Evaluation Report
2022-IT-B-006
March 23, 2022

Board of Governors of the Federal Reserve System

The Board Can Strengthen Inventory and Cybersecurity Life Cycle Processes for Cloud Systems

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

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

Executive Summary, 2022-IT-B-006, March 23, 2022

The Board Can Strengthen Inventory and Cybersecurity Life Cycle Processes for Cloud Systems

Findings

Overall, we found that the Board of Governors of the Federal Reserve System has established an information systems security life cycle that consists of several steps intended to ensure that cybersecurity risks for all systems, including those that are cloud based, are adequately managed. However, we found that the Board's security life cycle processes are not consistently implemented for select cloud systems across the agency.

Specifically, we found that while the Board has established the Cloud Resource Center to provide a central location for agency staff to obtain information on cloud policies and technologies in use, the inventory of cloud systems maintained by the Cloud Resource Center is incomplete. We also found that the Board had not developed a process to ensure that the Federal Risk and Authorization Management Program (FedRAMP) Project Management Office has an accurate inventory of the FedRAMP-approved systems used by the Board.

Further, we identified opportunities to ensure that the Board's cybersecurity life cycle processes are consistently implemented in the areas of assessment and authorization and monitoring for select cloud systems.

Recommendations

This report includes three recommendations designed to strengthen the Board's cloud system inventory and cybersecurity life cycle processes. In addition, we identified three matters for management consideration related to retroactive architectural reviews of early adopted cloud systems, obtaining awareness of cloud service providers' supply chain partners, and ensuring consistent tracking of costs for cloud computing systems. In its response to our draft report, the Board concurs with our recommendations and notes that the agency has made progress in addressing them. Further, the response states that the agency will provide plans of action and milestones to address our recommendations. We will continue to monitor the Board's progress in addressing these recommendations as part of future reviews.

Purpose

The Federal Information Security Modernization Act of 2014 requires that we perform an annual independent evaluation of the Board's information security program and practices, including testing the effectiveness of security controls for select information systems. Our specific objective was to evaluate the effectiveness of the Board's life cycle processes for ensuring that cybersecurity risks are adequately managed for cloud systems in use.

Background

The Board is increasingly using internet-based computing services (commonly referred to as *cloud services* or *cloud technologies*) to perform its mission and to meet its information technology needs. The Board has developed a cloud strategy that emphasizes solutions that support business capabilities and opportunities for the efficient execution of the Board's mission. Specifically, the strategy states that the Board seeks to embrace cloud services to create opportunities for people to be more productive; processes to be more flexible; and information to be accessed, integrated, and analyzed more effectively.

Recommendations, 2022-IT-B-006, March 23, 2022

The Board Can Strengthen Inventory and Cybersecurity Life Cycle Processes for Cloud Systems

Finding 1: The Board Can Strengthen Its Cloud Inventory Processes

Number	Recommendation	Responsible office
1	Ensure that the CRC's inventory of cloud projects in the configuration and production phases is comprehensive and periodically maintained.	Division of Information Technology
2	Develop and implement a process to ensure that the FedRAMP PMO has an accurate inventory of FedRAMP-approved cloud systems used by the Board.	Division of Information Technology

Finding 2: The Board Can Ensure That Specific Information Systems Security Life Cycle Processes Are Consistently Implemented for Cloud Systems

Number	Recommendation	Responsible office
3	Ensure that the Board's information security continuous monitoring standards and associated procedures provide consistent guidance on continuous monitoring frequencies and associated documentation review requirements for cloud service providers.	Division of Information Technology

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

MEMORANDUM

DATE: March 23, 2022

TO: Distribution List

FROM: Peter Sheridan
Associate Inspector General for Information Technology

SUBJECT: OIG Report 2022-IT-B-006: *The Board Can Strengthen Inventory and Cybersecurity Life Cycle Processes for Cloud Systems*

We have completed our report on the subject evaluation. We performed this evaluation pursuant to the requirements in the Federal Information Security Modernization Act of 2014 (FISMA). Specifically, FISMA requires that we conduct an annual independent evaluation of the Board of Governors of the Federal Reserve System's information security program, including testing controls for select systems. As part of our work, we tested the implementation of the Board's cybersecurity life cycle processes for four select cloud systems.

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 plans of action and milestones will be provided to address them. We have included your response as appendix B to our report.

