Audit Report
2017-IT-C-019
October 31, 2017

Consumer Financial Protection Bureau

2017 Audit of the CFPB's Information Security Program

Office of Inspector General
Board of Governors of the Federal Reserve System
Consumer Financial Protection Bureau

Office of Inspector General
Board of Governors of the Federal Reserve System
Consumer Financial Protection Bureau

Executive Summary, 2017-IT-C-019, October 31, 2017

2017 Audit of the CFPB's Information Security Program

Findings

The Consumer Financial Protection Bureau's (CFPB) overall information security program is operating at a level-3 (*consistently implemented*) maturity, with the agency performing several activities indicative of a higher maturity level. For instance, the CFPB's information security continuous monitoring process is effective and operating at level 4, with the agency tracking and reporting on performance measures related to supporting activities. In addition, the CFPB employs network access controls to detect unauthorized hardware and has implemented automated patch management tools. These areas are associated with a level-4 maturity.

The CFPB also has opportunities to mature its information security program to ensure that it is effective. Specifically, the agency can strengthen its ongoing efforts to establish an enterprise risk management program by defining a risk appetite statement and associated risk tolerance levels and developing and maintaining an agencywide risk profile. It can also improve configuration monitoring processes for agency databases and applications, multifactor authentication for internal network and systems, and assessments of the effectiveness of security awareness and training activities. Further, the CFPB has opportunities to mature its incident response and contingency planning capabilities to ensure that they are effective.

Finally, the CFPB has taken sufficient action to close one of the four recommendations from our past years' Federal Information Security Modernization Act of 2014 (FISMA) audits that remained open at the start of this audit. Efforts to address the remaining recommendations are underway, and we will continue to monitor the CFPB's progress as part of our future FISMA audits.

Recommendations

Our report includes seven new recommendations designed to strengthen the CFPB's information security program. In its response to our draft report, the CFPB concurs with our recommendations and outlines actions that are underway or will be taken to strengthen the CFPB's information security program. We will continue to monitor the agency's progress in addressing these recommendations as part of future audits.

Purpose

To meet our annual FISMA reporting responsibilities, we reviewed the information security program and practices of the CFPB. Our specific audit objectives, based on the legislation's requirements, were to evaluate the effectiveness of the CFPB's (1) security controls and techniques for select information systems and (2) information security policies, procedures, and practices.

Background

FISMA requires each agency Inspector General to conduct an annual independent evaluation of its agency's information security program, practices, and controls for select systems. U.S. Department of Homeland Security guidance for FISMA reporting directs Inspectors General to evaluate the maturity level (from a low of 1 to a high of 5) of their agencies' information security programs across several areas. Level 4 (*managed and measurable*) represents an effective level of security.

Recommendations, 2017-IT-C-019, October 31, 2017

2017 Audit of the CFPB's Information Security Program

Number	Recommendation	Responsible office
1	Ensure that a risk appetite statement and associated risk tolerance levels are defined and used to develop and maintain an agencywide risk profile.	Office of the Director
2	Develop and implement a tiered approach for implementing multifactor authentication that considers system risk levels and user roles and uses lessons learned to inform broader adoption.	Office of Technology and Innovation
3	Ensure that all contractors performing information technology functions have background investigations initiated before onboarding.	Office of the Chief Operating Officer
4	Develop and implement a plan to conduct periodic phishing exercises to measure the effectiveness of security awareness and training activities.	Office of Technology and Innovation
5	Ensure applicable alerts and logs from applications residing in the CFPB's new cloud computing environment are uploaded to the agency's central automated solution, which is used to detect and analyze incidents.	Office of Technology and Innovation
6	Ensure that containment strategies are developed and implemented for the key types of incidents applicable to the CFPB's environment.	Office of Technology and Innovation
7	Ensure that a. contingency plans for all CFPB systems are tested, as appropriate. b. contingency testing is integrated with the testing of related plans, such as those for incident response and continuity of operations, to the extent practicable. c. testing results are used to improve related processes, as needed.	Office of Technology and Innovation

Office of Inspector General
Board of Governors of the Federal Reserve System
Consumer Financial Protection Bureau

MEMORANDUM

DATE: October 31, 2017

TO: Distribution List

FROM: Peter Sheridan
Assistant Inspector General for Information Technology

SUBJECT: OIG Report 2017-IT-C-019: *2017 Audit of the CFPB's Information Security Program*

We have completed our report on the subject audit. We performed this audit pursuant to the Federal Information Security Modernization Act of 2014, which requires each agency Inspector General to conduct an annual independent evaluation of the effectiveness of the agency's information security program and practices. We also reviewed security controls for a select agency system, the details of which will be transmitted under separate, restricted cover. We will use the results of this audit to respond to specific questions in the U.S. Department of Homeland Security's *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*.

We provided you with a draft of our report for your review and comment. In your response, you concur with our recommendations and outline actions that have been or will be taken to address them. We have included your response as appendix B to our report.

We appreciate the cooperation that we received from CFPB personnel during our audit. Please contact me if you would like to discuss this report or any related issues.

cc: Dana James, Acting Chief Financial Officer and Acting Assistant Director, Office of the Chief Financial Officer
Zachary Brown, Chief Information Security Officer
Carlos Villa, Finance and Policy Analyst, Office of the Chief Financial Officer

Distribution:
Sartaj Alag, Chief Operating Officer and Associate Director, Division of Operations
Jerry Horton, Chief Information Officer
Marianne Roth, Chief Risk Officer

Contents

Introduction

Objectives

Our audit objectives, based on the requirements of the Federal Information Security Modernization Act of 2014 (FISMA), were to evaluate the effectiveness of the Consumer Financial Protection Bureau's (CFPB) (1) security controls and techniques for select information systems and (2) information security policies, procedures, and practices. Our scope and methodology are detailed in appendix A.

Background

FISMA requires agencies to develop, document, and implement an agencywide security program for the information and the information systems that support the operations and assets of the agency, including those provided by another agency, a contractor, or another source.[1] FISMA also requires that each Inspector General (IG) perform an annual independent evaluation to determine the effectiveness of the information security program and practices of its respective agency, including testing the effectiveness of information security policies, procedures, and practices for select systems.

To support annual independent evaluation requirements, the U.S. Department of Homeland Security (DHS) publishes annual FISMA reporting metrics for IGs to respond to. This guidance directs IGs to evaluate the effectiveness of agency information security programs across a variety of attributes grouped into seven security domains. These domains map to the five security functions defined by the National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework) (table 1).[2]

1. Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (2014) (codified at 44 U.S.C. §§ 3551-3558).

2. The Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise and provides IGs with guidance for assessing the maturity of controls to address those risks.

Table 1. Cybersecurity Framework Security Functions, Objectives, and Associated FISMA Domains

Security function	Security function objective	Associated FISMA security domain
Identify	Develop an organizational understanding to manage cybersecurity risk to agency assets	Risk management
Protect	Implement safeguards to ensure delivery of critical infrastructure services as well as to prevent, limit, or contain the impact of a cybersecurity event	Configuration management, identity and access management, and security training
Detect	Implement activities to identify the occurrence of cybersecurity events	Information security continuous monitoring
Respond	Implement processes to take action regarding a detected cybersecurity event	Incident response
Recover	Implement plans for resilience to restore any capabilities impaired by a cybersecurity event	Contingency planning

Source: U.S. Department of Homeland Security, *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*.

