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) 2022

Board Meeting
August 22, 2023

Agenda

- Objective and Scope
- Evaluation Method
- Audit Results
- Status of Prior Years' Recommendations
- Recommendations
- Appendix A: FY 2022 Domain Ratings

Objective and Scope

- Determine the effectiveness of FRTIB's information security program for FY 2022 reporting period (October 1, 2021 – June 30, 2022)
- Evaluate the design and implementation of entity wide and system specific controls with a particular focus on two (2) of FRTIB's information systems:
  - Financial and Reconciliation Services (FRS)
  - Converge
- Review the corrective actions taken by FRTIB to address previously issued recommendations

Evaluation Method

FY 2022 Inspector General (IG) Reporting Metrics

- 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

M-22-05 - Memorandum for the Heads of Executive Departments and Agencies

- Establishes a new annual FISMA reporting deadline for FY 2022 (July)
- Core group of metrics identified which represent highly valuable controls that must be evaluated annually
- The remainder of the standards and controls will be evaluated in metrics on a two-year cycle

Evaluation Method – FISMA Functions and Domains

Identify

- Risk Management (Five Core Metrics)
- Supply Chain Risk Management (One Core Metric)

Protect

- Configuration Management (Two Core Metrics)
- Identity and Access Management (Three Core Metrics)
- Data Protection and Privacy (Two Core Metrics)
- Security Training (One Core Metric)

Detect

- Information Security Continuous Monitoring (Two Core Metrics)

Respond

- Incident Response (Two Core Metrics)

Recover

- Contingency Planning (Two Core Metrics)

Evaluation Method – Maturity Model

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
- 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

Evaluation Method – Maturity Model

Audit Results - Overview

- FRTIB's information security program, supporting the two (2) in-scope systems, was deemed effective.
- Seven (7) FISMA domains maintained their maturity ratings and two (2) improved their maturity ratings.
- Three (3) previously issued recommendations were closed in FY 2022.
- Three (3) individual conditions were identified, and zero (0) recommendations were issued due to the nature of the conditions and pre-existing recommendations.

