Audit Report
2017-IT-B-018
October 31, 2017

Board of Governors of the Federal Reserve System

2017 Audit of the Board'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-B-018, October 31, 2017

2017 Audit of the Board's Information Security Program

Findings

The Board of Governors of the Federal Reserve System's (Board) 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 Board has enhanced its configuration management practices to more effectively detect unauthorized hardware and software on its network. Further, it has implemented an effective security training program that includes phishing exercises and associated performance metrics.

The Board also has opportunities to mature its information security program to ensure that it is effective. A consistent theme we noted is that the lack of an agencywide risk management governance structure and strategy, as well as the decentralization of information technology services, results in an incomplete view of the risks affecting the security posture of the Board and impedes its ability to implement an effective information security program. We also found that several security processes, such as configuration management and information security continuous monitoring, were not effectively implemented agencywide.

Finally, the Board has taken sufficient action to close 6 of the 10 recommendations from our prior 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 Board's progress as part of our future FISMA audits.

Recommendations

Our report includes nine new recommendations designed to strengthen the Board's information security program in the areas of risk management, configuration management, identity and access management, information security continuous monitoring, and contingency planning. In its response to our draft, the Board concurs with our recommendations and notes that actions are underway to strengthen the Board's information security program. We will continue to monitor the Board'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 Board. Our specific audit objectives, based on the legislation's requirements, were to evaluate the effectiveness of the Board's (1) security controls and techniques for select information systems and (2) information security policies, procedures, and practices.

Background

FISMA requires each 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. The guidance notes that level 4 (*managed and measurable*) represents an effective level of security.

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

Recommendations, 2017-IT-B-018, October 31, 2017

2017 Audit of the Board's Information Security Program

Number	Recommendation	Responsible office
1	Ensure that a. an optimal governance structure for enterprise risk management is implemented that includes considerations for a Chief Risk Officer or equivalent function. b. an enterprise risk management strategy is used to maintain a risk profile for the Board.	Office of the Chief Operating Officer
2	Work with the Chief Information Officer to ensure that the agency's standard contracting language includes the Board's security assurance requirements for third parties, as necessary.	Division of Financial Management
3	Work with the Chief Information Officer to evaluate applicable contracts with third-party providers to determine whether additional amendments are needed to ensure that the necessary security assurance requirements are referenced.	Division of Financial Management
4	Ensure that the Board's enterprise architecture includes technologies managed by all divisions, and work with the Chief Operating Officer to enforce associated review processes agencywide.	Division of Information Technology
5	Develop and implement an agencywide identity, credential, and access management strategy that assesses current processes, provides a vision for the desired future state, and identifies plans to achieve that future state.	Division of Information Technology
6	Work with divisions to update the Board's *Suitability* policy to include requirements for assigning risk and sensitivity designations and associated investigative requirements to agency positions.	Office of Chief Operating Officer
7	Ensure that a. the agency's updated *Suitability* policy is implemented across the organization and divisions assign risk and sensitivity designations for their respective positions. b. investigations are conducted in accordance with the updated *Suitability* policy.	Management Division
8	Develop, implement, and regularly update an information security continuous monitoring strategy that includes performance measures to gauge the effectiveness of related processes and provides agencywide security status.	Division of Information Technology
9	Ensure that the results of the Board's business impact analysis are used to make updates to the contingency planning program, as appropriate.	Management Division

OIG

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 Peter Sheridan
Assistant Inspector General for Information Technology

SUBJECT: OIG Report 2017-IT-B-018: *2017 Audit of the Board'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 state that actions 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 Board personnel during our audit. Please contact me if you would like to discuss this report or any related issues.

cc: Raymond Romero, Deputy Director, Division of Information Technology
Charles Young, Deputy Associate Director, Division of Information Technology
Tina White, Manager, Compliance and Internal Control, Division of Financial Management

Distribution:
Donald V. Hammond, Chief Operating Officer, Office of the Chief Operating Officer
Ricardo Aguilera, Chief Financial Officer and Director, Division of Financial Management
Sharon Mowry, Chief Information Officer and Director, Division of Information Technology
Michell Clark, Director, Management Division

Contents

Introduction **6**

Objectives 6

Background 6

FISMA Maturity Model 7

Summary of Findings **9**

Analysis of the Board's Progress in Implementing Key FISMA and DHS Information Security Program Requirements **12**

Identify 12

Risk Management 12

Protect 16

Configuration Management 16

Identity and Access Management 19

Security Training 22

Detect 25

Information Security Continuous Monitoring 25

Respond 27

Incident Response 27

Recover 31

Contingency Planning 31

Appendix A: Scope and Methodology **33**

Appendix B: Management's Response **34**

Abbreviations **35**

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 Board of Governors of the Federal Reserve System's (Board) (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 fall into 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 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

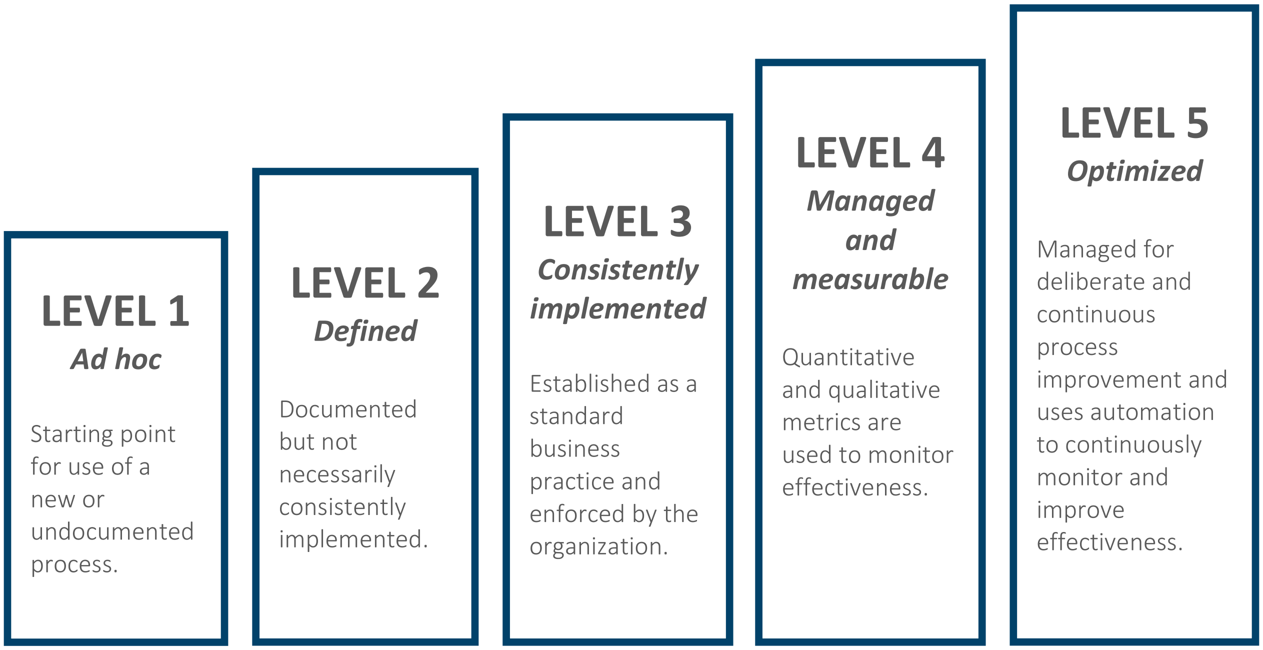
FISMA requires that IGs assess the effectiveness of information security controls that support the operations and assets of their respective agency. To that end, the Council of the Inspectors General on Integrity and Efficiency, in coordination with the Office of Management and Budget (OMB), DHS, and 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



LEVEL 1 ***Ad hoc***
Starting point for use of a new or undocumented process.

