Evaluation Report
2018-IT-B-020
November 5, 2018

Board of Governors of the Federal Reserve System

The Board Can Strengthen Information Technology Governance

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

Executive Summary, 2018-IT-B-020, November 5, 2018

The Board Can Strengthen Information Technology Governance

Findings

Overall, we found that certain aspects of the Board of Governors of the Federal Reserve System's (Board) organizational structure and authorities could inhibit the Board's achievement of its strategic objectives regarding technology as well as its achievement of an effective Federal Information Security Modernization Act of 2014 maturity rating. Although the Board has information technology (IT) governance mechanisms in place, we found opportunities for improvement in the areas of security, budgeting, procurement, and capital planning.

First, the Chief Information Officer (CIO) may not have appropriate visibility into all IT decisions made at the Board. The Board's *Delegations of Administrative Authority* authorizes Board Division Directors to make independent IT investment decisions for their divisions, including information security decisions, without prior review by the CIO. Further, divisions are not required to align their IT investments with the Board's enterprisewide architecture.

Second, the Board lacks a documented reporting hierarchy and authority structure for its various IT governance boards and committees. Further, the Investment Review Board lacks a mechanism to elevate concerns with an IT project to those with the authority to pause or cancel the project.

Third, Board divisions are not consistently tracking labor hours for the purpose of capitalizing software development costs. Therefore, the capitalized costs for the Board's internally developed software assets may be inaccurate.

Recommendations

Our report contains six recommendations designed to strengthen IT governance at the Board. In its response to our draft report, the Board concurs with our recommendations and states that actions have been or will be taken to address them. We will follow up to ensure that the recommendations are fully addressed.

Purpose

The National Institute for Standards and Technology recommends that each agency implement an information security governance structure to ensure an appropriate level of support for agency missions. In addition, various laws, executive orders, policies, guidance, and best practices address the need for IT governance structures to ensure that IT investments align with agency missions and objectives and that CIOs have appropriate visibility into or control over their agency's IT resources.

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. We conducted this evaluation to assess whether the Board's current organizational structure and authorities support its IT needs, specifically, the organizational structure and authorities associated with security, privacy, capital planning, budgeting, and acquisition.

Background

The Board relies on a variety of IT services to accomplish its mission. These services include applications management, help desk operations, compliance management, and technical operations management. The Board's governance structure for managing IT services consists of centralized and decentralized organizational responsibilities. The Director of the Division of Information Technology is responsible for budgeting and implementing centrally provided IT services in accordance with the Board's policies and procedures; however, some Board divisions maintain the security of their own data and computing facilities. The efficiency and effectiveness of the Board's agencywide information security program is contingent on organizationwide visibility into IT operations.

Recommendations, 2018-IT-B-020, November 5, 2018

The Board Can Strengthen Information Technology Governance

Finding 1: The *Delegations of Administrative Authority* and the Lack of a Policy on Divisions' IT Investments Inhibit Enterprisewide Visibility Into Technology Decisions

Number	Recommendation	Responsible office
1	In consultation with Board Legal, assess whether the *Delegations of Administrative Authority* provides the CIO with appropriate visibility into Board IT decisions.	Office of the Chief Operating Officer
2	Require divisions with embedded IT units to inform the CIO of their IT investment plans.	Division of Information Technology and Division of Financial Management, in conjunction with Office of the Chief Operating Officer
3	Require that all IT investments align with the Board's enterprisewide architecture unless such IT investments receive a waiver from the CIO.	Division of Information Technology, in coordination with Office of the Chief Operating Officer

Finding 2: The Board Has Not Defined a Hierarchy or Authority Structure for Its IT Governance Boards and Committees

Number	Recommendation	Responsible office
4	Clarify and document the roles and responsibilities of the Board's IT governance boards and committees and require division-level governance boards and committees to include the CIO, or their designee, as appropriate.	Office of the Chief Operating Officer, in coordination with Division of Information Technology
5	Update the IRB charter to include a mechanism for the IRB to elevate concerns with an IT project to those with the authority to pause or cancel the project.	Executive Committee

Finding 3: Board Divisions Are Inconsistently Tracking and Capitalizing Internal Software Development Labor Costs

Number	Recommendation	Responsible office
6	Ensure that a policy is in place for all divisions to consistently track labor hours and report the internal and contractor labor costs attributable to their software development activities where appropriate.	Division of Financial Management

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

MEMORANDUM

DATE: November 5, 2018

TO: Distribution List

FROM: Peter Sheridan
Associate Inspector General for Information Technology

SUBJECT: OIG Report 2018-IT-B-020: *The Board Can Strengthen Information Technology Governance*

We have completed our report on the subject evaluation. We conducted this evaluation to assess whether the Board of Governors of the Federal Reserve System's (Board) current organizational structure and authorities support its information technology needs associated with security, privacy, capital planning, budgeting, and acquisition. We performed this evaluation pursuant to requirements in 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.

Our report contains six recommendations designed to strengthen information technology governance at the Board. We provided you with a draft of our report for 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 C to our report.

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

cc: Tina White, Senior Manager, Compliance and Internal Control, Division of Financial Management

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

Contents

Introduction

Objective

Our overall objective was to assess whether the Board of Governors of the Federal Reserve System's (Board) current organizational structure and authorities support its information technology (IT) needs associated with security, privacy, capital planning, budgeting, and acquisition. We addressed this objective by conducting our evaluation in two phases. The first phase assessed the Board's organizational structure and authorities to determine their adequacy in meeting security and privacy needs. In this second phase, we assessed the Board's organizational structure and authorities to determine their adequacy in supporting capital planning, budgeting, and acquisition associated with IT needs. Our scope and methodology are detailed in appendix A.