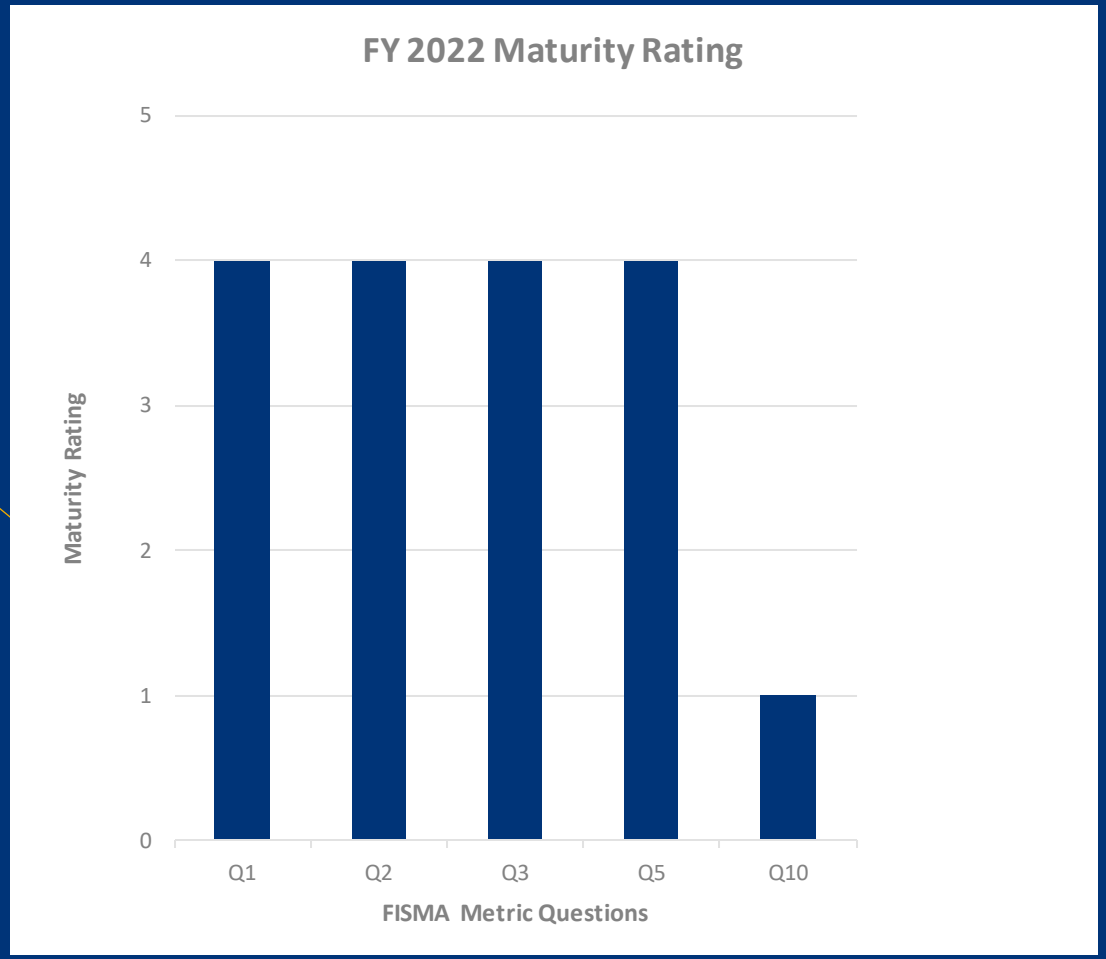
Audit Results – Overall Domain Ratings

FISMA Function	FISMA Domain	FY 2021 Rating	FY 2022 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 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 4

Appendix A:

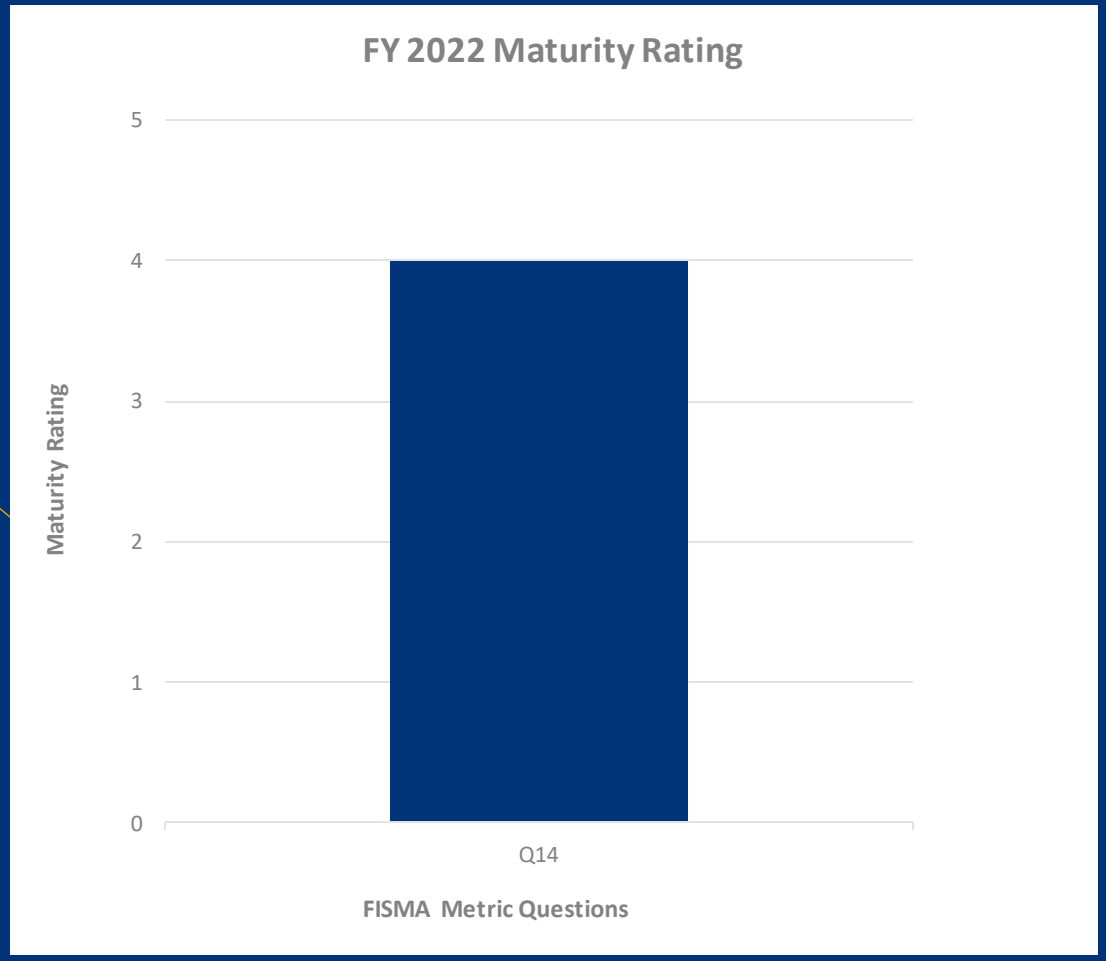
FY 2022 Domain Ratings

Audit Results – Risk Management



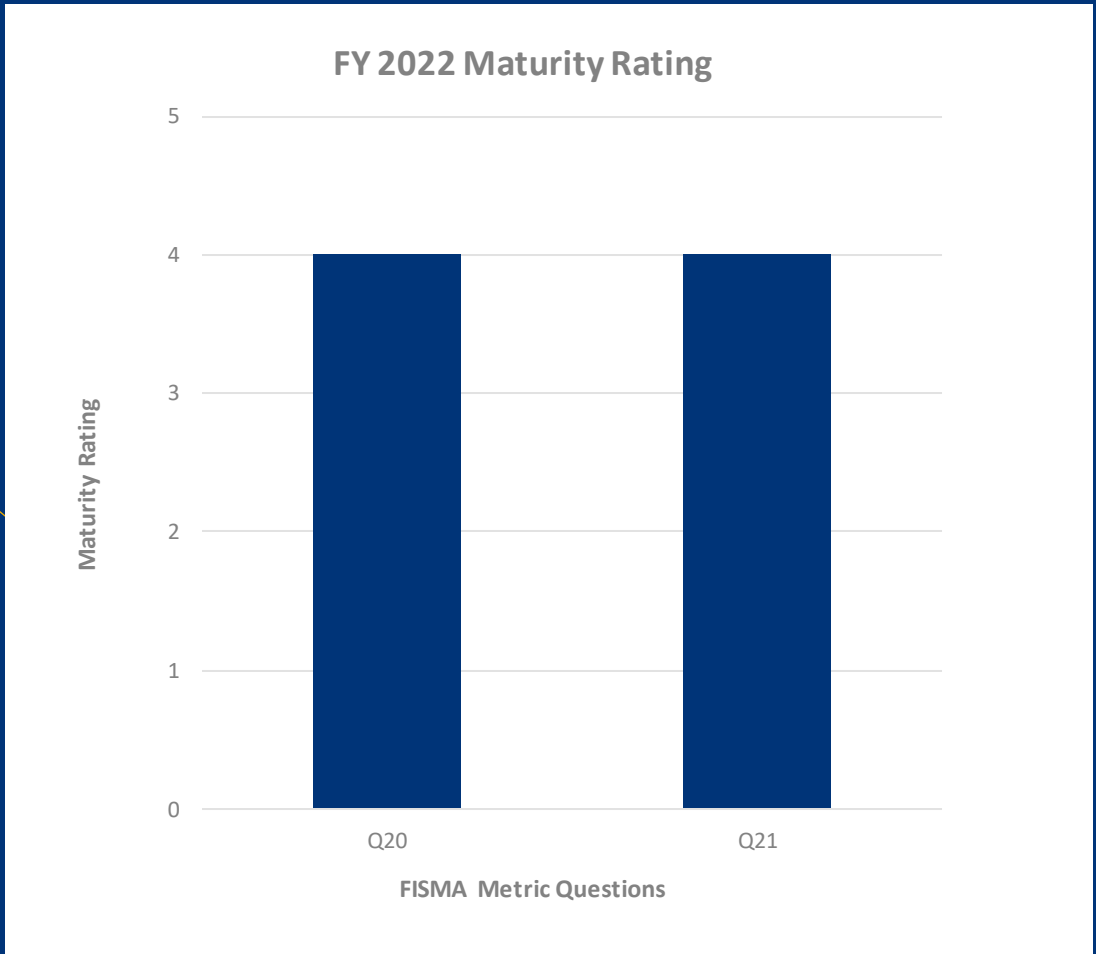
- FRTIB has developed and maintained a comprehensive and accurate inventory of information systems and supporting hardware and software component inventories.
- FRTIB has consistently implemented its policies and procedures to manage cybersecurity risk management activities at all three (3) organizational tiers.
- **Exception:** No technology/automation to provide a centralized, enterprise wide (portfolio) view of cybersecurity risk management activities.

