# FISCAL YEAR 2023
# IG FISMA Reporting

Khalid Hasan

Information Security and Privacy Advisory Board Meeting

*March 1-2, 2023*

# About Me

- Assistant Inspector General for Information Technology (IT) at the Office of Inspector General (OIG) for the Board of Governors of the Federal Reserve System and the Consumer Financial Protection Bureau

- Member of the Council of the Inspectors General on Integrity and Efficiency's (CIGIE) Technology Committee

- Chair of the IT subcommittee of the Federal Audit Executive Council

COUNCIL OF THE INSPECTORS GENERAL
ON INTEGRITY AND EFFICIENCY

Office of Inspector General
Board of Governors of the Federal Reserve System
Consumer Financial Protection Bureau

# Agenda

- Evolution of Inspector General (IG) evaluations under the Federal Information Security Modernization Act of 2014 (FISMA)
- New IG FISMA reporting process (FY 2022 – FY 2024)
- CIGIE FISMA capstone report
- Looking ahead

# Evolution of IG FISMA Reporting

# IG FISMA Requirements (42 USC 3555)

"Each year each agency shall have performed an independent evaluation of the information security program and practices of that agency to determine the effectiveness of such program and practices.

Each evaluation under this subsection shall include

(a) Testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems

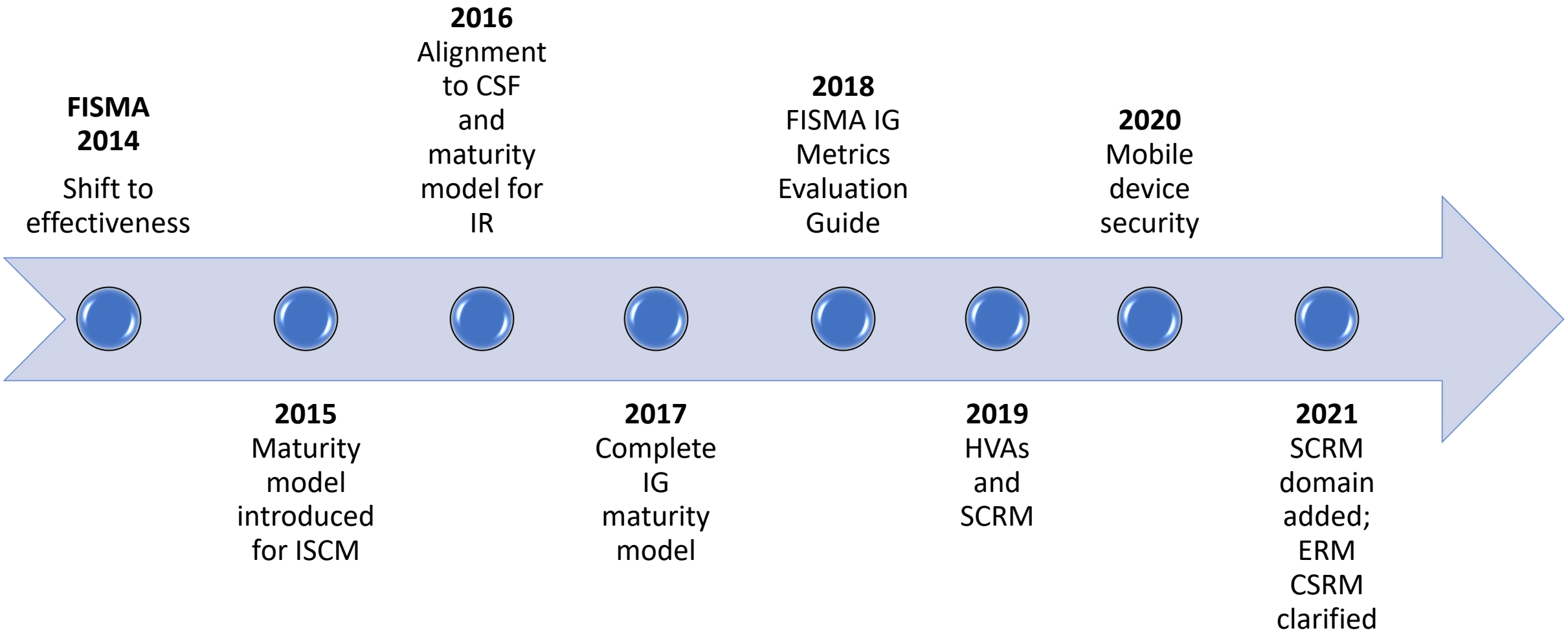
(b) An assessment of the effectiveness of the information security policies , procedures, and practices of the agency…"

# IG FISMA Reporting Process

- The Office of Management and Budget (OMB) consults with the Department of Homeland Security (DHS), CIGIE, and other parties on the development of annual FISMA reporting guidance for IGs
  - CIGIE FISMA metrics working group coordinates with federal partners