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

cc: Raymond Romero
Charles Young
Tara Pelitere
Reginald Roach
Gregory Evans
Timothy Maas
Annie Martin
Rebecca Kenyon
Fran Horne
Ghada Ijam
Tammy Hornsby-Fink
Jill Maier

Glenn Eskow
Ricardo A. Aguilera
Cheryl Patterson
Donna Butler

Distribution:
Patrick J. McClanahan, Chief Operating Officer
Sharon Mowry, Chief Information Officer
Winona H. Varnon, Director, Division of Management
Matthew J. Eichner, Director, Division of Reserve Bank Operations and Payment Systems

Contents

Introduction

Objective

Our objective was to evaluate the effectiveness of the Board of Governors of the Federal Reserve System's life cycle processes for ensuring that cybersecurity risks are adequately managed for cloud systems in use. Our scope and methodology are detailed in appendix A.

Background

Federal agencies, including the Board, are increasingly using internet-based computing services (commonly referred to as *cloud services* or *cloud technologies*) to perform their missions and meet information technology (IT) needs. The National Institute of Standards and Technology (NIST) defines *cloud computing* as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. NIST defines three service models for cloud computing:

- Software as a Service (SaaS), wherein the consumer uses the provider's application, which is running on a cloud-based infrastructure
- Platform as a Service (PaaS), wherein the consumer-created content is deployed onto the cloud infrastructure using programming languages and tools supported by the cloud provider
- Infrastructure as a Service (Iaas), wherein the consumer can provision processing, storage, or networks and run software, such as operating systems and applications, while using the provider's underlying cloud infrastructure

Planning for the adoption of cloud technologies for federal agencies formally began in 2010 with the issuance of the Office of Management and Budget's *25 Point Implementation Plan to Reform Federal Information Technology Management*. This plan encourages federal agencies to default to cloud-based solutions whenever a secure, reliable, and cost-effective option exists to meet their IT needs.

In 2019, the Office of Management and Budget published the *2019 Federal Cloud Computing Strategy—Cloud Smart*. This new strategy provided agencies with guidance in the areas of cloud security, procurement, and workforce, with the goal of driving continued successful adoption of cloud services. In May 2021, the president issued Executive Order 14028, *Improving the Nation's Cybersecurity*, which requires, among other things, that the head of each agency update existing plans to prioritize resources for the adoption and use of cloud technologies.

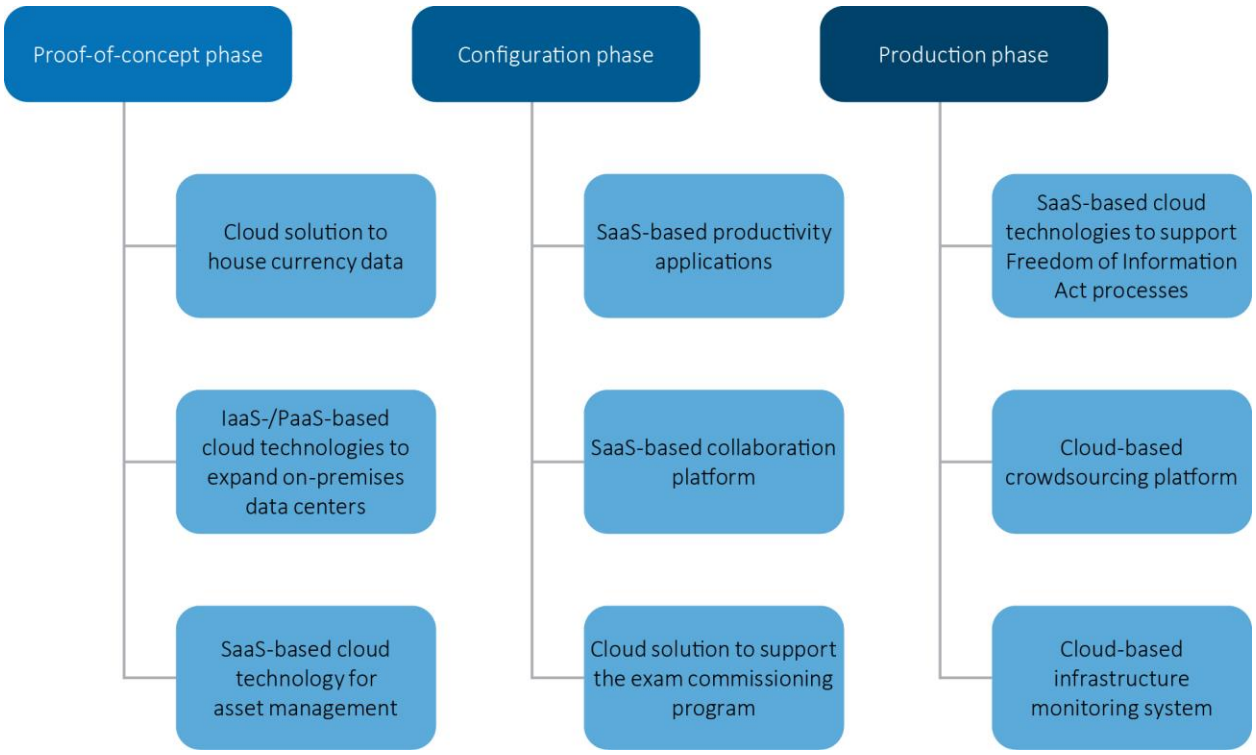
The Board's Cloud Computing Vision, Strategy, and Adoption