Audit Results – Supply Chain Risk Management



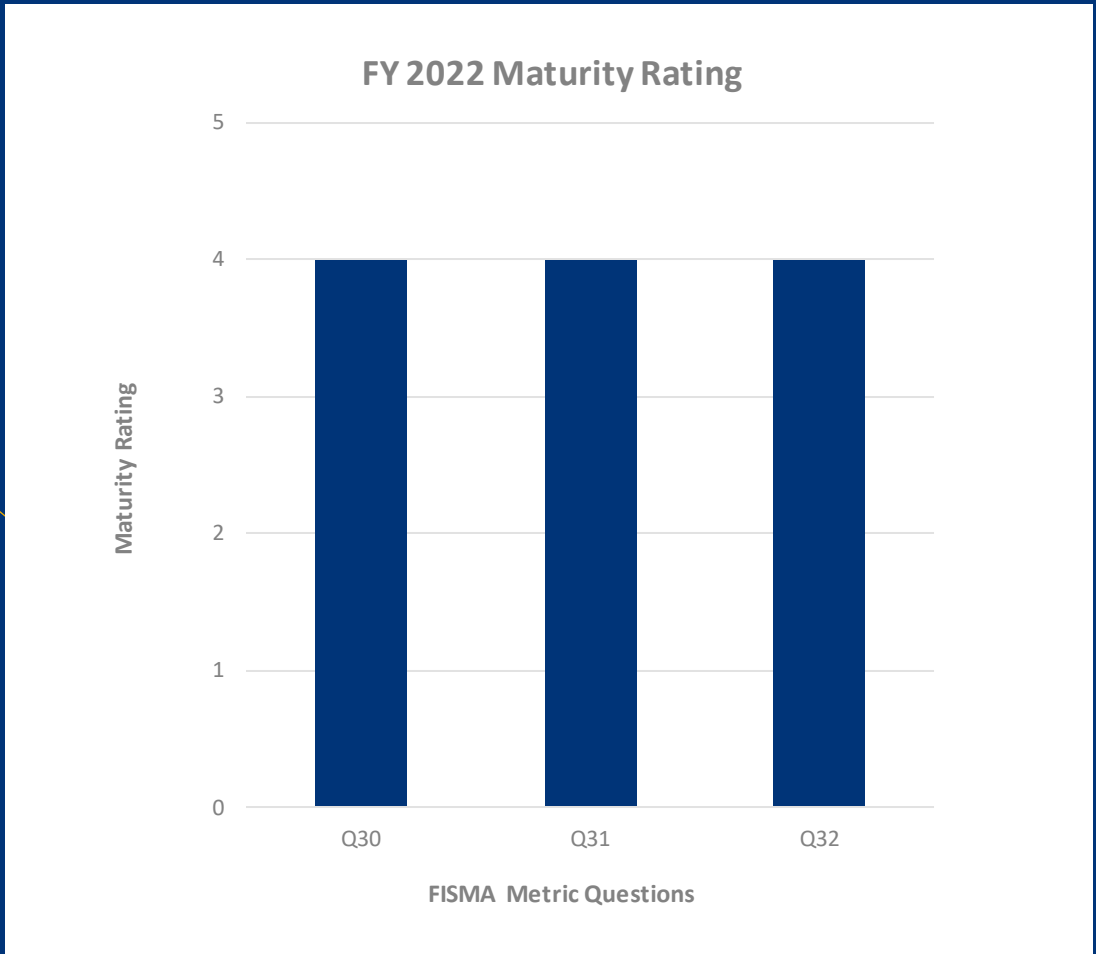
- FRTIB has implemented multiple process to ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain requirements.
- No exception identified.