FISMA Maturity Model

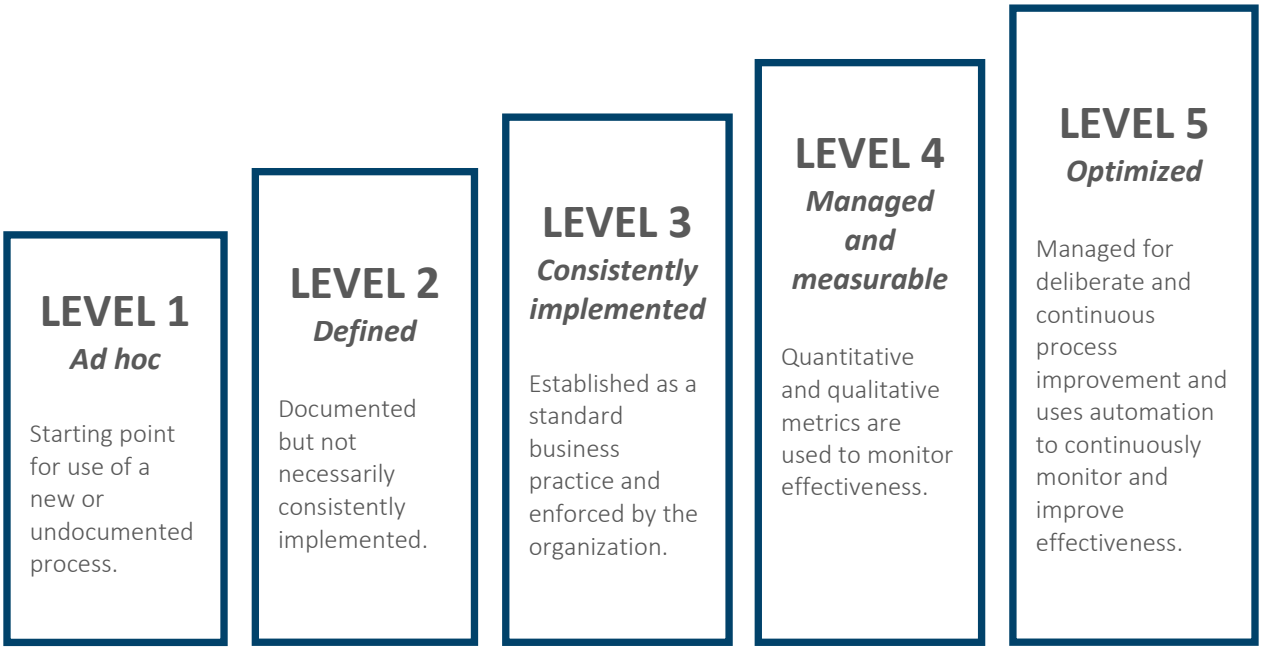
FISMA requires that IGs assess the effectiveness of information security controls that support the operations and assets of their respective agency. To that end, the Council of the Inspectors General on Integrity and Efficiency, in coordination with the Office of Management and Budget (OMB), DHS, and other key stakeholders, developed a maturity model intended to better address and report on the effectiveness of an agency's information security program. The purpose of the maturity model is (1) to summarize the status of agencies' information security programs and their maturity on a five-level scale; (2) to provide transparency to agency Chief Information Officers (CIOs), top management officials, and other interested readers of IG FISMA reports regarding what has been accomplished and what still needs to be implemented to improve the information security program; and (3) to help ensure that annual FISMA reviews are consistent across IGs.

The five levels of the IG FISMA maturity model are

1. *ad hoc*
2. *defined*
3. *consistently implemented*
4. *managed and measurable*
5. *optimized*

The foundational levels (1–3) of the model ensure that agencies develop sound policies and procedures, and the advanced levels (4–5) capture the extent to which agencies institutionalize those policies and procedures (figure 1). The maturity levels of each of the security domains will dictate the overall maturity of an organization's information security program. Within the context of the maturity model, level 4 (*managed and measurable*), represents an effective level of security.[3] This is the first year that all FISMA security domains will be assessed using a maturity model. Details on the scoring methodology for the maturity model can be found in appendix A.

Figure 1. FISMA Maturity Model Rating Scale



Source: OIG analysis of DHS FISMA reporting metrics.

3. NIST Special Publication 800-53, Revision 4, *Security and Privacy of Controls for Federal Information Systems and Organizations*, defines security control effectiveness as the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment, or enforcing or mediating established security policies.

Summary of Findings

The CFPB's overall information security program is operating at a level-3 (*consistently implemented*) maturity, with the agency performing several activities indicative of a higher maturity level. [4] For instance, the CFPB's information security continuous monitoring (ISCM) process is effective and operating at level 4, with the agency tracking and reporting on performance measures related to supporting activities. In addition, the agency employs network access controls to detect unauthorized hardware and has implemented automated patch management tools. These areas are associated with a level-4 maturity.

The CFPB has further opportunities to ensure that its information security program is effective in FISMA domains across all five Cybersecurity Framework security functions: *identify, protect, detect, respond,* and *recover* (table 2). Our report includes seven recommendations in these areas.

4. Appendix A of this report explains the scoring methodology used to determine the maturity of the CFPB's information security program.

Table 2. Summary of Opportunities to Mature the CFPB's Information Security Program

Cybersecurity function area and associated FISMA domain	Maturity rating	Opportunities for improvement
Identify		
Risk management	Level 3: *consistently implemented*	• Develop and implement an agencywide risk appetite statement and risk tolerance levels. • Evaluate technological options that facilitate a consistent and repeatable approach to risk management activities across the agency.
Protect		
Configuration management	Level 3: *consistently implemented*	• Evaluate options to use application whitelisting technology.
Identity and access management	Level 3: *consistently implemented*	• Develop and implement a tiered approach to implementing multifactor authentication. • Ensure that all contractors performing information technology (IT)–related functions have background investigations initiated before onboarding.
Security training	Level 3: *consistently implemented*	• Conduct periodic phishing exercises to measure the effectiveness of security awareness and training activities. • Use the National Initiative for Cybersecurity Education framework to strengthen the security training program.
Detect		
Information security continuous monitoring	Level 4: *managed and measurable*	• Strengthen monitoring of security configurations for databases and applications through greater automation. • Incorporate technologies and processes provided through the DHS continuous diagnostics and mitigation program when they are made available.
Respond		
Incident response	Level 3: *consistently implemented*	• Ensure that applicable alerts and logs from applications residing in the CFPB's new cloud computing environment are uploaded to the agency's central automated solution. • Ensure that containment strategies are developed and implemented for the key types of incidents applicable to the CFPB's environment.
Recover		
Contingency planning	Level 3: *consistently implemented*	• Strengthen contingency plan testing processes for CFPB systems.

Source: OIG analysis.

In addition, the CFPB has taken sufficient action to close one of the four open recommendations from our prior FISMA audits that remained open at the start of this audit. The closed recommendation involved strengthening access management processes for the agency's privileged users by ensuring that signed user-access forms and rules of behavior documents are maintained and accounts are annually recertified.

We are leaving open two recommendations from our 2016 FISMA audit for the CIO (1) to evaluate options and develop an agencywide insider threat program and (2) to perform an agencywide business impact analysis (BIA) and update the agency's continuity of operations plan and IT contingency plan accordingly. We are also leaving open a recommendation from our 2014 FISMA audit for the CIO to strengthen the CFPB's vulnerability management practices by implementing an automated solution and process to periodically assess and manage database and application-level security configurations. Efforts to address these recommendations are underway, and we will continue to monitor the CFPB's progress in these areas as part of our future FISMA audits.

Analysis of the CFPB's Progress in Implementing Key FISMA and DHS Information Security Program Requirements

The CFPB's overall information security program is operating at a level-3 (*consistently implemented*) maturity. Although the agency has strengthened its program since our last FISMA report, it has further opportunities to ensure that its information security program is effective across specific FISMA domains in all five Cybersecurity Framework security functions: *identify, protect, detect, respond,* and *recover*.

Identify

The objective of the *identify* function in the Cybersecurity Framework is to develop an organizational understanding of how to manage cybersecurity risks to agency systems, assets, data, and capabilities. The Cybersecurity Framework highlights risk management processes that organizations can implement to inform and prioritize decisions.

Risk Management

FISMA requires federal agencies to provide information security protections commensurate with their risk environment. Risk management refers to the program and supporting processes used to manage risk to organizational operations, assets, and individuals. This includes establishing the context for risk-related activities, assessing risks, responding to risks, and monitoring risks over time. NIST Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View* (SP 800-39), states that managing risk is a complex, multifaceted activity that requires the involvement of the entire organization. To accomplish this, risk management must be addressed at the enterprise, mission and business process, and information system levels.