In accordance with governmentwide directives and priorities, in May 2020 the Board developed a cloud computing vision and strategy. The Board's cloud vision statement notes that the agency embraces cloud services to create opportunities for people to be more productive; processes to be more flexible; and information to be accessed, integrated, and analyzed more effectively. As part of its cloud strategy, the

Board is focusing on building and enabling existing platforms; meeting increasing infrastructure demands; and strengthening data integration, analytics, and sharing capabilities.

Although the Board's vision statement and strategy were formulated in 2020, agency divisions had already been using cloud-based technologies for several years. For example, one Board division had been using a time tracking, SaaS-based cloud solution, and another division had been using a PaaS-based technology to host a public-facing website. In addition, the Board is using several cloud-based technologies that are in the proof-of-concept, configuration, and production phases (figure 1).[1]

Figure 1. Examples of Cloud Technologies at the Board in the Proof-of-Concept, Configuration, and Production Phases



Source: OIG review of the Board's Cloud Resource Center project listing.

The Board's Cloud Governance Framework

IT governance generally refers to a formal framework by which organizations ensure that IT investments support business objectives. To ensure a consistent approach to adopting and managing risks with all technologies, the Board uses a policy and procedure–driven IT governance structure. Specifically, the Division of Information Technology established a cloud awareness and adoption area of focus group to establish and implement foundational elements of the Board's cloud strategy. This area of focus group established the Cloud Resource Center (CRC) within the Division of IT, which serves as a central repository

[1] Cloud technologies in the proof-of-concept phase are being evaluated for possible use, those in the configuration phase are being developed and tested prior to implementation, and those in the production phase have been authorized to operate.

for agency staff to obtain information and guidance about cloud initiatives, services, processes, and policies. The Division of IT has issued cloud policies, procedures, and guidance documents related to strategy, project life cycle, and security (table 1). These policies, procedures, and guidance documents cover areas such as identifying and evaluating cloud-based products, performing a proof of concept, and obtaining a formal authorization to operate a cloud-based system.

Table 1. Examples of Cloud Policies, Procedures, and Guidance Issued by the Division of IT

Area	Document	Description
Strategy	*Board Cloud Vision Statement and Strategy*	Provides the Board's vision statement and strategy, focus areas, and considerations
Project life cycle	*Cloud Decision Guide*	Assists in identifying the information and the decisions needed to select a cloud product that meets business needs and addresses legal, information security, records management, and financial considerations
	Requesting a Cloud Product Evaluation Procedure	Defines how business owners request an evaluation of a cloud technology and how those reviews are conducted
	Cloud Proof of Concept Best Practices Reference	Provides recommendations for how to plan, conduct, and document a proof of concept for a cloud technology
Security	*Cloud Security Authorization Policy*	Outlines the minimum requirements for cloud-based systems that store, transmit, or process Board data or information
	Cloud Application Authentication Policy	Defines the standards by which the Board manages authentication to its cloud applications

Source: OIG review of cloud policies, procedures, and guidance issued by the Division of IT.

In addition, the Board has defined roles and responsibilities for key individuals and oversight bodies that are responsible for ensuring that cloud systems align with the agency's strategy (table 2). A key oversight body is the Architecture Review Board (ARB), which consists of subject-matter experts who provide architectural risk assessments and guidance for all Board IT projects, including cloud-based systems. The ARB reviews requests for the use of cloud-based systems and determines whether they meet Board standards, including those related to information security. Based on its review, the ARB makes a recommendation to the Board's chief information officer (CIO) as to whether to implement a cloud system.

Table 2. Key Roles and Responsibilities in the Board's Cloud Governance Processes

Role/Group	Responsibilities
Business owner	Submits a cloud product evaluation request
Project team	Provides technical input from the business owner's perspective
ARB	Reviews a cloud evaluation request, determines whether it meets Board requirements, and recommends final approval
Records Management Program	Reviews the cloud product to determine whether it contains Board records; if so, determines whether the cloud product will meet the Board's electronic recordkeeping requirements
CIO	Reviews the ARB's recommendation and makes a final determination as to whether the cloud product will be approved for Board use
Business owner's approving officer	Gives final approval to use a cloud product

Source: OIG review of the Board's *Requesting a Cloud Product Evaluation Procedure*.