- IG FISMA results are reported in DHS's Cyberscope application

# IG FISMA Reporting Evolution



# Components of IG FISMA Evaluations

- Risk Mgt
- Supply Chain Risk Mgt

Contingency Planning

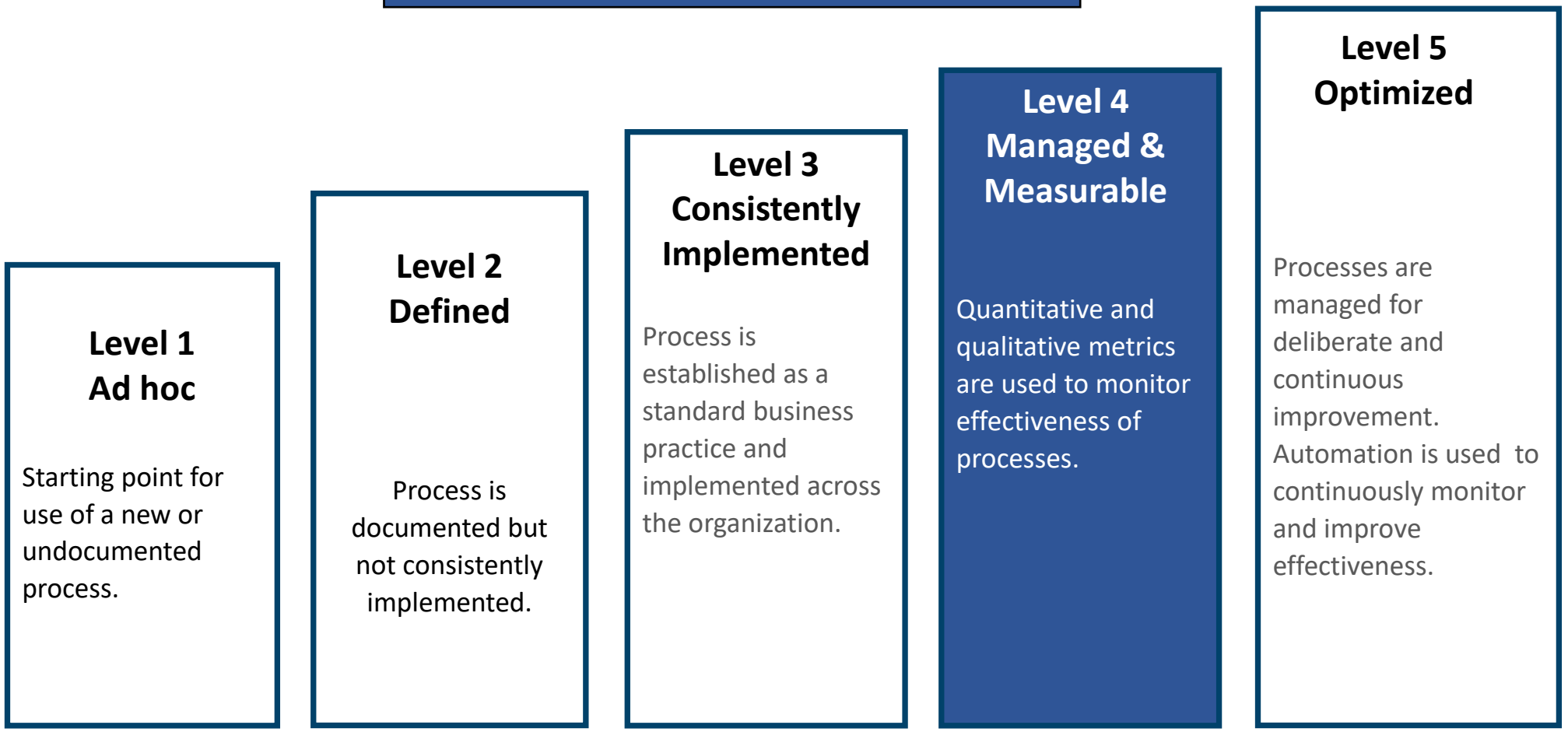

- Configuration Mgt
- Identity & Access
- Data Protection & Privacy
- Security Training

