Audit of the Effectiveness of Federal Retirement Thrift Investment Board (FRTIB)'s Information Security Program under Federal Information Security Modernization Act (FISMA) of 2014 Fiscal Year (FY) 2023

Board Meeting
August 22, 2023

Agenda

- Objective and Scope
- Evaluation Method
- Audit Results
- Status of Prior Years' Recommendations
- Recommendations
- Appendix A: FY 2023 Domain Ratings

Objective and Scope

- Determine the effectiveness of FRTIB’s information security program for FY 2023 reporting period (October 1, 2022 – June 30, 2023)
- Evaluate the design and implementation of entity wide and system specific controls with a particular focus on Converge
- Review the corrective actions taken by FRTIB to address previously issued recommendations

Evaluation Method

FY 2023 Inspector General (IG) Reporting Metrics

- Foundational levels ensure that agencies develop sound policies and procedures, and the advanced levels capture the extent that agencies institutionalize those policies and procedures
- Used to gauge the maturity of agency practices in connection with the nine (9) IG FISMA metric domains that are organized around the five (5) information security functions outlined in the Cybersecurity Framework

Evaluation Method

M-23-03 - Memorandum for the Heads of Executive Departments and Agencies: FY 2023 Guidance on Federal Information Security and Privacy Management Requirements

- Core Metrics – assessed annually and represent a combination of Administration priorities, high impact security processes, and essential functions necessary to determine security program effectiveness
- Supplemental Metrics – assessed at least once every two years and represent important activities conducted by security programs and contribute to the overall evaluation and determination of security program effectiveness

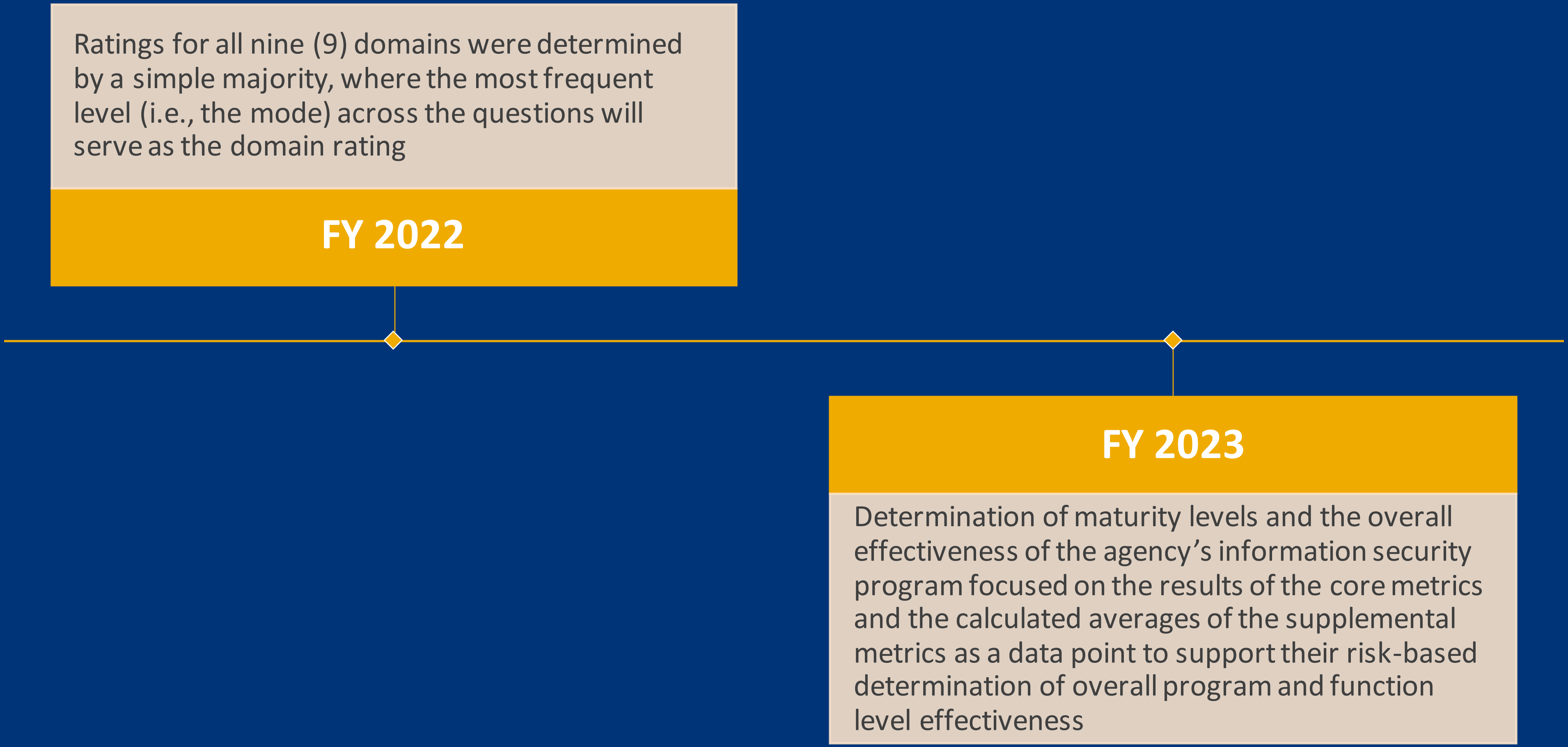
Evaluation Method

- FY 2022: 20 Core Inspector General (IG) FISMA Reporting Metrics
- FY 2023: 20 Core + 20 Supplemental IG FISMA Reporting Metrics