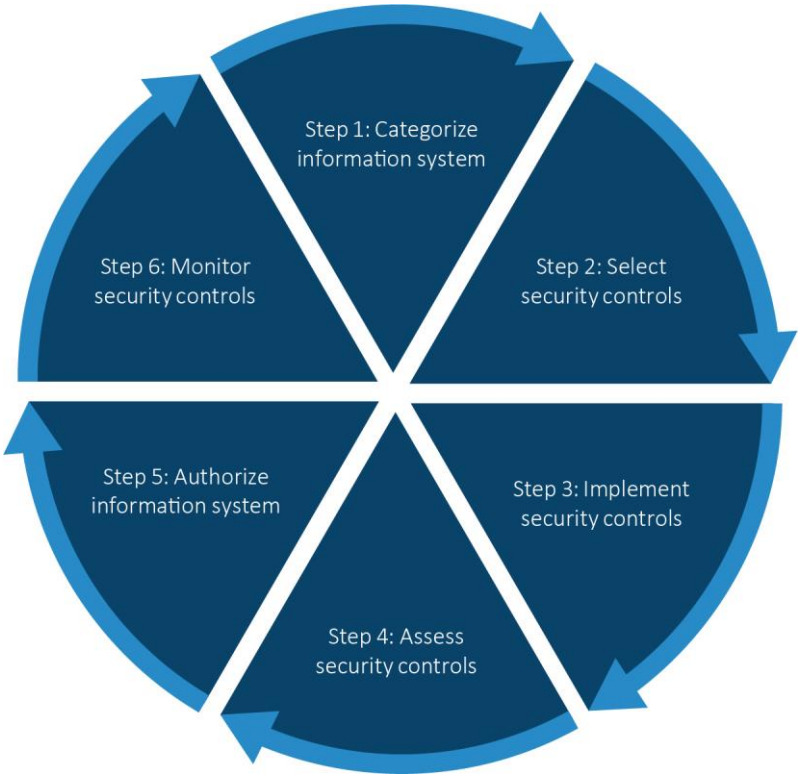
Once permission to use the cloud product is granted, the project team is required to follow Board processes to begin testing; to perform a security assessment; and, if Board data are to be used, to obtain an authorization to use in accordance with the *Board Information Security Program* (BISP).

The Board Information Security Program

In accordance with the Federal Information Security Modernization Act of 2014 (FISMA), the Board has developed an information security program that provides a framework to ensure the implementation of effective security controls over the information and information systems of the agency, including cloud-based systems. The BISP documents an information systems security life cycle that consists of certain activities that must be performed for each agency system throughout the various stages of the system's creation and existence. Based on NIST guidance,[2] the framework includes six steps that are designed to manage cybersecurity risks throughout a system's life cycle (figure 2).

[2] National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, Special Publication 800-37, Revision 2, December 20, 2018.

Figure 2. The Board's Information Systems Security Life Cycle Process



Source: OIG analysis of the BISP, version 3.1, June 2021.

The information security life cycle steps are as follows:

- Step 1: Categorize information system. The information system is assigned a security categorization or impact level of *low*, *moderate*, or *high*. This impact level is based on the information the system stores, processes, or generates.
- Step 2: Select security controls. The security control requirements are selected and documented in the information system security plan (SSP).
- Step 3: Implement security controls. The security controls specified in the SSP are implemented.
- Step 4: Assess security controls. The security controls documented in the SSP are assessed by the Information Security Compliance Unit (ISCU). The ISCU prepares a security assessment report documenting its findings and recommendations.
- Step 5: Authorize information system. As required by Board risk management standards, the information system owner presents the authorization package, which consists of the SSP, the risk assessment, the plan of action and milestones (POA&M), and the security assessment report to the authorizing official. The authorizing official determines whether the information system may go into or remain in production.
- Step 6: Monitor security controls. Selected security controls are monitored as part of the Board's continuous monitoring program.

.

Finding 1: The Board Can Strengthen Its Cloud Inventory Processes

We found that the Board can improve its cloud system inventory processes in two main areas. First, we noted that the inventory of cloud projects maintained by the CRC was incomplete. The Division of IT's *Requesting a Cloud Product Evaluation Procedure* states that a cloud product is to be added to the CRC's inventory once it is approved for use by the ARB and the CIO. We believe that this issue occurred because the Board has not performed a comprehensive review to determine the applicability of the agency's 2020 cloud inventory procedures and related guidance to cloud systems that were implemented prior to 2020. A complete inventory of cloud projects would help ensure that agency divisions are fully aware of existing cloud solutions that may meet their needs. Second, we found that the FedRAMP Marketplace inventory, which provides information on the cloud systems used by agencies across the government, did not include all cloud systems in use at the Board. Guidance from the Federal Risk and Authorization Management Program (FedRAMP) Project Management Office (PMO) states that agencies should provide the PMO with information on their use of FedRAMP systems so that the PMO can maintain an up-to-date marketplace inventory. The Board originally decided, based on security considerations, to not publicize the cloud systems it was using on the FedRAMP Marketplace. Ensuring that the PMO has a complete inventory of FedRAMP systems used by the Board would provide the agency with timely access to relevant security information.