Enterprise risk management (ERM) is an area that has seen increased emphasis in the federal government. It refers to an effective agencywide approach to addressing the full spectrum of the agency's external and internal risks, including those for information security. OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, provides guidance to agencies on implementing an ERM capability and governance structure that is coordinated with strategic planning and internal control processes.

In addition to a governance structure, components of an ERM program also include establishing a risk context, which includes the definition of risk appetite and tolerance levels; developing an agencywide risk management strategy; and completing a risk profile (table 3). An agencywide risk management strategy, in particular, is a key component of implementing ERM because it can help ensure a coordinated approach across the agency. It includes an unambiguous expression of risk tolerance for the agency, acceptable risk assessment methodologies, risk response strategies, a process for consistently evaluating

risk across the organization with respect to the agency's risk tolerance, and approaches for monitoring risk over time.

Table 3. Key Components of ERM

ERM component	Description
Risk context	An initial component of risk management that describes how an organization frames risk. Establishing the risk context includes defining the organization's risk tolerance and appetite levels.
Risk appetite	The broad-based amount of risk an organization is willing to accept in pursuit of its mission and vision. It is established by the organization's senior-most leadership and serves as the guidepost to set strategy and select objectives.
Risk tolerance	The acceptable level of variance in performance relative to the achievement of objectives. It is generally established at the program, objective, or component level. In setting risk tolerance levels, management considers the relative importance of the related objectives and aligns risk tolerance with risk appetite.
Risk management strategy	Outlines how the organization intends to assess, respond to, and monitor risk.
Risk profile	Provides an analysis of the risk that an agency faces toward achieving a strategic objective and identifies appropriate options for addressing significant risks.

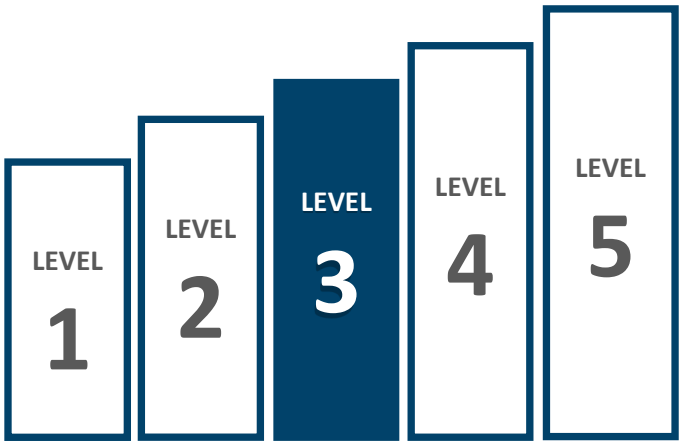
Source: NIST SP 800-39 and OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*.

Current Security Posture

The CFPB's risk management program is operating at level 3 (*consistently implemented*), with the agency performing several activities indicative of a higher maturity level. For instance, the CFPB analyzes and monitors performance measures on the effectiveness of its cybersecurity plan of actions and milestones process, which is indicative of a level-4 maturity. Further, the agency has consistently implemented cybersecurity risk management processes for its information systems, including for system categorization.

In addition, the CFPB has begun establishing an ERM program. As part of developing this program, the agency has designated a Chief

Figure 2. Risk Management, Level 3 (*Consistently Implemented*)



Source: OIG analysis.

Risk Officer in the Office of the Director. In addition, the CFPB has chartered an Enterprise Risk Committee responsible for ensuring that risks are managed as an interrelated portfolio. The CFPB has also developed an ERM process framework that contains elements of a risk management strategy, consistent with federal guidance.[5] For example, the CFPB has developed a risk taxonomy that organizes risks and establishes a common risk language across the organization and risk scales that consider likelihood, impact, and velocity. Further, the agency has drafted an ERM policy.

Our 2016 FISMA report includes a recommendation for the CIO to strengthen the agency's risk management processes around insider threats. Specifically, we recommended that the CIO evaluate options and develop an agencywide insider threat program that includes (1) a strategy to raise organizational awareness; (2) an optimal organizational structure; and (3) integration of incident response capabilities, such as ongoing activities around data loss prevention.[6] This year, CFPB officials informed us that the agency has contracted with a firm to evaluate options for developing an insider threat program, which would inform the development of an insider threat strategy. At the conclusion of our fieldwork, that work was ongoing. CFPB officials also noted that developing an insider threat program and strategy will require a coordinated effort across the agency. As such, the agency has transferred ownership of implementing our recommendation to the Office of the Chief Operating Officer. As such, we are leaving this recommendation open and will continue to monitor the CFPB's work in this area as a part of future audits.

Opportunities for Improvement

The CFPB has implemented a cybersecurity risk management program based on NIST SP 800-39 that addresses IT risks at the enterprise, business process, and information system levels. However, this program is not yet fully integrated with the ERM program, as efforts to define the ERM program are underway. For example, the CPFB's Office of Technology and Innovation is implementing a system to centralize the management of cybersecurity risks and the overall implementation of FISMA and IT security policies. However, the CFPB has not yet defined how it will use technology, such as management dashboards, at the organizational level to provide a centralized, enterprisewide view of risks.

The use of such technology, which could include an agencywide governance, risk management, and compliance tool, is a recommended component of ERM outlined in DHS's *FY 2017 Inspector General Federal Information Security Modernization Act Reporting Metrics* (FY 2017 FISMA Reporting Guidance for IGs).[7] We realize that the implementation of such technology depends on the CFPB's completing its agencywide risk management strategy and related components. As such, we are not making a recommendation in this area at this time. However, we suggest that the CFPB begin evaluating technological options that facilitate a consistent and repeatable approach to risk management activities across the organization. We will follow up on the CFPB's efforts as part of future FISMA audits.

5. United States Chief Financial Officers Council, *Playbook: Enterprise Risk Management for the U.S. Federal Government,* July 29, 2016.

6. Office of Inspector General, *2016 Audit of the CFPB's Information Security Program*, OIG Report 2016-IT-C-012, November 10, 2016.

7. U.S. Department of Homeland Security, *FY 2017 Inspector General Federal Information Security Modernization Act Reporting Metrics*, April 17, 2017.

We believe that while the CFPB has been performing components of ERM, it prioritized a holistic agencywide approach to risk management in late 2016 to meet new federal guidance. Meanwhile, the agency's approach to cybersecurity risk management has been in place for several years and, based on the results of our testing, has been consistently implemented. We believe that another cause for the lack of an optimal level of integration between the agency's ERM efforts and its cybersecurity risk management program is that the CFPB has not yet defined its risk appetite and tolerance levels. We recognize that the CFPB has outlined milestones for completing these activities. A risk appetite statement and associated tolerance levels will allow the CFPB to develop a comprehensive risk profile and better integrate its cybersecurity and ERM programs.

Recommendation

We recommend that the Chief Risk Officer continue to work with divisions across the CFPB to

1. Ensure that a risk appetite statement and associated risk tolerance levels are defined and used to develop and maintain an agencywide risk profile.

Management's Response

In its response to our draft report, CFPB management concurs with our recommendation and indicates that the agency is in the process of establishing an ERM program. Further, management notes that the CFPB will continue to build its ERM program in fiscal year 2018 by developing an ERM strategy, integrating ERM with the cybersecurity program, and defining the agency's risk appetite and tolerance levels.

OIG Comment

In our opinion, the actions described by CFPB management are responsive to our recommendation. We plan to follow up on the CFPB's actions to ensure that the recommendation is fully addressed.