Background

IT governance is a formal framework that provides a structure for organizations to ensure that IT investments support business objectives. The Board's strategic plan establishes its business objectives through six strategic pillars.[1] The Board believes that implementing its strategic pillars will better enable it to advance its mission, as well as prioritize investments and resources to address evolving organizational challenges.

Strategic pillar 4 addresses technology, with an overall goal to empower operational excellence, efficiency, and security through innovative technology platforms. To achieve this goal, the Board established several governance-focused technology objectives and initiatives. One of the objectives includes the development, implementation, and maintenance of a Boardwide technology roadmap driven by business needs that consistently improves the computing environment while strengthening a risk-based information security program. Key initiatives include specifying strategic investments in technology, developing a technology investment and implementation plan, and defining a governance plan.

The need for formal corporate and IT governance practices in the United States was fueled by the enactment of laws and regulations such as the Gramm-Leach-Bliley Act and the Sarbanes-Oxley Act in the 1990s and early 2000s; these laws were enacted in reaction to several high-profile corporate fraud and deception cases. The Federal Information Security Modernization Act of 2014 (FISMA) requires that federal agencies, including the Board, implement an effective agencywide information security program, which is a maturity rating of level 4.[2] Although not applicable to the Board, other laws, regulations, executive orders, and leading industry IT governance practices may be useful to the Board in achieving its strategic plan for technology and increasing its FISMA maturity rating. For example, the May 2018 *Executive Order Enhancing Effectiveness of Agency Chief Information Officers* identified that department and agency Chief Information Officers (CIOs) generally do not have appropriate visibility into or control

[1] Board of Governors of the Federal Reserve System, *Strategic Plan 2016–19*, October 2015.

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

over their agency's IT resources, resulting in duplication, waste, and poor service delivery.[3] The executive order states that enhancing the effectiveness of agency CIOs will better position agencies to modernize their IT systems, execute IT programs more efficiently, reduce cybersecurity risks, and serve the American people. Various publications from ISACA, a leading global organization for IT management professionals, address the need for strong IT governance.[4] ISACA's COBIT 5,[5] used by organizations worldwide, is a leading framework for governing the management of enterprisewide IT. COBIT 5 is mapped to the most relevant and frequently used standards and frameworks related to governance, including those in the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) joint technical committee publication, *Governance for the IT Organization*.[6]

IT Services at the Board

The Board relies on a variety of IT services to accomplish its mission. These services include applications management, help desk operations, compliance management, and technical operations management. The Board's governance structure for managing IT services consists of centralized and decentralized organizational responsibilities.

The Division of Information Technology (Division of IT) provides centralized IT services that are leveraged fully or partially by Board divisions. These services include setup and maintenance of Microsoft Windows–based computers, applications development, and help desk operations. The Director of the Division of IT, who also serves as the CIO, is also responsible for ensuring that these centrally provided IT services are budgeted for and implemented in accordance with the Board's policies and procedures.

Individual Board divisions also perform IT services in support of their business needs through embedded IT units. In some instances, these services overlap with those provided centrally by the Division of IT. For example, several Board divisions engage in their own systems development and help desk activities for applications supporting their business processes. In other instances, Board divisions perform IT services to support specific needs. For example, one division maintains a separate Linux-based infrastructure to support research and statistical applications used by economists and researchers. These decentralized IT

[3] Exec. Order No. 13,833 (May 15, 2018).

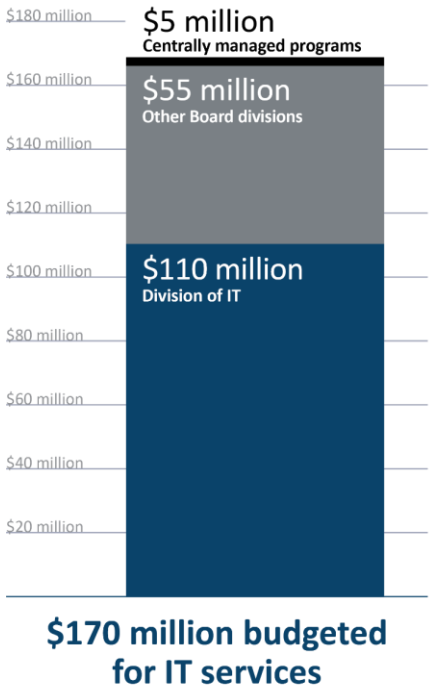
[4] ISACA is an independent, nonprofit, global association engaged in the development, adoption, and use of globally accepted, industry-leading knowledge and practices for information systems. ISACA serves approximately 140,000 IT professionals in 180 countries.

[5] *COBIT* stands for Control Objectives for Information and Related Technology.

[6] The ISO is an independent, nongovernmental international organization based in Geneva, Switzerland. It is a forum for experts to share knowledge and develop voluntary, consensus-based, market-relevant international standards that support innovation and provide solutions to global challenges, including IT. The IEC is the international standards and conformity assessment body for all fields of electrotechnology. ISO/IEC is a joint technical committee of the ISO and the IEC. Its purpose is to develop, maintain, and promote standards in the fields of IT and information and communications technology. ISO/IEC 38500 2015, *Governance for the IT Organization*, applies to the governance of an organization's current and future use of IT, including management processes and decisions related to the current and future use of IT.

services are implemented and managed by the divisions in which they are performed. All division-embedded IT units are required to comply with the CIO's policies.

Figure 1. The Board's 2018 IT Budget



Source. 2018 Board budget data.

Figure 1 highlights the budgeted costs for IT services at the Board for 2018. The 2018 budget for all IT services at the Board is $170 million, which is 23 percent of the Board's overall budget. Of the $170 million budgeted for 2018, the Division of IT accounts for $110 million (65 percent) and division-embedded IT units account for $55 million (32 percent). The remaining $5 million is budgeted for centrally managed programs, such as compensation and retirement, that are allocated IT activities.