The CRC Inventory Is Incomplete

We found that the Board CRC's inventory of cloud systems in the configuration and production phases was incomplete. Specifically, we found that one SaaS-based cloud system used for time tracking and another SaaS-based human resources system in the configuration phase were not included in CRC's inventory.

The CRC maintains an inventory of Board cloud projects that are in the proof-of-concept, purchasing, configuration, and production phases.[3] Board divisions can use this inventory to determine whether existing cloud solutions in use at the agency may meet their needs.

A key reason for these omissions is that the CRC issued guidance on its cloud inventory processes in 2020 and has not fully accounted for division cloud systems purchased prior to 2020. As noted in the CRC's *Board Cloud Decision Guide*, version 1.0, dated June 2020, divisions are required to review the CRC's inventory when evaluating new cloud projects to determine whether any already-implemented or already-evaluated solutions meet their needs and to identify any resource-sharing opportunities. In addition, the CRC's *Requesting a Cloud Product Evaluation Procedure*, version 1.0, dated June 2020, states

[3] The proof-of-concept and purchasing phases consist of evaluation, design, budgeting, and procurement activities. The configuration phase consists of development and testing activities. In the production phase, cloud systems are authorized to operate and implemented.

that once a cloud system is approved for use by the ARB and the CIO, it is then added to the CRC's inventory.

We believe that an accurate and complete CRC inventory could help limit duplication of effort and help identify cloud systems that could benefit multiple Board stakeholders.

The FedRAMP Marketplace Inventory Does Not Include All Board Cloud Systems

FedRAMP was established in 2011 to provide a cost-effective, risk-based approach for the adoption of cloud services by the federal government. The FedRAMP PMO maintains the FedRAMP Marketplace, which is a publicly available repository of systems that have been authorized for use across the federal government under the FedRAMP program. The PMO relies on the information in the marketplace to provide agencies with timely access to key security documentation for cloud service providers. We found that the FedRAMP Marketplace did not include all of the Board's FedRAMP-authorized systems. Specifically, we found that the Board did not notify the FedRAMP PMO of two of the agency-used, FedRAMP-approved cloud systems that we reviewed.[4]

The FedRAMP PMO requires agencies to provide it with authorization-to-operate letters when the agency begins using a FedRAMP-approved cloud system. The FedRAMP PMO uses this information to maintain the marketplace inventory and provide agencies with timely access to the FedRAMP authorization-to-operate package, continuous monitoring reports, and security incident information, among other things. When an agency is no longer using a FedRAMP-approved cloud technology, the agency is responsible for communicating this information to the PMO so that it can update the marketplace inventory.

Board officials stated that they initially decided to not provide this information to the PMO based on a legal determination that publicly advertising which systems the agency was using was not in keeping with the normal practice of the Board. The Board subsequently decided to begin collecting the necessary information to provide to the FedRAMP PMO; however, the agency has not formalized its processes in this area.

By ensuring that the FedRAMP PMO has an accurate inventory of the FedRAMP systems it is using, the Board will have more timely access to relevant security information that will allow for more effective continuous monitoring.

Recommendations

We recommend that the CIO

1. Ensure that the CRC's inventory of cloud projects in the configuration and production phases is comprehensive and periodically maintained.

[4] After the conclusion of our fieldwork, the Board added two of the systems we identified to the FedRAMP Marketplace inventory.

2. Develop and implement a process to ensure that the FedRAMP PMO has an accurate inventory of FedRAMP-approved cloud systems used by the Board.

Management Response

The CIO concurs with our recommendations and notes that POA&Ms will be established to detail the steps the Board will take to address the 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.

Finding 2: The Board Can Ensure That Specific Information Systems Security Life Cycle Processes Are Consistently Implemented for Cloud Systems

The Board has developed an information systems security life cycle, which consists of various activities that must be performed for each agency system throughout its creation and existence. We found that the Board can ensure that life cycle activities are consistently performed for cloud systems in the areas of assessment, authorization, and monitoring (steps 4–6 in table 3). A key reason for these issues is that although the Board finalized most of its governance processes for cloud-based solutions in 2020, it has not determined whether already-implemented cloud systems are compliant with these processes and its information systems security life cycle. By ensuring the consistent application of its information systems security life cycle processes, the Board will have greater assurance that cybersecurity risks are effectively managed for its cloud systems.