Identify	Protect	Detect	Respond	Recover
• Risk Management (1, 2, 3, 5, 7, 8, 9, 10) • Supply Chain Risk Management (12, 13, 14)	• Configuration Management (19, 20, 21, 22, 24) • Identity and Access Management (26, 27, 29, 30, 31, 32, 33) • Data Protection and Privacy (35, 36, 37) • Security Training (41, 42, 43)	• Information Security Continuous Monitoring (47, 48, 49)	• Incident Response (54, 55, 57, 58)	• Contingency Planning (60, 61, 63, 65)

Evaluation Method

Scoring Methodology



Ratings for all nine (9) domains were determined by a simple majority, where the most frequent level (i.e., the mode) across the questions will serve as the domain rating

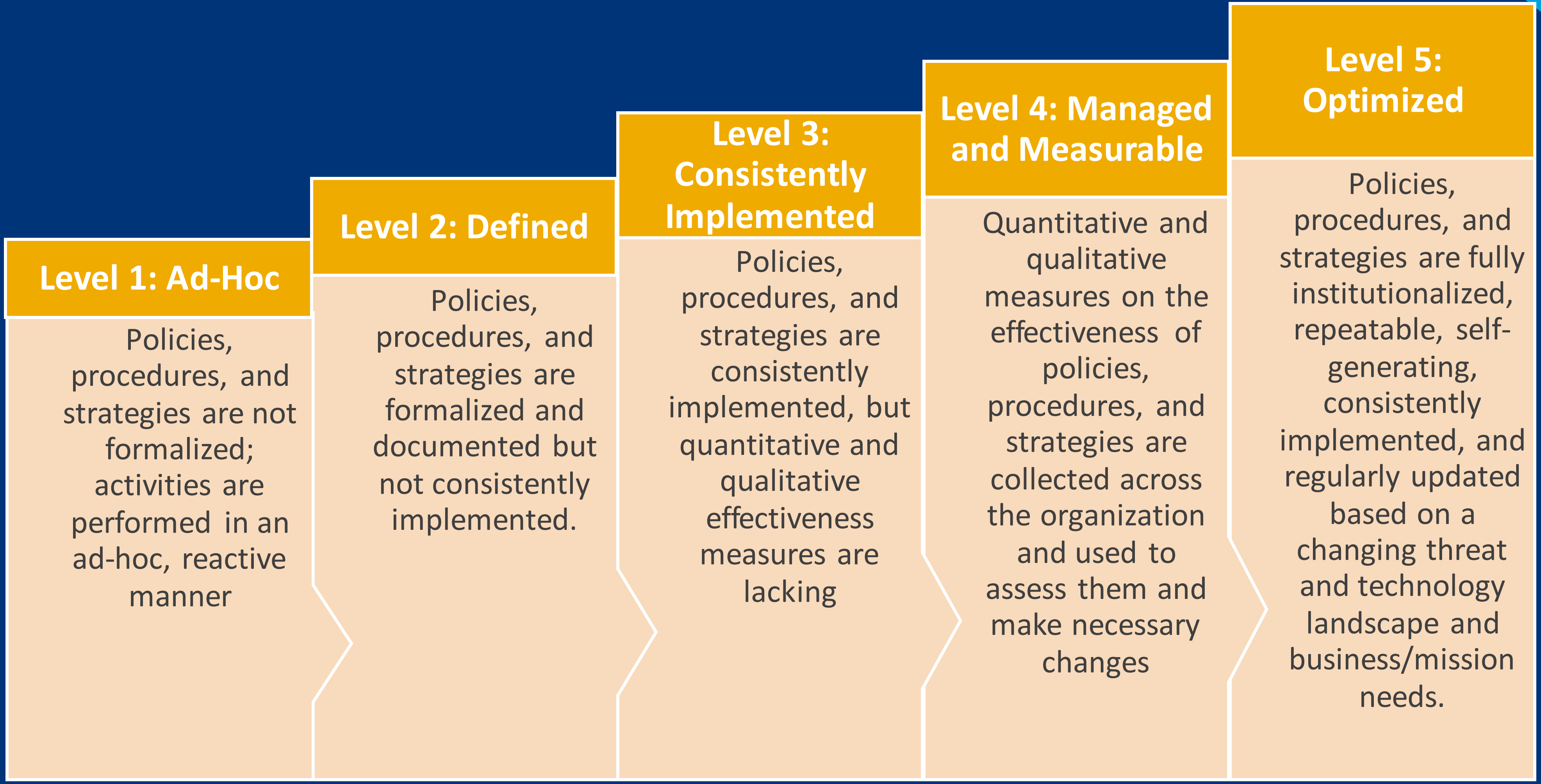
FY 2022

FY 2023

Determination of maturity levels and the overall effectiveness of the agency’s information security program focused on the results of the core metrics and the calculated averages of the supplemental metrics as a data point to support their risk-based determination of overall program and function level effectiveness

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.