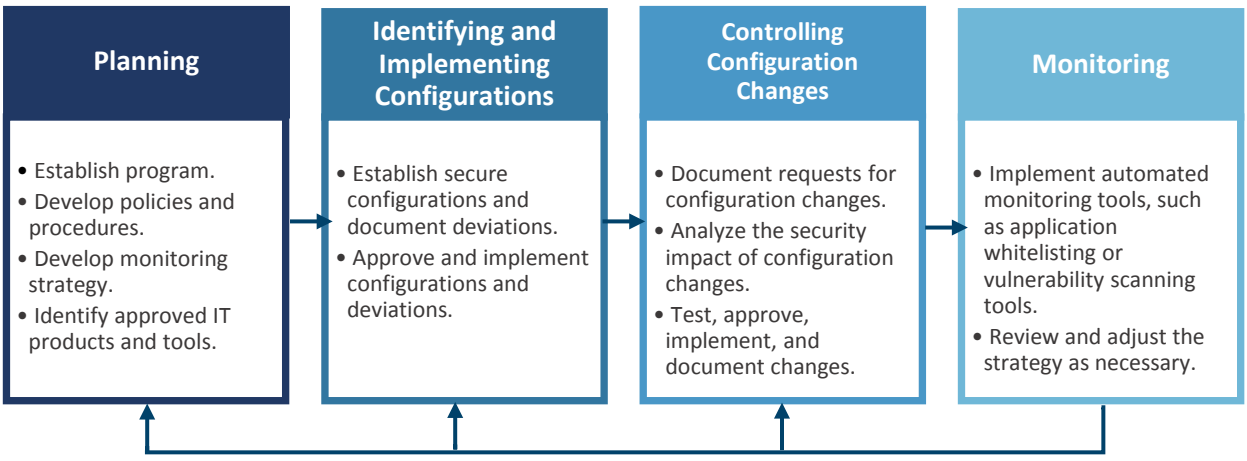
Protect

The objective of the *protect* function in the Cybersecurity Framework is to develop and implement safeguards to secure information systems. This function supports the ability to prevent, limit, or contain the impact of a cybersecurity event through applicable configuration management, identity and access management, and security training processes.

Configuration Management

FISMA requires agencies to develop an information security program that includes policies and procedures that ensure compliance with minimally acceptable system configuration requirements. Configuration management refers to a collection of activities focused on establishing and maintaining the integrity of products and information systems through the control of processes for initializing, changing, and monitoring their configurations. NIST Special Publication 800-128, *Guide for Security-Focused Configuration Management of Information Systems* (SP 800-128) recommends integrating information security into configuration management processes. Security-focused configuration management of information systems involves a set of activities that can be organized into four major phases: (1) planning, (2) identifying and implementing configurations, (3) controlling configuration changes, and (4) monitoring (figure 3).

Figure 3. Security-Focused Configuration Management Phases



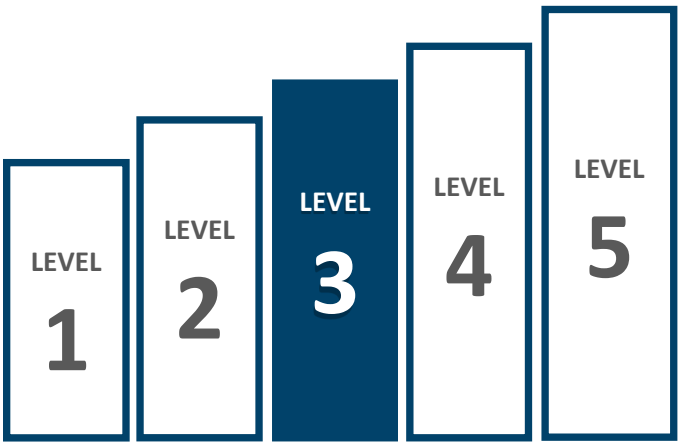
Source: NIST SP 800-128.

A key component of security-focused configuration management is monitoring, which involves validating that information systems are adhering to organizational policies, procedures, and approved secure configuration baselines. NIST SP 800-128 highlights the important role automated technologies play in monitoring by helping ensure that baseline configurations are implemented and maintained effectively. Two such technologies that are referenced in DHS's FY 2017 FISMA Reporting Guidance for IGs are vulnerability scanning and application whitelisting. Vulnerability scanning can help identify outdated software versions, missing patches, and misconfigurations, and help validate compliance with or deviations from an organization's security policy. Application whitelisting technologies are intended to stop the execution of malware and other unauthorized software and are used to control which applications are permitted to be installed or executed on a system.

Current Security Posture

The CFPB's configuration management program is operating at level 3 (*consistently implemented*), with the agency performing several activities indicative of a higher maturity level. For instance, the CFPB employs network access controls to detect unauthorized hardware, an activity associated with a level-4 maturity. In addition, the CFPB uses automated patch management tools and tracks and reports on performance measures related to its change management activities. Further, the agency has consistently implemented a vulnerability scanning process at the operating system and network levels for its systems.

Figure 4. Configuration Management, Level 3 (*Consistently Implemented*)



Source: OIG analysis.

Opportunities for Improvement

Our 2014 FISMA report includes a recommendation for the CIO to strengthen the CFPB's vulnerability management practices by implementing an automated solution and process to periodically assess and manage database- and application-level security configurations.[8] In 2015, the agency was working to evaluate its current scanning solutions to determine whether the capacity to perform these types of scans could be leveraged from tools already implemented within its environment. In 2016, however, agency officials informed us that database- and application-level scanning will require implementing tools from DHS's continuous diagnostics and mitigation (CDM) program. At the time of our fieldwork for this audit, the agency had researched various tools and was in the process of selecting one to implement. As such, we are keeping our 2014 recommendation open and will continue to monitor the agency's efforts to strengthen database- and application-level vulnerability management practices as part of our future FISMA audits.

Further highlighting the importance of implementing a database- and application-level scanning capability, we continue to identify security misconfigurations for CFPB databases and applications. These vulnerabilities could lead to unauthorized access, modification, or disclosure of data. Specifically, as part of our audit, we conducted database-level vulnerability scanning for a select system and noted that while security patches had been installed in a timely manner, the database was not configured in accordance with best practices.[9] For example, we found weaknesses in passwords for system accounts, inadequate audit logging, and excessive privileges granted to users. Further, our audit of security controls for the CFPB's public website[10] identified risks in configuration management. Although we are not making additional recommendations in this area, we strongly suggest that the CFPB prioritize the implementation

8. Office of Inspector General, *2014 Audit of the CFPB's Information Security Program*, OIG Report 2014-IT-C-020, November 14, 2014.

9. The best practices we are referring to are the guidelines published by the Center for Internet Security and the Defense Information Systems Agency.

10. Office of Inspector General, *Security Control Review of the CFPB's Public Website*, OIG Report 2017-IT-C-010, May 22, 2017.

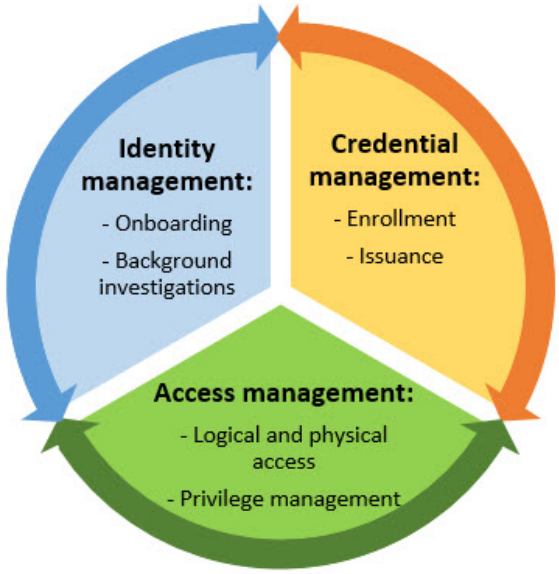
of an automated solution and process to periodically assess and manage database- and application-level security configurations.

We also identified an opportunity for the CFPB to strengthen its configuration management processes by implementing application whitelisting technologies, where appropriate. Such technologies could also enable the organization to further centralize its inventory of software applications and associated licenses and ensure that unauthorized software is prohibited from running. We recognize that such tools may not be applicable for all CFPB systems and could have operational effects on usability. Therefore, we are not making a recommendation in this area. However, we suggest that the CFPB evaluate options to implement application whitelisting in its environment, and we will continue to monitor the agency's efforts.

Identity and Access Management

Identity and access management includes implementing a set of capabilities to ensure that users authenticate to IT resources and have access to only those resources that are required for their job function, a concept referred to as *need to know*. Supporting activities include personnel screening and onboarding, issuing and maintaining user credentials, and managing logical and physical access privileges, which are collectively referred to as identity, credential, and access management (ICAM) (figure 5).