Table 3. The Board's Information Systems Security Life Cycle Process Steps and Identified Areas for Improvement

Information systems security life cycle step	Description	Improvement area
Step 1: Categorize information system	The information system is assigned a security categorization or impact level of *low*, *moderate*, or *high*.	We did not identify any areas for improvement.
Step 2: Select security controls	The security control requirements are selected and documented in the SSP.	We did not identify any areas for improvement.
Step 3: Implement security controls	The security controls specified in the SSP are implemented.	We did not identify any areas for improvement.
Step 4: Assess security controls	The security controls documented in the SSP are assessed by the ISCU.	The Board did not ensure that security assessments were performed for one of the four cloud systems we reviewed. After the conclusion of our fieldwork, the Board completed the security assessment for this system.
Step 5: Authorize information system	The authorizing official determines whether the information system may go into or remain in production based on the authorization package.	The Board did not ensure that one of the four cloud systems we reviewed was authorized to operate prior to being placed into production.

Information systems security life cycle step	Description	Improvement area
Step 6: Monitor security controls	Selected security controls are monitored as part of the Board's continuous monitoring program.	Continuous monitoring activities were inconsistently performed for two of the four cloud systems we reviewed. We also found that POA&Ms were inconsistently maintained for two of the four cloud systems we reviewed.

Source: BISP, version 3.1, June 2021, and OIG analysis.

The Security Assessment and Authorization Process Was Not Completed for One System We Reviewed

We found that the Board did not complete the security assessment and authorization process for one of the four cloud systems we reviewed. Specifically, this system did not have a security assessment performed, and the system retroactively received an authorization to use after it had been in production for several years.[5]

Once security controls are selected and implemented, the next steps in the information systems security life cycle involve the completion of a security assessment and the granting of an authorization to operate prior to the cloud system being placed into production.[6] As noted earlier, the BISP requires that all information systems (1) have a security assessment completed and (2) be authorized prior to being placed into production. In addition, the Board's February 2021 *Initiating a Cloud Project Procedure* states that until an authorization to use is granted, a team may not use Board information in a cloud product and may not connect the cloud product to any Board authentication or on-premises resources.

We believe that this issue arose because the system owner did not think the Board's information systems security life cycle processes were applicable to cloud systems implemented prior to 2020. Board officials informed us that at the time the cloud system was implemented, the officials believed that the Board's information systems security life cycle processes did not apply.

After the conclusion of our fieldwork, the Board completed a security assessment and authorization for the subject cloud system. As such, we are not making a formal recommendation in this area; we will continue to monitor the Board's efforts to strengthen the implementation of its information systems security life cycle as part of our future reviews. We believe that by ensuring that all cloud systems have a security assessment completed and are authorized prior to being placed in production, the Board will

[5] An *authorization to use* is granted to a team when the authorizing official has provided preliminary acceptance of the risk associated with using a cloud system for Board purposes.

[6] As noted in the BISP, as part of the security assessment, the controls documented in the SSP are assessed and the results serve as an input to the authorization decision. The *authorization decision* is management's official decision to accept the risk of operating the system based on an agreed-upon set of security controls.

have greater assurance that security controls have been implemented to reduce risks to an acceptable level.

Continuous Monitoring of Cloud Systems Was Not Consistently Performed

Once a system has been authorized to operate and placed into production, the next step in the Board's information systems security life cycle involves monitoring security controls to determine whether they continue to be effective over time. Key monitoring processes include change control, configuration management, vulnerability scanning, and annual FISMA testing by the ISCU. We identified two opportunities for improvement in continuous monitoring processes for the cloud systems we reviewed. First, we found that Board divisions were not maintaining an adequate level of situational awareness of cloud providers' risk environment, for example, by reviewing vendor-provided documentation. Second, we found that POA&Ms, which outline vulnerabilities and the tasks necessary to mitigate them, were not consistently maintained for two of the four systems we reviewed.

Cloud Service Providers' Continuous Monitoring Documentation Was Not Consistently Obtained and Reviewed

We found that Board divisions were not regularly obtaining and reviewing the required continuous monitoring documentation provided by the vendors for two of the four cloud systems we reviewed. Per contractual requirements, vendors make continuous monitoring documentation, such as POA&M items, vulnerability scans, security assessment reports, and system and organization controls reports, available to customers.[7] According to the Board's *Vendor Risk Management* standard, the contracting officer's representative is responsible for obtaining these documents and providing them to the information security and privacy compliance team on an annual basis. This team then works with the contracting officer's representative or the system owner to perform continuous monitoring of cloud providers.

