OFFICE OF INSPECTOR GENERAL

Audit Report 2014-IT-B-021

Opportunities Exist to Improve the Operational Efficiency and Effectiveness of the Board's Information Security Life Cycle

December 18, 2014

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
CONSUMER FINANCIAL PROTECTION BUREAU

Report Contributors

Andrew Gibson, Project Lead
Morgan Fletcher, IT Audit Intern
Peter Sheridan, Senior OIG Manager for Information Technology Audits
Andrew Patchan Jr., Associate Inspector General for Information Technology

Abbreviations

A-130	Office of Management and Budget Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000
ATO	authorization to operate
BISP	*Board Information Security Program*
Board	Board of Governors of the Federal Reserve System
CIO	Chief Information Officer
FISMA	Federal Information Security Management Act of 2002
ISCM	information security continuous monitoring
ISCU	IT Security Compliance Unit
ISO	Information Security Officer
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
RMF	risk management framework
SP 800-37	NIST Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
SP 800-53	NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
SP 800-137	NIST Special Publication 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*
SSP	system security plan

Executive Summary:

Opportunities Exist to Improve the Operational Efficiency and Effectiveness of the Board's Information Security Life Cycle

2014-IT-B-021 December 18, 2014

Purpose

Our objectives for this audit were (1) to assess the processes the Board of Governors of the Federal Reserve System (Board) employs to meet Federal Information Security Management Act of 2002 (FISMA) requirements for security categorization, certification and testing, security plans, and accreditation of its information systems and (2) to review how the Board compiles its FISMA documents and review activities within its automated workflow support tool. In addition, we analyzed the Board's recently adopted risk management framework (RMF) document against National Institute of Standards and Technology (NIST) guidance.

Background

Information security life cycle refers to prescribed activities that must be performed for each Board information system throughout the various stages of the system's creation and existence. The Board has developed a FISMA-compliant approach to managing and evaluating a Board information system throughout its entire life cycle. Information security life cycle tasks begin early in the system development life cycle and shape the security capabilities of the information system. The Board manages its information security program through a collection of policies and procedures and supporting appendixes called the *Board Information Security Program*.

Findings

Overall, we found that the Chief Information Officer (CIO) maintains a FISMA-compliant information security program that is consistent with requirements for certification and accreditation established by NIST and OMB; however, we identified opportunities to improve the operational efficiency and effectiveness of the Board's management of its information security life cycle. First, we found that elements of the Board's information security life cycle were missing for some systems. Additionally, we found that the Information Security Officer developed a program to implement the requirements of NIST's RMF and issued the *Risk Management Program and Risk Assessment Standard* document in June 2014. The document, however, is not intended to include all of the recommended NIST requirements. Some of the processes are documented in the *Board Information Security Program* appendixes, but the appendixes have not been updated to reflect the new RMF process as well as new NIST guidance. Without up-to-date guidance, individuals responsible for managing Board systems may be unaware of their roles and responsibilities.

Recommendations

Our report contains three recommendations that are designed to improve the operational efficiency and effectiveness of the Board's information security life cycle process. We recommend that the Chief Information Officer (CIO) evaluate the automated workflow tool and determine any improvements needed to ensure it can meet documentation requirements of the Board's information security life cycle processes. We also recommend that the CIO ensure that system owners develop and input the security documentation for all Board-owned and -operated systems into the automated workflow tool. Finally, we recommend that the CIO perform a thorough reconciliation between the existing policy documents and the new *Risk Management Program and Risk Assessment Standard* to determine which processes remain relevant and update the applicable policy documents.

The Director of the Division of Information Technology stated that she agrees with the recommendations and that the division will take action to address the recommendations. We plan to follow up on the division's actions to ensure that the recommendations are fully addressed.

