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

Board Meeting
February 23, 2021

Agenda

- Objective and Scope
- Audit Results Overview
- Evaluation Method
- Domain Ratings
- Root Causes
- Recommendations
- Next Steps

Objective and Scope

- Determine the effectiveness of FRTIB's information security program for Fiscal Year 2020 (October 1, 2019 – September 30, 2020)
- Assess management's remediation effort to address prior year recommendations
- Evaluate a combination of entity wide and system specific controls with a particular focus on three of FRTIB's information systems:
  - Financial and Reconciliation Services (FRS)
  - FRTIB Domain General Support System (GSS)
  - Identity, Credential, and Access Management (ICAM)

Audit Results Overview

- FRTIB has made significant improvements to its information security governance structure and implementation of the risk management framework resulting in an effective organization-wide information security program in FY 2020
- FRTIB’s information security program achieved a Level 4 (Managed and Measurable) maturity rating in seven (7) of eight (8) FISMA domains

Evaluation Method

FY 2020 Inspector General (IG) Reporting Metrics

- Align with the NIST Cybersecurity Framework for five function areas and eight underlying domains
- Ratings throughout the eight domains will be determined by a simple majority, where the most frequent level (i.e., the mode) across the questions will serve as the domain rating

FISMA Maturity Model

- Foundational levels ensure that agencies develop sound policies and procedures, and the advanced levels capture the extent that agencies institutionalize those policies and procedures

