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.