FRTIB

CISO BOARD BRIEFING

PRESENTED BY

PATRICK BEVILL

CHIEF INFORMATION SECURITY OFFICER

February 24, 2020

Thrift Savings Plan

FEDERAL RETIREMENT THRIFT INVESTMENT BOARD
tsp.gov

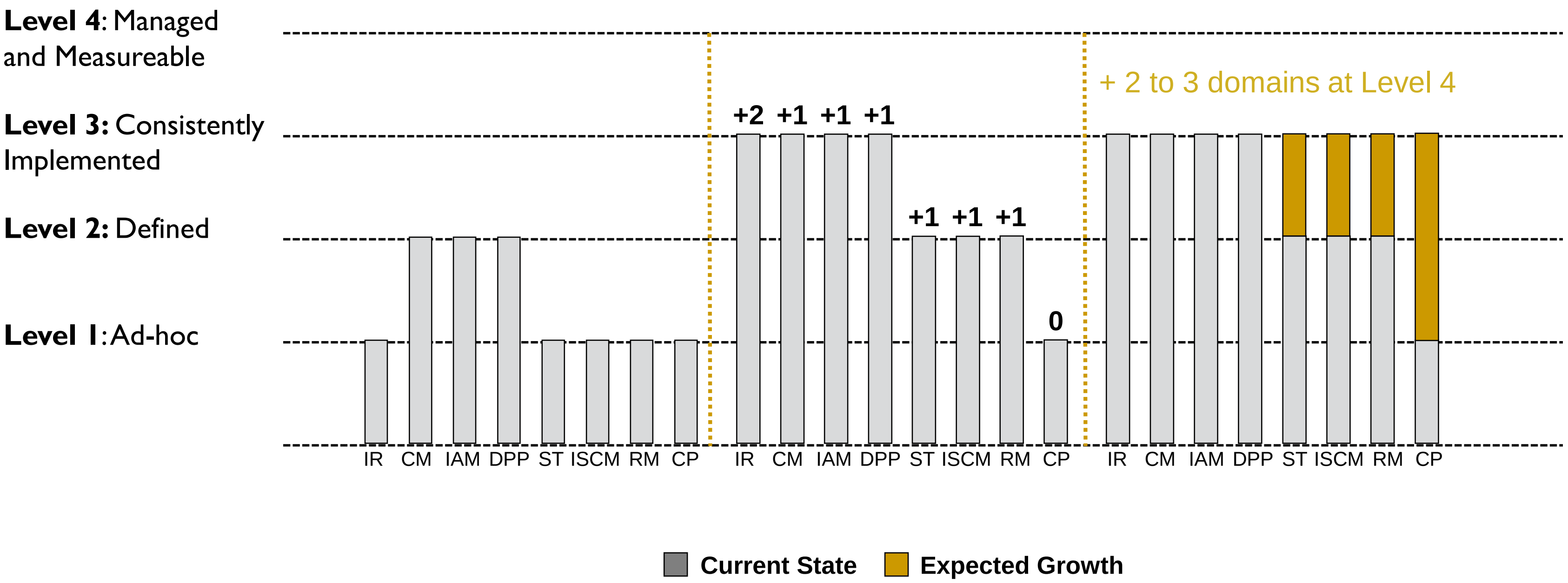
tsp4gov @

Agenda

Topic	Slide
Current and Target State Ratings	**3**
Williams Adley Recommendations & FRIB Response	**4-6**

Current State 2019 & Target State 2020

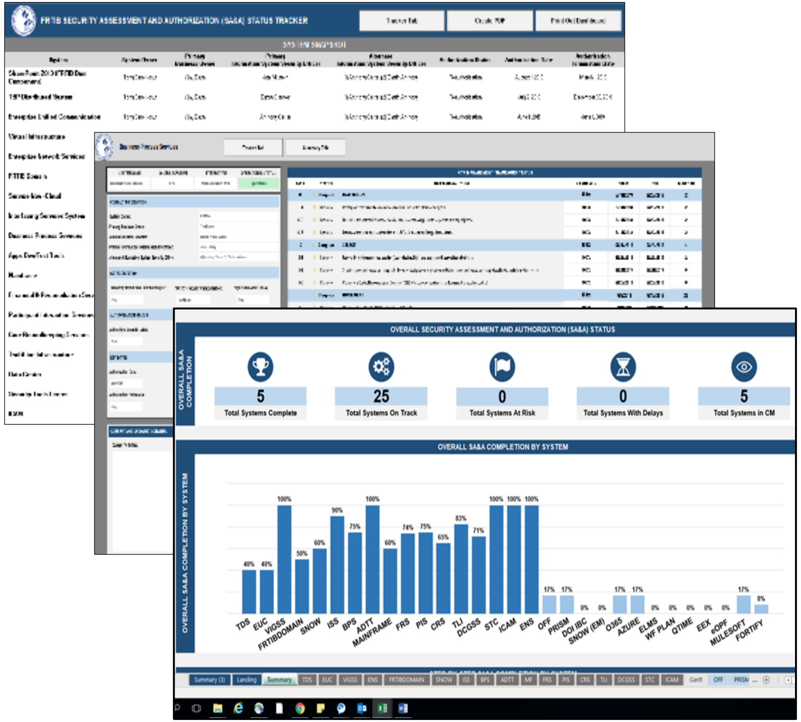
The below table outlines the audit results for the FY19 FISMA Audit.



