Federal Retirement Thrift Investment Board (FRTIB)

Board Meeting

Audit of the Effectiveness of FRTIB's Information Security Program Under Federal Information Security Modernization Act (FISMA) of 2014

February 25, 2019

WILLIAMS ADLEY

Agenda

1. FISMA Audit Overview
2. How the FRTIB Was Measured
3. Audit Highlights
4. Root Causes
5. Recommendations

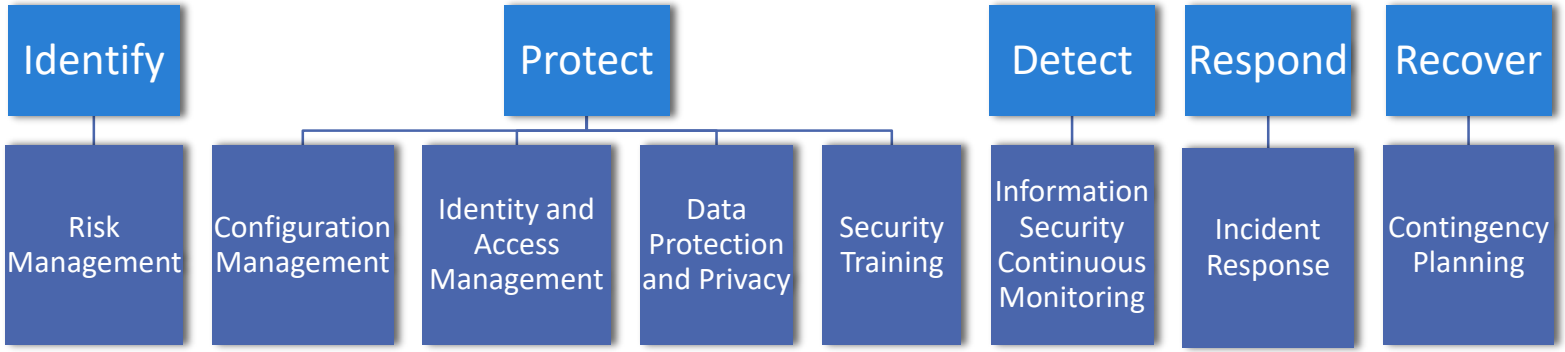
FISMA Audit Overview

- **Objective**
  - Determine the effectiveness of FRTIB's information security program.
- **Scope**
  - Agency-Level Controls
  - System-Specific Controls
- **Time Period**
  - October 1, 2017 –September 30, 2018

How the FRTIB Was Measured

FY 2018 Inspector General (IG) Reporting Metrics

- Align with the NIST Cybersecurity Framework for five function areas and eight underlying domains:



- The FY 2018 IG Reporting Metrics introduced the Data Protection and Privacy domain within the Protect Function.

How the FRTIB Was Measured

FY 2018 IG Maturity Model

- Each level must be satisfactory before advancing to next level

Maturity Level	Maturity Level Description
Level 1: Ad-Hoc	Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategies are formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess them and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Audit Highlights

- FRTIB has not fully developed and implemented an effective, organization-wide information security program and sufficiently implemented governance structures to ensure appropriate oversight and monitoring over information security.
- In early FY 2018, FRTIB began to focus on its security governance posture by initiating a comprehensive security assessment of all its systems to ensure information security risks are remediated and monitored.
- FRTIB undertook multiple projects to improve its information security posture during FY 2018. As a result, the maturity ratings of two FISMA domains improved from Level 1 (Ad-Hoc) to Level 2 (Defined) and the Data Protection and Privacy was rated at a Level 2 (Defined).
- FRTIB successfully closed 13 prior FISMA audit recommendations identified during the FY 2016 audit.

Audit Highlights

- The summary of the maturity levels for the applicable FISMA domains are detailed below:

FISMA Metric Domain	Maturity Model Rating
Risk management	Level 1 (Ad-Hoc)
Configuration management	**Level 2 (Defined)**
Identity and access management	**Level 2 (Defined)**
Data protection and privacy	**Level 2 (Defined)**
Security training	Level 1 (Ad-Hoc)
Information Security Continuous Monitoring	Level 1 (Ad-Hoc)
Incident response	Level 1 (Ad-Hoc)
Contingency planning	Level 1 (Ad-Hoc)

Root Causes

- FRTIB has not implemented an effective organization-wide information security program and governance structure because of:
  - Inconsistent execution of the Risk Management Framework;
  - Documented policies and procedures do not reflect current processes;
  - Updated processes are not mature enough to identify process improvements;
  - Responsibilities between FRTIB and its third party contractors are inadequately defined; and
  - Projects designed to improve information security posture are not complete.

Recommendations

- Perform a comprehensive review of the processes supporting the agency's assessment and authorization program.
- Update existing governing documents to ensure they are consistent with FRTIB's current process for privacy threshold analyses, privacy impact assessments, and incident response reporting and tracking.
- Develop and implement a process to ensure that all individuals with significant security responsibilities receive required specialized training before gaining access to information systems or before performing assigned duties.
- Develop ISCM strategy and its supporting policies and procedures.

Thank you.

Questions?