LEVEL 2 ***Defined***
Documented but not necessarily consistently implemented.

LEVEL 3 ***Consistently implemented***
Established as a standard business practice and enforced by the organization.

LEVEL 4 ***Managed and measurable***
Quantitative and qualitative metrics are used to monitor effectiveness.

LEVEL 5 ***Optimized***
Managed for deliberate and continuous process improvement and uses automation to continuously monitor and improve effectiveness.

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 Board'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 Board has enhanced its configuration management practices to more effectively detect unauthorized hardware and software on its network. It has also implemented an effective security training program that includes phishing exercises and associated performance metrics.

As highlighted in table 2 below, the Board has further opportunities to ensure its information security program is effective in FISMA domains across all five Cybersecurity Framework security functions: *identify, protect, detect, respond,* and *recover*. Our report includes nine recommendations in these areas. A consistent theme we noted is that the lack of an agencywide risk management governance structure and strategy, as well as the decentralization of information technology (IT) services, results in an incomplete view of the risks affecting the security posture of the Board and impedes the Board's ability to implement an effective information security program. Although the Board's CIO is responsible for developing and implementing the agency's information security program, several security processes, such as those for configuration management and information security continuous monitoring (ISCM), have not been effectively implemented agencywide.

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

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

Cybersecurity function area and associated FISMA domain	Maturity rating	Opportunities for improvement
Identify		
Risk management	Level 2: *defined*	- Implement an agencywide risk management governance structure and strategy. - Ensure that information security requirements are included in the procurement process for third parties.
Protect		
Configuration management	Level 3: *consistently implemented*	- Ensure that the Board's enterprise architecture includes technologies managed by all divisions and that associated review processes are enforced.
Identity and access management	Level 3: *consistently implemented*	- Develop and implement an identity, credential, and access management strategy and update the organization's suitability policy to account for risk designations for agency positions.
Security training	Level 4: *managed and measurable*	- Assess the knowledge, skills, and abilities of the agency's cybersecurity workforce.
Detect		
Information security continuous monitoring	Level 3: *consistently implemented*	- Develop and implement an ISCM strategy that includes performance measures to gauge the effectiveness of related processes and provides agencywide security status.
Respond		
Incident response	Level 3: *consistently implemented*	- Strengthen incident response policies, procedures, and standards.
Recover		
Contingency planning	Level 3: *consistently implemented*	- Incorporate the results of the business impact analysis to mature the agency's contingency planning program.

Source: OIG analysis.

In addition, the Board has taken sufficient action to close 6 of the 10 recommendations from our prior FISMA audits that remained open at the start of this audit. The closed recommendations relate to risk management, identify and access management, security training, ISCM, and incident response. We are leaving open 4 recommendations from our 2016 FISMA audit for the Board: (1) to strengthen insider threat activities by incorporating considerations for all types of sensitive information maintained by the Board into an agencywide insider threat program; (2) to implement multifactor authentication for nonprivileged users; (3) to update the incident handling standard; and (4) to develop and implement a plan to transition the external network to a Trusted Internet Connection service provider, as well as use the services offered by DHS's EINSTEIN program. Efforts to address these recommendations are underway, and we will continue to monitor the Board's progress in these areas as part of our future FISMA audits.

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

The Board's overall information security program is operating at a level-3 (*consistently implemented*) maturity. Although the agency has strengthened its program since our 2016 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. OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, provides guidance for implementing an ERM capability and governance structure that is coordinated with strategic planning and internal control processes.[5]

As part of the ERM governance structure, OMB Memorandum M-17-25, *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,* requires that agencies designate a senior accountable official for risk management. This official is responsible for (1) ensuring that risk management processes are aligned with strategic, operational, and budgetary planning processes and (2) reporting to DHS and OMB on risk management decisions and the agency's

[5] Although OMB Circular A-123 is not directly applicable to the Board, other agencies, such as nonexecutive agencies, are encouraged to adopt the circular.

plan to implement the NIST Cybersecurity Framework. In addition to a governance structure, the development of an agencywide risk context is a key component of ERM. Other key components of ERM include defining risk appetite and risk tolerance levels, a risk management strategy, and a risk profile (table 3).

Table 3. Key Components of ERM

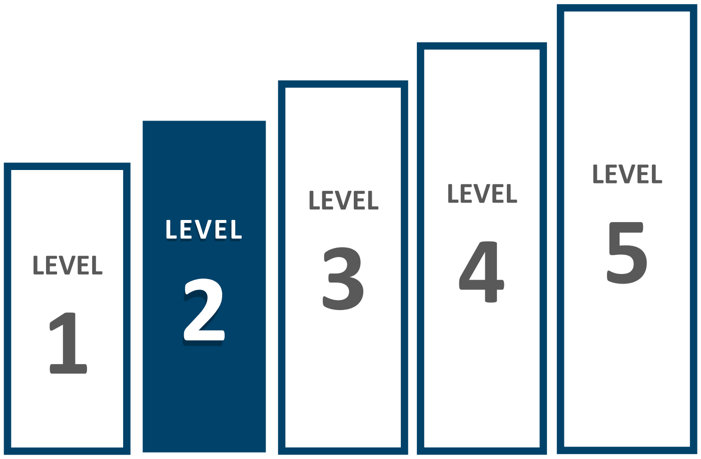
ERM component	Description
Risk context	An initial component of risk management that describes how an organization frames risk. Establishing the risk context includes defining the organization's risk tolerance and appetite levels.
Risk appetite	The broad-based amount of risk an organization is willing 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 Board's risk management program is operating at level 2 (*defined*), with the agency performing several activities indicative of a higher maturity level. For instance, the Board has consistently implemented its policies and procedures for categorizing information and information systems, conducting information system risk assessments, implementing its tailored security control baseline, and reviewing plans of action and milestones (POA&Ms), which are all associated with a level-3 maturity. In addition, the Board has enhanced its risk management process by incorporating its enterprise IT risks into its

Figure 2. Risk Management, Level 2 (*Defined*)



Source: OIG analysis.

automated workflow tool, which is used to assess information system risks. The Board has also designated the Chief Operating Officer (COO) as the senior accountable official for risk management.