We believe that a key cause for this issue is that the Board's *Continuous Monitoring Standard* does not provide specific guidance for cloud systems and associated providers on the types of documentation to review or the level or frequency of monitoring. Although the Board's *Vendor Risk Management Standard* provides additional continuous monitoring guidance that is applicable to all third-party systems at the Board, we believe that ensuring consistency between these two standards documents could provide additional clarity to system owners. Another reason for this issue is that, in our opinion, system owners were relying on the ISCU's annual testing of continuous monitoring controls rather than reviewing vendor-provided documentation at the time it was made available.

By ensuring that continuous monitoring documentation is obtained and reviewed in a timely manner, the Board will have additional assurance that changes in cloud service providers' risk environments are identified and adequately assessed.

[7] System and organization controls reports are intended to meet the needs of a broad range of users that need detailed information and assurance about the controls at a service organization relevant to the security, availability, and processing integrity of the systems the service organization uses to process users' data and the confidentiality and privacy of the information processed by these systems.

POA&Ms Were Not Consistently Maintained for Two Cloud Systems

We found that for one of the four cloud systems we reviewed, POA&M items were not created for vulnerabilities identified from continuous monitoring activities. Board officials informed us that this issue occurred because this system was in the process of getting a formal authorization to operate. For another cloud system we reviewed, we found that the security weaknesses identified as part of a security assessment were not included in a POA&M. Further, the POA&M created for this system was not included in the Board's FISMA compliance tool. This omission occurred because the system owner was following internal division procedures and not the Board's POA&M standard.

FISMA requires that agency information security programs include a process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the agency. In accordance with FISMA, the BISP requires system owners to maintain POA&Ms for all information systems in which an IT security weakness has been found and for which the risk will not be accepted. In addition, the *Board Plan of Actions and Milestones Standard* requires system security officials to maintain POA&Ms that address IT security weaknesses identified during continuous monitoring activities. Further, the standard requires system security officials to maintain POA&Ms in the agency's FISMA compliance tool.

After the conclusion of our fieldwork, the Board strengthened POA&M processes for the two systems we identified issues with. Specifically, the Board included the POA&M items for these two systems in the agency's FISMA compliance tool. As such, we are not making a formal recommendation in this area; we will continue to monitor the Board's efforts to strengthen the implementation of its information systems security life cycle as part of our future reviews. We believe that by ensuring that POA&Ms are maintained and included in the agency's FISMA compliance tool, the Board will have greater assurance that security vulnerabilities are being effectively managed and mitigated.

Recommendation

We recommend that the CIO

3. Ensure that the Board's information security continuous monitoring standards and associated procedures provide consistent guidance on continuous monitoring frequencies and associated documentation review requirements for cloud service providers.

Management Response

The CIO concurs with our recommendation and notes that POA&Ms will be established to detail the steps the Board will take to address the recommendation.

OIG Comment

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

Matters for Management Consideration

We identified three matters for management consideration related to (1) the application of ARB review processes to cloud systems implemented before the establishment of the CRC and the finalization of the Board's cloud policies and procedures, (2) the identification of third-party suppliers that are a component of cloud service providers' products and services and (3) the consistent use of accounting codes to track spending on cloud computing technologies throughout the Board. While we are not making formal recommendations in these areas, we will monitor the Board's progress to strengthen cloud governance and security processes as part of our future reviews.

Application of ARB Review Processes for Early-Adopted Cloud Systems

The ARB is a key oversight body that provides architectural risk assessments and guidance for all Board IT projects, including cloud-based systems. Specifically, the ARB reviews requests for the use of cloud-based systems and determines whether they meet Board standards, including those related to information security. In June 2020, the Division of IT issued *Requesting a Cloud Product Evaluation Procedure*, which requires formal ARB review and endorsement of cloud systems prior to implementation. Prior to the issuance of this procedure document, ARB approval was required only for applications deployed on the Board's IT infrastructure and not for cloud service providers.[8] Two of the four cloud systems we reviewed were implemented prior to June 2020, and as such, had not received a formal endorsement from the ARB.

As part of the ARB review process, areas such as business continuity and disaster recovery, data access, encryption, hosting provider and data location, and vendor financial stability are assessed.[9] While we recognize that these areas may have been assessed for the two cloud systems in our sample via other processes, we believe that the ARB's review of cloud systems implemented prior to June 2020 could mitigate potential risks.

Maintaining Awareness of Cloud Service Providers' Suppliers

For one of the four systems we reviewed, we noted that the cloud service provider is relying on Amazon Web Services (AWS) for the underlying infrastructure. However, AWS is not listed on the CRC's inventory of cloud systems. The CRC maintains an inventory of Board cloud projects that are in the proof-of-

[8] The Division of IT's *Application Development Security Standards for Board Hosted Applications*, version 1.0, June 19, 2018, requires that all new applications or applications undergoing major enhancements for deployment on Board infrastructure must undergo an ARB design review. Additional design reviews must be completed prior to the development of new applications and for any major enhancements to existing applications.