Audit Results – Configuration Management



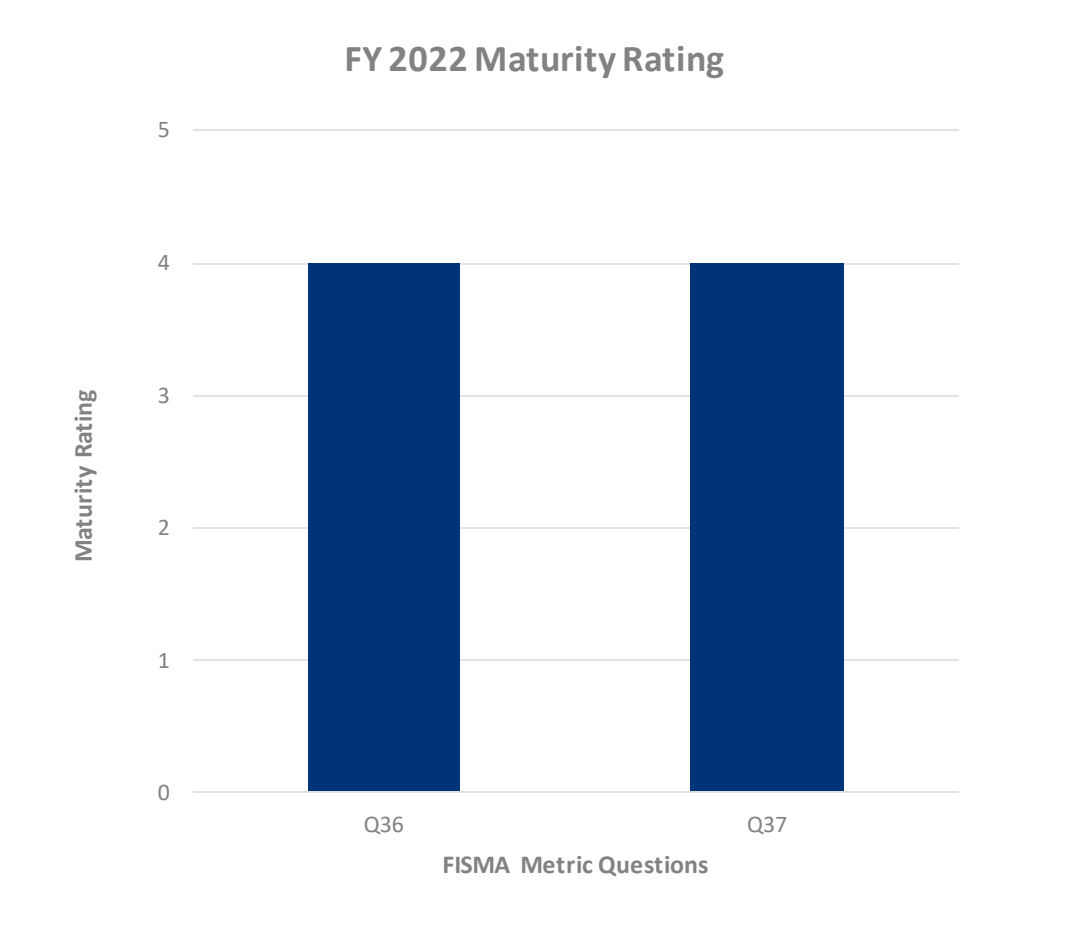
- FRTIB has consistently implemented its configuration management activities.
- FRTIB has evaluated the effectiveness of its configuration management activities using qualitative and quantitative performance measures.
- **Exception:** Three (3) low risk configuration failures associated with one FRS host IP Address did not have a documented deviation approval.

Audit Results – Identity and Access Management



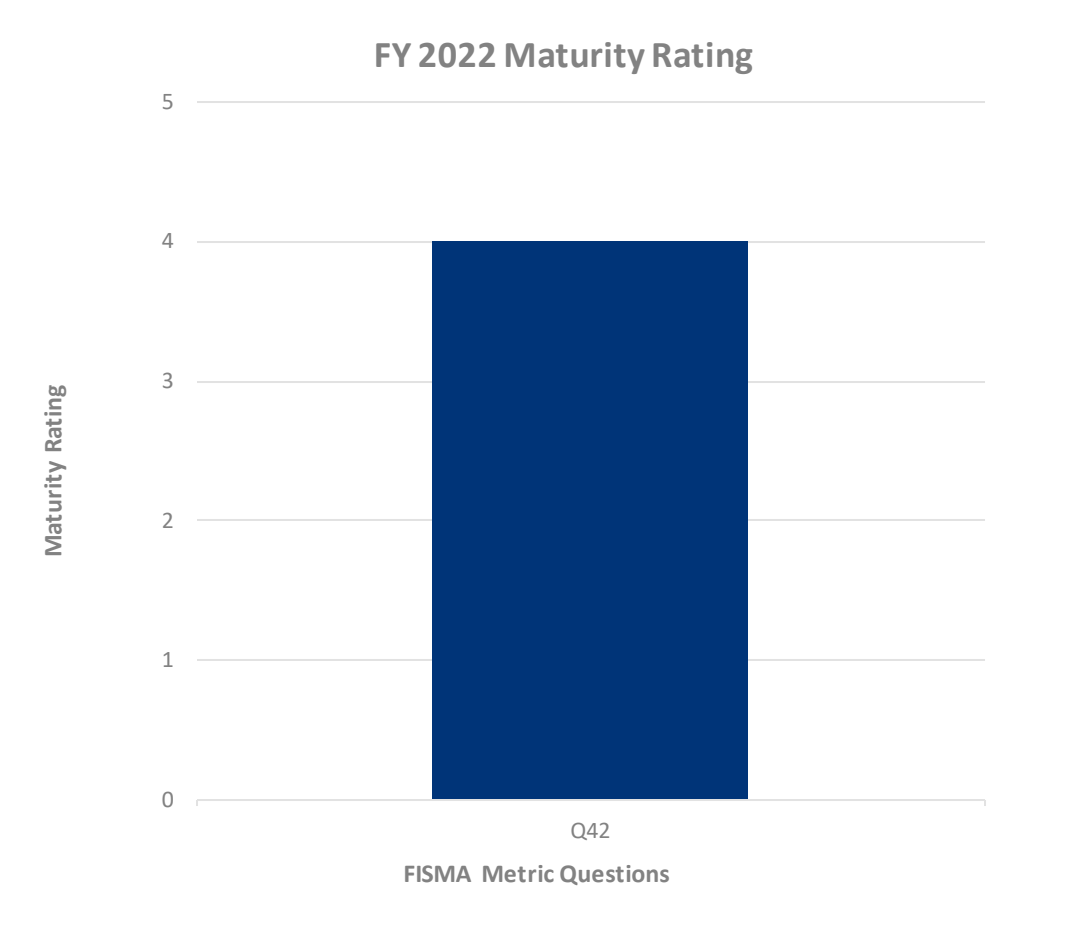
- FRTIB has designed its method of authentication to require the use of PIV credentials for its non-privileged and privileged users.
- FRTIB has consistently implemented processes for provisioning, managing, and reviewing privileged accounts, as well as utilizes automated scripts to revoke/disable inactive accounts from its network.
- No exception identified.

