM-2019-004

May 7, 2019

scans and penetration tests necessarily implies that it require examiners to actually perform those assessments, as set forth in its updated guidance. Consequently, we are re-opening our recommendation that DBR require examiners to document design assessments.

We provided FHFA the opportunity to respond to a draft of this report. The DBR Deputy Director provided no comments or a formal reponse but reiterated in an email to us his dedication to the commitments described in this report.

This report was prepared by Alisa Davis, Senior Policy Advisor, and Karen E. Berry, Senior Investigative Counsel. We appreciate the cooperation of FHFA staff, as well as the assistance of all those who contributed to the preparation of this report.

This report has been distributed to Congress, the Office of Management and Budget, and others and will be posted on our website, www.fhfaoig.gov.

David M. Frost
Acting Deputy Inspector General for Compliance & Special Projects

TABLE OF CONTENTS

ABBREVIATIONS .....

DBR	Division of Federal Home Loan Bank Regulation
FHFA or Agency	Federal Housing Finance Agency
FHLBanks	Federal Home Loan Banks
FSOC	Financial Stability Oversight Council
IS Module	Information Security Module
IT	Information Technology
IT Module	Information Technology Module
OIG	Federal Housing Finance Agency Office of Inspector General

BACKGROUND

Overview of the FHLBanks' Cybersecurity Programs

Federal financial regulators, including FHFA, consider cybersecurity to be among the foremost risks facing the banking and financial services industries, making it a priority for examinations. Beginning with its first annual report in 2011 through its most recent annual report in 2018, the Financial Stability Oversight Council (FSOC),[1] of which FHFA is a member, has recognized the existence of a significant threat to financial institutions posed by cyber attackers. The FHLBanks and the Agency also recognize that a failure or breach of the FHLBanks' information systems caused by a cyber attack could disrupt the FHLBanks' business or result in significant losses or reputational damage.

In response to the threat from cyber attacks, the FHLBanks and the Office of Finance have established cyber risk management programs. An effective cyber risk management program has numerous components and internal controls, one of which is vulnerability management. Vulnerability management has been defined as "the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities."[2]

As part of their vulnerability management, the FHLBanks and the Office of Finance conduct (through contractors) vulnerability scans and penetration tests. Vulnerability scanning examines computers, systems, networks, and applications to identify security weaknesses. Penetration testing attempts to determine whether an attacker could successfully reach a specific database or system by circumventing existing controls.

Our 2016 Audit Report Found that DBR Examinations in 2013 and 2014 Did Not Include an Assessment of the Design of FHLBanks' Critical Cybersecurity Controls

In a 2016 audit report,[3] we found that in 14 of 15 information technology (IT) examinations conducted at 10 of the FHLBanks in 2013 and 2014, DBR examiners did not assess the design of vulnerability scanning and penetration testing performed by the FHLBanks' contractors. In the one instance where DBR examiners did review the design of the FHLBank's vulnerability scanning and penetration testing, they concluded that the penetration testing, as designed, was

[1] The FSOC is charged with identifying risks to the financial stability of the U.S., promoting market discipline, and responding to emerging risks to the financial system.

[2] Park Foreman, *Vulnerability Management*, CRC Press, 2010.

[3] *FHFA Should Improve its Examinations of the Effectiveness of the Federal Home Loan Banks' Cyber Risk Management Programs by Including an Assessment of the Design of Critical Internal Controls* (Feb. 29, 2016) (AUD-2016-001).

conducted in the database's test environment and would not identify vulnerabilities in the FHLBank's "live" IT environment.

We stated in our report that an examination of the operational effectiveness of IT controls can only be reliable when examiners understand the design of those controls[4] so that they can assess whether the controls would adequately mitigate risks. We found that without an assessment of the design of key IT internal controls, such as vulnerability scans and penetration tests, FHFA lacked assurance that such testing was meaningful. Furthermore, we found that FHFA's failure to assess the design of vulnerability scanning and penetration tests as part of its examination of operational effectiveness created significant risks to FHFA's DBR examination program, because poorly designed vulnerability scans and penetration tests may not detect vulnerabilities and may produce findings that are not reliable or accurate.