Figure 5. ICAM Conceptual Design



Source: CIO Council, *Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance.*

A component of ICAM that has been increasingly emphasized in federal guidance is the use of multifactor authentication for privileged and nonprivileged users of an agency's IT systems. For example, as part of OMB's Cybersecurity Sprint in 2015, agencies are required to implement multifactor authentication using personal identity verification (PIV) or a comparable solution for all internal system users.[11] Further, DHS's FY 2017 FISMA Reporting Guidance for IGs directs IGs to assess the degree to which PIV or a comparable solution has been deployed to provide strong authentication.

In support of federal ICAM requirements, the CFPB has developed and implemented policies and procedures that cover multiple functions throughout the life cycle of a user's digital identity. For example, the CFPB's policies and procedures cover requirements for account management, multifactor authentication, audit logging, background investigations, and onboarding. Further, the agency's suitability policy requires risk designations and fingerprint checks for personnel (employees and contractors) before

11. A 30-day Cybersecurity Sprint was launched by OMB in June 2015 to further improve federal cybersecurity and protect systems against evolving threats.

starting employment. For employees, once employment has started based on a favorable fingerprint check, the agency initiatives a full background check based on the position's risk designation. For contractors, a background check is required to be initiated after a favorable fingerprint check is performed and before employment begins.

Current Security Posture

The CFPB's identity and access management program is operating at level 3 (*consistently implemented*). As part of its ICAM program, the CFPB has defined roles and responsibilities at the organizational and system levels for stakeholders, is working to consolidate ICAM investments across the agency, and has defined an implementation strategy. As part of that strategy, the CFPB has met milestones for enabling multifactor authentication for internal agency users.

Figure 6. Identity and Access Management, Level 3 (*Consistently Implemented*)

Source: OIG analysis.

Our 2016 FISMA report includes a recommendation for the CFPB to strengthen access management processes for the agency's privileged users. Specifically, we recommended that the CIO ensure that (1) a signed user-access form and rules of behavior document are on file and maintained for each privileged user and (2) all privileged user accounts are annually recertified.[12] This year, the CPFB has implemented a new process to track user-access forms and rules of behavior documents for privileged users. Further, the CFPB has implemented a privileged account recertification process and has taken steps to ensure that requisite forms and documents are on file, which we verified through sampling. As such, we are closing our 2016 recommendation and will continue to monitor the CFPB's efforts in this area.[13]

Opportunities for Improvement

Our 2016 FISMA audit report highlights that the CFPB had an ongoing project to manage identity and access credentials. As a part of this project, the CFPB had enabled PIV across its enterprise. Although PIV was not enforced, the agency had developed a project plan to deploy PIV credentials and resolve outstanding technical issues. This year, the CFPB has not made significant progress in this area and does not mandate the use of PIV credentials for its privileged and nonprivileged users. Although the agency employs two-factor, token-based authentication for remote access, it has not resolved technical challenges with integrating PIV-based authentication for all of its systems. Further, the agency has implemented several compensating controls, but the lack of strong authentication, which can be attained

12. Office of Inspector General, *2016 Audit of the CFPB's Information Security Program*, OIG Report 2016-IT-C-012, November 10, 2016.

13. For a select system we reviewed, we noted that for three privileged users, user-access forms or signed rules of behavior had not been re-signed in a timely manner or were not on file. The results of our review for this system will be transmitted under separate, restricted cover.

with PIV cards, poses an increased risk of unauthorized access to the CFPB's information systems. As such, we believe that the agency should prioritize PIV using a tiered approach that considers system risk levels and user roles.

In addition, the CFPB has not ensured that background checks are completed for contractor personnel performing IT work. In a judgmental sample of 12 CFPB personnel (4 employees and 8 contractors), 2 contractors had been hired but left the agency within 6 weeks without having a background check initiated. Three other contractors had been working at the agency for at least 4 months but never received their background initiation paperwork. Of these individuals, 2 had access to the CFPB consumer response system, 1 of them with privileged access. Background checks had not been completed consistently for contractor personnel because the CFPB's personnel office had not ensured that the requisite checks were initiated with the Office of Personnel Management. We believe that ensuring the timely initiation of background checks for contractor personnel will better inform and mitigate the agency's risk of insider threats.

Recommendations

We recommend that the CIO

2. Develop and implement a tiered approach for implementing multifactor authentication that considers system risk levels and user roles and uses lessons learned to inform broader adoption.

We recommend that the Chief Operating Officer

3. Ensure that all contractors performing IT functions have background investigations initiated before onboarding.

Management's Response

In its response to our draft report, CFPB management concurs with our recommendations. Management notes that the agency will continue to implement multifactor authentication across the enterprise with consideration for system risk levels and user roles. Further, the agency will review and reevaluate its procedures for initiating background investigations for onboarding contractors who peform IT functions.

OIG Comment

In our opinion, the actions described by CFPB management are responsive to our recommendations. We plan to follow up on the CFPB's actions to ensure that the recommendations are fully addressed.

Security Training

FISMA requires agencies to develop an information security program that provides security awareness training to personnel, including contractors, who support the operations and assets of the organization, as well as role-based training for individuals with significant information security responsibilities. NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*, notes that, in general, people are one of the weakest links in attempting to secure agency systems and

networks.[14] As such, a robust, enterprisewide awareness and training program is key to ensuring that people understand their IT security responsibilities, organizational policies, and how to properly use and protect the IT resources entrusted to them.

Phishing has garnered additional focus for training and incident response in the federal government as a result of increased cyberattacks perpetrated using such means. Phishing refers to tricking individuals into disclosing sensitive personal information through deceptive computer-based means. Often, phishing involves authentic-looking emails that request information from users or direct them to malicious websites. One way to guard against phishing attacks is through security awareness training and periodic testing exercises. DHS's FY 2017 FISMA Reporting Guidance for IGs notes that an effective security training program includes phishing exercises and follow-up training, as appropriate.

Current Security Posture

The CFPB's security training program is operating at level 3 (*consistently implemented*). For instance, the CFPB leverages an automated security awareness training solution for employees and contractors, posts cybersecurity tips of the week on its intranet, and participates in other cybersecurity awareness activities throughout the year. Moreover, the CFPB ensures that all system users complete the agency's security awareness training (or a comparable training for contractors) before granting system access and periodically thereafter and maintains completion records. Further, the CFPB ensures that individuals with significant security responsibilities are provided with specialized security training before provision of information system access or performance of assigned duties and periodically thereafter.

Figure 7. Security Training, Level 3 (*Consistently Implemented*)

Source: OIG analysis.

Opportunities for Improvement

The CFPB does not conduct phishing exercises to measure the effectiveness of its security awareness and training activities. A key reason for this is that the agency has prioritized the development of its role-based training program for individuals with significant security responsibilities, which was finalized in 2016. Phishing exercises could be used to further educate the agency's workforce on security best practices and better protect the CFPB's systems from potential phishing attacks.

In addition, the CFPB has begun defining its processes for assessing the knowledge, skills, and abilities of its cybersecurity workforce. The Federal Cybersecurity Workforce Assessment Act of 2015 requires

14. Per NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*, individuals with significant security responsibilities include system and network administrators, managers, and security officers.

agencies to assess and align their cybersecurity workforce with NIST Special Publication 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* (SP 800-181). SP 800-181 provides a common, consistent lexicon to describe cybersecurity work by category, specialty area, and work role. It also provides a set of cybersecurity knowledge, skills, and abilities. SP 800-181 emphasizes that the NICE framework will allow employers to use focused, consistent language in professional development programs, in their use of industry certifications and academic credentials, and in their selection of relevant training opportunities for their workforce. The NICE framework was finalized in August 2017, and CFPB officials informed us that they plan to use it in the coming year.

We believe that the NICE framework could help strengthen the CFPB's security awareness and training program. However, in accordance with OMB guidance, agencies typically are given 1 year to incorporate new NIST guidance into their information security programs. As such, we are not making a recommendation in this area, and we will continue to monitor the CFPB's process in implementing the Federal Cybersecurity Workforce Assessment Act of 2015 and the NICE framework.