Evaluation Method – FISMA Functions

Identify

- Risk Management

Protect

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

Detect

- Information Security Continuous Monitoring

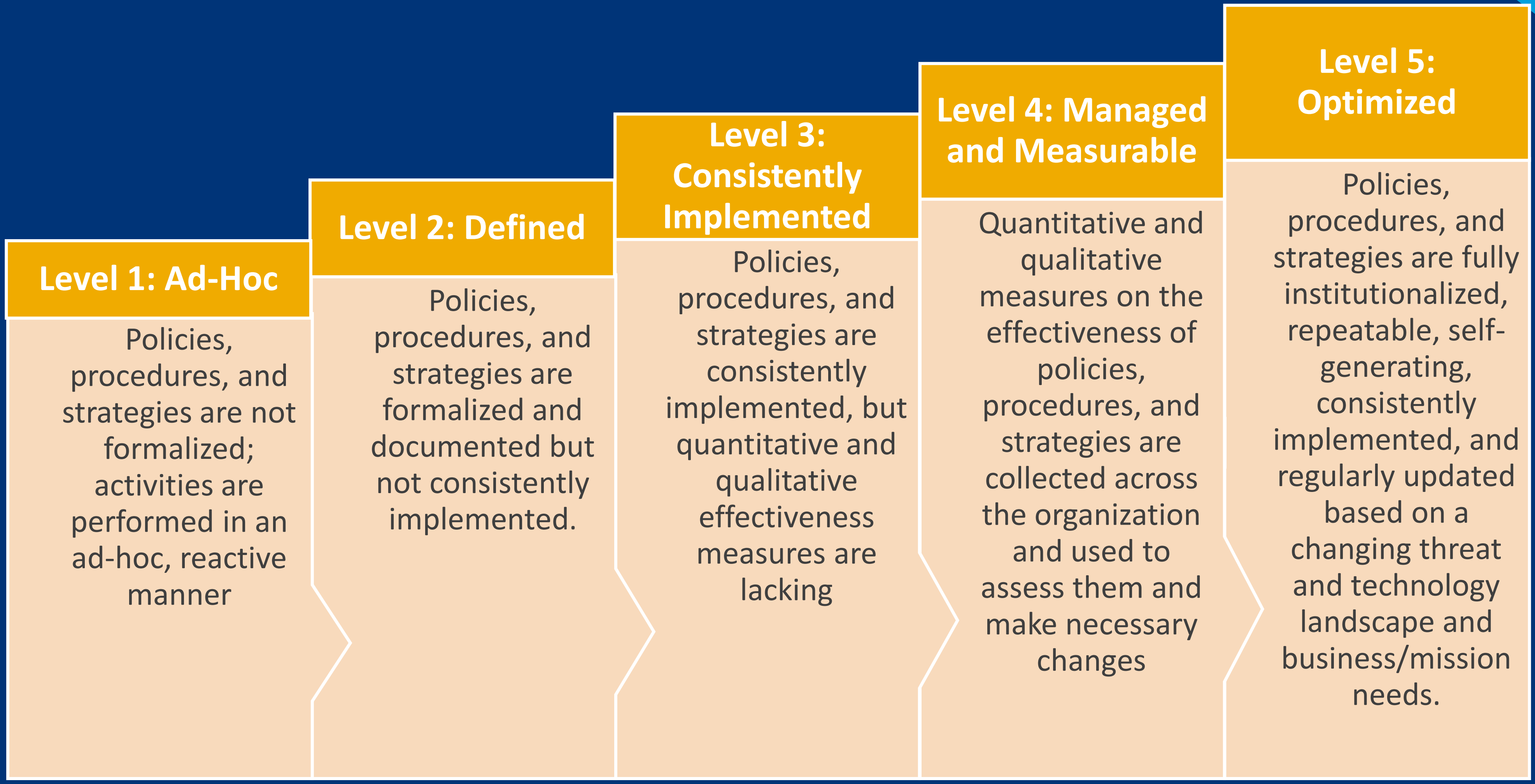
Respond

- Incident Response

Recover

- Contingency Planning

Evaluation Method – Maturity Model



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

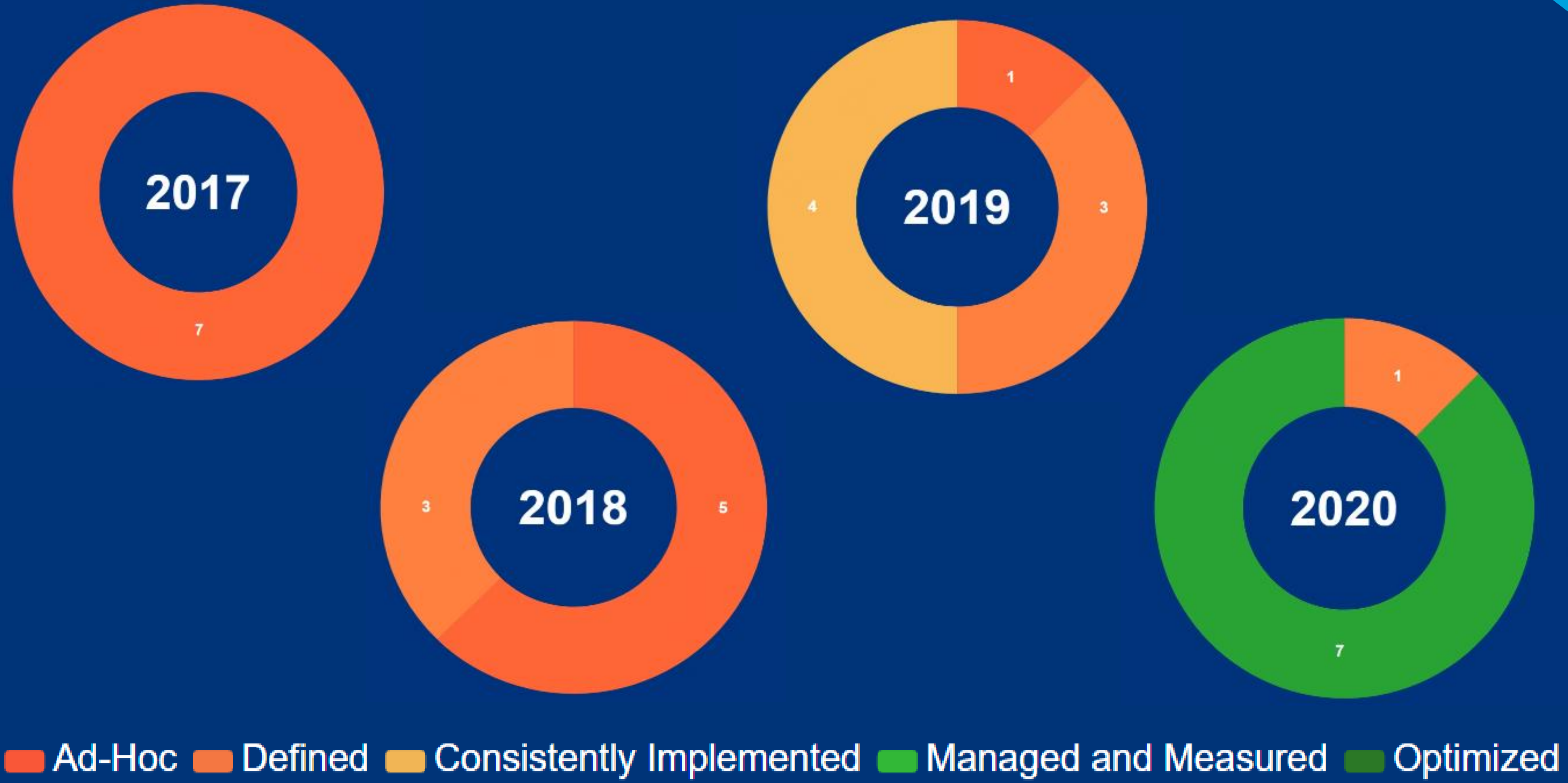
Level 5: Optimized

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.

Domain Ratings – Year to Date

FISMA Function	FISMA Domains	FY 2019 Rating	FY 2020 Rating
Identify	Risk Management	Level 2	Level 4
Protect	Configuration Management	Level 3	Level 4
Protect	Identity and Access Management	Level 3	Level 4
Protect	Data Protection and Privacy	Level 3	Level 4
Protect	Security Training	Level 2	Level 4
Detect	ISCM	Level 2	Level 4
Respond	Incident Response	Level 3	Level 4
Recover	Contingency Planning	Level 1	Level 2

Domain Ratings – FY 2017 to FY 2020



Root Causes

- Williams Adley believes that the conditions identified as a part of the FY 2020 FISMA are due to the following reasons:
  - Plan of Action and Milestones (POA&M) are not yet tracked and managed within Telos Xacta to support FRTIB's POA&M process because the agency needs to reconcile its legacy POA&Ms to eliminate similar or duplicate entries
  - FRTIB has not defined the method(s) to obtain data supporting account recertification and metrics analysis activities in a manner which ensures their accuracy, completeness, and consistency
  - Human error during the performance of defined processes

Recommendations

- Williams Adley provides the following recommendations:
  - *Recommendation 1:* Update and reconcile legacy POA&Ms prior to their migration into Telos Xacta to ensure that all required fields are complete and duplicate POA&Ms are eliminated
  - *Recommendation 2:* Define the process to obtain data supporting account recertification and metrics analysis activities in a manner which ensures their accuracy, completeness, and consistency

Next Steps

- Evaluate the implementation of FRTIB's information security program across the remaining systems and any newly introduced systems
- Evaluate the improvements made to address outstanding recommendations and reporting metrics which didn't reach Level 4, where applicable

THANK YOU!

Williams Adley

Phone

(202) 371-1397

Website

https://www.williamsadley.com