Our 2016 FISMA report includes a recommendation to improve the Board's information system risk management processes. Specifically, we recommended that the CIO strengthen oversight processes to ensure that all Board systems, as appropriate, have a current authorization to operate that is based on comprehensive selection, implementation, and assessment of security controls.[6] This year, we found that the Board's Information Security Officer had taken steps to improve its the Board's oversight processes as it worked through the current controls testing cycle. Based on the systems we sampled, we verified that those steps sufficiently addressed our recommendation. As such, we are closing this recommendation and will continue to monitor the Board's work in this area as a part of future audits.

Our 2016 FISMA report also includes a recommendation for the CIO to work with the COO to perform a risk assessment to determine which aspects of an insider threat program are applicable to the types of information maintained by the Board. This year, we found that a draft strategy had been created but not finalized. Further, Board officials informed us that the agency is prioritizing updates to its suitability program and processes. Once completed, the updated suitability program should better inform the development of an insider threat strategy. Therefore, we are leaving this recommendation open and will continue to monitor the Board's progress in this area as part of our future audit activities.

Opportunities for Improvement

The Board's CIO has implemented an enterprise IT risk management program based on NIST SP 800-39 that addresses IT risks at the enterprise, business process, and information system levels. However, we found that the Board has not defined the key components of an ERM program, including an optimal governance structure, organizationally defined risk management strategy, risk appetite, risk tolerance, and risk profile. The Board has delegated the responsibility for the development of an ERM program to Office of the Chief Financial Officer and has also designated a senior agency official accountable for risk management. However, the Board has not determined how the agency will fulfill the function of a Chief Risk Officer, who would coordinate the implementation of the agency's risk management strategy, per OMB Circular A-123. Board officials informed us that the agency is evaluating options for how best to execute the responsibilities of a Chief Risk Officer within the agency's current organizational environment.

We understand that the Office of the Chief Financial Officer is working to develop an ERM framework, which will include inputs from several ongoing work streams, including those related to insider threats and the Board's suitability policy. We believe that developing an agencywide risk management strategy and optimal governance structure will enable the Board to better evaluate the combined effects of risks as an interrelated portfolio and to effectively prioritize resource allocations to meet the Board's mission.

Further, the Board can improve its risk management processes for third-party providers. Although the Division of Information Technology (Division of IT) has defined security assurance requirements for third parties to be included in contracts, we found that several of these requirements were not specifically referenced in three sampled IT service contracts. We believe that these omissions resulted from two primary reasons. First, the Board's standard solicitation, offer, and award (SOA) contracting language

[6] Office of Inspector General, *2016 Audit of the Board's Information Security Program*, OIG Report 2016-IT-B-013, November 10, 2016.

does not individually specify many of the Division of IT's security requirements defined for third parties. Instead, the SOA largely contains high-level statements for general compliance with FISMA and the Board's information security program. Second, there are inconsistencies between the SOA and the Board's security assurance requirements for third parties. For example, the Board's *Third Party Risk Management Standard* notes that a security assessment of the third party's security program will be completed by the Board's IT Security Compliance group. However, the SOA states that a review of the security program is required only if security artifacts presented by the third party do not meet the Board's standards. As such, contracts may be entered into that do not give the Board the proper authority to enforce its security assurance requirements for third parties.

Recommendations

We recommend that the COO

1. Ensure that

   a. an optimal governance structure for ERM is implemented that includes considerations for a Chief Risk Officer or equivalent function.

   b. an ERM strategy is used to maintain a risk profile for the Board.

We recommend that the Chief Financial Officer

2. Work with the CIO to ensure that the agency's standard contracting language includes the Board's security assurance requirements for third parties, as necessary.

3. Work with the CIO to evaluate applicable contracts with third-party providers to determine whether additional amendments are needed to ensure that the necessary security assurance requirements are referenced.

Management's Response

In its response to our draft report, Board management concurs with our recommendations and notes that POA&Ms will be established to detail the steps the Board will take to address our recommendations.

OIG Comment

We plan to follow up on the steps outlined in the Board's POA&Ms to ensure that the recommendations are fully addressed.

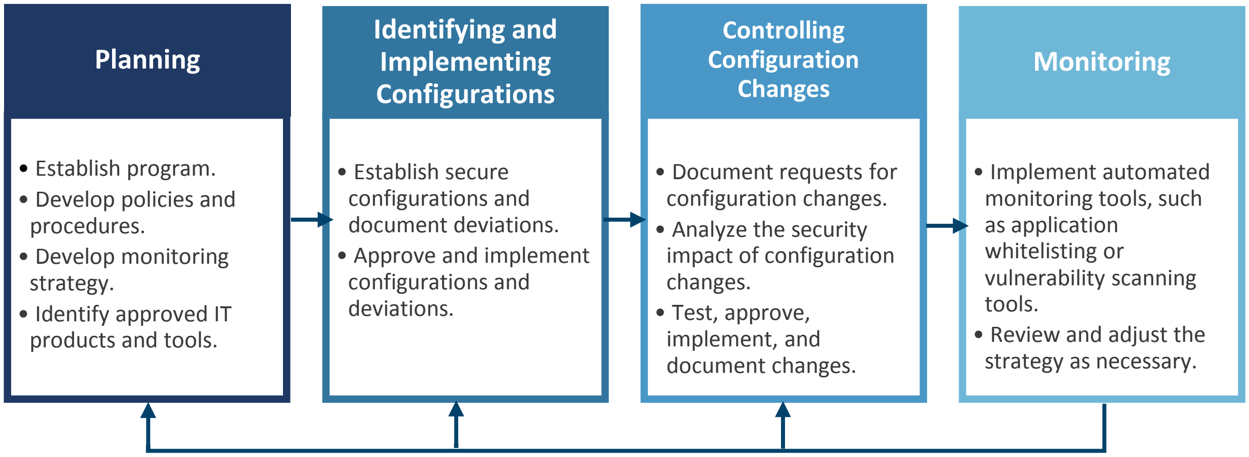
Protect

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



Planning
- Establish program.
- Develop policies and procedures.
- Develop monitoring strategy.
- Identify approved IT products and tools.

Identifying and Implementing Configurations
- Establish secure configurations and document deviations.
- Approve and implement configurations and deviations.

Controlling Configuration Changes
- Document requests for configuration changes.
- Analyze the security impact of configuration changes.
- Test, approve, implement, and document changes.

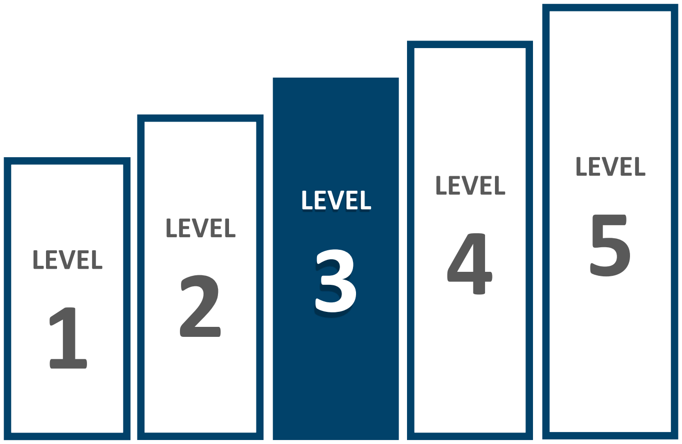
Monitoring
- Implement automated monitoring tools, such as application whitelisting or vulnerability scanning tools.
- Review and adjust the strategy as necessary.