Audit Results - Overview

- Effective information security program
- Six (6) FISMA domains maintained their maturity ratings
- Three (3) FISMA domains improved their maturity ratings
- One (1) previously issued recommendation remains open
- One (1) individual condition was identified
- No recommendations issued due to the nature of the condition

Audit Results – Overall Domain Ratings

FISMA Function	FISMA Domain	FY 2022 Rating	FY 2023 Rating
Identify	Risk Management	Level 4	Level 4
Identify	Supply Chain Risk Management	Level 1	Level 4
Protect	Configuration Management	Level 4	Level 4
Protect	Identity and Access Management	Level 4	Level 5
Protect	Data Protection and Privacy	Level 4	Level 4
Protect	Security Training	Level 4	Level 4
Detect	ISCM	Level 4	Level 5
Respond	Incident Response	Level 4	Level 5
Recover	Contingency Planning	Level 4	Level 4

Audit Results – Domain Highlights

Identity and Access Management

- Automation to support the completion and review of end user access agreements on a real time basis
- Implementation of a centralized enterprise-wide authentication solution, Octa
- Progress towards implementing EL3's advanced requirements for user behavior monitoring

Information Security Continuous Monitoring

- Integration of ISCM program with the activities outlined within its supply chain risk management, configuration management, incident response, and business continuity programs

Incident Response

- Progress towards implementing EL3's advanced requirements for its logging capabilities
- Implementation of Splunk as a Security Information and Event Management (SIEM) tool for event logging, log retention, and log management

Status of Prior Years’ Recommendations

One (1) prior year recommendation remains open at the conclusion of the FY 2023 FISMA Audit

- Develop a standard data elements/taxonomy to maintain a complete and accurate population of data breaches (FY 2021)*

*This recommendation was issued to FRTIB in FY 2021 to support FISMA reporting metric 38. However, FISMA reporting metric 38 was not selected as a Core or Supplemental FISMA metric for the FY 2023 FISMA evaluation.

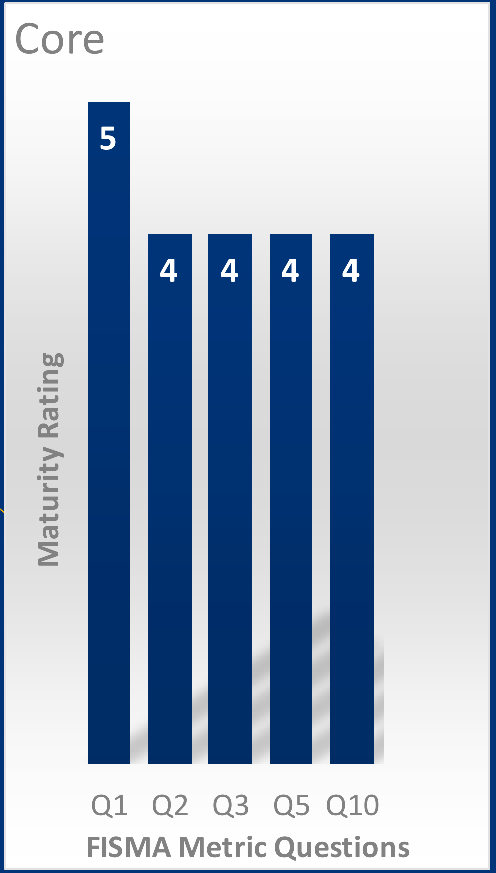
Recommendations

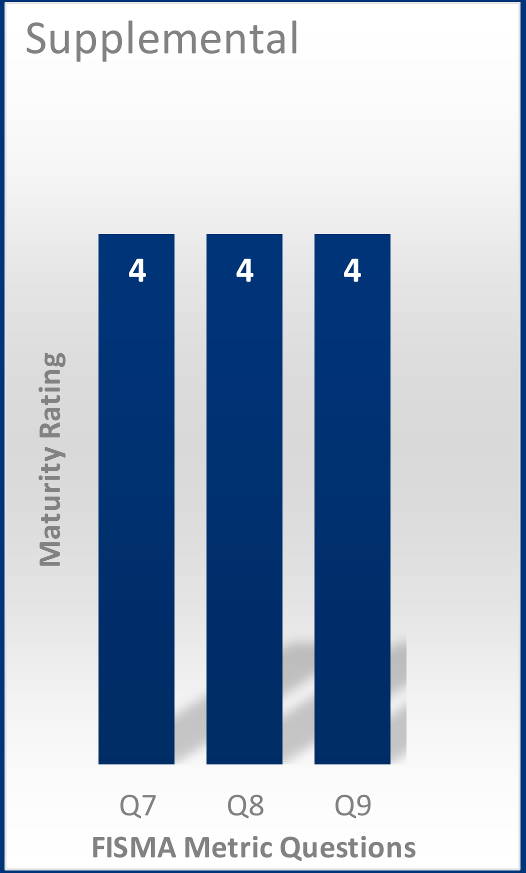
- No recommendations were issued due to the nature of the conditions and pre-existing recommendations.