Audit Results – Data Protection and Privacy



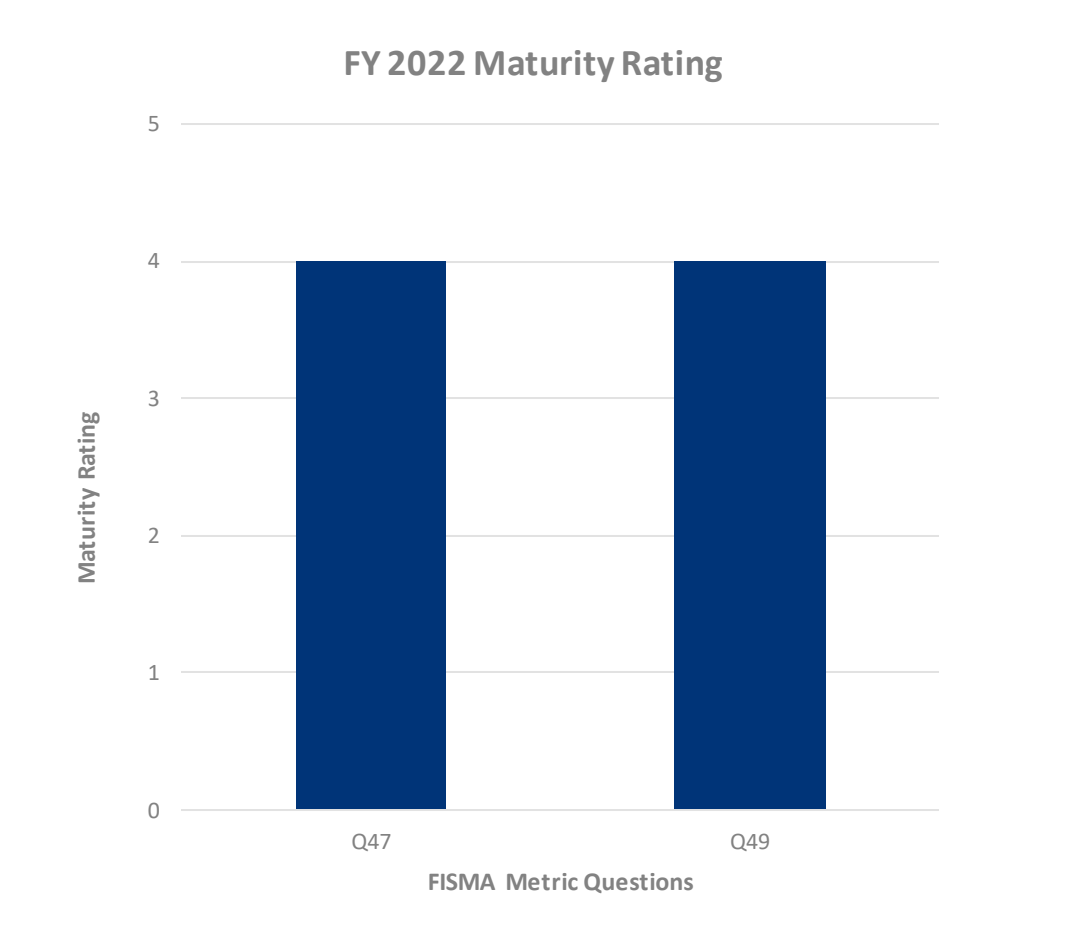
- FRTIB protects personally identifiable information (PII) collected, used, maintained, shared, and disposed by its information systems through the implementation of security controls designed to encrypt sensitive data and prevent data exfiltration
- FRTIB evaluates the effectiveness of the its privacy program activities using qualitative and quantitative performance measures to govern and make changes, as necessary.
- No exception identified.