Recommendation

We recommend that the CIO

4. Develop and implement a plan to conduct periodic phishing exercises to measure the effectiveness of security awareness and training activities.

Management's Response

In its response to our draft report, CFPB management concurs with our recommendation and states that the agency plans to provide specialized training and exercises to educate users regarding phishing.

OIG Comment

In our opinion, the actions described by CFPB management are responsive to our recommendation. We plan to follow up on the CFPB's actions to ensure that the recommendation is fully addressed.

Detect

The objective of the *detect* function in the Cybersecurity Framework is to implement activities to discover and identify the occurrence of cybersecurity events in a timely manner. The Cybersecurity Framework notes that continuous monitoring processes are used to detect anomalies and changes in the organization's environment of operation, knowledge of threats, and security control effectiveness.

Information Security Continuous Monitoring

ISCM refers to the process of maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. Best practices for implementing ISCM are outlined in NIST Special Publication 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations* (SP 800-137). They are

1. **Define** an ISCM strategy based on risk tolerance that maintains clear visibility into assets, awareness of vulnerabilities, up-to-date threat information, and mission and business impacts.

2. **Establish** an ISCM program determining metrics, status monitoring frequencies, control assessment frequencies, and a technical architecture.

3. **Implement** an ISCM program and collect the security-related information required for metrics, assessments, and reporting. Automate collection, analysis, and reporting of data where possible.

4. **Analyze** the data collected and report findings, determining the appropriate response.

5. **Respond** to findings with technical, management, and operational mitigating activities or acceptance, transference/sharing, or avoidance/rejection.

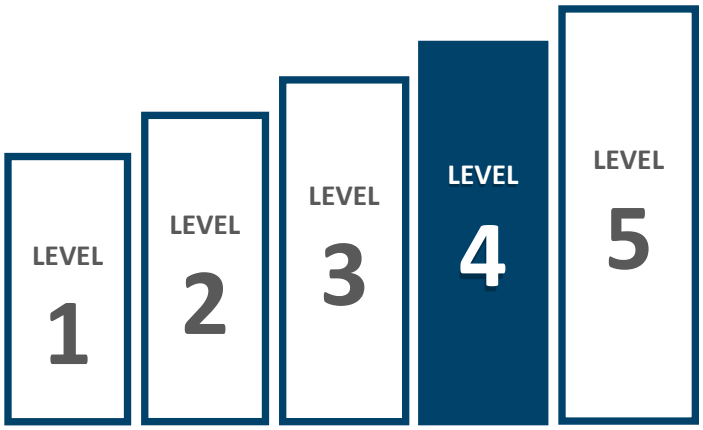
6. **Review** and update the ISCM program, adjusting the strategy and maturing measurement capabilities to increase visibility into assets and awareness of vulnerabilities, further enable data-driven control of the security of an organization's information infrastructure, and increase organizational resilience.

In particular, SP 800-137 highlights the importance of an organization's ISCM strategy in ensuring that ISCM activities are integrated across the organization. Specifically, the publication notes that that an ISCM strategy is meaningful only in the context of broader organizational needs, objectives, or strategies and as part of a broader risk management strategy.

Current Security Posture

The CFPB's ISCM program is effective and operating at level 4 (*managed and measurable*). The agency has made improvements in several areas in 2017. For instance, it is collecting and reporting on metrics that measure the effectiveness of ISCM automation areas. These areas include ongoing assessments, software assurance, and asset management. In addition, the CFPB has implemented a lessons-learned process and has developed and implemented an ISCM strategy that includes objectives, goals, requirements, and guidelines for monitoring and managing risk across the agency.

Figure 8. ISCM, Level 4 (*Managed and Measurable*)



Source: OIG analysis.

Opportunities for Improvement

We identified several areas for improvement in the agency's information security program that will affect the ability of the agency to maintain and improve the maturity of its ISCM program. For example, not all the CFPB's applications that have recently been transitioned to a new cloud computing environment are configured to provide alerts and logs to the central automated solution the agency uses to monitor security events and incidents. The Incident Response section below provides further details and offers a recommendation in this area.

Further, as noted earlier in this report, the CFPB has not developed an agencywide risk management strategy to help ensure that risks across the organization are consistently assessed, prioritized, and monitored over time. Once this strategy is developed, the agency will need to update its ISCM program accordingly. Also, as detailed in the Configuration Management section above, we continue to find opportunities to strengthen the CFPB's vulnerability management practices for its databases and applications. Addressing these areas will help the CFPB maintain and improve the maturity of its ISCM program and provide it with greater visibility into the effectiveness of supporting processes. Although we are not making recommendations in these areas, we will continue to monitor the CFPB's progress in addressing them and their potential effect on the maturity of the agency's ISCM program.

The CPFB can also improve its ISCM program and capabilities by using DHS's CDM program, where appropriate. DHS provides federal departments and agencies with capabilities and tools that help identify cybersecurity risks on an ongoing basis, prioritize these risks based on potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first. CFPB officials informed us that DHS has placed the CFPB in group F, along with other small agencies, which has a target rollout of CDM capabilities in the November 2017–May 2018 time frame. We will continue to monitor the CFPB's progress in implementing the capabilities of the CDM program as part of our future FISMA audits.

Respond

The objective of the *respond* function in the Cybersecurity Framework is to implement processes to contain the impact of detected cybersecurity events. Activities include developing and implementing incident response plans and procedures, analyzing security events, and effectively communicating incident response activities.

Incident Response

FISMA requires each agency to develop, document, and implement an agencywide information security program that includes policies and procedures for incident response. Best practices for incident response are detailed in NIST Special Publication 800-61, Revision 2, *Computer Security Incident Handling Guide* (SP 800-61), which notes that an incident response process consists of four main phases: preparation; detection and analysis; containment, eradication, and recovery; and postincident activity (table 4).

Table 4. Key Incident Response Phases

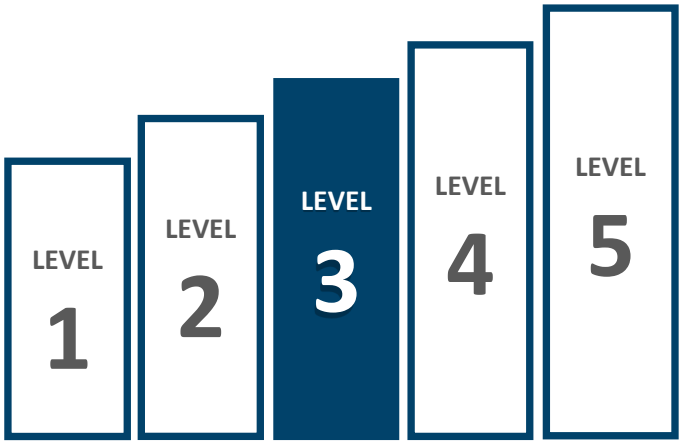
Incident response phase	Description
Preparation	Establish and train the incident response team and acquire the necessary tools and resources.
Detection and analysis	Detect and analyze precursors and indicators. A precursor is a sign that an incident may occur in the future and an indicator is a sign that an incident may have occurred or is occurring currently. Technology, such as a security information and event monitoring tool, can be used to centralize and more effectively detect and analyze incident-related information.
Containment, eradication, and recovery	Contain an incident to limit its impact, gather and handle evidence, eliminate components of the incident, and restore affected systems to normal operations. Organizations should create separate containment strategies for each major incident type, with criteria documented clearly to facilitate decisionmaking.
Postincident activity	Capture lessons learned to improve security measures and the incident response process.

Source: NIST SP 800-61.

Current Security Posture

The CFPB's incident response program is operating at level 3 (*consistently implemented*). For instance, the CFPB has defined and implemented its *Cybersecurity Incident Response Plan* and its *Computer Security Incident Response Team (CSIRT) Standard Operating Procedures* document. Further, the agency's policies and procedures on incident response generally align with the U.S. Computer Emergency Readiness Team's *Federal Incident Notification Guidelines* and the phases outlined in SP 800-61. We also found that the agency is analyzing incident precursors and indicators that are internally generated and those provided by the United States Computer Emergency Readiness Team.