Summary of Recommendations, OIG Report No. 2014-IT-B-021

Rec. no.	Report page no.	Recommendation	Responsible office
1	5	Evaluate the automated workflow tool and determine any improvements needed to ensure it can meet documentation requirements of the Board's information security life cycle processes.	Division of Information Technology
2	5	Ensure that system owners develop and input the security documentation for all Board-owned and -operated systems into the automated workflow tool.	Division of Information Technology
3	7	Perform a thorough reconciliation between the existing policy documents and the new *Risk Management Program and Risk Assessment Standard* to determine which processes remain relevant and update the applicable policy documents.	Division of Information Technology

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

CONSUMER FINANCIAL PROTECTION BUREAU

December 18, 2014

MEMORANDUM

TO: Sharon Mowry
Chief Information Officer and Director, Division of Information Technology
Board of Governors of the Federal Reserve System

FROM: Andrew Patchan Jr.
Associate Inspector General for Information Technology

SUBJECT: OIG Report No. 2014-IT-B-021: *Opportunities Exist to Improve the Operational Efficiency and Effectiveness of the Board's Information Security Life Cycle*

The Office of Inspector General has completed its report on the subject audit. We conducted this audit to assess the Board of Governors of the Federal Reserve System's (Board) processes to meet Federal Information Security Management Act of 2002 (FISMA) requirements for security categorization, certification and testing, security plans, and accreditation of its information systems. In addition, we reviewed how the Board compiles its FISMA documents and review activities within the online commercial-off-the-shelf tool. Lastly, we analyzed the Board's recently adopted risk management framework document against National Institute of Standards and Technology guidance.

We provided a draft of our report for review and comment. In your response, you outlined actions that will be taken to address our recommendations. We have included your response as appendix C to our report.

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

cc: Donald Hammond, Chief Operating Officer
Raymond Romero, Chief Privacy Officer
Charles Young, Information Security Officer
William Mitchell, Chief Financial Officer
J. Anthony Ogden, Deputy Inspector General
Matthew Simber, OIG Manager for Policy, Planning, and Quality Assurance

Contents

Introduction

Objectives

Our objectives for this audit were (1) to assess the Board of Governors of the Federal Reserve System's (Board) processes to meet Federal Information Security Management Act of 2002 (FISMA) requirements for security categorization, certification and testing, security plans, and accreditation of its information systems and (2) to review how the Board compiles its FISMA documents and review activities within its automated workflow support tool. In addition, we analyzed the Board's recently adopted risk management framework (RMF) document against National Institute of Standards and Technology (NIST) guidance. Appendix A provides details on our scope and methodology.

Background

FISMA requires organizations to develop and implement an organization-wide information security program for the information and information systems that support the operations and assets of the organization, including those provided or managed by another organization, contractor, or other source. For non-national-security programs and information systems, agencies must follow NIST standards and guidelines.

The Board has developed and implemented an organization-wide information security program that is documented in the *Board Information Security Program* (BISP). This document outlines the purpose, scope, and key objectives of the Board's information security program and describes the principles and practices the Board uses to secure information. The BISP is a collection of policies and procedures and supporting appendixes that provides guidance on each phase of a system's information security life cycle.

Early guidance on the information security life cycle came from Office of Management and Budget (OMB) Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000 (A-130), which established a minimum set of controls to be included in federal automated information security programs and assigns federal agency responsibilities for the security of automated information, along with the requirement for certification and accreditation.

In 2010, NIST Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (SP 800-37) transformed the traditional certification and accreditation process into the six-step RMF. The revised process emphasizes the following:

1. building information security capabilities into federal information systems through the application of management, operational, and technical security controls

2. maintaining awareness of the security state of information systems on an ongoing basis though enhanced monitoring processes

3. providing essential information to senior leaders to facilitate decisions regarding the acceptance of risk to organizational operations and assets, individuals, other organizations, and the nation arising from the operation and use of information systems

SP 800-37 incorporates the traditional processes that the Board uses to authorize its information systems but expands the concept of risk management and promotes the NIST RMF. NIST's RMF outlines steps of the information security life cycle as follows:

RMF step 1—categorize information system
RMF step 2—select security controls
RMF step 3—implement security controls
RMF step 4—assess security controls
RMF step 5—authorize information system
RMF step 6—monitor security controls

In September 2011, NIST issued Special Publication 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* (SP 800-137). SP 800-137 ties continuous monitoring into the NIST RMF with a target audience of individuals with implementation and operational responsibilities for mission/business processes, system development and integration, system and/or security management oversight, security control assessment and monitoring, and security.

Appendix B provides a list of additional guidance applicable for this review. The list is not intended to be all encompassing but rather to highlight the laws, regulations, and guidance that are current and relevant to this process.