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 notes that organizations are encouraged to implement baseline configurations in a centralized and automated manner using configuration management tools, scripts, or vendor-provided mechanisms. Further, NIST SP 800-128 states that organizations should review configuration changes for consistency with an organizational enterprise architecture.

Current Security Posture

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



Source: OIG analysis.

The Board'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 Board employs network access controls and application whitelisting to detect unauthorized hardware and software on the network, which are associated with a level-4 maturity. In addition, the Board is working to centralize its vulnerability remediation process within its security incident and event management (SIEM) tool, which is used to monitor the status of vulnerability remediation as well as correlate vulnerabilities, among other things. Further, the Board uses system configuration management tools to automatically enforce and redeploy configuration settings at regular intervals, which is associated with a level-5 maturity.

Our 2015 FISMA report includes a recommendation to the CIO to strengthen the Board's software asset management processes by using automation to provide greater visibility into authorized and unauthorized software across the organization.[7] In 2016, we found that the Board had the capability to produce a point-in-time inventory of its hardware and software; however, the process was not automated. This year, we found that the Board has implemented an automated application whitelisting tool that allows the agency to identify authorized and unauthorized software on the network and take appropriate action. The tool monitors software on the network and integrates with the agency's SIEM product. As such, we are closing this recommendation. However, as detailed below, we have identified further opportunities to strengthen configuration monitoring across the Board.

Opportunities for Improvement

We found opportunities to mature the Board's configuration monitoring processes through greater centralization and automation. Specifically, the Board's SIEM tool and application whitelisting tool do not fully cover all components of Board's network. One Board division maintains its own SIEM tool to secure its systems and network. The vulnerability remediation information from this division's SIEM tool is not fully integrated within the agency's SIEM tool. Similarly, the Board's application whitelisting tool does not cover this division because the tool is deployed through the agencywide SIEM tool. As a result, the Information Security Officer does not have a readily available view of the vulnerability remediation status or security configurations for all information system components connected to the Board's network.

[7] Office of Inspector General, *2015 Audit of the Board's Information Security Program*, OIG Report 2015-IT-B-019, November 13, 2015.

We believe there are two key reasons for these issues. First, the Board does not have a comprehensive enterprise architecture and associated review processes that are enforced agencywide.[8] Specifically, in accordance with best practices, the Division of IT has developed an architecture for the technologies it manages. However, the architecture is specific to the technologies managed by the Division of IT. Further, the Division of IT has established an Architecture Review Board to ensure that technologies introduced to the Board's environment are in line with the agency's security standards and do not threaten the integrity of infrastructure components. However, not all divisions consult with the Architecture Review Board before implementing technologies that they have purchased.[9]

Recommendation

We recommend that the CIO

4. Ensure that the Board's enterprise architecture includes technologies managed by all divisions, and work with the COO to enforce associated review processes agencywide.

Management's Response

In its response to our draft report, Board management concurs with our recommendation and notes that a POA&M will be established to detail the steps the Board will take to address our recommendation.

OIG Comment

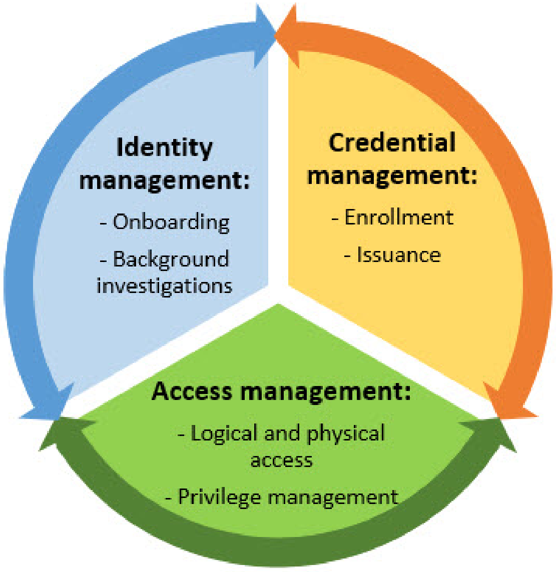
We plan to follow up on the steps outlined in the Board's POA&M to ensure that the recommendation is fully addressed.

[8] An enterprise architecture aligns business and technology resources to the mission or business function they support and helps agencies eliminate waste and duplication. An enterprise architecture describes the baseline architecture, target architecture, and a transition plan to achieve the target architecture.

[9] The Board's *Delegations of Administrative Authority*, dated December 20, 2013, outlines the delegation of administrative responsibilities, including those for IT management. The Board's delegation of authority provides divisions the autonomy to maintain information security associated with the data and computer facilities under their control in accordance with policies established by the CIO.

Identity and Access Management

Figure 5. ICAM Conceptual Design



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

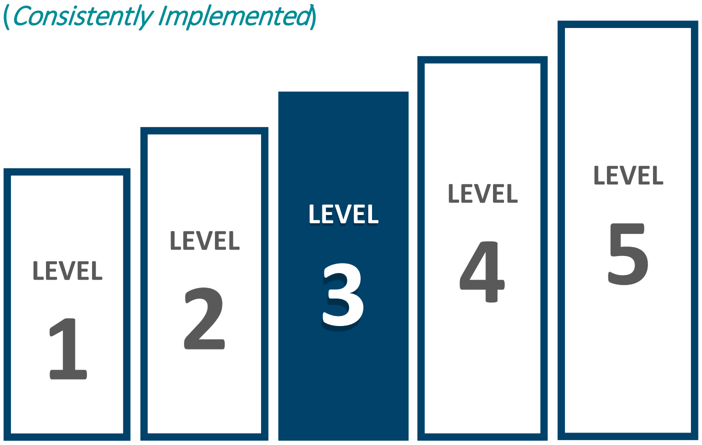
Identity and access management includes implementing a set of capabilities to ensure that users authenticate to IT resources and have access to only those resources that are required for their job function, a concept referred to as *need to know*. Supporting activities include onboarding and personnel screening, 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).

Effective identity and access management is a key control area for managing the risk from insider threats, and FISMA requires agencies to implement controls to preserve authorized restrictions on access and disclosure. A key component of effective identity and access management is developing a comprehensive strategy that outlines the components of the agency's ICAM program within the business functions that they support. The CIO Council has published the *Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance* to present the government with a common framework and implementation guidance to plan and execute ICAM programs. The guidance highlights several interrelated activities and use cases that should be considered when developing an ICAM strategy, including (1) an agency's specific ICAM challenges in their current state, (2) the desired method for completing the ICAM function, and (3) the gaps that exists between the as-is and target states.

The Board's information security policies and procedures cover multiple ICAM functions throughout the life cycle of a user's digital identity. For example, the Board conducts background investigations to determine an individual's suitability to be employed in certain positions or to obtain access to certain types of information. The scope of a background investigation depends on the nature of an individual's work and the degree to which that work affects the security and effectiveness of Board operations. Further, users with access to the Board's network and data are required to read, understand, and agree to the agency's permissible use policy and rules of behavior as a part of their annual security awareness training. Individuals that are granted access to classified information are required to sign a nondisclosure agreement.

