Federal Housing Finance Agency
Office of Inspector General

# 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

Audit Report • AUD-2016-001 • February 29, 2016

AUD-2016-001

February 29, 2016

## Executive Summary

Federal financial regulators, including the Federal Housing Finance Agency (FHFA), consider cyber security to be among the foremost risks facing the banking and financial services industries and have identified it as a supervisory priority for examinations. FHFA is one of ten voting members of the Financial Stability Oversight Council (FSOC) established by the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, which 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. In its 2015 annual report, which was approved by its voting members, FSOC recognized that "financial sector organizations and other U.S. businesses experienced numerous cyber incidents, including large-scale data breaches that compromised financial information. Malicious cyber activity is likely to continue, and financial sector organizations should be prepared to mitigate the threat posed by cyber attacks that have the potential to destroy critical data and systems and impair operations."

The Federal Home Loan Bank System is comprised of 11 regional Federal Home Loan Banks (collectively, the Banks or FHLBanks) and their Office of Finance, whose primary mission is to support housing finance. Since 2008, FHFA has been the regulator for the Banks and their Office of Finance. As their regulator, FHFA is responsible for ensuring that the Banks operate in a financially safe and sound fashion, remain adequately capitalized and able to raise funds in the capital markets, and operate in a manner consistent with their housing finance mission. The Division of Federal Home Loan Bank Regulation (DBR) has responsibility for conducting these supervisory activities, which include on-site annual examinations and off-site monitoring. Recognizing that effective management of cyber risk is vital to the performance and success of the Banks' operations, FHFA's examinations include reviews of the Banks' information technology (IT) risk management programs.

The Federal Housing Finance Agency Office of Inspector General (OIG) conducted this audit to assess whether DBR's examination of the effectiveness of the Banks' cyber risk management programs included review of the design of their vulnerability scanning and penetration testing efforts. This audit was conducted pursuant to OIG's 2015 Audit and Evaluation Plan and reflects our continued focus on FHFA's supervision of cyber risks by the entities that it regulates. Our audit found that, in 14 of 15 of DBR's IT examinations performed between 2013 and 2014 that included vulnerability scanning and/or penetration testing, DBR did not assess the design of those tests performed by contractors at the Banks' direction. Some DBR examiners determined that such an assessment was outside of the scope of the examination plan and all 14 of the

AUD-2016-001

February 29, 2016

work programs lacked steps to perform the assessment. Absent any examination of the design of vulnerability scans or penetration tests, we found that FHFA lacks reasonable assurance that such testing can accomplish its intended purpose. We made two recommendations to FHFA to address these shortcomings and FHFA agreed with our recommendations.

This report was prepared by Tara Lewis, Director, with assistance from Alisa Davis, Senior Auditor, Julio Santos, Lead Auditor, and Pamela L. Williams, Auditor. 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.

Stacey Nahrwold
Acting Deputy Inspector General for Audits

# TABLE OF CONTENTS

## ABBREVIATIONS

| | |
|---|---|
| Banks or FHLBanks | Federal Home Loan Banks |
| COSO | Committee of Sponsoring Organizations of the Treadway Commission |
| DBR | Division of Federal Home Loan Bank Regulation |
| FFIEC | Federal Financial Institutions Examination Council |
| FHFA | Federal Housing Finance Agency |
| FSOC | Financial Stability Oversight Council |
| GAO | Government Accountability Office |
| Green Book | *Standards for Internal Control in the Federal Government* |
| IT | Information Technology |
| Module | FHFA Information Technology Risk Management Program Module |
| OIG | Federal Housing Finance Agency Office of Inspector General |

# BACKGROUND

## Federal Financial Regulators Recognize the Critical Risks from Cyber Attacks on Financial Institutions

Beginning in its first annual report published in 2011, FSOC, of which FHFA is a member, has recognized the threat to financial institutions from successful cyber attacks. Each of FSOC's subsequent annual reports has highlighted the increasing threats to financial institutions from cyber attacks, as the sophistication and volume of cyber attacks on financial institutions has continued to increase. FSOC has cautioned that a successful cyber attack has the potential to impair financial sector operations. The director for the Center for Cyber and Homeland Security at the George Washington University testified on June 16, 2015, before the U.S. House of Representatives Committee on Financial Services that:

> The U.S. financial services sector in particular is in the crosshairs as a primary target. To give you a sense of the magnitude of the problem, consider the following figures which were provided to me recently by a major U.S. bank on a not-for-attribution basis: just last week, they faced 30,000 cyber attacks. This amounts to an attack every 34 seconds, each and every day. And these are just the attacks that the bank actually knows about, by virtue of a known malicious signature or IP address.[1]