Appendix A:

FY 2023 Domain Ratings

Risk Management

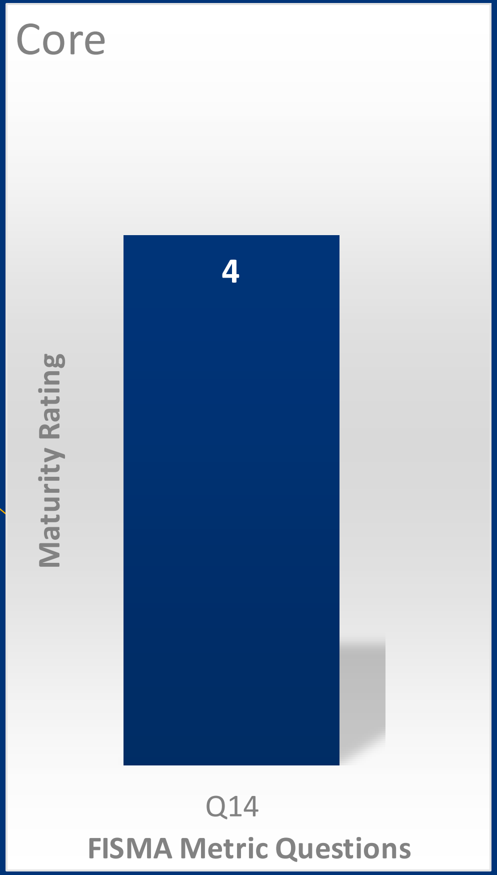


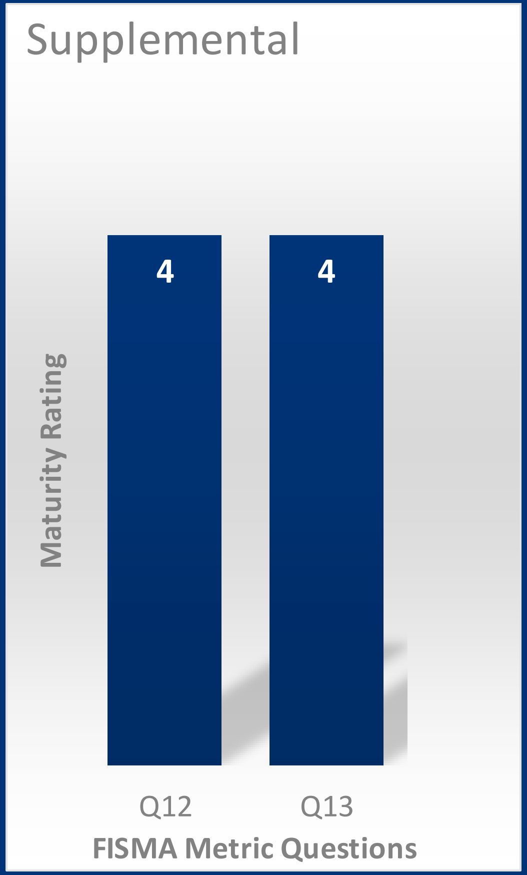


Conditions Identified:

- None

Supply Chain Risk Management

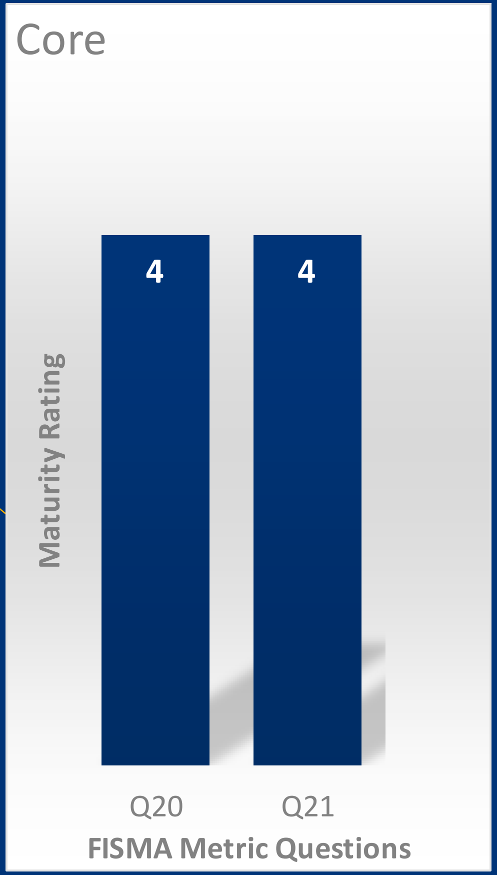


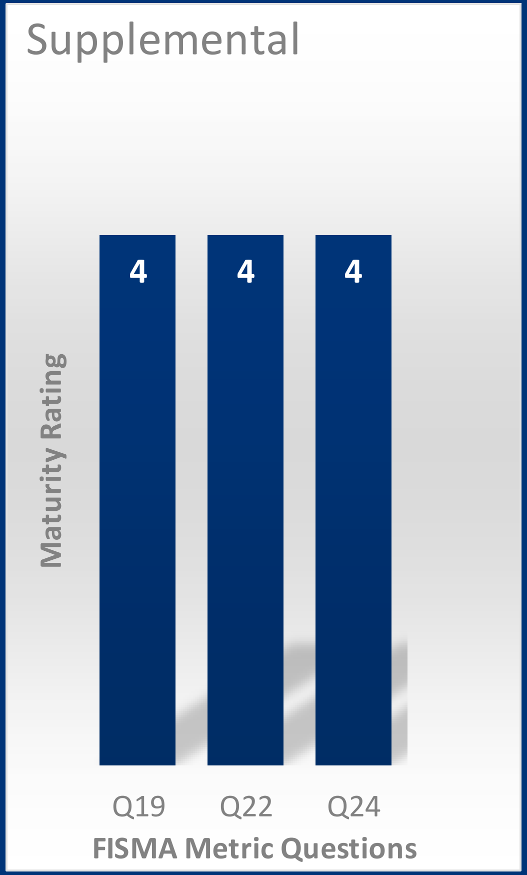


Conditions Identified:

- None

Configuration Management

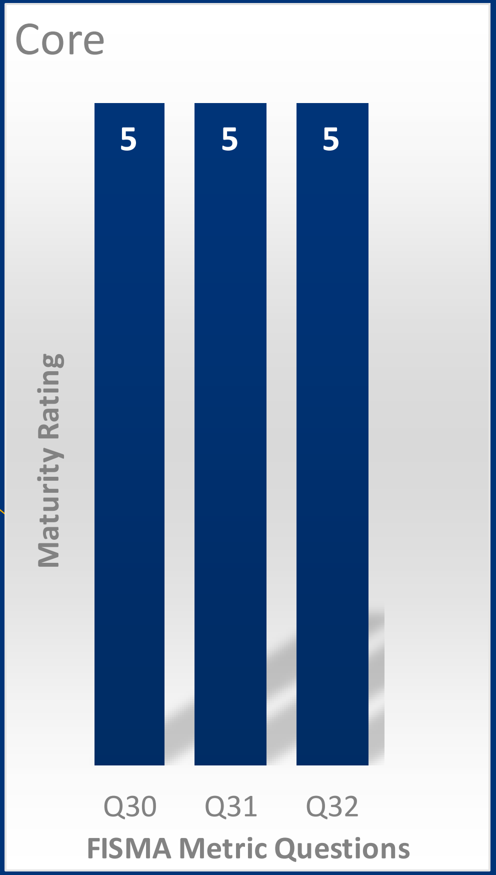


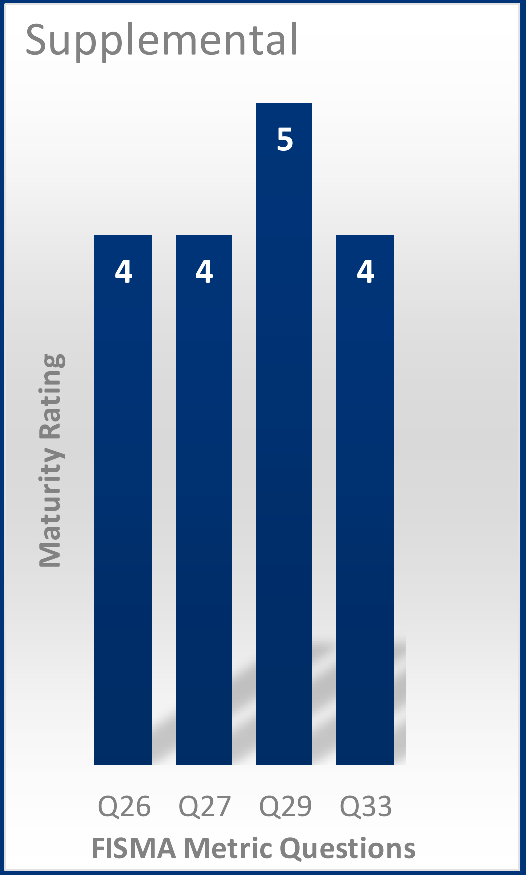


Conditions Identified:

- None

Identity & Access Management

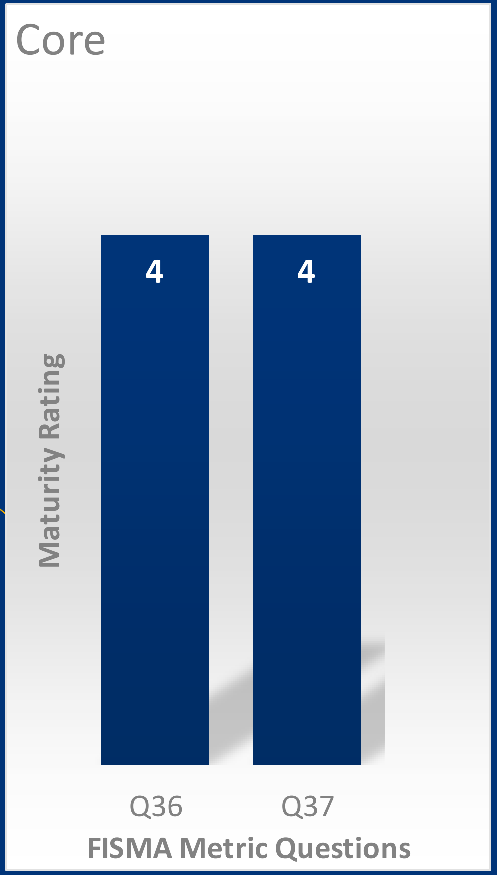


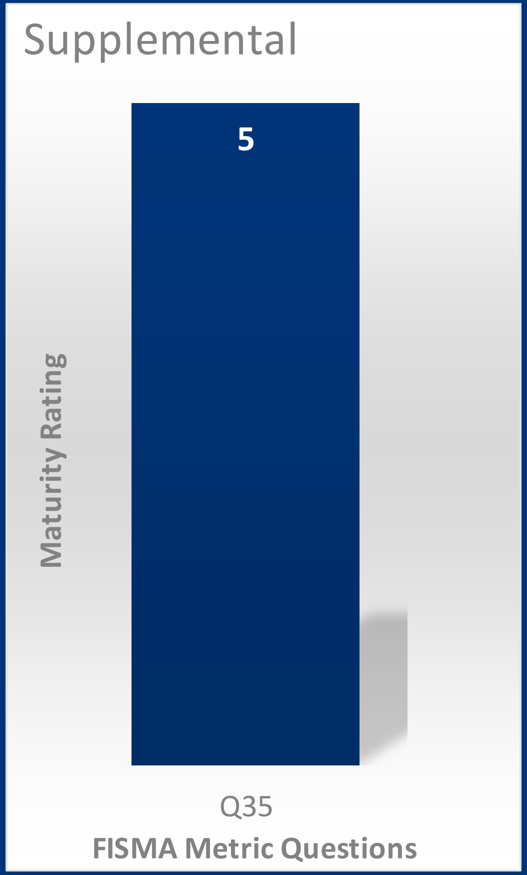


Conditions Identified:

- None

Data Protection & Privacy

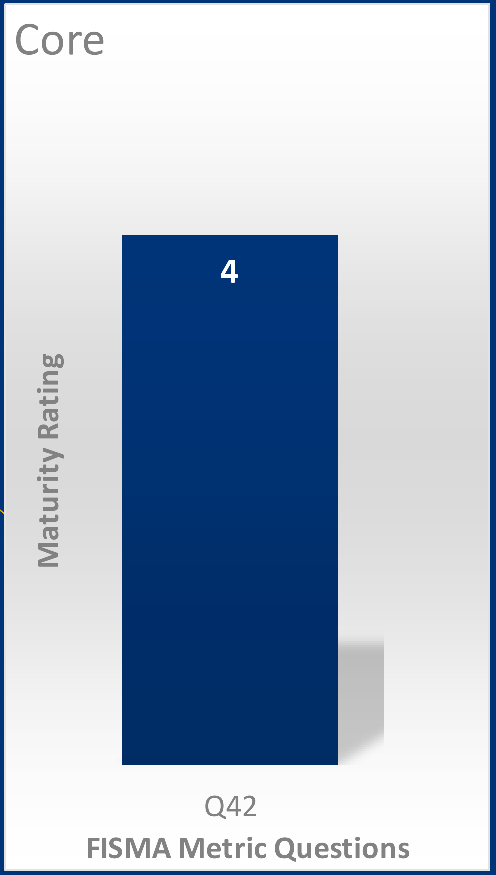


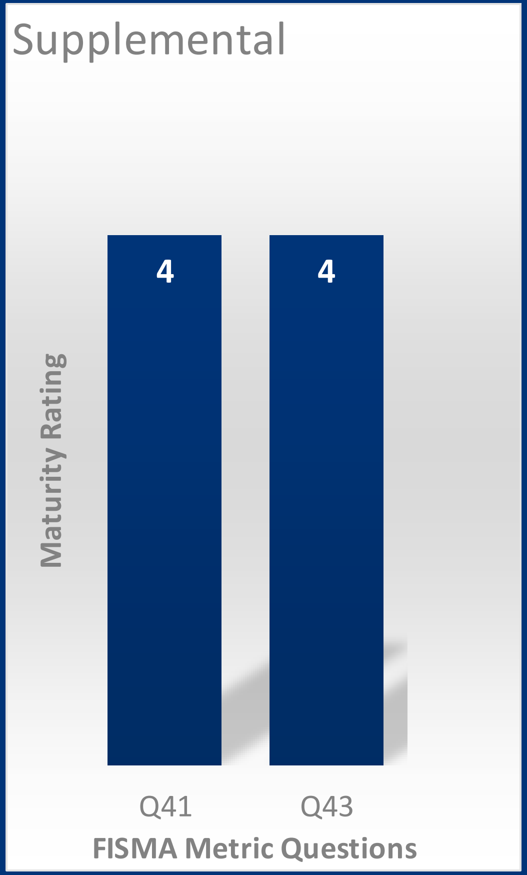


Conditions Identified:

- None

Security Training

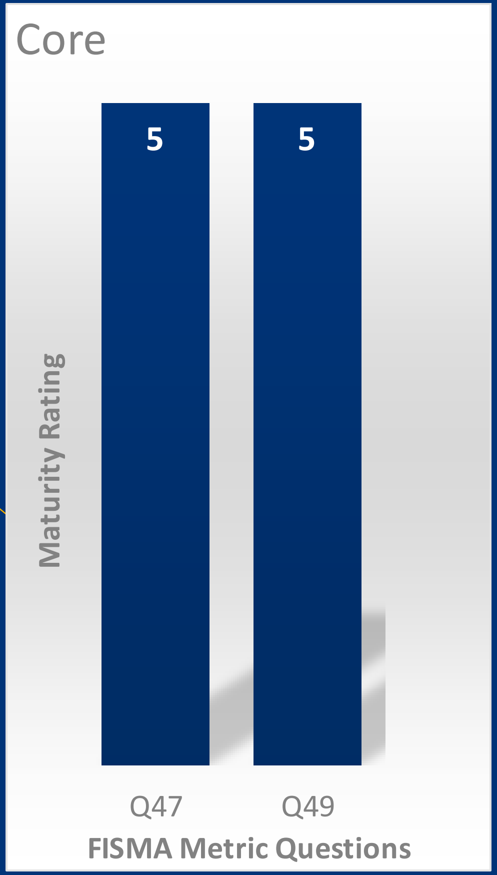

Core

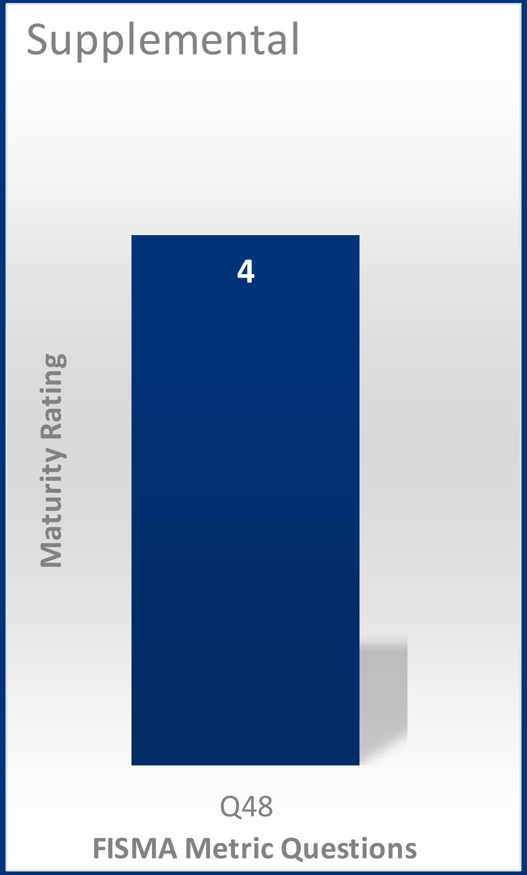

Supplemental

Conditions Identified:

- None

ISCM

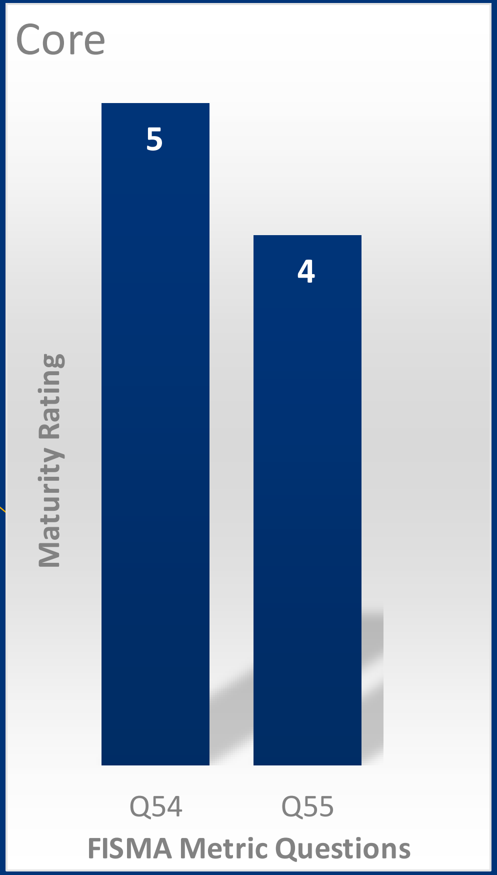


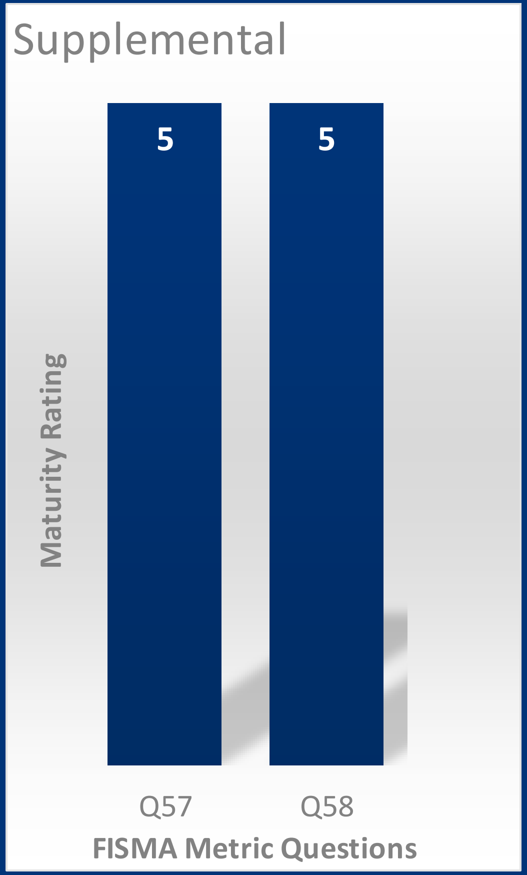


Conditions Identified:

- None

Incident Response

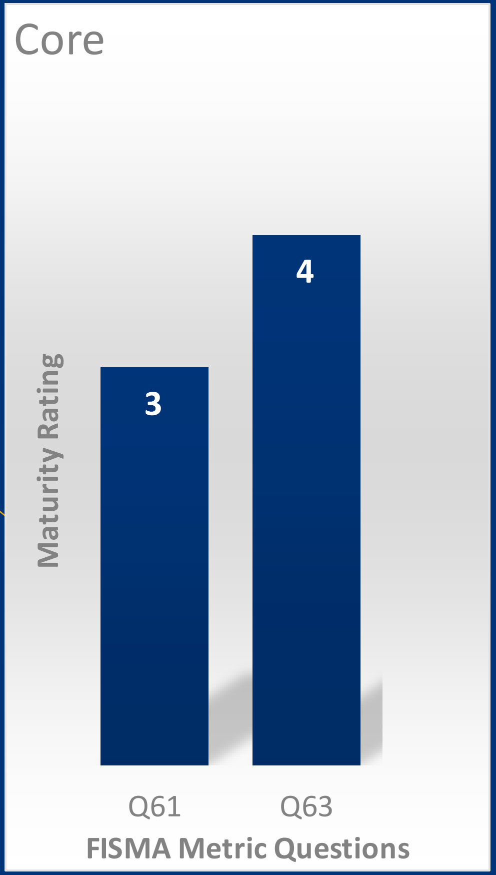


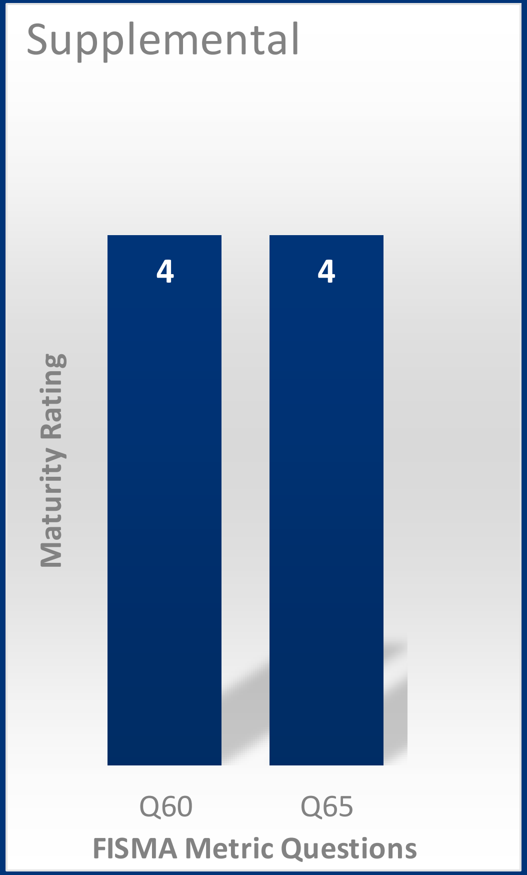


Conditions Identified:

- None

Contingency Planning





Conditions Identified:

- FRTIB did not conduct an agency level BIA within the audit period (Finding CP-1)

THANK YOU!

Williams Adley

Phone

(202) 371-1397

Website

https://www.williamsadley.com