# Federal Retirement Thrift Investment Board (FRTIB)

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

February 24, 2020

WILLIAMS
ADLEY

# Agenda

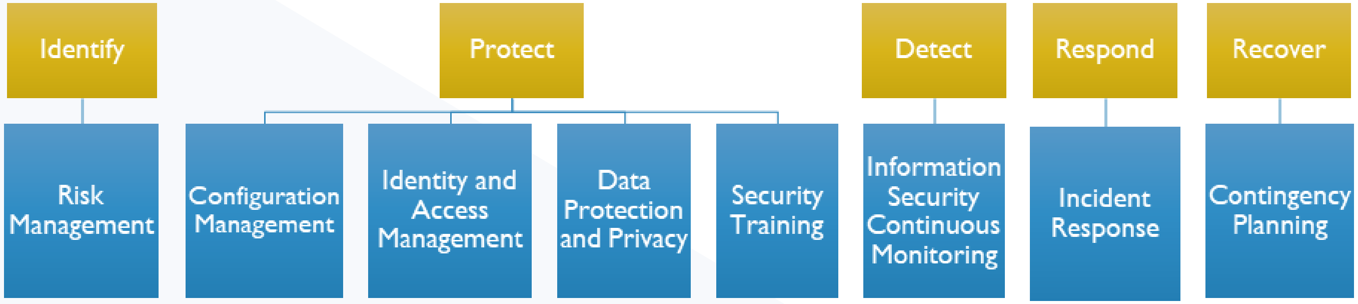
- FISMA Audit Overview
- How the FRTIB Was Measured
- Audit Highlights
- Root Causes
- Recommendations

# FISMA Audit Overview

- Objective
  - Determine the effectiveness of FRTIB’s information security program.
- Scope
  - Agency-Level Controls
  - System-Specific Controls
- Time Period
  - October 1, 2018 - September 30, 2019

# How the FRTIB Was Measured

- FY 2019 Inspector General (IG) Reporting Metrics*
  - Align with the NIST Cybersecurity Framework for five function areas and eight underlying domains:



Identify
- Risk Management

Protect
- Configuration Management
- Identity and Access Management
- Data Protection and Privacy
- Security Training

Detect
- Information Security Continuous Monitoring

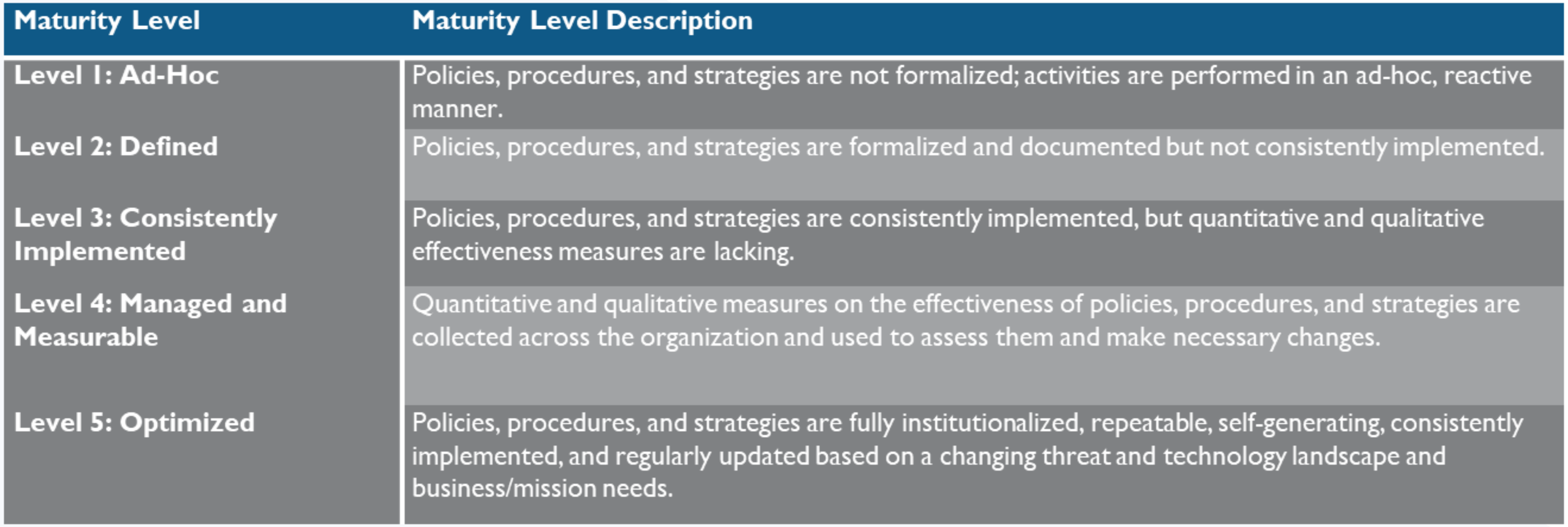
Respond
- Incident Response

Recover
- Contingency Planning

  - The FY 2019 IG Reporting Metrics introduced additional maturity indicators regarding the evaluation of an agency’s High Value Asset (HVA) programs.

# How the FRTIB Was Measured

- FY 2019 IG Maturity Model
  - Each level must be satisfactory before advancing to next level
  - Each of the eight domains must be at level 4 for the information security program to be considered "effective."