[9] Cloud Product Evaluation: ARB Evaluation Form, version 1.1, last updated January 4, 2021.

concept, configuration, and production phases. We did not find evidence that Board officials obtained sufficient assurance that the security controls provided by AWS meet Board requirements.

NIST's *Framework for Improving Critical Infrastructure Cybersecurity* states that organizations should ensure that suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber–supply chain risk assessment process.[10] Maintaining greater awareness into all supply chain providers associated with cloud technologies used by the agency could help the Board determine the level of controls assessment and assurances it may need to ensure that Board data are adequately protected.

Consistent Use of Cloud Computing Accounting Codes

We noted that select Board divisions were not consistent in their use of accounting codes to track costs associated with cloud computing technologies. The Board's *2019 Chart of Operating Accounts Guide* states that divisions should use the Cloud Computing Arrangement accounting code when they purchase cloud technologies involving a software product that is run on the servers of a vendor or a third party rather than on Board data center servers. However, we found that some divisions were using the Software and Contractual Professional Services codes to track costs associated with cloud computing technologies that should have been classified under the Cloud Computing Arrangement code.

A key cause of this issue is that these divisions purchased cloud technologies prior to the issuance of the 2019 guide, and the Board has not ensured that cloud purchases made prior to the issuance of the guide are using the Cloud Computing Arrangement code to track costs. Consistent use of the Cloud Computing Arrangement accounting code would enable the Board to accurately quantify agencywide spending on cloud computing.

[10] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.1, April 16, 2018.

Appendix A: Scope and Methodology

The objective of our evaluation was to evaluate the effectiveness of the Board's system development life cycle processes in ensuring that risks are adequately managed for cloud systems in use. Specifically, we reviewed IT governance and cybersecurity life cycle processes for a sample of four Board cloud systems used to support project time tracking, identification and authentication, website hosting and content management, and financial management.

To accomplish our objective, we

- analyzed the Board's cloud governance and cybersecurity policies, procedures, and related documentation
- reviewed the Federal Reserve System's processes and procedures for inventorying cloud systems that process, maintain, or store Board information
- interviewed Board and System officials responsible for implementing and overseeing the security of cloud systems
- tested security controls in the access control, assessment, authorization, monitoring, contingency planning, incident response, media protection, system and communications protection, and system and information integrity families for a judgmentally selected sample of four production cloud systems managed by three Board divisions
- reviewed contracts and related agreements for the four cloud systems in our sample
- analyzed cloud computing–related purchase orders from 2019 and 2020

We performed our fieldwork from April 2020 to January 2021. We performed our evaluation in accordance with the *Quality Standards for Inspection and Evaluation* issued by the Council of the Inspectors General on Integrity and Efficiency.

Appendix B: Management Response

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

DIVISION OF
INFORMATION TECHNOLOGY

March 9, 2022

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 "The Board Can Strengthen Inventory and Cybersecurity Life Cycle Processes for Cloud Systems" prepared as part of your office's oversight responsibilities pursuant to the Federal Information Security Modernization Act of 2014 (FISMA). The report evaluates the effectiveness of the Board of Governors of the Federal Reserve System's life cycle processes for ensuring that cybersecurity risks are adequately managed for cloud systems in use. The report highlights the progress the Board has made in articulating a cloud vision and strategy and in developing supporting security life cycle processes.

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 Plan of Actions and Milestones (POA&Ms) shortly and review our status towards addressing those 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,

SHARON MOWRY
Digitally signed by SHARON MOWRY
Date: 2022.03.09 11:48:41 -05'00'

Sharon Mowry
Chief Information Officer (CIO)

cc: Mr. Peter Sheridan
Mr. Raymond Romero

www.federalreserve.gov

Mr. Glenn Eskow
Mr. Charles Young
Ms. Annie Martin
Mr. Pat McClanahan

Abbreviations

ARB	Architecture Review Board
AWS	Amazon Web Services
BISP	*Board Information Security Program*
CIO	chief information officer
CRC	Cloud Resource Center
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Modernization Act of 2014
IaaS	Infrastructure as a Service
ISCU	Information Security Compliance Unit
IT	information technology
NIST	National Institute of Standards and Technology
PaaS	Platform as a Service
PMO	Project Management Office
POA&M	plan of action and milestones
SaaS	Software as a Service
SSP	system security plan

Report Contributors

Jeffrey Woodward, Project Lead
Justin Byun, IT Auditor
Trang Do, IT Auditor
Nick Gallegos, IT Auditor
Andrew Gibson III, Senior OIG Manager for Management and Operations
Khalid Hasan, Senior OIG Manager for Information Technology
Peter Sheridan, Associate 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