Federal Retirement Thrift Investment Board (FRTIB)

Board Meeting

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

February 26, 2018

WILLIAMS ADLEY

Agenda

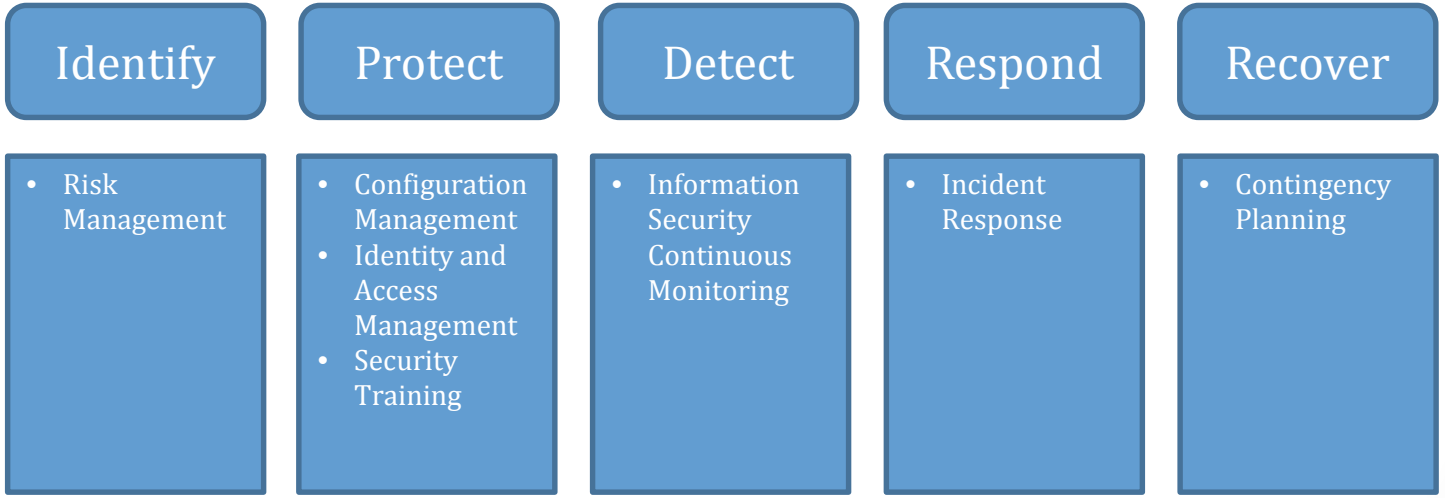
1. Federal Information Security Modernization Act of 2014 (FISMA) Audit Overview
2. How the Federal Retirement Thrift Investment Board (FRTIB) Was Measured
3. Audit Results
4. Root Causes
5. Recommendations

FISMA Audit Overview

- **Objective:** Determine the effectiveness of FRTIB's information security program.
- **Scope:**
  - Agency Level Controls
  - System Specific Controls
- **Time Period:**
  - October 1, 2016 – September 30, 2017

How the FRTIB Was Measured

- **Fiscal Year (FY) 2017 Inspector General (IG) Reporting Metrics:**
  - Aligns with the five National Institute of Standards and Technology (NIST) Cybersecurity Framework functions and the seven underlying domains:



  - Changes from the FY 2016 IG Reporting Metrics include a focus on how controls are effectively implemented throughout the fiscal year, instead of a point in time assessment.

How the FRTIB Was Measured

- **FY 2017 IG Maturity Model:**
  - Five levels
  - Each level must be satisfactory before advancing to next level

Level	Description
Level 1: Ad-Hoc	Policies, procedures, and strategy are not formalized; activities are performed in an Ad-Hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategy are formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategy 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 strategy are collected across the organization and used to assess them and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Audit Results[1]

- FRTIB has not fully developed and implemented an effective organization-wide information security program.
- Williams Adley identified a number of control deficiencies related to people, process, and technology across all seven IG FISMA metric domains.
- Williams Adley has concluded that the appropriate maturity level for each of the seven FISMA domains is Ad-Hoc.

[1] Please refer to our report dated October 31, 2017, for additional information.

Root Causes

- Williams Adley believes that FRTIB has not implemented an effective organization-wide information security program due to the following reasons:
  - Ad-Hoc and control-driven information security processes;
  - Inadequately defined responsibilities between FRTIB and its third party contractors;
  - Inappropriate oversight over third party contractors;
  - Misaligned efforts to focus on addressing symptoms and not sufficiently analyzing root causes of previously-identified information security weaknesses; and
  - Consistent turnover in key management positions.

Recommendations

- Williams Adley made two overarching recommendations to improve FRTIB's information security program, as summarized below:
  - *Recommendation 1:*
    - FRTIB should clearly define an organization-wide risk-based information security program that is tailored to FRTIB's information technology (IT) environment and information security risks.
  - *Recommendation 2:*
    - FRTIB should reevaluate its existing governance structures to ensure appropriate oversight and monitoring over its information security program.