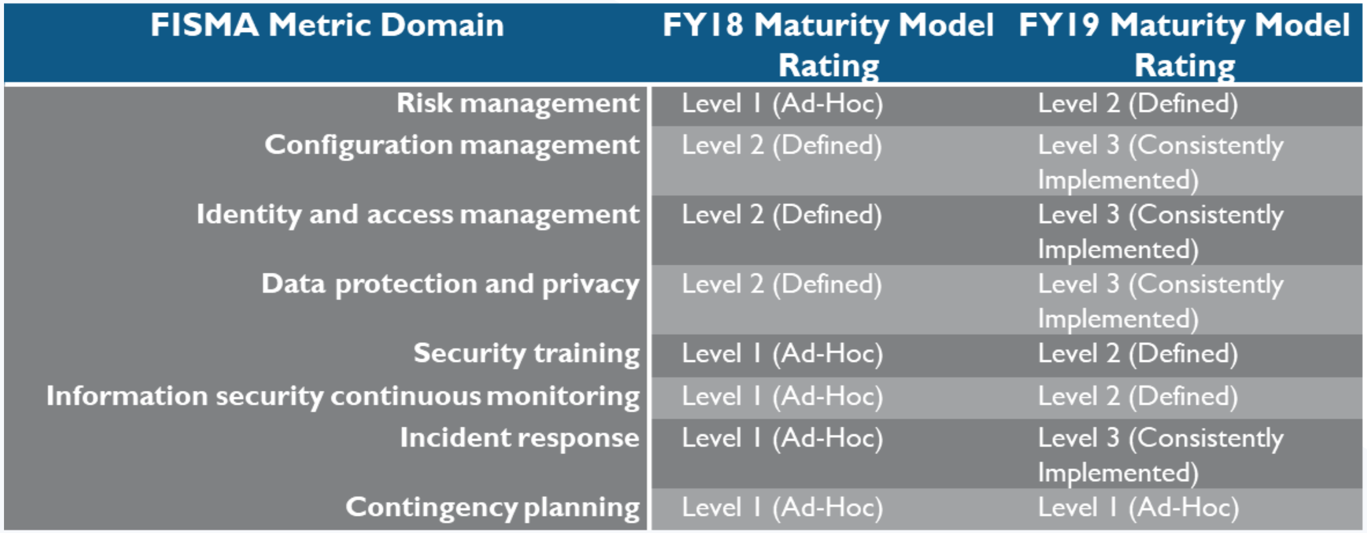
| Maturity Level | Maturity Level Description |
|---|---|
| Level 1: Ad-Hoc | Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner. |
| Level 2: Defined | Policies, procedures, and strategies are formalized and documented but not consistently 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 made marked improvements to its information security program through the:
  - Development of strategic and governing documents
  - Implementation of control activities defined in the prior year
- Seven (7) FISMA metric domains improved one (1) maturity level or more:
  - Three (3) domains improved from Level 1 to Level 2
  - Three (3) domains improved from Level 2 to Level 3
  - One (1) domain improved from Level 1 to Level 3

# Audit Highlights

- FRTIB has not fully developed and implemented an effective, organization-wide information security program due to reoccurring or unresolved issues
- The summary of the maturity levels for the applicable FISMA domains are detailed below:



| FISMA Metric Domain | FY18 Maturity Model Rating | FY19 Maturity Model Rating |
|---|---|---|
| Risk management | Level 1 (Ad-Hoc) | Level 2 (Defined) |
| Configuration management | Level 2 (Defined) | Level 3 (Consistently Implemented) |
| Identity and access management | Level 2 (Defined) | Level 3 (Consistently Implemented) |
| Data protection and privacy | Level 2 (Defined) | Level 3 (Consistently Implemented) |
| Security training | Level 1 (Ad-Hoc) | Level 2 (Defined) |
| Information security continuous monitoring | Level 1 (Ad-Hoc) | Level 2 (Defined) |
| Incident response | Level 1 (Ad-Hoc) | Level 3 (Consistently Implemented) |
| Contingency planning | Level 1 (Ad-Hoc) | Level 1 (Ad-Hoc) |

# Root Causes

- FRTIB has not completely implemented an effective organization-wide information security program and governance structures due to the following reasons:
  - Inconsistent implementation of established processes and commitment to plans to implement the Risk Management Framework;
  - Conflicting priorities resulting in a lack of resources to support information security initiatives; and
  - Undefined metrics and performance measures to support the continuous improvement of the agency’s information security program.

# Recommendations

- ***Recommendation 1:*** Follow documented A&A policies and procedures to support consistent, informed, and timely authorization decisions and ensure security and privacy requirements/controls are implemented to support FRTIB’s enterprise and information security architectures.
- ***Recommendation 2:*** Establish metrics and performance measures to evaluate the effectiveness of information security policies and procedures, and processes to collect data, analyze results, and develop corrective actions.

# Recommendations

- ***Recommendation 3:*** Define an information system contingency planning program by developing a strategy and supporting policies and procedures which adhere to NIST requirements. Furthermore, update existing BIAs and ISCPs to reflect changes made within the most recent agency level BIA.

Thank you.

Questions?