* Based on current FISMA construct; if new questions or domains are added, the outcomes are subject to revision.

#1 **Security Assessment and Authorization (SA&A) Policies and Procedures:** Risk Management Framework (RMF) and SA&A Tracker

- FRTIB leverages the RMF to align itself to NIST guidance, which provides a standardized and repeatable process for authorizing Agency systems
    - This framework serves as a guide and is flexible enough to ensure the agency is managing risk and maintaining business agility, while also complying with standards and guidance
- Continued use of SA&A Tracker as overarching governance tool for executive level reporting, maintaining high levels of management insight into status



FRTIB SECURITY ASSESSMENT AND AUTHORIZATION (SA&A) STATUS TRACKER

SYSTEM SNAPSHOT

OVERALL SECURITY ASSESSMENT AND AUTHORIZATION (SA&A) STATUS

OVERALL SA&A COMPLETION

5	25	0	0	5
Total Systems Complete	Total Systems On Track	Total Systems At Risk	Total Systems With Delays	Total Systems in CM

OVERALL SA&A COMPLETION BY SYSTEM

#2 Information Security Performance Measures: Process Health Measurement Project

- Initiative is designed to validate FRTIB security processes are performing within acceptable ranges.
- Nearly completed an analysis of “Level 4 – Managed and Measurable” characteristics to develop performance measurement criteria
- As FRTIB security capabilities mature, processes will be refined and yield real-time data insights to defend against security risks

Project Objectives

1 **Develop Performance Management Function**

Develop an internal function to assess quality of FRTIB processes and improve operational performance

2 **Collect and Operationalize Data**

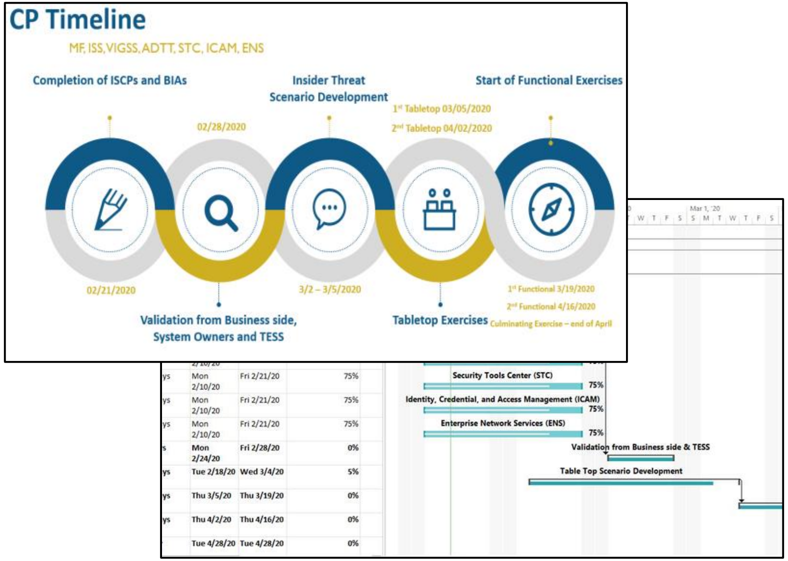
Develop a method to continuously collect and operationalize data analysis and dissemination

3 **Drive Continuous Process Improvement with Data**

Feed data into “lessons learned” for ongoing process and metrics refinement

#3 Contingency Planning Program: Planning and Testing Refresh

- FRTIB plans to have complete ISCPs & supporting BIAs for all current operational systems by the end of FY 2020.
- FRTIB will execute tabletop exercises, functional exercises, and tests for critical systems during April 2020
- In addition, a data center failover exercise is planned for September 2020
- Lessons learned will drive improvements to maturity rating in Contingency Planning domain



CP Timeline

MF, ISS, VIGSS, ADTT, STC, ICAM, ENS

Completion of ISCPs and BIAs

02/21/2020

02/28/2020

Validation from Business side, System Owners and TESS

Insider Threat Scenario Development

3/2 – 3/5/2020

1st Tabletop 03/05/2020

2nd Tabletop 04/02/2020

Tabletop Exercises

Start of Functional Exercises

1st Functional 3/19/2020

2nd Functional 4/16/2020

Culminating Exercise – end of April

ys	Mon 2/10/20	Fri 2/21/20	75%
ys	Mon 2/10/20	Fri 2/21/20	75%
ys	Mon 2/10/20	Fri 2/21/20	75%
s	Mon 2/24/20	Fri 2/28/20	0%
ys	Tue 2/18/20	Wed 3/4/20	5%
ys	Thu 3/5/20	Thu 3/19/20	0%
ys	Thu 4/2/20	Thu 4/16/20	0%
	Tue 4/28/20	Tue 4/28/20	0%

Mar 1, '20
W T F S S M T W T F S
Security Tools Center (STC)
75%
Identity, Credential, and Access Management (ICAM)
75%
Enterprise Network Services (ENS)
75%
Validation from Business side & TESS
Table Top Scenario Development

BIA = Business Impact Analysis ISCP = Information System Contingency Plan