In expending funds for IT, the Board requires divisions to identify whether the assets created or purchased should be capital assets.[7] The Board's *Accounting for Capital Assets* policy establishes 13 capital asset categories, including a category for software that is internally developed. The Board's capitalization guidance states that internally developed software projects must have development or improvement costs that exceed $500,000 to meet the threshold for capitalization. The Board defines internally developed software as software that is developed and deployed using internal Board labor or external contract labor and is not commercially available.

The Board capitalizes internal labor and external contract labor costs associated with software development, including labor costs incurred to develop software internally and to modify purchased software. Board officials stated that when a division expects to capitalize labor hours for a project, Division of Financial Management (DFM) personnel provide the necessary capitalization policies and procedures to the project team. According to Board officials, the project team sends DFM the labor hours eligible for capitalization, and DFM accounts for them.

The Board's Delegations of Administrative Authority

The Board's *Delegations of Administrative Authority* sets forth the delegations of the Board's internal administrative authority. The *Delegations of Administrative Authority* states that the Chairman of the Board has delegated to the Administrative Governor the responsibility for administrative oversight of the Board's operations and resources. The Administrative Governor has in turn delegated this responsibility to the Chief Operating Officer (COO). The COO has redelegated the administration of IT security and

[7] According to the Board's *Accounting for Capital Assets* policy, to be classified as a capital asset, an asset must have (1) a useful life of more than a year and (2) an initial value above the capitalization threshold for the particular asset. The useful life of an asset is the period during which it is expected to be usable for the purpose for which it was acquired. It may or may not correspond with the item's actual physical life or economic life. The policy also identifies asset categories, their maximum useful life, and the capitalization threshold.

privacy to the CIO and the Chief Privacy Officer (CPO), respectively. Specifically, the COO has redelegated to the CIO and CPO the responsibilities for

- automation, telecommunications, and other IT matters
- information security
- formulation, approval, and implementation of the management policies for IT security and privacy
- formulation, approval, and implementation of all privacy policies, including
    - ensuring the Board's implementation of information privacy protections, which includes the Board's compliance with applicable federal laws, regulations, and policies relating to information privacy, such as the Privacy Act of 1974
    - providing input to the Board's development and evaluation of legislative, regulatory, and other policy proposals regarding information privacy issues, with the exception that approving and reviewing privacy impact assessments must be coordinated with the CIO

The Division of IT is organizationally placed under the COO. The Director of the Division of IT is also the Board's CIO. The CPO, who is also the Board's Chief Information Security Officer (CISO), works in the Division of IT and reports to the CIO (figure 2).

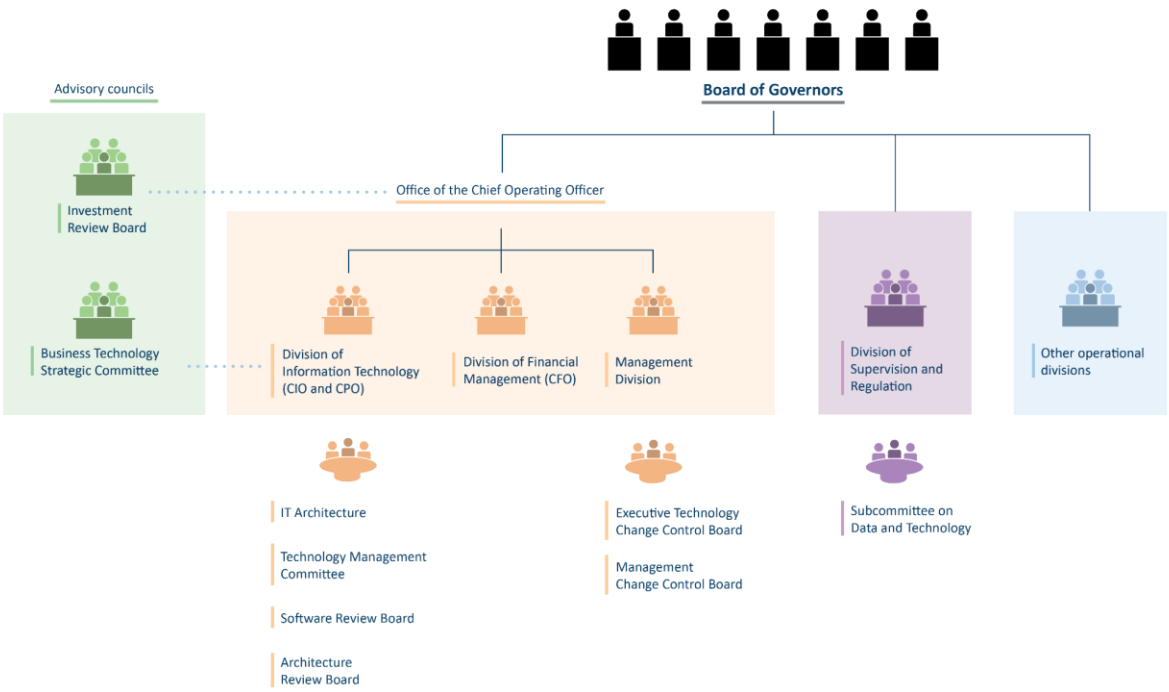
Governance Boards and Committees at the Board

The Board has several enterprisewide IT governance boards and committees, including the Investment Review Board (IRB) and the Business Technology Strategic Committee (BTSC). The IRB reviews capital projects to support consistency and coordination across the Board and to help ensure project success. The IRB membership currently includes representatives from 13 of the 15 Board divisions and offices. The COO, who currently chairs the IRB, stated that the IRB's overall goal is to develop better project management at the Board. The BTSC is responsible for promoting an enterprisewide view of the implementation and administration of IT services in a consistent, cost-sensitive, and secure manner that is informed by business needs.