Figure 9. Incident Response, Level 3 (*Consistently Implemented*)



Source: OIG analysis.

Opportunities for Improvement

As noted in the section on ISCM, not all the CFPB's applications that have recently been transitioned to a new cloud computing environment are configured to provide alerts and logs to the central automated solution the agency uses to detect and analyze incidents. For a select system that was transitioned to this new environment, CFPB management initially accepted the risk of not configuring alerts to integrate with the central solution on migration. Ensuring that the CFPB's central automated solution for detection and analysis of incidents contains alerts and logs from all CFPB systems, as appropriate, can help ensure that the agency is detecting and analyzing incident precursors and indicators in a timely manner.

We also found that the CFPB has not developed containment strategies for key incident types that may affect the agency. Specifically, although the agency has developed strategies to contain incidents involving a denial of service, email campaign, or malicious code, it has not done so for incidents using the internet, impersonation or spoofing, improper usage, or loss or theft of equipment as attack vectors. We believe that one reason for this is that the agency is in the early stages of developing an insider threat program. Agency officials notified us that the insider threat program would include risk considerations resulting from improper usage and loss or theft of equipment. As a result, the agency may not be able to limit the effect of an incident in a timely manner.

Recommendations

We recommend that the CIO

5. Ensure applicable alerts and logs from applications residing in the CFPB's new cloud computing environment are uploaded to the agency's central automated solution, which is used to detect and analyze incidents.

6. Ensure that containment strategies are developed and implemented for the key types of incidents applicable to the CFPB's environment.

Management's Response

In its response to our draft report, CFPB management concurs with our recommendations. Management notes that the CFPB will continue its efforts to ensure that applicable alerts and logs from agency systems and service providers are uploaded to the CFPB's centralized automated solution to identify cybersecurity incidents. Further, management notes that the agency will update standard operating procedures for incident response to include containment strategies for key types of incidents.

OIG Comment

In our opinion, the actions described by CFPB management are responsive to our recommendations. We plan to follow up on the CFPB's actions to ensure that the recommendations are fully addressed.

Recover

The objective of the *recover* function in the Cybersecurity Framework is to ensure that organizations maintain resilience by implementing appropriate activities to restore capabilities or infrastructure services that were impaired by a cybersecurity event. The Cybersecurity Framework outlines contingency planning processes that support timely recovery to normal operations and reduce the effect of a cybersecurity event.

Contingency Planning

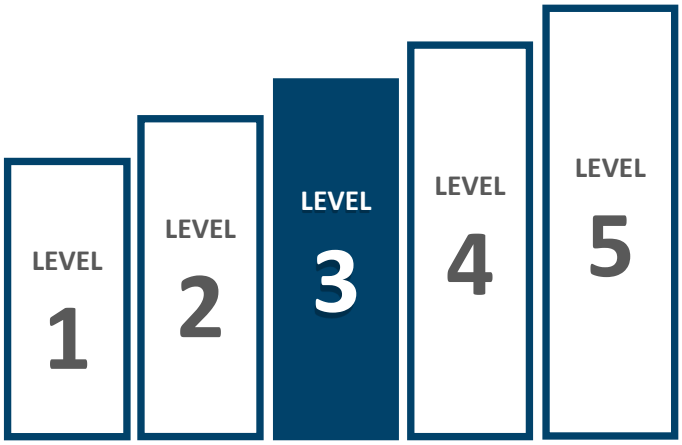
FISMA requires agencies to develop, document, and implement plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the organization. Information system contingency planning refers to a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of information systems, operations, and data after a disruption. NIST Special Publication 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, provides best practices for information system contingency planning. It highlights the importance of conducting a BIA, which helps identify and prioritize information systems and components critical to supporting the organization's mission and business processes, as a foundational step to effective contingency planning. A BIA allows an organization to measure priorities and interdependencies (internal or external to the entity) by risk factors that could affect mission-essential functions. Further, NIST Special Publication 800-53, Revision 4, *Security and Privacy of Controls for Federal Information Systems and Organizations*, requires periodic testing of IT contingency plans to determine effectiveness and organizational readiness. Plan testing can be conducted through tabletop exercises, simulations, and more comprehensive exercises.

Current Security Posture

The CFPB's contingency planning program is operating at level 3 (*consistently implemented*). For instance, the CFPB has defined and communicated roles and responsibilities for contingency planning and reinforces these during individual system training sessions. Further, the agency has established teams to implement contingency planning strategies.

Our 2016 FISMA audit report includes a recommendation for the CIO to strengthen the agency's contingency program by (1) performing an agencywide BIA and (2) updating the agency's continuity of operations plan and IT contingency plan to

Figure 10. Contingency Planning, Level 3 (*Consistently Implemented*)



Source: OIG analysis.

reflect the results of the BIA and the CFPB's current operating environment.[15] Efforts were underway in 2017 to address our recommendation. For example, the Office of the Chief Operating Officer is taking the lead in developing a BIA and has reached out to several federal agencies to inquire about best practices and approaches. The CFPB has set an initial target of completing a BIA by the end of 2017. As such, we are keeping our recommendation open, and we will continue to monitor the CFPB's progress in developing a BIA as part of our future FISMA audits.

Opportunities for Improvement

The CFPB had not ensured that contingency plans for its IT systems are tested. Specifically, for the eight systems listed on the agency's inventory, the contingency plan for only one had been tested. Further, dates for testing the contingency plan for the remaining seven systems had not been scheduled at the time of our review. Although the CFPB's information security policy requires that contingency plans for IT systems be tested annually, agency officials informed us that they are prioritizing the development of the plans and associated training strategies before establishing milestones for testing. Ensuring that IT contingency plans are periodically tested will provide the CPFB with additional assurance that system recovery capabilities can be implemented effectively.

Recommendation

We recommend that the CIO

7. Ensure that

    a. contingency plans for all CFPB systems are tested, as appropriate.

    b. contingency testing is integrated with the testing of related plans, such as those for incident response and continuity of operations, to the extent practicable.

    c. testing results are used to improve related processes, as needed.

Management's Response

In its response to our draft report, CFPB management concurs with our recommendation and states that the agency will execute testing and exercises to assess contingency capabilities. Further, management notes that lessons learned will be used to continuously improve the agency's contingency planning and recover capabilities.

OIG Comment

In our opinion, the actions described by CFPB management are responsive to our recommendation. We plan to follow up on the CFPB's actions to ensure that the recommendation is fully addressed.

15. Office of Inspector General, *2016 Audit of the CFPB's Information Security Program*, OIG Report 2016-IT-C-012, November 10, 2016.

Appendix A: Scope and Methodology

Our specific audit objectives, based on FISMA requirements, were to evaluate the effectiveness of the CFPB's (1) security controls and techniques for select information systems and (2) information security policies, procedures, and practices. To accomplish our objectives, we reviewed the effectiveness of the CFPB's information security program across the five function areas outlined in DHS's FISMA reporting metrics: *identify*, *protect*, *detect*, *respond*, and *recover*. These five function areas consist of seven security domains: risk management, configuration management, identity and access management, security training, ISCM, incident response, and contingency planning. To assess the CFPB's information security program, we interviewed agency management and staff; analyzed security policies, procedures, and documentation; and observed and tested specific security processes and controls. We also assessed the implementation of select security controls for an agency system. The detailed results of our review of this system will be transmitted under a separate, restricted cover.

To rate the maturity of the CFPB's information security program and functional areas, we used the scoring methodology defined in DHS's FISMA reporting metrics. The maturity ratings are determined by a simple majority, where the most frequent level (that is, the mode) across the domains serves as the overall rating. Per DHS, IGs are given flexibility to adjust maturity ratings based on the unique risk environments of their respective agency.

We performed our fieldwork from June 2017 to September 2017. We conducted this audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence we obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix B: Management's Response

Consumer Financial Protection Bureau

1700 G Street NW, Washington, DC 20552

October 27, 2017

Mr. Peter Sheridan
Associate Inspector General for Information Technology
Board of Governors of the Federal Reserve System &
Consumer Financial Protection Bureau
20th and C Streets, NW
Washington, DC 20551

Thank you for the opportunity to review and comment on the Office of Inspector General's (IG) draft report on the *2017 Audit of the CFPB's Information Security Program.* We are pleased that you found that the Bureau's information security program is operating at an overall level three (consistently implemented) maturity and certain components of the program operating at a level four (managed and measurable) maturity based on the IG Federal Information Security Modernization Act (FISMA) maturity model. In fiscal year (FY) 2018, we will continue to enhance our processes and technologies to raise our overall maturity levels and address each recommendation cited in the draft report.