Current Security Posture

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



Source: OIG analysis.

The Board's ICAM program is operating at level 3 (*consistently implemented*), with the agency performing several activities indicative of a higher maturity level. For instance, the Board has implemented multifactor authentication through the use of personal identity verification (PIV) cards for all privileged users on its network. The Board is also working toward fully integrating its PIV-based multifactor solution with its enterprise single sign-on capability for agency systems. Further, the Board has automated several of its ICAM processes for provisioning, managing, and reviewing privileged user accounts and has taken steps to strengthen access controls over sensitive information maintained by the organization.

Our 2016 FISMA audit report includes a recommendation for the Board to strengthen its ICAM program. Specifically, we recommended that the CIO work with Board divisions and the Federal Reserve Banks, as appropriate, to develop and implement a continuous monitoring approach for ensuring that sensitive Board information maintained in the agency's and the Federal Reserve System's enterprisewide collaboration environments is appropriately restricted.[10] In response, the Board's Division of IT has implemented several regularly scheduled scripts to monitor user access to sensitive data within the Board's collaboration environment and has begun to pilot a digital rights management solution to encrypt sensitive data downloaded from the environment in order to prevent users from maliciously or unintentionally sharing the data with unauthorized individuals. Our testing identified improvement in access controls for sensitive Board information on both the Board's and the Federal Reserve System's collaboration environments. As such, we are closing our 2016 recommendation.

Our 2016 FISMA audit report also includes a recommendation for the CIO to develop and implement an identity and access management plan that includes a risk-based determination on how multifactor authentication will be implemented for nonprivileged users of the Board's internal IT resources. This year, we found that although the Board has made multifactor authentication available as an option for nonprivileged users, this policy cannot yet be fully implemented due to compatibility issues with some systems. However, the agency has defined a plan to require multifactor authentication for all users. Therefore, we are leaving this recommendation open, and we will continue to monitor the Board's progress in this area as part of our future audit activities.

[10] Office of Inspector General, *2016 Audit of the Board's Information Security Program*, OIG Report 2016-IT-B-013, November 10, 2016.

Opportunities for Improvement

At the enterprise level, the Board improved the effectiveness and automation associated with several ICAM processes, including mandating the use of PIV credentials for privileged users. However, these activities were not guided by an enterprisewide ICAM strategy. Elements of an ICAM strategy include an assessment of the current state of activities as presently performed, a vision for the desired target state, and a plan to bridge any gaps between the two. The Board's ICAM program cuts across numerous offices, programs, and systems across the agency. As a result, some components of the program are directed and managed outside the Division of IT. Board officials have stated that although they do not currently have a formal enterprisewide ICAM strategy, they have developed plans for specific ICAM activities, such as multifactor authentication, that should begin execution this year. We believe that the development and implementation of an enterprisewide ICAM strategy will further integrate the Board's activities and ensure that the agency's sensitive information is appropriately protected.

We found that for a sample of 35 Board users with privileged access to the agency's systems and network, about 65 percent of those users were (1) not granted security clearances, (2) screened in accordance with the Board's lowest sensitivity designation, or (3) not required to sign nondisclosure agreements. NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, notes that agencies must assign risk designations to all organizational positions and establish screening criteria for individuals filling those positions, in accordance with guidance from the Office of Personnel Management. Further, title 5, *Code of Federal Regulations*, part 731, notes that agency heads are required to designate every covered position in the agency at a *high*, *moderate*, or *low* risk level as determined by the position's potential for adverse effect to the efficiency or integrity of the service. All positions subject to investigation must also receive a sensitivity designation of Special-Sensitive, Critical-Sensitive, or Noncritical-Sensitive, when appropriate. This sensitivity designation complements the risk designation and may have an effect on the position's investigative requirement.[11]

A key reason for these identity management weaknesses is that although sensitivity designations have been assigned to each position in the organization, the Board's *Suitability* policy does not address the assignment of risk designations to Board positions. Further, Board officials informed us that each division is responsible for considering and communicating risk designations and additional screening requirements for its respective positions.

We realize that the Board is performing a detailed review of its *Suitability* policy. As part of this review, the Board is benchmarking with other federal financial regulators to determine the best approach for implementing position risk designations. We believe that the use of both risk and data sensitivity designations to guide the personnel screening of individuals at the Board will better inform and mitigate the agency's risk of insider threats.

[11] While title 5, *Code of Federal Regulations*, part 731, does not apply to the Board, it does offer practices that can be considered in addition to guidance from NIST and the Office of Personnel Management with respect to position risk designations and screening criteria.

Recommendations

We recommend that the CIO

5. Develop and implement an agencywide ICAM strategy that assesses current processes, provides a vision for the desired future state, and identifies plans to achieve that future state.

We recommend that the COO

6. Work with divisions to update the Board's *Suitability* policy to include requirements for assigning risk and sensitivity designations and associated investigative requirements to agency positions.

We recommend that the Director of the Management Division

7. Ensure that

    a. the agency's updated *Suitability* policy is implemented across the organization and divisions assign risk and sensitivity designations for their respective positions.

    b. investigations are conducted in accordance with the updated *Suitability* policy.

Management's Response

In its response to our draft report, Board management concurs with our recommendations and notes that POA&Ms will be established to detail the steps the Board will take to address our recommendations.

OIG Comment

We plan to follow up on the steps outlined in the Board's POA&Ms to ensure that the recommendations are fully addressed.

Security Training

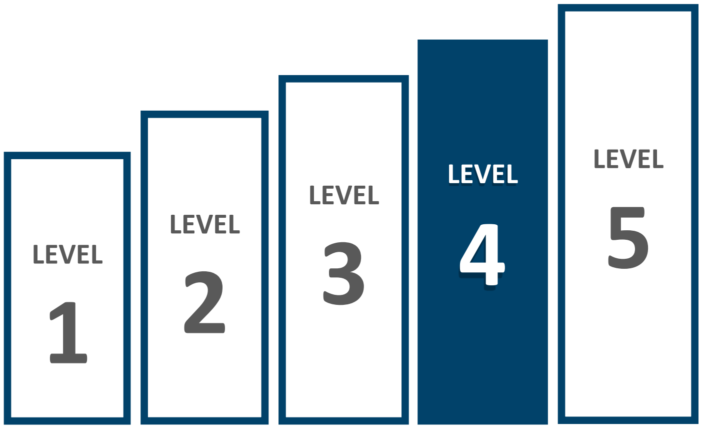
FISMA requires agencies to develop an information security program that provides security awareness training to personnel, including contractors, that support the operations and assets of the organization, as well as role-based training for individuals with significant information security responsibilities. 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. As such, a robust, enterprisewide security awareness and training program is paramount to ensuring that people understand their IT security responsibilities, organizational policies, and how to properly use and protect the IT resources entrusted to them.

In accordance with FISMA requirements, the Board's information security program notes that all employees and contractors with access to agency information systems must receive security awareness training before being permitted access to the Board network and each year thereafter. The program also requires that role-based training be provided for individuals with significant security responsibilities and that records of awareness and role-based training be maintained.