The Executive Committee granted the IRB the authority to review capital projects, including IT projects with estimated costs and funding that exceed $1 million or projects that the IRB determines to be significant to the Board.[8] Such projects are subject to IRB review prior to the project's inclusion in the annual budget request to the Board, and after such inclusion to monitor the project's status. An IRB review covers project plan analysis and objective review as well as the project's management, governance structure, and cost estimates.

[8] The Executive Committee is composed of all the Division Directors and is chaired by the COO. It is a forum for the Division Directors to discuss major administrative issues or concerns that affect the Board.

Figure 2. The Board's Organizational Structure for IT



Source. OIG review of Board organization charts.

Note. Figure 2 only shows the divisions and offices relevant to this evaluation.

In addition to the IRB, several Board divisions have established their own boards and committees to provide governance and oversight to their respective IT projects. Some of these boards and committees focus more on project management, while others focus on alignment with the Boardwide strategic plan and governance. Appendix B highlights the other Board groups related to IT and the key IT boards and committees in the Division of IT, the Management Division, and the Division of Supervision and Regulation. These committees have a role that is separate from that of the IRB.

Taken together, figure 2 and appendix B highlight the differing levels of oversight and governance a project can be subject to, depending on which division is sponsoring the project. For example, a major project in the Division of Supervision and Regulation must go through the Subcommittee on Data and Technology, a Federal Reserve System governance board, for approval.

Summary of Findings

Although we found that the Board has implemented several aspects of effective governance, certain weaknesses could inhibit the Board's achievement of its strategic objectives regarding technology as well as its achievement of an *effective* FISMA maturity rating.

We found that the CIO and the CPO are appropriately positioned to oversee security and privacy, respectively, and have been granted those respective authorities through the *Delegations of Administrative Authority*. Additionally, the Board has centralized budget and procurement under DFM and granted the Chief Financial Officer (CFO) the authority to oversee these and other functions. We also found that the IRB reviews all IT capital projects if the amount actually funded for the investment is over $1 million in total estimated project costs or is determined to be significant to the Board prior to a project having an approved budget and throughout the implementation of the project. The IRB received its authority through the Executive Committee and is chaired by the COO.

We identified opportunities to strengthen IT governance in the areas of security, budgeting, and capital planning. Regarding security, we found that the Board's *Delegations of Administrative Authority* allows Division Directors to make independent IT investment decisions for their divisions, including information security decisions, without prior review by the CIO. Such IT investments are not required to align with the Board's enterprisewide architecture. We also found that the Board lacks a hierarchy and authority structure for the various IT governance boards and committees because their reporting relationships and spans of authority are not defined. Additionally, we found that the IRB lacks a mechanism to elevate concerns with an IT project to those with the authority to pause or cancel the project. Finally, we found that divisions are inconsistently tracking software development labor hours. Board policy requires that software development labor costs be capitalized. Failure to identify labor hours could affect the accuracy of the Board's capitalized software assets.

We also identified an item for management's consideration regarding resources allocated to the Board's privacy program.

Finding 1: The *Delegations of Administrative Authority* and the Lack of a Policy on Divisions' IT Investments Inhibit Enterprisewide Visibility Into Technology Decisions

The *Delegations of Administrative Authority* allows Division Directors to independently make IT investment decisions for their divisions, including information security decisions, without prior review by the CIO and without a requirement that they align with the Board's enterprisewide IT architecture. The Board's *Delegations of Administrative Authority* delegates authority to the CIO to create, approve, and implement management policies for IT security and privacy; however, the Board does not require the CIO to review the IT investment decisions made by divisions with embedded IT groups. The absence of policy to address these weaknesses in governance increases the risk that the Board's IT security and privacy requirements may not be met and that Board resources may be inefficiently expended on IT investments.

The *Delegations of Administrative Authority* Authorizes Division Directors to Make IT Decisions Independently of the CIO

Although the CIO has the authority to create, approve, and implement management policies related to IT, including information security and privacy policies, the *Delegations of Administrative Authority* authorizes Division Directors to make and implement IT investment decisions without prior review by the CIO. The *Delegations of Administrative Authority* states that Division Directors may maintain the security of their data and computing facilities in accordance with policies established by the CIO and may autonomously procure and internally develop IT solutions. As a result, the CIO may not always have appropriate visibility into technology decisions made by divisions with embedded IT, including those that affect information security and privacy.

For example, the Board has deployed centralized recruitment software, but we identified a division that decided the tool did not meet its needs and used its embedded IT unit to internally develop its own recruitment software and interface. Board IT officials were unaware of this interface until we informed them of its existence, and their response was that policy grants the division autonomy to make those types of business decisions. Further, our *2017 Audit of the Board's Information Security Program* report identified an example of a division that maintained its own security incident and event management (SIEM) tool.[9] The vulnerability remediation information from this division's SIEM tool is not fully

[9] Office of Inspector General, *2017 Audit of the Board's Information Security Program*, OIG Report 2017-IT-B-018, October 31, 2017.

integrated into the agencywide SIEM tool. In addition, that division was not covered by the Board's application whitelisting tool, which allows the agency to identify authorized and unauthorized software on the network and take appropriate action.[10]

National Institute of Standards and Technology Special Publication 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process*, states that generally, operating units, with approval from the agency CIO, use their discretion when funding investments that are below $1 million. However, for investments that are e-Gov,[11] high profile, or over $1 million, a full review by the CIO, among others, is necessary to demonstrate that all requirements are met and that the investment aligns with the agency's mission.