Futhermore, we recognize that the draft report states the following:

- The CFPB is operating at a level three maturity for the **Identify** function. The Bureau is in the process of establishing an enterprise risk management (ERM) program and has designated a Chief Risk Officer within the Office of the Director. The Bureau has already implemented foundational ERM program components, such as a risk taxonomy, an ERM process framework, and the Enterprise Risk Committee. In FY 2018, we will continue to build the ERM program by developing an enterprise risk management strategy, integrating ERM with the Cybersecurity program, and defining the Bureau's risk appetite and tolerance levels.
- The CFPB operates at a level three maturity for the **Protect** function. The Bureau operates at a level four maturity for certain aspects of the **Protect** function, such as the use of network access controls to detect unauthorized hardware, automated patch management tools, and reporting of performance measures for change management. We are pleased that you have found that the Bureau addressed the FY 2016 recommendation regarding user access forms and recertification of privileged user accounts. In FY 2018, we will continue to mature our identity

and access management capabilities and our security and awareness training program, with the goal of achieving level four maturity for the entire Protect function.

- The CFPB's **Detect** function and our information security continuous monitoring (ISCM) program have matured from level three to level four. We collected and reported on ISCM metrics for ongoing assessments, software assurance, and asset management. We also established a lessons learned process and ISCM strategy to strengthen our ISCM capabilities. We have shared our progress about partnering with the Department of Homeland Security's (DHS) Continuous Diagnostics and Monitoring (CDM) Program to augment our detection capabilities and identify potential cybersecurity risks, and we plan to implement CDM capabilities as they are made available by DHS.
- The CFPB's **Respond** function is operating at a level three maturity and that our incident response policies and procedures generally align with the United States – Computer Emergency Readiness Team (US-CERT) Federal Incident Notification Guidelines. The Bureau analyzes internal and US-CERT provided incident precursors and indicators. We acknowledge that not all applications and systems are integrated with our centralized solution for incident detection and analysis. Due to capacity constraints, we plan to prioritize integration based on criticality in FY 2018.
- The CPFB's **Recover** function is operating at a level three maturity. The Bureau has defined and communicated the roles and responsibilities for contingency planning and has held training sessions for contingency planning personnel. The Bureau has also established teams to implement contingency planning strategies. In FY 2018, with this foundation established, we have shared with you our plans to schedule and execute our contingency plan tests for all remaining systems and integrate testing of our incident response and continuity of operations plans where appropriate.

We appreciate your noting our progress on remediating recommendations from previous Inspector General (IG) reviews. We value your objective, independent viewpoints and consider our IG to be a trusted source of informed, accurate, and insightful information.

Thank you for the professionalism and courtesy that you and all of the OIG personnel demonstrated throughout this review. We have provided comments for each recommendation.

Sincerely,

Jerry Horton
Chief Information Officer

consumerfinance.gov

Response to recommendations presented in the Draft IG Report,
"2017 Audit of the CFPB's Information Security Program."

Recommendation 1: We recommend that the Chief Risk Officer continue to work with divisions across the CFPB to ensure that a risk appetite statement and associated risk tolerance levels are defined and used to develop and maintain an agencywide risk profile.

Management Response: The Bureau concurs with this recommendation. The CFPB will continue to work across the Bureau to ensure that a risk appetite statement and associated risk tolerance levels are defined and used to develop and maintain a Bureau-wide risk profile.

Recommendation 2: Develop and implement a tiered approach for implementing multifactor authentication that considers system risk levels and user roles and uses lessons learned to inform broader adoption.

Management Response: The Bureau concurs with this recommendation. We will continue to implement multi-factor authentication solutions across the enterprise that considers system risk levels and user roles. For example, in FY2017, the CFPB began issuing personal identity verification cards to eligible contractors to enable desktop-based multi-factor authentication. In FY 2018, the CFPB will continue to integrate our IAM solution across the enterprise to enable risk-based multi-factor authentication. We will also gather lessons learned during each multi-factor authentication solution implementation activity to inform broader adoption across the entire enterprise.

Recommendation 3: Ensure that all contractors performing information technology functions have background investigations initiated before onboarding.

Management Response: The Bureau concurs with this recommendation. We will review and reevaluate our procedures for having background investigations initiated before onboarding contractors performing information technology functions.

Recommendation 4: Develop and implement a plan to conduct periodic phishing exercises to measure the effectiveness of security awareness and training activities.

Management Response: The Bureau concurs with this recommendation. We will provide specialized training and exercises to help educate our users regarding phishing and enhance our existing security education, training, and awareness program.

Recommendation 5: Ensure applicable alerts and logs from applications residing in CFPB's new cloud computing environment are uploaded to the agency's central automated solution used to detect and analyze incidents.

Management Response: The Bureau concurs with this recommendation. We will continue in our efforts to ensure that applicable alerts and logs from CFPB systems and service providers are

uploaded to the Bureau's centralized automated solution for alerts and log analysis to identify cybersecurity incidents.

Recommendation 6: Ensure that containment strategies are developed and implemented for the key types of incidents applicable to CFPB's environment.

Management Response: The Bureau concurs with this recommendation. The Bureau's is making steady progress towards updating standard operation procedures for incident response to include containment strategies for key types of incidents. Those strategies will be assessed and implemented in the coming year.

Recommendation 7: Ensure that (a) contingency plans for all CFPB systems are tested, as appropriate; (b) contingency testing is integrated with testing of related plans, such as those for incident response and continuity of operations, to the extent practicable; and (c) testing results are used to improve related processes, as needed.

Management Response: The Bureau concurs with this recommendation. In FY 2017, the CFPB established a strong foundation for IT contingency planning and began to execute testing and exercises to assess contingency capabilities. We will contintue to execute according to schedule and incorporate the results and lessons learned from those exercises into continuous improvement of the Bureau's ITCP and Recover capabilities.

Abbreviations

BIA	business impact analysis
CDM	continuous diagnostics and mitigation
CFPB	Consumer Financial Protection Bureau
CIO	Chief Information Officer
Cybersecurity Framework	*Framework for Improving Critical Infrastructure Cybersecurity*
DHS	U.S. Department of Homeland Security
ERM	enterprise risk management
FISMA	Federal Information Security Modernization Act of 2014
FY 2017 FISMA Reporting Guidance for IGs	*FY 2017 Inspector General Federal Information Security Modernization Act Reporting Metrics*
ICAM	identity, credential, and access management
IG	Inspector General
IT	information technology
ISCM	information security continuous monitoring
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PIV	personal identity verification
SP 800-39	Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*
SP 800-61	Special Publication 800-61, Revision 2, *Computer Security Incident Handling Guide*
SP 800-128	Special Publication 800-128, *Guide for Security-Focused Configuration Management of Information Systems*
SP 800-137	Special Publication 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*
SP 800-181	Special Publication 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*

Report Contributors

Khalid Hasan, Senior OIG Manager
Paul Vaclavik, OIG Manager
Andrew Gibson, OIG Manager
Daniel Megalo, Project Lead
Kaneisha Johnson, IT Auditor
Jeffrey Woodward, IT Auditor
Emily Martin, IT Audit Intern
Peter Sheridan, Assistant Inspector General for Information Technology

Contact Information

General

Office of Inspector General
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Mail Stop K-300
Washington, DC 20551

Phone: 202-973-5000
Fax: 202-973-5044

Media and Congressional

OIG.Media@frb.gov

Hotline

Report fraud, waste, and abuse.

Those suspecting possible wrongdoing may contact the OIG Hotline by mail, web form, phone, or fax.

OIG Hotline
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Mail Stop K-300
Washington, DC 20551

Phone: 800-827-3340
Fax: 202-973-5044