FEDERAL HOUSING FINANCE AGENCY

ADVISORY BULLETIN

AB 2015-06

INFORMATION TECHNOLOGY INVESTMENT MANAGEMENT

Purpose

This advisory bulletin provides Federal Housing Finance Agency (FHFA) guidance on information technology (IT) investment management by Fannie Mae and Freddie Mac (the Enterprises). FHFA expects that each Enterprise's IT investment management will include sound governance and effective monitoring and reporting that reflect relevant risk assessments of the Enterprise.

Background

The Enterprises' investments to maintain and improve their IT environments are critical to the success of business operations and strategic initiatives. Effective IT investment management contributes to safe and sound operations by enabling an Enterprise to confirm that IT investments are aligned with strategic priorities, support business operations, and deliver expected returns on investment. An effective process for funding IT projects should assist an Enterprise to assess costs and benefits of investments, manage interdependencies among related projects, identify risk exposures to third-party vendors, and plan the funding of multi-year projects over multiple budget cycles.

FHFA's standards for safe and sound operations are generally set forth in the Prudential Management and Operations Standards (PMOS) at 12 CFR Part 1236. In particular, PMOS Standard 1.4 (Internal Controls and Information Systems, Framework) articulates the requirement for an effective system of internal controls, which includes a board-approved organizational structure that clearly assigns responsibility, authority, and reporting relationships, as well as appropriate segregation of duties.

Guidance

FHFA expects that each Enterprise's IT investment management will include sound governance and effective monitoring and reporting that reflect relevant risk assessments of the Enterprise. An Enterprise may develop and refine its IT investment management based on sound industry practices, such as the Control Objectives for Information and Related Technology (COBIT) framework issued by the Information Systems Audit and Control Association (ISACA).

Governance

Each Enterprise should maintain sound governance over IT investments using a risk-based approach at both the portfolio level and at the project level to confirm that the Enterprise's IT investments are aligned with enterprise strategic priorities and line of business objectives. Governance should address funding of IT projects and prioritization of project funding based upon risk assessments for proposed investments, cost-benefit analyses, and requirements for diversity and inclusion practices in contracting, [1] among other factors.

The governance over IT investments should clearly define the roles and responsibilities of stakeholders, including the board of directors, business leads, and IT management. Delegations of authority should be established and subject to periodic review, and exceptions to delegated authority should be documented. The governance process should confirm that appropriate risk control functions have input into IT funding decisions at both project and portfolio levels.

Setting IT investment priorities is a key component of governance. Risk assessments should be performed for IT funding proposals to identify potential risks at the project and portfolio level. In addition, cost-benefit analyses should be conducted to inform the prioritization of IT investments and funding decisions.

Ensuring sustainability of IT investments is essential for mitigating risks such as operational disruptions, security lapses, or system degradation. Strong governance and oversight of IT investments should be designed to enable an Enterprise to ensure that its IT environment remains current and that IT investments are sustainable. Budgeting should include long-term IT investments over multiple budget cycles, not only for new projects, but also for ongoing maintenance such as routine service, periodic modification, equipment replacement, enhancement of security features, and patch management. Effective IT investment governance should also include a regular review function to monitor project management practices against established standards, practices, and internal controls.

[1] 12 CFR § 1207.21 requires that the Enterprises develop, implement, and maintain policies and procedures to ensure, to the maximum extent possible in balance with financially safe and sound business practices, the inclusion and utilization of minorities, women, individuals with disabilities, and minority-, women-, and disabled-owned businesses in procurement and all types of contracts.

Monitoring and Reporting

Each Enterprise should maintain a process for tracking IT investments and the performance of funded projects. Monitoring and reporting are essential tools for management to ensure timely identification of changes to project schedules or budgets and the opportunity to ensure that issues are addressed through appropriate governance mechanisms. Effective monitoring and reporting for IT investments should assist management in ensuring ongoing alignment of the IT project portfolio with strategic objectives and business operating plans, and in maintaining current information on budgets, timelines, and project interdependencies.

IT investment management requires periodic performance reporting that provides senior management and the board of directors with appropriate dashboards or similar reports to capture results for performance objectives. Such reports should inform decision-makers about the sustainability and viability of both existing and future projects.

Related Guidance

Guidance on Cyber Risk Management, Federal Housing Finance Agency Advisory Bulletin AB-2014-05, May 19, 2014.

Guidance on the Retirement of the Microsoft Windows XP Operating System, Federal Housing Finance Agency Advisory Bulletin AB-2014-04, March 20, 2014.

Operational Risk Management, Federal Housing Finance Agency Advisory Bulletin AB-2014-02, February 18, 2014.

Safety and Soundness Standards for Information, Office of Federal Housing Enterprise Oversight Policy Guidance PG-01-002, December 19, 2001.

Advisory Bulletins communicate guidance to FHFA supervision staff and the regulated entities on specific supervisory matters pertaining to the Federal Home Loan Banks, the Office of Finance, Fannie Mae, and Freddie Mac. This advisory bulletin is effective immediately upon issuance. Contact Bobbi Montoya, Associate Director, Examination Standards Branch at Bobbi.Montoya@fhfa.gov or (202) 649-3406, John McNicholas, Senior Examiner (Policy), Examination Standards Branch at John.McNicholas@fhfa.gov or (202) 649-3525, or Anne Paulin, Principal Risk Analyst, Risk Analysis Branch at Anne.Paulin@fhfa.gov or (202) 649-3421 with comments or questions pertaining to this bulletin.