According to the combined financial report for the Federal Home Loan Banks for the year ended December 31, 2014, each Bank, like other federally supervised financial institutions, relies heavily on its information systems and other technology to conduct and manage its business. While we were advised by FHFA that none of the Banks have experienced any material effect or losses related to cyber attacks as of December 2015, the Banks recognize that "a failure or breach, including as a result of cyber attacks, of the information systems of the FHLBanks and the Office of Finance, and those of critical vendors and third parties, could disrupt the FHLBanks' businesses or result in significant losses or reputational damage."[2] As a consequence, management of cyber risk is vital to the performance and success of the Banks' operations.

---

[1] U.S. House of Representatives, Committee on Financial Services, Subcommittee on Oversight and Investigations, *A Global Perspective on Cyber Threats* (June 16, 2015) (online at http://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=103674).

[2] Federal Home Loan Banks Office of Finance, *Combined Financial Report for the Year Ended December 31, 2014* (March 27, 2015) (online at www.fhlb-of.com/ofweb_userWeb/resources/2014Q4Document-web.pdf).

### The Banks' Efforts to Mitigate the Risks of Cyber Attacks

An effective cyber risk management program has numerous components and internal controls, of which one is vulnerability management. Each of the Banks' cyber risk management programs includes vulnerability management. As part of their vulnerability management efforts, the Banks conduct (through contractors they retain) vulnerability scanning and/or penetration testing. Vulnerability scanning is a thorough examination of computers, computer systems, networks, and applications to identify security weaknesses. Once security weaknesses identified through vulnerability scanning have been remediated, the penetration testing is conducted in an effort to determine whether an attacker could successfully reach a specific "live" database or system, such as a customer database or Human Resource records, by circumventing existing controls.

## FACTS AND ANALYSIS .....

### FHFA Examination of the Banks' Cyber Security Programs

As regulator for the Banks, FHFA is responsible for ensuring that they operate in a financially safe and sound fashion, remain adequately capitalized and able to raise funds in the capital markets, and operate in a manner consistent with their housing finance mission.[3] DBR has responsibility for conducting these regulatory activities, which include examination of each Bank at least annually,[4] through on-site annual examinations and off-site monitoring. DBR's examinations and monitoring focus on the Banks' processes for managing risks associated with their strategies or activities, and DBR examiners assess the Banks' condition and performance, governance, credit risk, market risk, and operational risks and existing controls to mitigate those risks. FHFA considers information technology to be an operational risk.

#### *FHFA's Information Technology Risk Management Program Module*

To assist its examiners in conducting examinations of the Banks' existing cyber risk management programs, FHFA issued an Information Technology Risk Management Program Module (Module). The Module details specific exam steps to be performed so that examiners can assess the operational effectiveness of the Banks' cyber security controls.

---

[3] *See* Section 1102(a) of the Housing and Economic Recovery Act of 2008, Pub. L. No. 110-289, 122 Stat. 2654, 2663 (codified at 12 U.S.C. § 4513(a)(1)(B)).

[4] *See* 12 U.S.C. §§ 4512(d) and 1440.

While the Module, by its terms, does not need to be performed by DBR examiners annually, it directs that when it is "included in the examination scope, the examiner must perform worksteps sufficient in coverage to document the basis for conclusions on the quantity of risk and quality of risk management pertaining to" IT infrastructure.

The Module's scope includes:

- Determining the existence of vulnerabilities to the institution's information security;
- Reviewing independent security tests performed by the Bank or its contractors, as applicable;
- Reviewing the most recent IT audit reports, plans, and scopes, and any external audit outsourcing engagement letters, and determining the adequacy of scope, frequency, accuracy, and timeliness of IT-related internal audit reports;
- Assessing the quality of the Banks' IT internal audit function, and if the work, or any portion of it, is outsourced to external vendors, determining the effectiveness and whether the Bank can appropriately rely on that work;
- Evaluating the adequacy of contractual terms regarding security responsibilities, controls, and reporting; and,
- Reviewing and assessing policies, procedures, and standards as they apply to the institution's IT environment and controls.

***Guidance for Evaluating Internal Controls – COSO, GAO, and FFIEC***

The Committee of Sponsoring Organizations of the Treadway Commission (COSO), formed by five professional financial and accounting associations and institutes in the United States, developed a comprehensive framework on, among other things, internal controls and enterprise risk management. The COSO Internal Control-Integrated Framework, released in 1992 and updated in 2013, has become one of the most widely accepted internal control frameworks in the world and enables organizations to effectively and efficiently develop systems of internal control that adapt to changing business and operating environments, and mitigate risks to acceptable levels.