Current Security Posture

The Board's security awareness and training program is effective and operating at level 4 (*managed and measurable*). For instance, the Board includes a variety of topics in its annual awareness training, including phishing, malware, mobile device security, and security incident reporting. The Board has also established a validation and follow-up process to ensure that all information system users complete annual security awareness training. Further, the Board conducts ongoing security awareness activities for its workforce throughout the year.

Figure 7. Security Training, Level 4 (*Managed and Measurable*)



Source: OIG analysis.

Our 2016 FISMA report includes a recommendation for the Board to develop and implement a plan to periodically evaluate the effectiveness of the agency's security awareness and training program. Specifically, we noted that the Board had not conducted social engineering and phishing exercises to measure the effectiveness of its security and privacy training programs in 2016.[12] This year, the Board developed a plan to conduct periodic phishing exercises. Further, it conducted a phishing exercise that was targeted to all the agency's users and continues to track metrics on the effectiveness of the exercise. The Board has also implemented a new email tool for users to more efficiently report suspicious emails. As such, we are closing our 2016 recommendation. However, we suggest that the Board evaluate options to tailor its phishing exercises based on job function and the user's role in the organization. We believe this will provide additional information on the effectiveness of the agency's security awareness and training program.

Opportunities for Improvement

Although the Board provides specialized security training to Board staff with significant security responsibilities, it has not established a process for assessing the knowledge, skills, and abilities of its workforce holding cybersecurity-related positions. The Federal Cybersecurity Workforce Assessment Act of 2015 requires federal agencies to conduct and report to Congress a baseline assessment of their existing workforce, identifying (1) the percentage of staff with IT, cybersecurity, or cyber-related functions who currently hold appropriate industry-recognized certifications; (2) the level of preparedness of staff without credentials to take certification exams; and (3) a strategy for mitigating any gaps identified with appropriate training and certification for existing staff.

We believe that a key reason the Board has not established such a process is the decentralized nature of its IT security workforce. As such, not all individuals performing cybersecurity responsibilities report to the CIO or the Information Security Officer. As a result, the Board may not be able to identify knowledge

[12] Office of Inspector General, *2016 Audit of the Board's Information Security Program,* OIG Report 2016-IT-B-013, November 10, 2016.

gaps for individuals with significant security responsibilities and provide additional security awareness and training, as needed.

To help implement the requirements in the Federal Cybersecurity Workforce Assessment Act of 2015, NIST published the *National Initiative for Cybersecurity Education Cybersecurity Workforce Framework* in August 2017. The framework provides a resource to support a workforce capable of meeting an organization's cybersecurity needs. Per 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 this year, and we will continue to monitor the Board's progress in implementing the Federal Cybersecurity Workforce Assessment Act of 2015 and the *National Initiative for Cybersecurity Education Cybersecurity Workforce Framework.*

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). SP 800-137 notes that a key component of an effective ISCM program is a comprehensive 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.

NIST SP 800-137 emphasizes that an ISCM strategy is meaningful only within the context of broader organizational needs, objectives, or strategies, and as part of a broader risk management strategy. Once a strategy is defined, NIST SP 800-137 notes that the next step in establishing an effective ISCM program is to establish and collect security-related metrics to support risk-based decisionmaking throughout the organization. An ISCM strategy is periodically reviewed to ensure that it sufficiently supports the organization in operating within acceptable risk tolerance levels, metrics remain relevant, and data are current and complete.

Current Security Posture

The Board's ISCM program is operating at level 3 (*consistently implemented*), with the agency performing several activities indicative of a higher maturity level. The Board has consistently implemented its processes for performing ongoing security control assessments, granting system authorizations, and monitoring security controls to provide a view of the organizational security posture. The Board has also developed and implemented a *Continuous Monitoring Standard* that outlines the key components of its ISCM program at the system level. Further, the Division of IT has established a security dashboard that captures metrics on IT security operations. These metrics are related to incident response activities, phishing exercises, user activity, web traffic, and data loss prevention.

Figure 8. ISCM, Level 3 (*Consistently Implemented*)

LEVEL 1
LEVEL 2
LEVEL 3
LEVEL 4
LEVEL 5

Source: OIG analysis.

Opportunities for Improvement

Although the Board captures several ISCM-related operational metrics at the information system level, it has not defined metrics that indicate the effectiveness of all ISCM processes and the security status across the agency. We believe that this is due to two key contributing factors. First, the Board has not developed an agencywide ISCM strategy that defines specific metrics to gauge the security status of the enterprise. Second, as noted in the risk management section above, the Board has not developed an ERM strategy and defined an organizational risk tolerance and risk appetite level. As noted earlier, an ISCM strategy is meaningful only within the context of broader organizational needs, objectives, or strategies, and as part of a broader risk management strategy. We recognize that the Board is in the planning phase of establishing an ERM strategy and supporting governance structure. We believe that integrating an ISCM strategy with the ongoing efforts to develop an ERM program will enable the Board to have a greater understanding of its security posture and whether it is operating within its organizational risk tolerance.

Recommendation

We recommend that the CIO

8. Develop, implement, and regularly update an ISCM strategy that includes performance measures to gauge the effectiveness of related processes and provides agencywide security status.

Management's Response

In its response to our draft report, Board management concurs with our recommendation and notes that a POA&M will be established to detail the steps the Board will take to address our recommendation.

OIG Comment

We plan to follow up on the steps outlined in the Board's POA&M to ensure that the recommendation is fully addressed.

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*, 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). It further notes that establishing an incident response capability should include creating an incident response policy and plan; developing procedures for performing incident handling and reporting; and establishing relationships and lines of communications between the incident response team and other groups, both internal and external to the agency.

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.
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.
Postincident activity	Capture lessons learned to improve security measures and the incident response process.

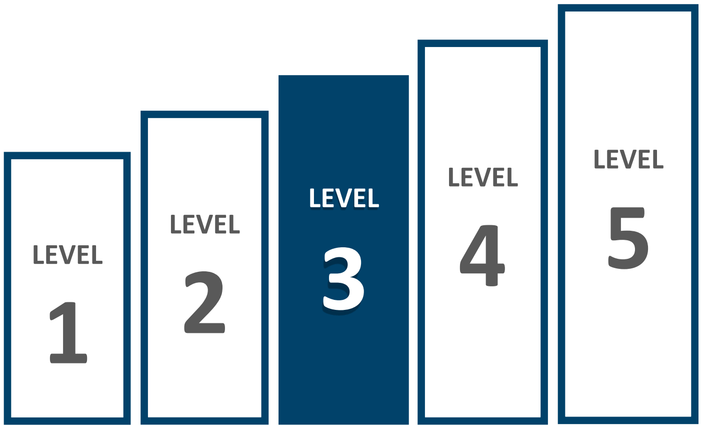
Source: NIST Special Publication 800-61, Revision 2, *Computer Security Incident Handling Guide.*

The Board's *Information Security Incident Handling Standard* documents the procedures for addressing the detection, response, and reporting of information security incidents related to Board data and resources. The procedures include scope, roles and responsibilities, incident notification and escalation tasks, external reporting requirements, and a threat vector taxonomy. The Board also uses the services of the National Incident Response Team, which is an IT service provider for the Federal Reserve System that administers intrusion detection, incident response, and security intelligence services.