OIG Recommendations

We made two recommendations to FHFA. We recommended that the Agency:

- Update its Information Technology Risk Management Program Module (IT Module)[5] to direct examiners to assess the design of the FHLBanks' vulnerability scans and penetration tests when assessing the operational effectiveness of such controls; and

- Require examiners to document their assessments of the design of the FHLBanks' vulnerability scans and penetration tests as part of their assessment of the operational effectiveness of such controls.

Based on FHFA's Corrective Actions, OIG Closed the Recommendations

FHFA agreed with both recommendations. DBR agreed to update the IT Module to include guidance on assessing the design of vulnerability scans and penetration tests at the

[4] See the Committee of Sponsoring Organizations of the Treadway Commission *Internal Control – Integrated Framework* (May 2013) and *Standards for Internal Control in the Federal Government*, at 7 (Sept. 2014) (GAO-14-704G) (online at www.gao.gov/assets/670/665712.pdf) (accessed Feb. 25, 2019).

[5] The IT Module is one of many examination components in the *FHFA Examination Manual*. The IT Module provides instructions and worksteps for IT examinations.

FHLBanks.[6] The Agency also agreed to apply existing requirements for examiners to document their work when assessing vulnerability scans and penetration tests.[7]

In January 2017, DBR updated the IT Module to specifically require examiners, when assessing the operational effectiveness of vulnerability scans and penetration testing, to assess the design of those controls.

The guidance suggested four factors[8] for examiners to consider during assessments of the design of vulnerability scans and penetration tests:[9]

- Whether the parties that perform the vulnerability scans and penetration tests are sufficiently independent (i.e., not responsible for the design, installation, maintenance, and operation of any of the tested systems);
- Whether the institution's security risk assessment informs the frequency of the vulnerability scans and penetration tests;
- Whether the scopes and strategies of the vulnerability scans and penetration tests are commensurate with the institution's technology environment; and
- Whether the institution adequately addressed the findings from such vulnerability scans and penetration tests or has an adequate plan for remediation.

On February 17, 2017, we closed our recommendations based on DBR's responses and its inclusion of the new guidance in the IT Module.[10]

---

[6] The IT Module is applicable to examinations of Fannie Mae, Freddie Mac, and the FHLBank System. FHFA's corrective actions to our recommendations from the 2016 audit report and, therefore, this compliance review, extend to the FHLBanks and the Office of Finance.

[7] DBR identified for us three documentation standards for examiners: the *FHFA Examination Manual*, at 8 (Dec. 2013); 2016-DBR-OPB-01 (July 29, 2016); and 2014-DBR-OPB-003 (Dec. 24, 2014). These standards require examiners to document, in detail, their examination activities. Accordingly, such activities as the assessments of the design of vulnerability scans and penetration tests should be documented.

[8] For ease of reference in this paper, we call the illustrative guidance the "four factors" that relate to the design of protective measures, such as vulnerability scans and penetration tests.

[9] FHFA, *Information Technology Risk Management Program*, p. 26.

[10] Subsequent to our closing the recommendation, FHFA issued a preliminary version of a new module, the Information Security Module (IS Module), to serve as a reference for examinations of information security programs. The IS Module, which remains under review, contains the same basic requirement and the same four suggested factors relating to assessing the design of vulnerability scans and penetration testing as exists in the IT Module.

FINDING

We initiated this compliance review in December 2018 to determine whether DBR, consistent with its undertakings in response to our recommendations, documented assessments of the design of vulnerability scans and penetration tests when it examined the operational effectiveness of such controls during examinations of FHLBanks and the Office of Finance from February 18, 2017, through December 31, 2018 (review period). We found that, in most cases, DBR did not conduct or document such assessments.

DBR Examiners Did Not Conduct Assessments of the Design of Vulnerability Scans and Penetration Tests in 11 of 18 Examinations

From February 18, 2017, through December 31, 2018, DBR conducted 18 examinations in which it assessed the operational effectiveness of vulnerability scans and penetration tests. In over one-third, or 7 of the 18 examinations, examiners considered all four of the factors suggested in DBR guidance when assessing the design of vulnerability scans and penetration tests, and documented their assessments.[11] For the other examinations (11 of 18), however, examiners considered fewer than the four factors suggested in DBR guidance; in most instances, DBR documents reflect that the examiners considered only one or two of the suggested factors.