Although the COSO Framework was designed to specifically assist management to better control an organization and provide a board of directors with added ability to oversee internal control, the internal monitoring an organization performs to assess its controls and ensure their effectiveness is akin to the supervisory responsibility and role performed by DBR examiners in overseeing the Banks' internal controls.

One of the principles in both the original and updated COSO Framework is ongoing monitoring of the internal control system to determine whether it continues to operate effectively as management intended. Principle 16 makes clear that an assessment of the operational effectiveness of internal controls necessarily includes consideration of the design of those controls.[5] An examination of the operational effectiveness of IT controls, as directed by FHFA's Module, can only be reliable where examiners understand the design of those controls so that they are able to assess whether the controls will adequately mitigate the risks.

The updated COSO Framework, with its principles and components of internal controls, has been adapted by the Government Accountability Office (GAO) in its September 2014 *Standards for Internal Control in the Federal Government* (known as the Green Book). The revised Green Book, effective fiscal year 2016, sets the standards for an effective internal control system for federal government entities. Among other things, the Green Book makes clear that a control cannot be effectively implemented if it was not effectively designed and that any assessment of the effectiveness of an internal control must include testing of its design and testing of its implementation.

In the same vein, the Federal Financial Institutions Examination Council (FFIEC) has issued guidance in one of its examination booklets for IT examinations, which includes sections on independent testing and examination procedures. While FHFA is not a member of FFIEC and is not required to follow its standards, the Module in FHFA's Examination Manual instructs examiners to "understand the implications and applicability of each of the referenced resources below," one of which is FFIEC's Information Security Booklet. Because the IT examination procedures for federally supervised financial institutions conducted by FFIEC members are similar to FHFA's examination procedures for the FHLBanks and because FHFA has directed its examiners to understand the FFIEC examination protocol, FFIEC's guidance is relevant to FHFA's examinations under its Module.

In sum, the COSO Framework, the Green Book, and FFIEC's Information Security Booklet acknowledge that a review of the design of internal controls is an important element to assess whether the controls accomplish their intended purpose and reduce operational risk.

### *DBR's Information Technology Examinations in 2013 and 2014*

During 2013 and 2014, the Banks retained contractors to perform vulnerability scanning and penetration testing (and other cyber risk tests), and these contractors prepared written reports

[5] COSO, *Internal Control-Integrated Framework* (2013), Principle 16 guidance states that "[u]nderstanding the design and current state of a system of internal control provides useful baseline information for establishing ongoing and separate evaluations. When using monitoring activities it is necessary to have an understanding of how management has designed its system of internal control[.]" Thus, COSO contemplates assessing both the design and effectiveness of internal controls in order to render a judgment about their value. *See also* COSO, *Internal Control-Integrated Framework (1992).*

with their findings. DBR examiners, in their examinations of the Banks in 2013 and 2014, relied on the results of the tests performed by the Banks' contractors to determine the extent of cyber security threats.

OIG reviewed a total of 15 IT examinations conducted by DBR for 2013 and 2014. For 14 of the 15 IT examinations conducted by DBR during this period that included vulnerability scanning and/or penetration testing, DBR officials confirmed to OIG that DBR examiners did not assess the design of the tests performed by the Banks' contractors related to the vulnerability scanning and penetration testing. For 1 of the 15 examinations, DBR examiners assessed the design of both the vulnerability scanning and penetration tests because they were concerned by the lack of sufficient detail in the Bank's network diagrams noted in prior DBR examination work papers, the Bank's history of difficulties in implementing an effective IT security program during a period of financial stress, and ongoing implementation of the Bank's IT security program due to changes in a key IT management position. After examining the design of the vulnerability scanning and penetration test,[6] DBR found that the overall scope of the penetration test for an operational database containing a large volume of personally identifiable information was not fully adequate in that it only reviewed for vulnerabilities in the database's test environment and not when the database was operating "live." DBR examiners recommended that the design of the penetration test of the Bank's database be revised so that future testing would be performed on the live database. DBR did not document any findings regarding design of the vulnerability scanning tests.