Although not applicable to the Board, certain federal laws and associated guidance address the need for CIOs to have appropriate insight into their IT operations. For example, the White House recently issued *Executive Order Enhancing Effectiveness of Agency Chief Information Officers* to help ensure that agency CIOs have a significant role, including, as appropriate, as lead advisor, in all annual and multiyear planning, programming, budgeting, and execution decisions, as well as in all management, governance, and oversight processes related to IT.[12] In addition, the Office of Management and Budget (OMB) issued guidance for implementing the Federal Information Technology Acquisition Reform Act of 2014 (FITARA).[13] To implement the requirements of FITARA, OMB requires that covered agencies have their CIOs review and approve major IT investment portions of budget requests. The agency CFO and CIO must jointly affirm within the budget request that the CIO had a significant role in reviewing planned IT support for major program objectives and significant increases and decreases in IT resources.[14]

In 2017, we reported that the effectiveness of the Board's IT administrative function could be improved.[15] We found that the Board's decentralized structure and consensus-driven culture creates a gap between the perceived authority of the CIO, the COO, the CFO, and the Chief Human Capital Officer and their delegated authority as defined in Board policy. This gap creates challenges in implementing enterprisewide administrative initiatives. Therefore, we issued two recommendations to the Board of Governors to review, communicate, and reinforce the Board of Governors' expectations of the COO and the heads of the administrative functions, and one recommendation to the COO and the heads of the administrative functions to implement processes to report on enterprisewide actions to ensure

---

[10] 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.

[11] The E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899 (2002), was enacted to enhance the management and promotion of electronic government services and processes by establishing a federal CIO within the Office of Management and Budget and a broad framework of measures that requires using internet-based IT to enhance public access to government information and services, and for other purposes.

[12] Exec. Order No. 13,833 (May 15, 2018).

[13] FITARA was enacted to improve governmentwide acquisition of IT. FITARA requires covered agencies to, among other things, enhance CIO authorities for approving IT budget requests and contracts and requires the CIO to be involved in how the agency uses IT resources to achieve its objectives. The Board is not required to comply with FITARA.

[14] Office of Management and Budget, *Management and Oversight of Federal Information Technology*, OMB Memorandum M-15-14, June 10, 2015.

[15] Office of Inspector General, *The Board's Organizational Governance System Can Be Strengthened*, OIG Report 2017-FMIC-B-020, December 11, 2017.

compliance with policies. Further, our *2017 Audit of the Board's Information Security Program* report noted a consistent theme in the lack of an agencywide risk-management governance structure and strategy, as well as the decentralization of IT services, resulting in an incomplete view of the risks affecting the security posture of the Board and impeding its ability to implement an effective information security program. This resulted in lower maturity ratings for several security processes, including risk management, configuration management, and information security continuous monitoring.

Currently, the Board does not require the CIO to review proposed IT investments by divisions with embedded IT groups to ensure that they comply with Board requirements, including those related to security and privacy. This lack of CIO review of proposed investments could inhibit the Board's ability to achieve its Boardwide technology roadmap objective, as investments could potentially be misaligned with the enterprisewide architecture.

The Board Does Not Require or Ensure That IT Investments Align With Enterprisewide Architecture

The Division of IT has created an enterprisewide architecture for the technology it manages. However, some divisions with embedded IT units have enterprise architectures that are separate from that of the Division of IT. Division of IT officials stated that a majority of the Board's IT devices are centrally managed by the Division of IT and therefore are under the Division of IT's enterprisewide architecture.

An enterprisewide architecture is critical to IT governance and, thus, the successful achievement of the Board's strategic plan for technology. An enterprisewide architecture helps to align business and technology resources to the mission or business function they support and helps the Board to eliminate waste and duplication. Further, an enterprisewide architecture describes the baseline architecture, the target architecture, and a transition plan by which to achieve the target architecture. Effective use of an enterprisewide architecture is a hallmark of successful organizations and can be important to maximizing institutional mission performance and outcomes. Among other things, the effective use of enterprisewide architecture includes the following:

- realizing cost savings through consolidation and reuse of shared services and the elimination of antiquated and redundant mission operations
- enhancing information sharing through data standardization and system integration
- optimizing service delivery through streamlined and normalized business processes and mission operations

Although not applicable to the Board, various federal laws and implementation guidance,[16] as well as leading industry practices such as COBIT 5, address the need for organizations to develop and maintain an effective enterprisewide architecture as part of their IT governance program.

In 2014, we reported on a matter for management consideration associated with the Division of IT's lack of an enterprisewide architecture.[17] We found that the Division of IT's efforts to develop an enterprisewide architecture did not include all the technologies and services used across Board divisions and that Board divisions are not required to follow the enterprisewide architecture standards that the Division of IT creates. We suggested that the Director of the Division of IT work with Board divisions to identify the IT standards, services, and technologies in use at the time across Board divisions and those needed to meet future strategic goals and objectives, and then define a transition plan.

In addition, in our *2017 Audit of the Board's Information Security Program* report, we note that the lack of an enterprisewide architecture contributed to the CISO not having a full view of the vulnerability remediation status or security configurations for all information system components connected to the Board's network. We recommended that the CIO ensure that the Board's enterprisewide architecture includes technologies managed by all divisions and work with the COO to enforce associated review processes agencywide. The Board has begun taking steps to address this recommendation by compiling division-specific enterprise architectures.

Division-embedded IT groups are able to procure as well as internally develop IT solutions that may not align with Board IT initiatives or architecture. For the Board to develop and implement its technology investment and implementation plan and governance plan as part of its overall strategic plan for technology, division-embedded IT units must either ensure that their IT investments align with the Board's enterprisewide architecture for IT or request a waiver. The lack of a requirement for divisions' IT solutions to align with the Board's architecture also increases risk to the Board that IT investments will not meet the Board's security and privacy requirements and will not be cost effective.

Recommendations

We recommend that the COO

1. In consultation with Board Legal, assess whether the *Delegations of Administrative Authority* provides the CIO with appropriate visibility into Board IT decisions.

