Audit of the Effectiveness of Federal Retirement Thrift Investment Board (FRTIB)'s Information Security Program under Federal Information Security Modernization Act (FISMA) of 2014 for Fiscal Year (FY) 2021

Board Meeting
August 24, 2022

Agenda

- Objective and Scope
- Evaluation Method
- Audit Results
- Root Causes
- Recommendations

Objective and Scope

- Determine the effectiveness of FRTIB’s information security program for FY 2021 (October 1, 2020 – September 30, 2021)
- Assess management’s remediation effort to address previously issued recommendations
- Evaluate a combination of entity wide and system specific controls with a particular focus on two (2) of FRTIB’s information systems:
  - Mainframe
  - Office 365 (O365)

Evaluation Method

FY 2021 Inspector General (IG) Reporting Metrics

- Align with the NIST Cybersecurity Framework for five function areas and nine (9) underlying domains
- 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[2]

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

[2] – A weighted average rating system was piloted in preparation for a future change to the reporting metrics in FY 2022.

Evaluation Method – FISMA Functions and Domains

Identify

- Risk Management
- Supply Chain Risk Management

Protect

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

Detect

- Information Security Continuous Monitoring

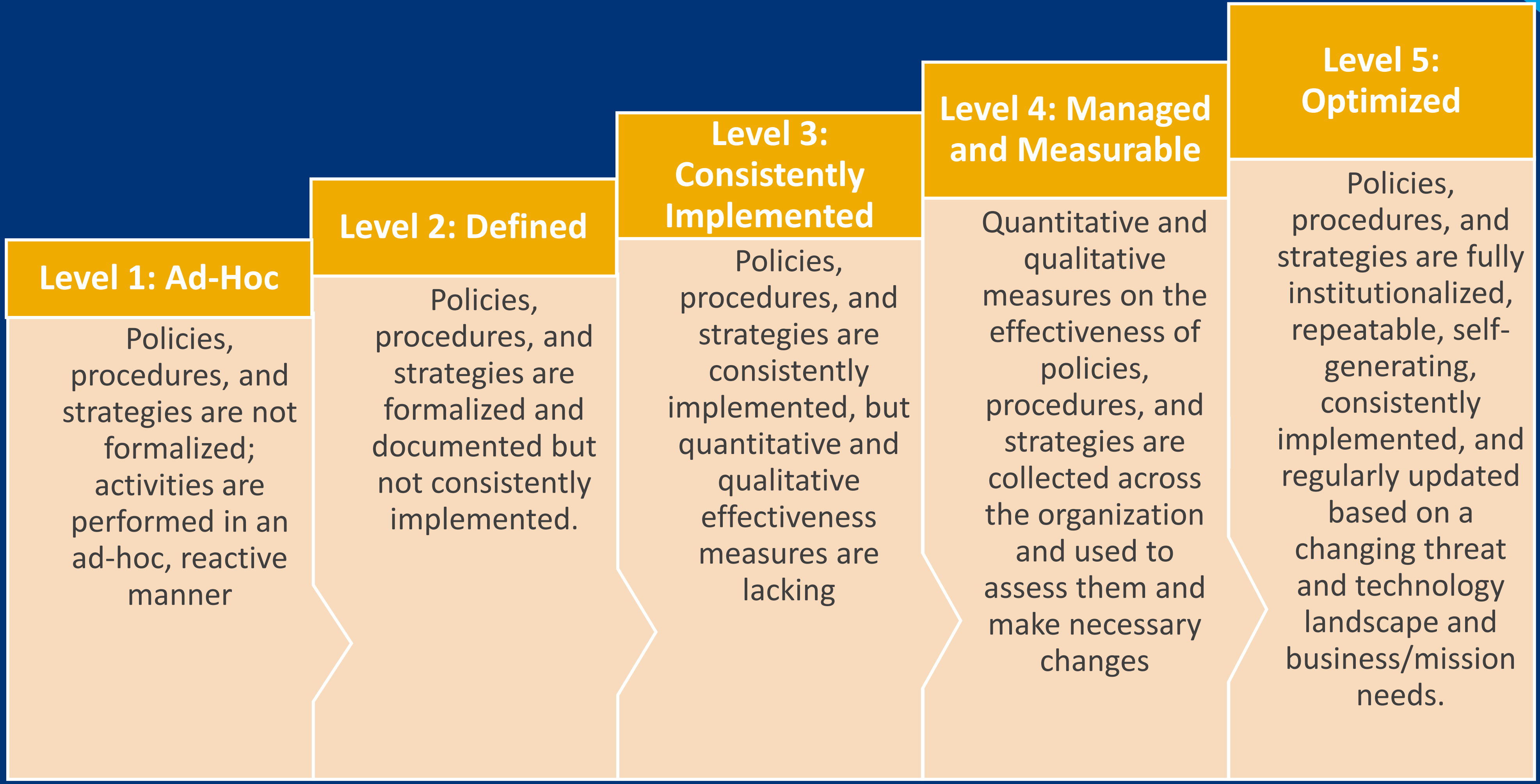
Respond

- 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.

Audit Results - Overview

- FRTIB’s information security program, supporting the two (2) in-scope systems, was deemed effective.
- All eight (8) repeat FISMA domains maintained their maturity rating[1].
- Four (4) previously issued recommendations were closed in FY 2021.
- Ten (10) individual conditions were identified, and four (4) recommendations were issued to address their root causes.

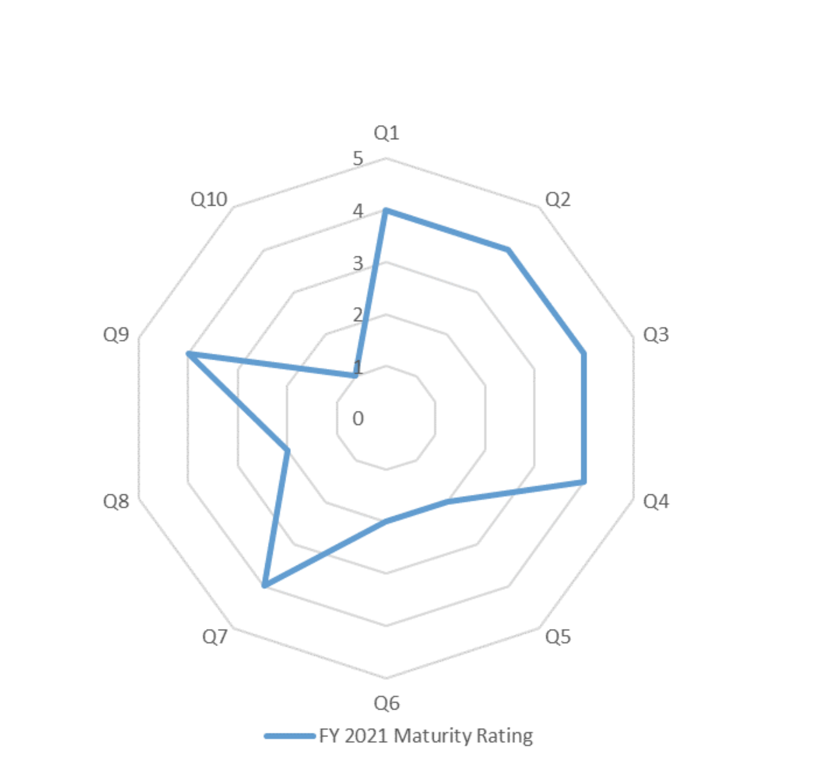
[1] – The Supply Chain Risk Management domain was introduced in FY 2021 and its maturity rating (Level 1 – Ad-Hoc) was not used in the calculation of the Agency’s maturity ratings.