***Reasons for Not Assessing the Design of Internal Controls***

FHFA's Module sets forth a scope of examination work to be performed to assess the operational effectiveness of controls that includes, among other things, determining the effectiveness of, and whether the outsourced work, such as vulnerability scanning and penetration testing, can be reasonably relied upon. DBR officials reported to us that DBR examiners did not assess the design of the vulnerability scanning and penetration testing in 14 of the 15 IT exams for a number of reasons, including:

- DBR examiners were only reviewing what vulnerabilities, if any, were identified through penetration testing and vulnerability scanning conducted by the Banks' contractors;
- The examination scope only "included high level reviews of the penetration testing process";

[6] In this case, the penetration test was done in the test environment.

- DBR examiners reviewed the results of contractor testing and found the results reasonable; and,

- DBR examiners reviewed the Bank's oversight of its contractor and, where that oversight was found sufficient, these examiners relied on the testing conducted by the Bank contractors.

Additionally, DBR officials reported to us that DBR examiners for 5 of the 14 IT examinations did not view assessment of the design as part of their scope of work. Our review of the work programs for all 14 IT examinations found that none contained steps to assess the design of the vulnerability scanning and penetration tests.

## FINDINGS

1. An examination of the operational effectiveness of IT controls, directed by FHFA's Module, can only be reliable where examiners understand the design of those controls (as set forth in the updated COSO Framework and Green Book) so that they are able to assess whether the controls will adequately mitigate the risks.

2. In 14 of 15 IT examinations conducted at 10 of the Banks in 2013 and 2014, DBR examiners did not assess the design of vulnerability scanning and penetration testing performed by contractors retained by the Banks as part of their IT examinations of the Banks. Without an assessment of the design of key IT internal controls, such as vulnerability scanning and/or penetration testing, FHFA lacks assurance that such testing was meaningful. In the one instance where FHFA examiners reviewed the design of the Bank's vulnerability scanning and penetration testing, they concluded that the penetration testing as designed, was conducted in the database's test environment and would not identify vulnerabilities in the Bank's "live" IT environment.

3. Failure to assess the design of key IT internal controls, such as vulnerability scanning and penetration tests, as part of FHFA's examination of operational effectiveness creates significant risks to FHFA's DBR examination program. Poorly designed IT controls may not detect vulnerabilities and may produce findings that are not reliable or accurate.

## CONCLUSION

As regulator of the Banks, FHFA is responsible for ensuring that the Banks operate in a financially safe and sound fashion, remain adequately capitalized and able to raise funds in the capital markets, and operate in a manner consistent with their housing finance mission. FHFA supervises the Banks through on-site annual examinations and off-site monitoring.

Recognizing that effective management of cyber risk is vital to the performance and success of the Banks' operations, DBR examiners routinely examine the effectiveness of the Banks' internal controls to mitigate this risk. The scope of DBR's IT examinations of the Banks is defined by FHFA's Module, which includes an assessment of operational effectiveness.

In this audit, OIG found that in 14 of 15 IT examinations conducted by DBR in 2013 and 2014, DBR examiners did not assess the design of vulnerability scanning and penetration testing conducted by contractors at the Banks' direction, both of which are key IT internal controls. Going forward, DBR would benefit from adopting a piece of the COSO Framework and Green Book requiring examination of the design of controls. Absent examination of the design of such controls, FHFA lacks reasonable assurance that these controls will accomplish their intended purpose.

## RECOMMENDATIONS

OIG recommends that FHFA:

1. Update its Information Technology Risk Management Program Module 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 assessment of the design of the Banks' vulnerability scans and penetration tests as part of their assessment of the operational effectiveness of such controls.

# OBJECTIVE, SCOPE, AND METHODOLOGY .....

The objective of this audit was to assess whether DBR's examination of the effectiveness of the Banks' cyber risk management programs included review of the design of their vulnerability scanning and penetration testing efforts.

We reviewed FHFA's IT examination work performed during 2013 and 2014 for 10 of the 11 Banks where FHFA included vulnerability scanning and/or penetration testing as part of the scope of the examination. We excluded one of the Banks from the scope of our audit because that Bank merged with another Bank during our review.

OIG conducted this audit from March 2015 through December 2015 at FHFA's headquarters in Washington, D.C. and the main office of one of the Federal Home Loan Banks.

To accomplish the audit objective, OIG performed the following:

- Reviewed FHFA's Examination Manual and the Information Technology Risk Management Program Module;
- Reviewed COSO's 2013 Internal Control-Integrated Framework, GAO's 2014 Standards for Internal Control in the Federal Government, and FFIEC's Information Security Booklet;
- Reviewed FHFA's examination work papers related to 15 examinations performed during 2013 and 2014 related to the Banks' IT programs;
- Discussed FHFA examination work performed on IT examinations in 2013 and 2014 with the examiners-in-charge via electronic mail communication;
- Interviewed Federal Home Loan Bank officials regarding their information technology programs; and,
- Interviewed FHFA officials regarding IT-related examination processes.