Current Security Posture

The Board's incident response program is operating at level 3 (*consistently implemented*), with the agency performing several activities which are indicative of a level-4 maturity. For instance, the Board analyzes qualitative and quantitative performance measures on the effectiveness of its incident response processes. It has also assigned responsibility for monitoring and tracking the effectiveness of incident response activities. Further, it uses a governmentwide intrusion prevention capability to detect malicious traffic.

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



Source: OIG analysis.

Our 2016 FISMA audit report includes four recommendations for the Board to strengthen its incident response program. We are closing two of the four recommendations and will continue to monitor the Board's efforts to transition its external network to a Trusted Internet Connections service provider and update its *Information Security Incident Handling Standard*, as part of our future FISMA audits (table 5).

Table 5. Status of 2016 FISMA Audit Recommendations Related to Incident Response

Recommendation	Status
Update the Board's *Information Security Incident Handling Standard* to include considerations for handling major incidents and work with appropriate parties to ensure that the escalation procedures outlined in the Federal Reserve System's incident handling guide for Board information is updated accordingly.	Open. The Board is finalizing its revised *Information Security Incident Handling Standard*. As such, we are keeping this recommendation open and will continue to monitor the Board's efforts in this area.
Ensure that all lost laptop computers and mobile devices are reported consistent with guidance from the U.S. Computer Emergency Readiness Team.	Closed. U.S. Computer Emergency Readiness Team officials informed us that incidents should only be reported to them if there is a potential compromise to the confidentiality, integrity, or availability of federal data. They further noted that if compensating controls are in place, reporting to them is not necessary. We found that the Board has implemented encryption controls to mitigate the risk. As such, we are closing this recommendation.
Develop and implement a plan to (a) transition the Board's external network to a Trusted Internet Connections service provider, and (b) utilize the services offered by DHS's EINSTEIN program, as appropriate.	Open. The Board is in the process of entering into a contract with a Trusted Internet Connections service provider. We will continue to monitor the Board's efforts in this area.
Define and implement performance measures to gauge the effectiveness of the Board's incident response program, including services provided by the National Incident Response Team.	Closed. The Board is tracking performance measures from a variety of incident response processes, as well as performing trend analysis for incidents over time. Although we are closing this recommendation, we believe that additional metrics could be implemented to further mature the Board's incident response program.

Source: Office of Inspector General, *2016 Audit of the Board's Information Security Program,* OIG Report 2016-IT-B-013, November 10, 2016.

Opportunities for Improvement

The Board's *Information Security Incident Handling Standard* and supporting policies and procedures do not address incident containment, eradication, and recovery. We believe this resulted from the incident handling standard and supporting policies not being identified as a priority area requiring updates. As a result, the Board may not be able to effectively limit the impact of a security incident, gather and handle evidence, and restore affected systems to normal operations. As noted above, our 2016 FISMA audit includes a recommendation for the Board to update its *Information Security Incident Handling Standard*. As the Board is in the process of updating its standard, we suggest that considerations for incident containment, eradication, and recovery be included. We will follow up on the Board's efforts in this area as a part of our future FISMA audits.

The Board also has opportunities to mature its incident response performance measures to provide additional lessons learned. For example, the Board could benefit from additional performance measures to track whether it is becoming more effective in responding to similar incidents over time. Further, the Board could track the timeliness of incident reporting to external stakeholders, such as the U.S. Computer Emergency Readiness Team. DHS's *Federal Incident Notification Guidelines* note that agencies must report information security incidents in which the confidentially, integrity, and availability are potentially comprised within 1 hour of agency identification. As such, we suggest that the Board consider tracking additional performance metrics that highlight whether the agency is becoming more effective in responding to similar incidents and reporting to external parties in a timely manner.

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 impact of a cybersecurity event.

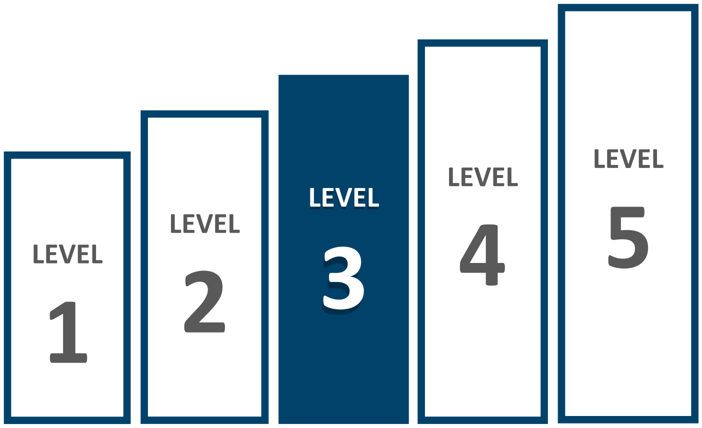
Contingency Planning

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 business impact analysis, 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 business impact analysis allows an organization to measure priorities and interdependencies (internal or external to the entity) by risk factors that could affect mission-essential functions.

Current Security Posture

The Board's contingency planning program is operating at level 3 (*consistently implemented*). We found that the Board conducts contingency plan testing to ensure that plans can be activated if needed. In addition, the Board has ensured that its backup site is configured with equivalent information security safeguards as its primary facility. Further, for a select system that we reviewed, contingency planning controls were effectively implemented to ensure availability of system functions and data. Finally, Board officials informed us that the agency is taking steps to coordinate its ERM and contingency planning efforts.

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



Source: OIG analysis.

Opportunities for Improvement

In October 2014, we issued an audit report on the Board's contingency planning and continuity of operations program.[13] As part of that report, we recommended that the Board's Management Division

[13] Office of Inspector General, *The Board Can Better Coordinate Its Contingency Planning and Continuity of Operations Program*, OIG Report 2014-IT-B-018, October 30, 2014.

perform a comprehensive business process analysis to identify and prioritize all the inputs and outputs that are necessary to perform the Board's mission-essential functions. In March 2017, we performed follow-up work on this recommendation and found that the Board had completed a business process analysis and was in the process of performing a business impact analysis. A business process analysis identifies and prioritizes the inputs and outputs necessary to perform mission-essential functions and is typically conducted before a business impact analysis. At the conclusion of our fieldwork, we noted that the business impact analysis has not been finalized. A key reason for this is that the Board's Management Division had prioritized the development of the business process analysis, as well as the agency's devolution and reconstitution plans.[14] As a result, the Board may not have an accurate picture of the recovery priorities of its mission-essential functions and systems.

Recommendation

We recommend that the Director of the Management Division

9. Ensure that the results of the Board's business impact analysis are used to make updates to the contingency planning program, as appropriate.

Management's Response

In its response to our draft report, Board management concurs with our recommendation and notes that a POA&M will be established to detail the steps the Board will take to address our recommendation.