We recommend that the CIO and CFO, in coordination with the COO,

2. Require divisions with embedded IT units to inform the CIO of their IT investment plans.

[16] Congressional mandates for IT architecture are contained in the Clinger-Cohen Act of 1996, which was updated and revised by the E-Government Act of 2002 to include enterprise architecture. Further, related implementation guidance from OMB is contained in various documents, including Circulars A-11 and A-130; Memorandums 97-16, 00-10, 05-22, 11-29, and 12-10; and the *Digital Government Strategy*.

[17] Office of Inspector General, *Opportunities Exist to Achieve Operational Efficiencies in the Board's Management of Information Technology Services*, OIG Report 2014-IT-B-003, February 26, 2014.

We recommend that the CIO, in coordination with the COO,

3. Require that all IT investments align with the Board's enterprisewide architecture unless such IT investments receive a waiver from the CIO.

Management's Response

In its response to our draft report, the Board concurs with our recommendations. The Board notes that plans of action and milestones will be established to address our recommendations.

OIG Comment

We believe that the Board's official comments are responsive to our recommendations. We will follow up to ensure that the recommendations are fully addressed.

Finding 2: The Board Has Not Defined a Hierarchy or Authority Structure for Its IT Governance Boards and Committees

The reporting hierarchy and breadth of authority among the various Board IT governance boards and committees have not been defined. Further, the IRB lacks a mechanism to elevate concerns with an IT project to those with the authority to pause or cancel the project. Federal best practices recommend that agencies document the policies and procedures that define each IT investment board's span of authority and describe how investment board activities are to be coordinated. As of August 2018, the Board did not require the IRB to oversee division-level governance boards and committees. As a result, Board capital projects can be approved and undertaken without sufficient oversight, which may lead to projects being managed inefficiently and ineffectively.

IT Governance Boards and Committees Do Not Have a Defined Reporting Hierarchy or Spans of Authority

The reporting hierarchy and spans of authority for the various Board IT governance boards and committees are not defined. Further, review of IT projects by the two enterprisewide governance committees that discuss IT projects—the IRB and the BTSC—is not always required. The various division-level governance and review boards and committees are not formally accountable to the IRB, and the CIO is not involved in the decisions made by these boards and committees.[18] The IRB only reviews capital projects if the total estimated project cost for the investment is over $1 million or if the project is determined to be significant to the organization prior to the project having an approved budget and remains significant to the organization throughout the implementation of the project.

Leading industry and government entities have established best practices related to IT governance structures. For example, COBIT 5 cites the need to ensure that organizations identify and align their enterprise goals and IT-related goals and that a shared, cohesive view of IT governance is achieved across an organization. COBIT 5 cites ISO/IEC 38500, which states that IT solutions should not be considered in isolation or as just a technology project or service. A government-sponsored technology firm's system engineering guide states that to achieve the greatest value and effect from IT governance, governance

[18] See appendix B for examples of division-level boards and committees related to the four divisions included in this evaluation.

requires a framework or structure that defines roles and responsibilities, processes, policies, and criteria, among other things, to foster sound decisionmaking.[19]

The U.S. Government Accountability Office's Information Technology Investment Management framework is a best practice that can be used to enhance an agency's ability to manage its IT investments.[20] The framework states that the enterprise IT investment board must maintain ultimate responsibility for lower-level board activities. The framework further states that for cases in which lower-level investment boards are chartered to carry out the responsibilities of the enterprisewide IT investment board within their own business units, the enterprisewide IT investment board still must maintain ultimate responsibility for the lower-level boards' activities. These subordinate boards should have the same broad representation as the enterprisewide board, though at the subordinate unit's level. The framework also states that organizations with multiple IT investment boards should have an enterprisewide investment process guide that documents the policies and procedures that define each IT investment board's span of authority and describes how investment board activities are to be coordinated. When multiple boards execute the organization's IT investment governance process, criteria aligning these boards must be defined such that there are no overlaps or gaps in the boards' authorities and responsibilities.

A key cause for the lack of a hierarchy and spans of authority in the Board's IT governance structure is that the CIO has not required divisions to ensure they seek out and meet with the IRB and the BTSC. In addition, there is no requirement that the CIO or the Division of IT be represented in all management, governance, and oversight processes related to IT. To develop and implement a governance plan for technology as set forth in the Board's strategic plan, the Board should define a hierarchy and spans of authority for its IT governance bodies.

In our 2017 governance evaluation, we identified issues with the documented authorities for the higher-level Board committee structures. The evaluation recommended that all eight of the standing Board committees develop charters that document, among other things, the authorities of the committee chair.

The IRB Lacks a Mechanism to Elevate Concerns With an IT Project to Those With the Authority to Pause or Cancel the Project

The IRB charter lacks a way to elevate project management concerns to those with the authority to pause or cancel an IT project. In practice, only the division-level IT governance boards and committees are able to make budget decisions for their respective division's capital projects that would pause or cancel projects. According to the IRB chair, the IRB was designed to develop better project management at the

[19] MITRE Corporation is a not-for-profit organization that operates federally funded research and development centers sponsored by the U.S. government to assist it with scientific research and analysis, development and acquisition, and systems engineering and integration. MITRE Corporation's *System Engineering Guide* is a compilation of best practices and lessons learned for MITRE system engineers.

[20] U.S. Government Accountability Office, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, GAO-04-394G, March 2004.

Board, and according to a Board official, it currently does not make decisions regarding project status. Additionally, divisions, rather than the IRB, prioritize and determine the appropriate mix of IT projects.

The IRB charter requires that the IRB review a project prior to its incorporation into the Board's annual budget and monitor the status of each project that it has reviewed and implemented. The review consists of analyzing the divisions' submission of each project, including the project plan and objectives; the management and governance structure; and the financial estimates. This review aligns with the authority granted to the IRB by the Executive Committee to review capital projects that meet certain criteria prior to a project's budget being submitted in the annual budget request to the Board and afterward to monitor the status of each project. We verified that the IRB's review occurs prior to the Board's approval of the budget. National Institute of Standards and Technology Special Publication 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process*, states that the members of an IRB are to evaluate both proposed IT investments and existing IT investments to determine the appropriate mix of investments that will allow the agency to achieve its goals.