Audit Results – Security Training



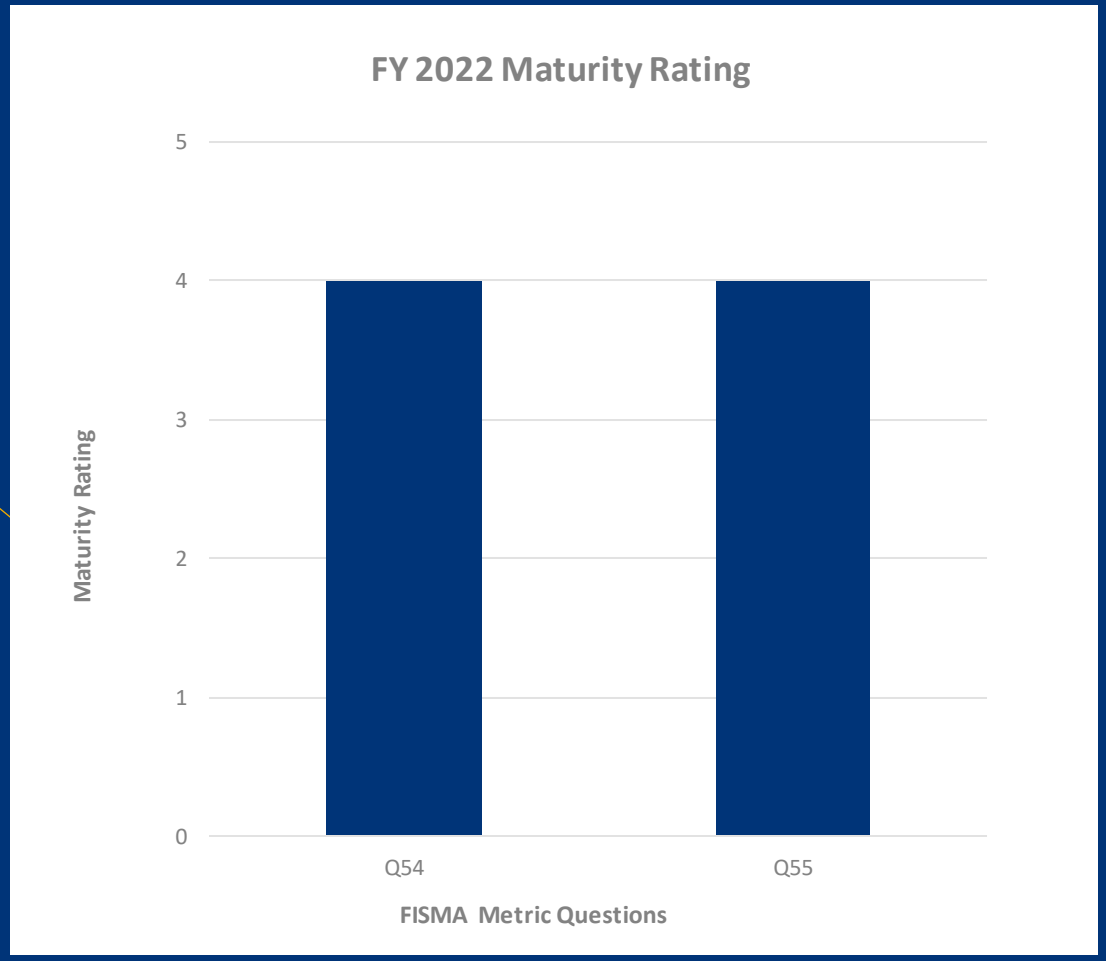
- FRTIB performs assessments of the skills, knowledge, and abilities of its workforce every two years to identify gaps and potential areas for improvement.
- FRTIB provided its workforce with multiple general, and role specific trainings tailored to address the gaps identified as a part of its FY 2020 assessment.
- No exception identified.