Audit Results – Overall Domain Ratings

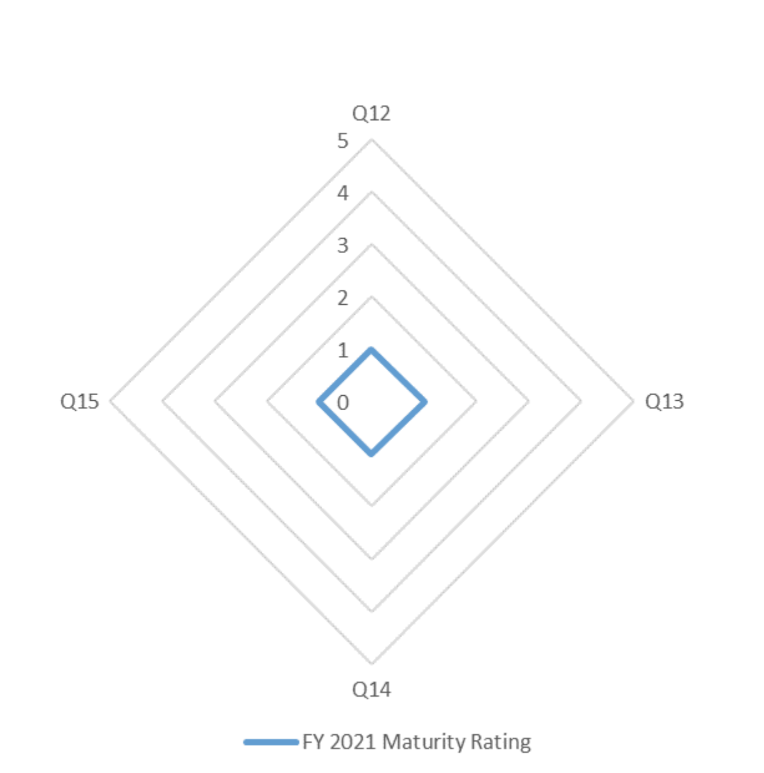
FISMA Function	FISMA Domains	FY 2020 Rating	FY 2021 Rating
Identify	Risk Management	Level 4	Level 4
Identify	Supply Chain Risk Management	N/A	Level 1
Protect	Configuration Management	Level 4	Level 4
Protect	Identity and Access Management	Level 4	Level 4
Protect	Data Protection and Privacy	Level 4	Level 4
Protect	Security Training	Level 4	Level 4
Detect	ISCM	Level 4	Level 4
Respond	Incident Response	Level 4	Level 4
Recover	Contingency Planning	Level 2	Level 2