As mentioned previously, our 2017 governance evaluation also identified issues with documented authorities for the higher-level Board committee structure. According to Board officials, the IRB is only authorized to review projects; it does not make decisions regarding project status. To develop an effective technology investment and implementation plan, the IRB should have a mechanism through which it can elevate concerns with projects that it believes should be paused or canceled. Such a mechanism would help allow the Board to achieve an appropriate mix of IT investments.

Recommendations

We recommend that the COO, in coordination with the CIO,

4. Clarify and document the roles and responsibilities of the Board's IT governance boards and committees and require division-level governance boards and committees to include the CIO, or their designee, as appropriate.

We recommend that the Executive Committee

5. Update the IRB charter to include a mechanism for the IRB to elevate concerns with an IT project to those with the authority to pause or cancel the project.

Management's Response

In its response to our draft report, the Board concurs with our recommendations. The Board notes that plans of action and milestones will be established to address our recommendations.

OIG Comment

We believe that the Board's official comments are responsive to our recommendations. We will follow up to ensure that the recommendations are fully addressed.

Finding 3: Board Divisions Are Inconsistently Tracking and Capitalizing Internal Software Development Labor Costs

Divisions with embedded IT functions are inconsistently tracking and capitalizing their software development labor costs. Although the Board has a formal requirement to capitalize labor costs incurred for software development activities, there is no policy or procedure prescribing how divisions are to track the hours and associated costs of those activities. As a result, the Board's capital assets and related amortization expenses may be inaccurate for accounting and financial reporting purposes.

Capitalized Costs for Software Assets May Be Inaccurate Due to Inconsistent Tracking and Capitalizing of Internal Software Development Labor Costs

Divisions with embedded IT functions have varying practices associated with tracking and capitalizing their software development labor costs. Specifically, one of the four divisions we reviewed is not tracking the hours of internal personnel working on software development projects. Another division is tracking the internal and contractor labor hours associated with software development but only capitalizing the cost of contractor personnel labor. The other two divisions track and capitalize the hours of internal and contractor personnel working on software development projects as required by the Board's policy.

The Board's policy on accounting for capitalizable software development assets was created by the Director of DFM, who is also the CFO. According to DFM officials, the capitalizable hours are sent by the division to DFM to be accounted for. DFM officials stated that when a project is identified as having capitalizable hours, DFM provides guidance and documentation to the division to ensure that the project leadership understands Board policy.

The Board's *Accounting for Capital Assets* policy states that any internal software development is to be capitalized once the project's costs reach the $500,000 threshold. According to the policy, software development includes software that is developed and deployed using internal Board labor or external contract labor. The Financial Accounting Standards Board establishes financial accounting and reporting standards for public and private companies and not-for-profit organizations that follow generally accepted accounting principles; the Board follows these standards. The Financial Accounting Standards Board's *Accounting Standards Codification—Intangibles—Goodwill and Other—Internal-Use Software*, subtopic 350-40 on internal software development, states that costs of computer software developed or obtained for internal use that shall be capitalized include (1) external direct costs of materials and services consumed in developing or obtaining internal-use computer software and (2) payroll-related

costs for employees who are directly associated with and who devote time to the internal-use software project.[21]

Although Board policy requires divisions to capitalize the internal and external labor costs incurred for software development activities, no policy or procedure prescribes how divisions are to track the hours and associated costs of those activities. In 2014, we reported on the inconsistent tracking of IT service costs. During that review, we found that the Board does not have a consistent process to track costs for IT services across Board divisions. We attributed this inconsistency to the Board's decentralized budgeting processes and the absence of policies and procedures for accounting for IT services costs. We recommended that the CIO work with the COO and DFM to identify and define specific cost centers for IT in consultation with the Board divisions and implement a consistent process to account for and track costs for IT services across Board divisions. This recommendation was closed in 2017 based on actions taken by the Board.

Our 2017 governance evaluation found that the CFO, along with others, has limited ability to implement enterprisewide initiatives. The evaluation identified that because other Division Directors may perceive the COO, as well as the CFO, the Chief Human Capital Officer, and the CIO (the heads of the administrative functions), to have less authority than they actually do per Board policy, these four officials have met with resistance when exercising their delegated authority. As such, we issued two recommendations to the Board of Governors to review, communicate, and reinforce the Board of Governors' expectations of the COO and the heads of the administrative functions and one recommendation to the COO and the heads of the administrative functions to implement processes to report on enterprisewide actions to ensure compliance with policies.

With inconsistent practices for tracking the hours of embedded IT functions engaged in software development activities, Board divisions may not be able to accurately account for the number of hours spent on a software development project and the associated cost. Ultimately, the Board may not be appropriately capitalizing software assets.

Recommendation

We recommend that the CFO

6. Ensure that a policy is in place for all divisions to consistently track labor hours and report the internal and contractor labor costs attributable to their software development activities where appropriate.

Management's Response

In its response to our draft report, the Board concurs with our recommendation. The Board notes that a plan of action and milestones will be established to address our recommendation.

[21] Financial Accounting Standards Board, *Accounting Standards Codification—Intangibles—Goodwill and Other—Internal-Use Software*, subtopic 350-40, July 1, 2009.

OIG Comment

We believe that the Board's official comments are responsive to our recommendations. We will follow up to ensure that the recommendation is fully addressed.