We asked DBR to clarify how, in these 11 examinations, it conducted the recommended assessments of the design of the vulnerability scans and penetration tests. In response, DBR acknowledged that it "did not seek to assess the design adequacy of vulnerability scans and penetration tests" in those 11 examinations, and thus did not document assessments of the design of such controls using all four factors.

When we inquired further as to why examiners did not assess the design of vulnerability scans and penetration tests in these 11 instances, the DBR Deputy Director said that he could not specify why the assessments were not performed. However, he committed to implementing several measures to ensure that DBR assesses the design of vulnerability scans and penetration tests using all four factors at each examination, beginning in the second quarter of 2019 through the end of 2020. Specifically, the Deputy Director communicated to DBR senior staff that:

[11] Documentation in seven examinations show consideration of: (1) the independence of those performing vulnerability scans and penetration tests; (2) whether security risk assessments informed the frequency of such controls; (3) whether the scopes and strategies of vulnerability scans and penetration tests were commensurate with the technology environment; and (4) the extent to which the FHLBanks adequately addressed the findings from such vulnerability scans and penetration tests.

- Examiners must document at the beginning of the examination that each of the four factors will be assessed and subsequently document the assessments once the work is performed;

- Examiners must communicate at designated times to the respective examination supervisors that the four factors were evaluated and documented, and DBR senior staff will assure the Deputy Director that the required assessments were performed; and

- Examination work related to these four factors will be peer reviewed and subject to quality control, with the Deputy Director receiving reports on whether the four factors were evaluated and satisfactorily documented.

The Deputy Director said he would determine at the end of 2020 the appropriate frequency for assessing the design of vulnerability scans and penetration tests in DBR's examinations where the FHLBank or the Office of Finance performed a vulnerability scan or penetration test since the prior examination.

We find that DBR did not fully follow our recommendation to require examiners to document assessments of the design of vulnerability scans and penetration tests because it did not require that those assessments be performed, as set forth in DBR guidance.

Consequently, we are re-opening our recommendation that DBR require examiners to document design assessments.

CONCLUSION

We recommended in 2016 that DBR update its guidance to ensure examiners both assess and document their assessment of the design of the vulnerability scans and penetration tests. DBR added guidance to its IT Module instructing examiners to perform assessments of the design of vulnerability scans and penetration tests (when assessing the operational effectiveness of vulnerability scans and penetration testing) and has existing requirements for examiners to document their work. However, its examiners did not always document design assessments because they did not always perform them. Examiners did not assess such controls in approximately two-thirds of the examinations we reviewed. In an environment in which cybersecurity remains a critical risk area, it is essential to ensure the operational effectiveness of vulnerability scans and penetration tests, including an assessment of the design of those scans and tests.

OIG provided FHFA an opportunity to respond to a draft of this report. In an email, the DBR Deputy Director stated he that he did not have technical comments and would not provide a

formal response; rather, he reiterated his dedication to the commitments described in this report.

As a result we are re-opening our recommendation that examiners document assessments of the design of vulnerability scans and penetration tests when examining the operational effectiveness of those controls.

OBJECTIVE, SCOPE, AND METHODOLOGY .....

The objective of this review was to determine if FHFA complied with the second recommendation in the underlying audit report to require examiners to document its assessment of the design of vulnerability scans and penetration testing if also assessing those controls for operational effectiveness. Specifically, we determined if DBR had implemented the applicable revised guidance in its IS Module (or the IT Module, if the examiners did not complete a separate IS Module). To accomplish our objective, we met with Agency officials responsible for creating the IS Module and overseeing examinations performed in accordance with the IS Module. We reviewed the scope memoranda and completed IS Modules for examinations with work plans approved from February 18, 2017, through December 31, 2018. We tested whether DBR examiners documented their assessment of the design of vulnerability scans and penetration tests as instructed by the IS Module's illustrative guidance. We reviewed additional information from DBR in instances where the examination documentation was unclear regarding its assessment of the design of vulnerability scans and penetration tests.

We conducted our compliance review from December 2018 through April 2019 under the authority of the Inspector General Act of 1978, as amended, and in accordance with the *Quality Standards for Inspection and Evaluation* (January 2012), which were promulgated by the Council of the Inspectors General on Integrity and Efficiency.

We provided a draft of this report to FHFA for its review and comment.

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