Finding 1: Elements of the Board's Information Security Life Cycle Were Missing for Some Systems

Overall, we found that the Chief Information Officer (CIO) maintains a FISMA-compliant information security program that is consistent with requirements for certification and accreditation established by NIST and OMB; however, we identified some systems that lacked documentation for authorizations to operate (ATOs), some system security plans (SSPs) that lacked recommended elements of NIST, and some information systems that did not receive a security assessment. Additionally, we identified that the IT Security Compliance Unit (ISCU) uses multiple repositories to manage security documentation. Inconsistent documentation of ATOs, SSPs, and security assessments indicates the potential for noncompliance with federal regulations and poses information security risks.

ATOs for Some Systems Are Not Documented

We found that 4 of the 53 systems selected for review did not have a documented ATO either in hard copy or in electronic form in the automated workflow support tool. Additionally, we found that 4 systems with a documented ATO in the automated workflow tool were approved by someone other than the documented authorizing official.

NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (SP 800-53), requires that organizations assign a senior-level executive or manager as the authorizing official for the information system and ensure that the authorizing official authorizes the information system for operation before the system is implemented. By authorizing an information system, an agency official accepts responsibility for the security of the system and is fully accountable for any adverse impacts to the agency if a breach of security occurs.

We believe that the varied use of hard copy and electronic form, as well as the use of multiple repositories to house the ATO documentation as discussed below, contributed to these inconsistencies. The Information Security Officer (ISO) stated that until the next version of the workflow tool becomes available, the Board will have to continue to maintain both hard copy and electronic ATOs. A single view of the ATOs will help the ISO monitor the authorization state of all systems.

SSPs Lacked Recommended Elements

We found that 10 of the 53 systems we reviewed had SSPs that lacked documentation on the authorization boundaries, and 11 of the 53 systems lacked system environments documentation. Furthermore, we found that the SSP template in the automated workflow tool did not include SP 800-53 requirements for the inclusion of system interconnections.

SP 800-53 requires that organizations develop a security plan for the information system that explicitly defines the authorization boundary for the system, describes the operational context of

the information system in terms of missions and business processes, and describes the operational environment for the information system and relationships with or connections to other information systems. Further, the BISP states that SSPs are developed for all information systems in order to fully describe the security environment of the information system.

ISCU staff stated that the exclusion of critical information in some SSPs is a result of lack of understanding by system owners and managers of the requirements of certain fields within the automated workflow tool. Without fully documenting the system interconnections, authorization boundaries, and system environment, the authorizing official may be accepting undocumented risks.

Some Systems Did Not Receive a Security Assessment

We found that 4 of the 53 systems we reviewed did not undergo annual security testing. SP 800-53 requires organizations to develop a security assessment plan, assess the security controls in the information system and its environment of operation, and produce a security assessment report that documents the results of the assessment. ISCU staff stated that the security assessments were not completed due to other priority reviews.

The Board Maintains Multiple Repositories

Currently, ATOs and SSPs are maintained electronically in one of two repositories or in hard copy. The ISCU uses an automated workflow tool to manage the security documentation for Board information systems, and the Division of Banking Supervision and Regulation developed a separate internal compliance management tool that manages the security documentation for its systems and its Technology Portfolio Management function. The information security–related purpose of Technology Portfolio Management is to secure supervision and regulation information by coordinating, on a national basis, all BISP and other policy compliance requirements for the Division of Banking Supervision and Regulation's systems.

According to OMB Memorandum M-14-03, *Enhancing the Security of Federal Information Systems*, in order to fully implement information security continuous monitoring (ISCM) across the federal government, OMB recommends that agencies standardize the requirement to establish ISCM as an agency-wide solution by deploying enterprise ISCM products and services. Further, SP 800-137 recommends that organizations look for automated solutions to lower costs, enhance efficiency, and improve the reliability of monitoring security-related information.

During our audit, the Division of Banking Supervision and Regulation was exploring tools to replace its internally built compliance management tool, which is being phased out due to technical support issues. Additionally, during this audit the ISCU had upgraded its version of the automated workflow tool.

Recommendations

We recommend that the CIO

1. Evaluate the automated workflow tool and determine any improvements needed to ensure it can meet documentation requirements of the Board's information security life cycle processes.

2. Ensure that system owners develop and input the security documentation for all Board-owned and -operated systems into the automated workflow tool.