Other Matter for Management's Consideration

The Board has made progress in dedicating resources to its privacy program since the first phase of our evaluation. The Board has designated the Division of IT as responsible for carrying out its privacy program. Further, the Board has identified a Senior Agency Official for Privacy and named him the CPO. The Senior Agency Official for Privacy is also the Deputy Director of the Division of IT and the CISO. As Deputy Director, this individual is in charge of information security and the information architecture of the Board. The CPO is responsible for ensuring that the Board implements all privacy requirements and considers the privacy effects of all Board actions and policies that involve personally identifiable information.

Although not applicable to the Board, OMB Memorandum M-16-24, *Role and Designation of Senior Agency Officials for Privacy*,[22] provides requirements to CFO Act agencies[23] that could assist the Board with enhancing its privacy program. Specifically, the guidance states that agencies should assess the resource needs of the designated Senior Agency Official for Privacy and the privacy program and provide the official with the resources needed to ensure that he or she can carry out privacy responsibilities.

Since the start of this evaluation, the Board has made progress in addressing resource constraints and the maturity of the privacy program.

1. The section within the Division of IT responsible for the privacy program has changed its name to include the word *privacy*—it is now the Information Security and Privacy Program.
2. The resources available as of August 2018 include a full-time privacy employee as well as security compliance personnel who share their time between privacy and security compliance responsibilities. The CPO stated at that time that with the addition of a full-time privacy employee, he had the necessary resources for the privacy program.
3. The Board created and issued several privacy program plans and policies in 2018, including the *Privacy Policy*, the *Incident Notification and Breach Response Plan*, and the *Sensitive Personally Identifiable Information (SPII) Data Standard*.

In light of these efforts, we are not making a recommendation in this area. In our future audit and evaluation work, we will monitor the extent to which the Board's privacy resources are producing an effective privacy program.

[22] Office of Management and Budget, *Role and Designation of Senior Agency Officials for Privacy*, OMB Memorandum M-16-24, September 15, 2016.

[23] The CFO Act agencies are designated in 31 U.S.C. § 901(b)(1)-(b)(2).

Appendix A: Scope and Methodology

Our overall evaluation objective was to assess whether the Board's current organizational structure and authorities support its IT needs, specifically, the organizational structure and authorities associated with security, privacy, capital planning, budgeting, and acquisition. In the first phase of this evaluation, we assessed the Board's organizational structure and authorities to determine their adequacy in meeting security and privacy needs. In the second phase of this evaluation, we assessed the Board's organizational structure and authorities to determine their adequacy in supporting capital planning, budgeting, and acquisition associated with IT needs.

To accomplish these objectives, we reviewed applicable laws, regulations, and best practices; conducted a governmentwide benchmarking exercise; examined the Board's delegations of authority, organizational charts, and operating plans; reviewed applicable Board policies and procedures, including committee charters; interviewed key Board officials in IT and financial management roles; and examined documentation of enterprisewide IT-related expenses.

We performed our fieldwork from April 2017 to July 2018. 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: Examples of IT Governance Boards and Committees

Table B-1. Examples of IT Governance Boards and Committees at the Board

Division	Boards and committees	Function
Enterprisewide	Business Technology Strategic Committee	Provides a business perspective in its review of high-level IT goals and strategies for the Board's business and support functions; fosters the implementation of approved IT goals and strategies across the divisions.
IT	Technology Management Committee	Serves as the oversight management group for the Division of IT; manages analysis and information for technical initiatives and projects.
IT	Architecture Review Board	Provides stability to projects and a forum for constructive feedback; ensures the integrity of infrastructure components and ensures that security standards are being met.
IT	IT Architecture	Serves as a mechanism for the Technology Management Committee to initiate and complete large-scale directives; provides direction on Board IT standards.
IT	Software Review Board	Reviews Software Approval Request forms; provides recommendations to the Technology Management Committee on approval or denial of new software.
Management	Executive Technology Change Control Board	Serves as the strategic oversight and approval body of technology assets for the Management Division and DFM.
Management	Management Change Control Board	Serves as the management oversight body to the technology product suite for the Management Division and DFM.
Federal Reserve System; used by the Division of Supervision and Regulation	Subcommittee on Data and Technology	Manages the priorities of their portfolios; collaborates to determine divisions' comprehensive technology strategy; works through competing priorities among portfolios.

Source. OIG analysis of Board group and committee charters.

Appendix C: Management's Response

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

DONALD V. HAMMOND
CHIEF OPERATING OFFICER

October 23, 2018

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 Information Technology Governance" prepared as part of your office's oversight responsibilities pursuant of the Federal Information Security Modernization Act of 2014 (FISMA). The review assessed whether the Board of Governors of the Federal Reserve System's (Board) current organizational structure and authorities support its information technology needs associated with security, privacy, capital planning, budgeting, and acquisition.

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: Ms. Sharon Mowry
Mr. Ricardo Aguilera
Mr. Peter Sheridan
Mr. Ray Romero
Mr. Charles Young

E-MAIL: DONALD.HAMMOND@FRB.GOV • TELEPHONE: 202-452-3660 • FACSIMILE: 202-728-5800

Abbreviations

Board	Board of Governors of the Federal Reserve System
BTSC	Business Technology Strategic Committee
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COO	Chief Operating Officer
CPO	Chief Privacy Officer
DFM	Division of Financial Management
Division of IT	Division of Information Technology
FISMA	Federal Information Security Modernization Act of 2014
FITARA	Federal Information Technology Acquisition Reform Act of 2014
IEC	International Electrotechnical Commission
IRB	Investment Review Board
ISO	International Organization for Standardization
IT	information technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
SIEM	security incident and event management

Report Contributors

Brent Melson, Senior OIG Manager
Andrew Gibson, OIG Manager
Jeffrey Woodward, Project Lead
Rebecca Kenyon, Senior IT Auditor
Morgan Fletcher, IT Auditor
Nick Gallegos, IT Auditor
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

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