Audit Results – Detailed Domain Ratings

Risk Management

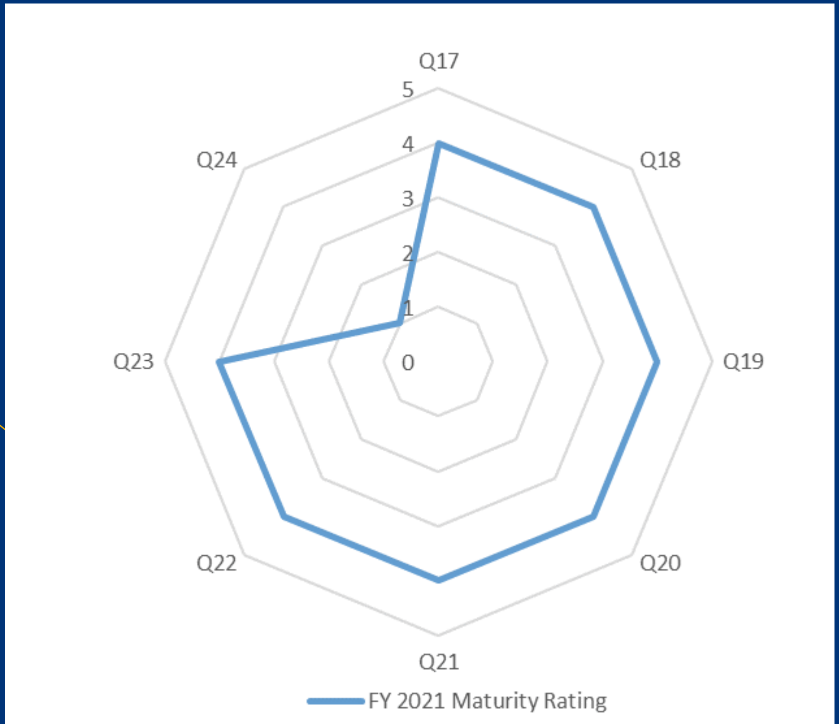


Supply Chain Risk Management

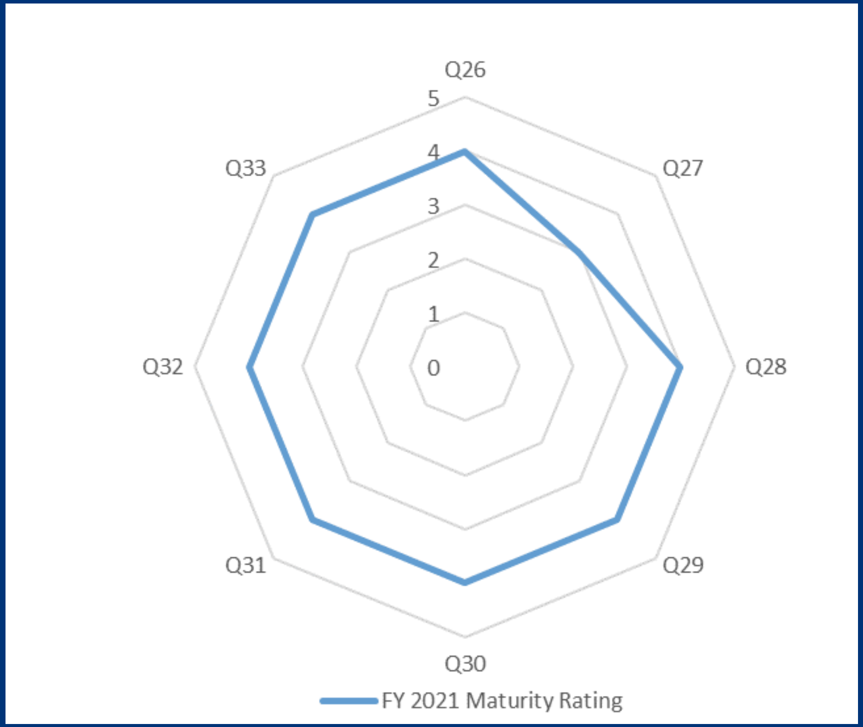


Audit Results – Detailed Domain Ratings

Configuration Management

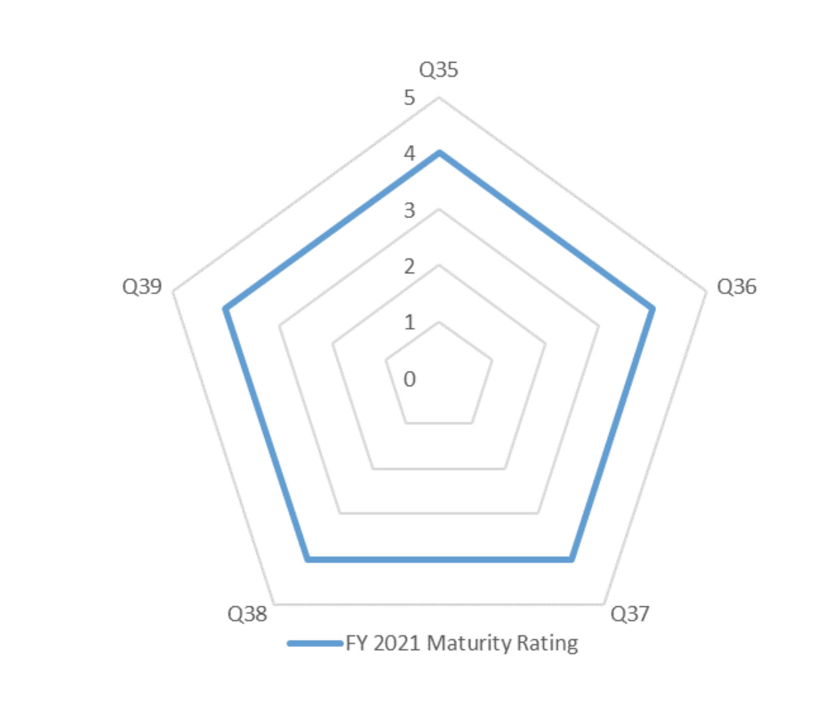


Identity and Access Management

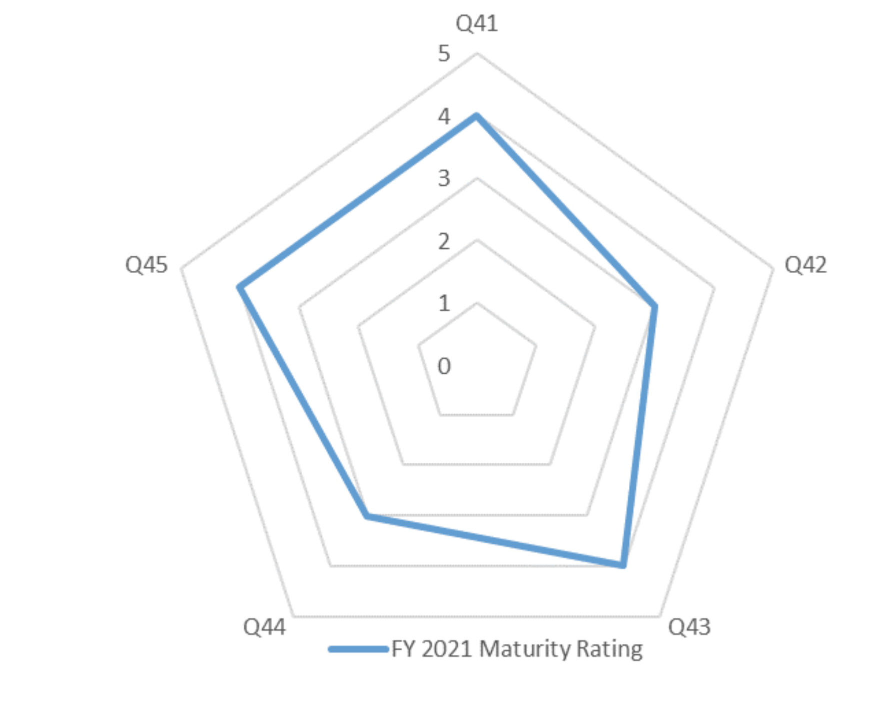


Audit Results – Detailed Domain Ratings

Data Protection and Privacy

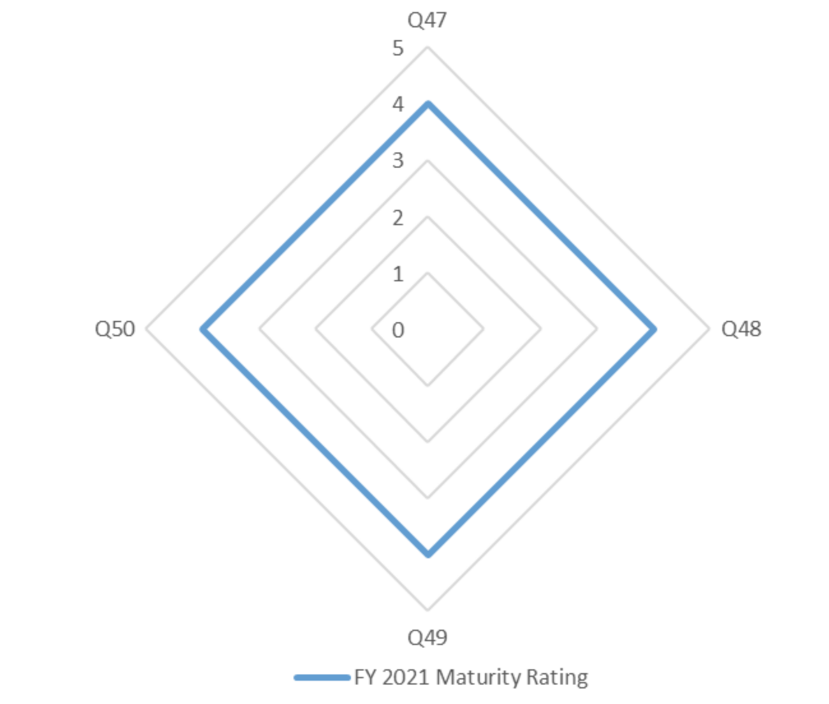


Security Training

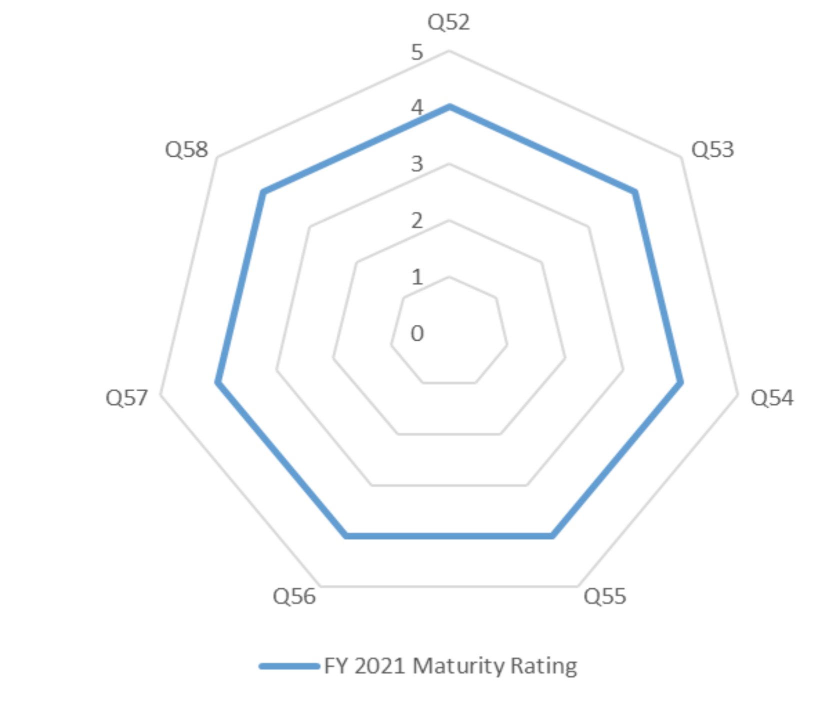


Audit Results – Detailed Domain Ratings

Information Security Continuous Monitoring

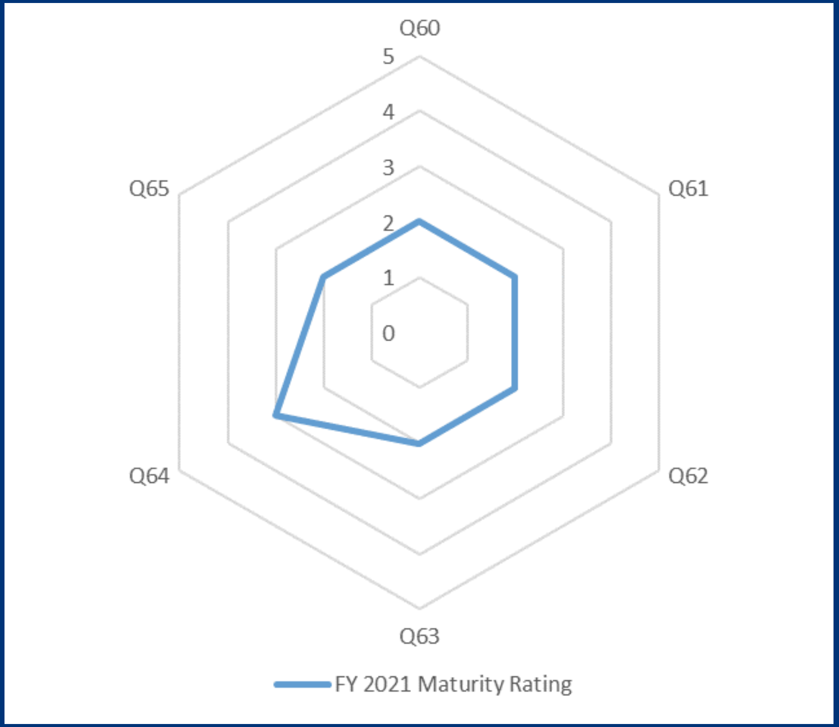


Incident Response



Audit Results – Detailed Domain Ratings

Contingency Planning



Root Causes - Conditions Identified

- Williams Adley believes that the conditions identified as a part of the FY 2021 FISMA are due to the following reasons:
  - FRTIB is still in process of implementing corrective actions plans to previously issued recommendations
  - FRTIB has not developed a standard data elements/taxonomy to maintain a complete and accurate population of data breaches within its environment
  - FRTIB has not implemented its penalty table to ensure users complete required training in a timely manner
  - Certain metrics within the Process Health Management (PHM) process rely on manual methods of data gathering and entry
  - FRTIB is still in process of updating its contingency planning program to account for third party managed systems

Recommendations

- To address the conditions identified and their associated root causes, Williams Adley recommends that FRTIB:
  - *Recommendation 1:* Develop a standard data elements/taxonomy to maintain a complete and accurate population of data breaches
  - *Recommendation 2:* Implement a penalty table to ensure users complete required training in a timely manner
  - *Recommendation 3:* Develop additional data validation processes to ensure manually tracked metrics are captured and recorded accurately within the PHM process
  - *Recommendation 4:* Update existing contingency planning policies, procedures, and processes to account for third party managed systems

THANK YOU!

Williams Adley

Phone

(202) 371-1397

Website

https://www.williamsadley.com