Management's Response

The Director of the Division of Information Technology stated that the Information Security Compliance Program is currently in the process of enhancing the automated compliance tool and plans to incorporate the areas for improvement defined in our report. Once the automated compliance tool is fully upgraded, the Board plans to use the system as the sole FISMA information system inventory and report generating tool.

OIG Comment

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

Finding 2: BISP Policies and Procedures Are Not Consistently Updated

We found that the ISO developed a program to implement the requirements of NIST's RMF and issued the *Risk Management Program and Risk Assessment Standard* document in June 2014. The document, however, is not intended to include all of the recommended NIST requirements. Some of the processes are documented in BISP appendixes, but the appendixes have not been updated to reflect the new RMF process as well as new NIST guidance. ISCU staff stated that IT policy updates, including to the BISP, occur every three years, but due to other priority compliance matters as well as limited staff, the BISP has not been updated. Without up-to-date guidance, individuals responsible for managing Board systems may be unaware of their roles and responsibilities.

BISP Policies Have Not Been Updated to Reflect All Components of the New RMF

As previously noted, SP 800-37 transformed the traditional certification and accreditation process into the six-step RMF. SP 800-37 outlines risk management tasks that begin early in the system development life cycle and are important in shaping the security capabilities of the information system. If these tasks are not adequately performed during the initiation, development, and acquisition phases of the system development life cycle, the tasks will, by necessity, be undertaken later in the life cycle and be more costly to implement.

To bring the Board's program into compliance with NIST guidance, the ISO has developed and finalized the *Risk Management Program and Risk Assessment Standard*, which covers the enterprise, business, and information system level risks. This document is not intended to include all recommended NIST requirements and relies on previously established components of the BISP; however, these appendixes and templates have not been updated to reflect the changes in the new standard.

For example, the Board's *Appendix H—Certification & Accreditation Standard* addresses several SP 800-37–recommended tasks included in the Board's RMF, such as common control identification, security control implementation, assessment preparation, and ongoing control assessments; however, this appendix also includes processes of the prior certification and accreditation program. Because the *Risk Management Program and Risk Assessment Standard* was issued without concurrent full updates of the BISP policy document and its appendixes, system owners may follow outdated procedures.

In addition to issuing the *Risk Management Program and Risk Assessment Standard*, the ISO has started transitioning some BISP processes from appendixes and templates to standalone documents. The ISO recently finalized several standalone procedure documents, including the *Inventory Standard*; however, the BISP policy document has not been updated since 2010. Appendix H was also last updated in 2010 to fully reflect the program changes, even though NIST subsequently issued additional guidance around the certification and accreditation

process. Without proper alignment with NIST guidance, individuals responsible for managing Board systems may be unaware of their roles and responsibilities. Further, the Board will not have assurance that its information systems will be appropriately managed throughout their life cycle, which could lead to security risks.

In 2014, NIST issued *Supplemental Guidance on Ongoing Authorizations*, which states that when an RMF has been effectively applied across an organization and the organization has effectively implemented a robust ISCM program, organizational officials, including authorizing officials, are provided with a view of the organizational security and risk posture, and each information system's contribution to that security and risk posture, on demand. Thus, organizational information systems may move from a static, point-in-time authorization process to a dynamic, near-real-time ongoing authorization process.

Without up-to-date guidance, individuals responsible for managing Board systems may be unaware of their roles and responsibilities, which could lead to noncompliance with federal regulations and limit the effectiveness of the authorization process. ISCU staff stated that information technology policies are updated every three years, but due to other priority compliance matters and staffing limitations, the BISP has not been updated.

Recommendation

We recommend that the CIO

3. Perform a thorough reconciliation between the existing policy documents and the new *Risk Management Program and Risk Assessment Standard* to determine which processes remain relevant and update the applicable policy documents.

Management's Response

The Director of the Division of Information Technology stated that for the 2015 FISMA program year, the ISCU plans on performing a reconciliation between existing policy documents and will look for opportunities to consolidate or provide further clarification to current policies and procedures.

OIG Comment

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

Appendix A
Scope and Methodology

To accomplish our audit objective, we obtained the Board's FISMA inventory and extracted the major systems and general support systems from the listing because Board systems with those categorizations have the most strenuous documentation requirements. Based on the Board's inventory as of April 2014, we selected a sample of 53 systems from the Board's FISMA inventory. We examined supporting documentation for the current FISMA inventory as well as security categorization, authorization, security plan, and certification and testing documentation from the 2013 FISMA reporting period for compliance with NIST and internal guidance.