OIG conducted this audit in accordance with generally accepted government auditing standards. Those standards require that OIG plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusion based on the audit objective. OIG believes that the evidence obtained provides a reasonable basis for the findings and conclusion included herein based on the audit objective.

We held an exit conference with FHFA officials on February 1, 2016.

# APPENDIX A .....

## FHFA's Comments on OIG's Findings and Recommendations

Federal Housing Finance Agency

**MEMORANDUM**

TO: Stacey Nahrwold, Acting Deputy Inspector General for Audits

FROM: Fred Graham, Deputy Director, Division of FHLBank Regulation 2/11/16

SUBJECT: Audit Report: *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*

DATE: February 11, 2016

This memorandum transmits the Federal Housing Finance Agency's (FHFA) management responses to the recommendations resulting from the audit performed by your staff from February 2015 to February 2016. As stated in report, the purpose of the audit was "to assess whether DBR's examination of the effectiveness of the Banks' cyber risk management programs included review of the design of their vulnerability scanning and penetration testing efforts."

**Recommendation 1:**

*OIG recommends that FHFA update its Information Technology Risk Management Program module to direct examiners to assess the design of the Banks' vulnerability scans and penetration tests, when assessing the operational effectiveness of such controls.*

**Management Response:** FHFA agrees with the recommendation. FHFA will update the Information Technology module of its examination manual so that it includes guidance on assessing the design of vulnerability scans and penetration tests at the FHLBanks. In updating the examination manual, we will make use of relevant published standards as appropriate. As with other guidance in the examination manual, examiners will use the new material as-needed and as part of FHFA's risk-based examinations of the FHLBanks.

We will complete this revision to the examination manual by January 31, 2017.

**Recommendation 2:**

*OIG recommends that FHFA require examiners to document their assessment of the design of the Banks' vulnerability scans and penetration tests as part of their assessment of the operational effectiveness of such controls.*

**Management Response:** FHFA agrees with the recommendation. Consistent with the FHFA examination module *Examination Program Overview*, examiners are required to document their examination work. By completing the first recommendation above, we will effectively extend

that requirement to any examiner assessments of vulnerability scans and penetration tests. Consequently, we expect to address this recommendation by addressing the first one.

# APPENDIX B.....

## OIG's Response to FHFA's Comments

On February 11, 2016, FHFA provided comments to a draft of this report, agreeing with both recommendations and identifying FHFA actions to address each recommendation. OIG considers the actions sufficient to resolve the recommendations, which remain open until OIG determines that agreed upon corrective actions are completed and responsive to the recommendations. OIG has attached the Agency's full response (see Appendix A), which was considered in finalizing this report. Appendix C provides a summary of management's comments on the recommendations and the status of agreed-to corrective actions.

# APPENDIX C.....

## Summary of Management's Comments on the Recommendations

This table presents management's response to the recommendations in the OIG report and the status of the recommendations as of when the report was issued.

| Rec. No. | Corrective Action: Taken or Planned | Expected Completion Date | Monetary Benefits | Resolved Yes or No[a] | Open or Closed[b] |
|---|---|---|---|---|---|
| 1. | FHFA will update the Information Technology module of its examination manual so that it includes guidance on assessing the design of vulnerability scans and penetration tests at the FHLBanks. In updating the examination manual, we will make use of relevant published standards as appropriate. As with other guidance in the examination manual, examiners will use the new material as-needed and as part of FHFA's risk-based examinations of the FHLBanks. | 01/31/2017 | $0 | Yes | Open |
| 2 | Consistent with the FHFA examination module *Examination Program Overview*, examiners are required to document their examination work. By completing the first recommendation above, we will effectively extend that requirement to any examiner assessments of vulnerability scans and penetration tests. Consequently, we expect to address this recommendation by addressing the first one. | 01/31/2017 | $0 | Yes | Open |
| Total | | | $0 | | |

[a] Resolved means: (1) management concurs with the recommendation, and the planned, ongoing, or completed corrective action is consistent with the recommendation; (2) management does not concur with the recommendation, but alternative action meets the intent of the recommendation; or (3) management agrees to the OIG monetary benefits, a different amount, or no amount ($0). Monetary benefits are considered resolved as long as management provides an amount.

[b] Once OIG determines that agreed-upon corrective actions have been completed and are responsive, the recommendation can be closed.

# 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