OIG Comment

We plan to follow up on the steps outlined in the Board's POA&M to ensure that the recommendation is fully addressed.

[14] A devolution plan includes procedures to transfer authority and responsibilities from an organization's primary operating staff and facilities to another designated staff and one or more facilities for the purpose of sustaining essential functions. A reconstitution plan outlines the process by which surviving or replacement personnel resume normal operations.

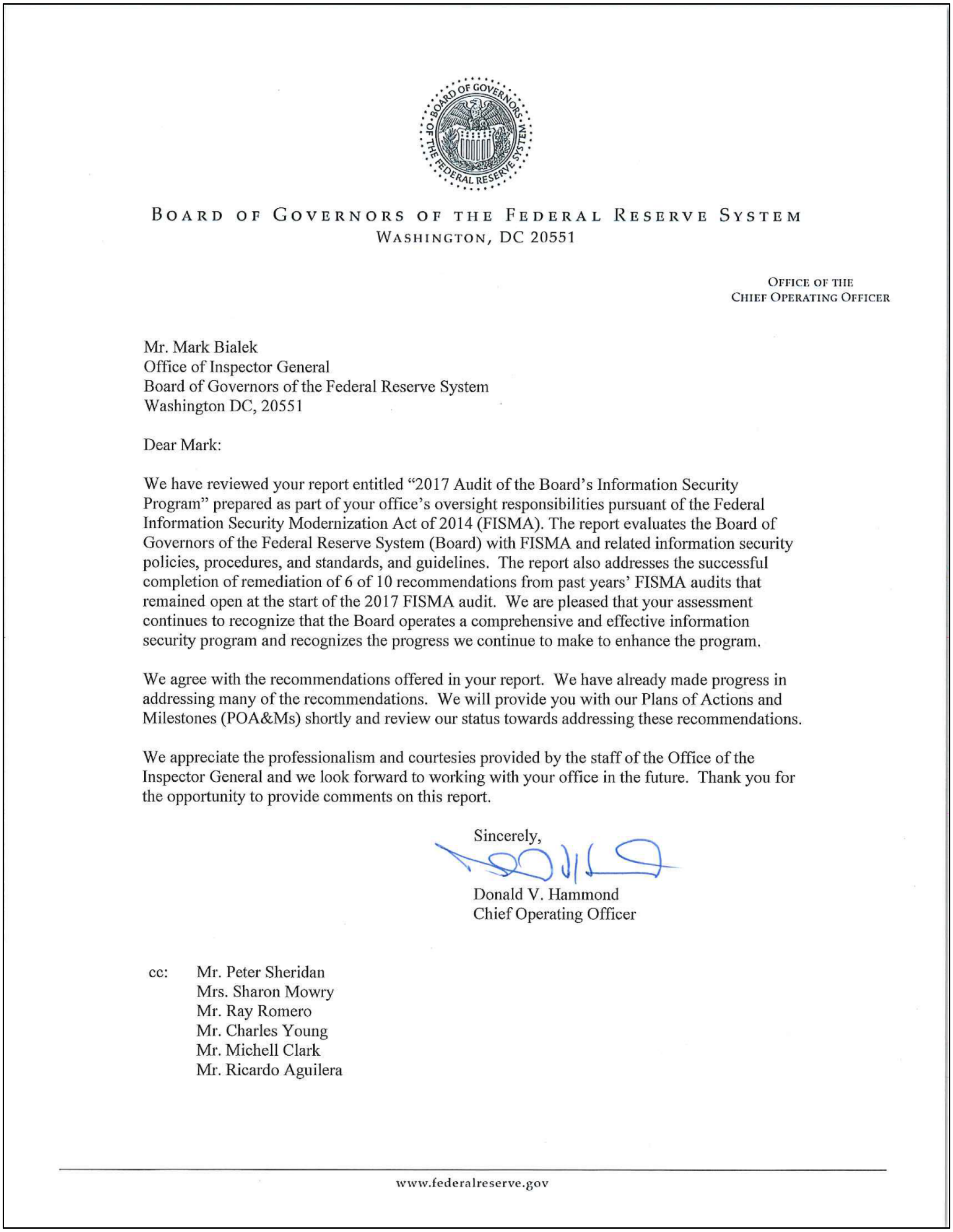
Appendix A: Scope and Methodology

Our specific audit objectives, based on FISMA requirements, were to evaluate the effectiveness of the Board'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 Board'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 Board's information security program, we interviewed Board 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 a select agency system.

To rate the maturity of the Board's information security program and functional areas, we used the scoring methodology defined in DHS's *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*. The maturity ratings are determined by a simple majority, where the most frequent level (that is, the mode) across the metrics serves as the overall rating.

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



BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
WASHINGTON, DC 20551

OFFICE OF THE
CHIEF OPERATING OFFICER

Mr. Mark Bialek
Office of Inspector General
Board of Governors of the Federal Reserve System
Washington DC, 20551

Dear Mark:

We have reviewed your report entitled "2017 Audit of the Board's Information Security Program" prepared as part of your office's oversight responsibilities pursuant of the Federal Information Security Modernization Act of 2014 (FISMA). The report evaluates the Board of Governors of the Federal Reserve System (Board) with FISMA and related information security policies, procedures, and standards, and guidelines. The report also addresses the successful completion of remediation of 6 of 10 recommendations from past years' FISMA audits that remained open at the start of the 2017 FISMA audit. We are pleased that your assessment continues to recognize that the Board operates a comprehensive and effective information security program and recognizes the progress we continue to make to enhance the program.

We agree with the recommendations offered in your report. We have already made progress in addressing many of the recommendations. We will provide you with our Plans of Actions and Milestones (POA&Ms) shortly and review our status towards addressing these recommendations.

We appreciate the professionalism and courtesies provided by the staff of the Office of the Inspector General and we look forward to working with your office in the future. Thank you for the opportunity to provide comments on this report.

Sincerely,

Donald V. Hammond
Chief Operating Officer

cc: Mr. Peter Sheridan
Mrs. Sharon Mowry
Mr. Ray Romero
Mr. Charles Young
Mr. Michell Clark
Mr. Ricardo Aguilera

Abbreviations

Board	Board of Governors of the Federal Reserve System
CIO	Chief Information Officer
COO	Chief Operating Officer
Cybersecurity Framework	Framework for Improving Critical Infrastructure Cybersecurity
DHS	U.S. Department of Homeland Security
Division of IT	Division of Information Technology
ERM	enterprise risk management
FISMA	Federal Information Security Modernization Act of 2014
ICAM	identity, credential, and access management
IG	Inspector General
ISCM	information security continuous monitoring
IT	information technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIV	personal identity verification
POA&M	plan of action and milestones
SIEM	security incident and event management
SOA	solicitation, offer, and award
SP 800-39	Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*
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*

Report Contributors

Khalid Hasan, Senior OIG Manager
Paul Vaclavik, OIG Manager
Joshua Dieckert, Senior IT Auditor
Morgan Fletcher, IT Auditor
Nick Gallegos, IT Auditor
Rebecca Kenyon, IT Auditor
Chelsea Willis, IT Auditor
Sean Carney, 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

OIG

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