We compared the Board's *Risk Management Program and Risk Assessment Standard* to the recommended tasks identified in SP 800-37.

For our final objective, we examined technical and user documentation associated with the Board's automated workflow tool to assess its functionality. Based on that inspection, we selected a limited sample of controls to test for compliance with SP 800-53.

We conducted our fieldwork from March 2014 to July 2014. 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 obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix B
Federal Guidance Applicable to the Security Life Cycle Issued Since 2010

Year	Federal guidance	Purpose
2010	NIST Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010	To provide guidelines for applying the RMF to federal information systems, to include conducting the activities of security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring.
2011	NIST Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011	To provide guidance for an integrated, organization-wide program for managing information security risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the nation resulting from the operation and use of federal information systems.
	NIST Special Publication 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations,* September 2011	To assist organizations in the development of an ISCM strategy and the implementation of an ISCM program that provides awareness of threats and vulnerabilities as well as visibility into organizational assets and the effectiveness of deployed security controls.
2013	NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* April 2013	To provide guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government to meet the requirements of Federal Information Processing Standards 200, *Minimum Security Requirements for Federal Information and Information Systems*. The guidelines apply to all components of an information system that processes, stores, or transmits federal information.
	OMB Memorandum 14-03, *Enhancing the Security of Federal Information Systems,* November 2013	To provide agencies with guidance for managing information security risk on a continuous basis and builds on efforts to achieve the cybersecurity cross-agency priority goal.
	OMB Memorandum 14-04, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, November 2013	To provide fiscal year 2013 FISMA metrics issued by the U.S. Department of Homeland Security, which establish minimum and target levels of performance for these priorities, as well as metrics for other key performance areas.
2014	NIST Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Supplemental Guidance on Ongoing Authorizations*, June 2014	To amplify current NIST guidance on security authorization and ongoing authorization contained in SP 800-37, SP 800-39, SP 800-53, SP 800-53A, and SP 800-137. This guidance does not change current OMB policies or NIST guidance with regard to risk management, information security, security categorization, security control selection, implementation, assessment, continuous monitoring, or security authorization.

Source: Compiled by the OIG from the NIST and OMB websites.

Appendix C
Management's Response

BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM
WASHINGTON, D. C. 20551

DIVISION OF
INFORMATION TECHNOLOGY

December 11, 2014

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 "Audit of the Board's Security Lifecycle" prepared as part of your office's oversight responsibilities pursuant to the Federal Information Security Management Act of 2002 (FISMA). The report evaluates the Board of Governors of the Federal Reserve System (Board) Security Lifecycle with the applicable FISMA and related information security policies, procedures, standards, and guidelines. We are pleased that your assessment recognized that the Board operates a comprehensive and effective information security lifecycle.

We agree with the three recommendations offered in your report. The Information Security Compliance Program is currently in the process of enhancing our automated compliance tool and plan to incorporate the areas for improvement defined in the report. Once the automated compliance tool is fully upgraded, we plan on using the system as the sole FISMA information system inventory and report generating tool. For the 2015 FISMA program year, the IT Security Compliance Unit plans on performing a reconciliation between existing policy documents and will look for opportunities to consolidate or provide further clarification to current policies and procedures. Overall, we view the findings identified as continuous improvement opportunities and will follow the suggestions for improvement. The Information Technology Division's Plan of Actions and Milestones will be updated to reflect these corrective actions.

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,

Sharon Mowry
Director, Information Technology

cc: Mr. Wayne Edmondson
Mr. Don Hammond
Mr. Andrew Patchan
Mr. Ray Romero
Mr. Charles Young

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
CONSUMER FINANCIAL PROTECTION BUREAU

HOTLINE

1-800-827-3340

OIGHotline@frb.gov

Report Fraud, Waste, and Abuse

Those suspecting possible wrongdoing may contact the OIG Hotline by mail, e-mail, fax, or telephone.

Office of Inspector General, c/o Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW, Mail Stop K-300, Washington, DC 20551
Attention: OIG Hotline

Fax: 202-973-5044

Questions about what to report?

Visit the OIG website at www.federalreserve.gov/oig
or
www.consumerfinance.gov/oig