Audit Results – Information Security Continuous Monitoring



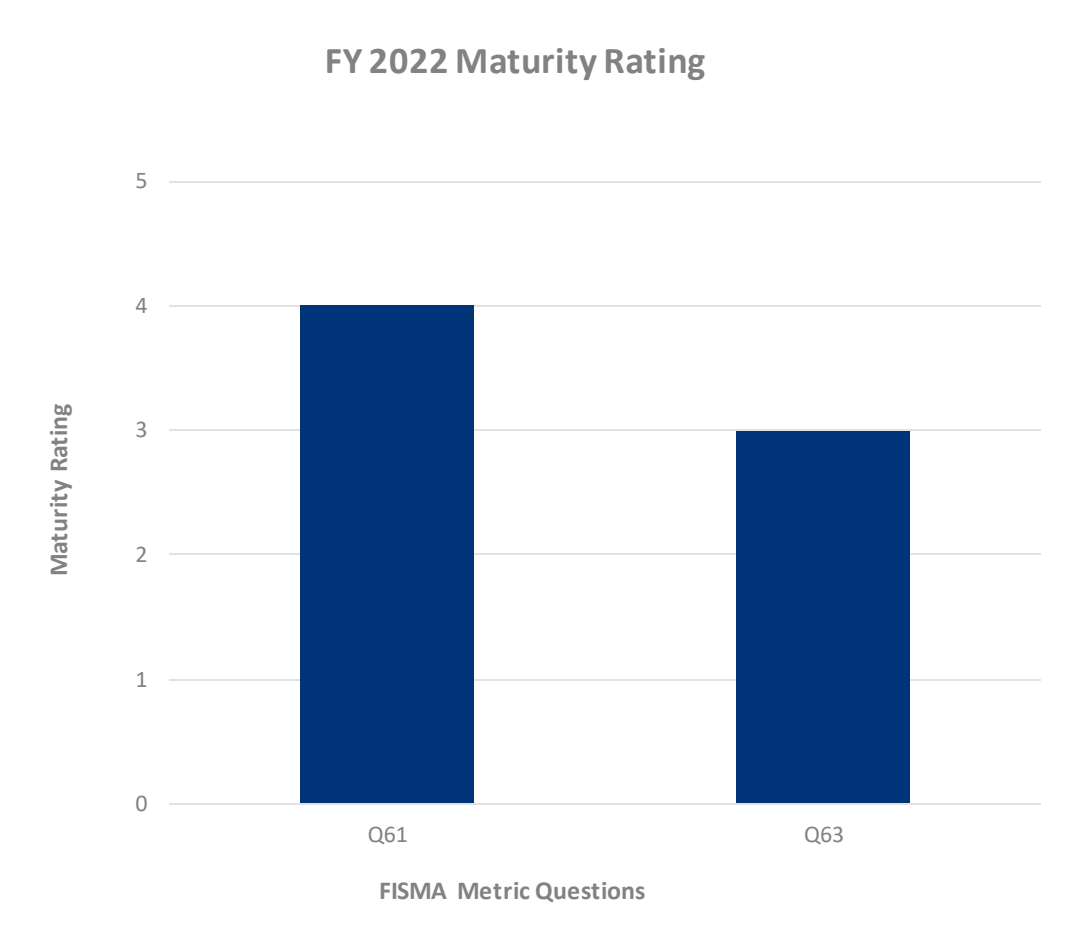
- FRTIB has established and implemented ISCM program to support continuous monitoring (ConMon) activities, as described within its ISCM strategy, across all three (3) organizational tiers.
- **Exception:** The values for two (2) metrics were incorrectly inputted into one month's dashboard. These issues were determined to be low risk.

Audit Results – Incident Response



- FRTIB has consistently implemented its incident response activities to ensure incidents are handled in accordance with established policies and procedures.
- No exception identified.

Audit Results – Contingency Planning



- FRTIB ensured that business impact analyses are performed and used to guide contingency planning efforts, and tabletop exercises were performed to ensure supporting personnel understand their roles and responsibilities and identify potential areas of improvement.
- No exception identified.

Status of Prior Years' Recommendations

- Four (4) remain open at the conclusion of the FY 2022 FISMA Audit:
  - 2021 – Develop a standard data elements/taxonomy to maintain a complete and accurate population of data breaches.
  - 2021 – Develop additional data validation processes to ensure manually tracked metrics are captured and recorded accurately within the Process Health Management (PHM) process.
  - 2020 – Update and reconcile legacy plans of actions and milestones (POA&Ms) prior to their migration into Telos Xacta to ensure that all required fields are complete and duplicate POA&Ms are eliminated.
  - 2017 – Williams Adley recommends that FRTIB clearly define an organization-wide risk-based information security program that is tailored to FRTIB's IT environment and information security risks.

Recommendations

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

THANK YOU!

Williams Adley

Phone

(202) 371-1397

Website

https://www.williamsadley.com