Incident Response

Information Security Continuous Monitoring

# IG FISMA Maturity Model

**OMB has defined Level 4 as being Effective**

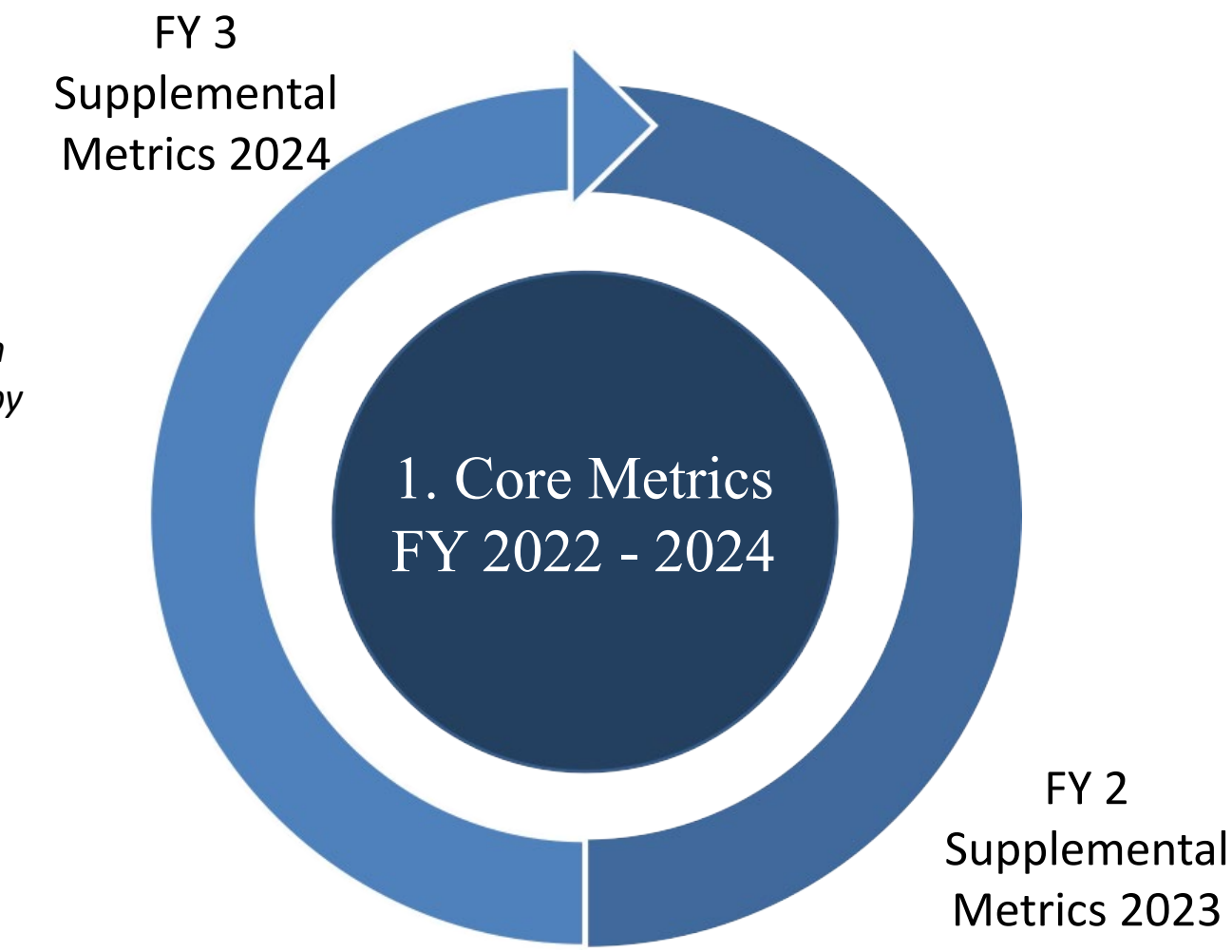


# New IG FISMA Reporting Process FY 22 - 24

# IG FISMA Reporting Process Shift (FY 22-24)

***M-22-05 FISMA Guidance on IG Reporting for FY22***
*"OMB will select a core group of metrics, representing a combination of Administration priorities and other 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 based on a calendar agreed to by CIGIE, the CISO Council, OMB, and CISA."*

***M-23-03 FISMA Guidance on IG Reporting for FY23***
*"OMB selected a core group of metrics, representing a combination of Administration priorities and other highly valuable controls, that must be evaluated annually. The remainder of the standards and controls will continue to be evaluated in metrics on a 2-year cycle based on a calendar agreed to by CIGIE, the CISO Council, OMB, and CISA. These changes do not in any way limit the scope of IG authority to evaluate information systems on an as-needed or ad-hoc basis."*



# Core IG Metrics

| Function | Core Metrics Area |
|---|---|
| Identify | • Inventory and asset mgt<br>• Cyber risk mgt<br>• Third party security risk mgt |
| Protect | • Secure configurations and flaw remediation<br>• Multifactor authentication and privileged account mgt<br>• Encryption of data at rest and in transit<br>• Data exfiltration<br>• Cyber workforce assessment |
| Detect | • Information security continuous monitoring strategy<br>• Ongoing assessments and authorizations |
| Respond | • Incident detection, analysis, and handling |
| Recover | • Business impact analyses and contingency testing |

EO 14028

Zero trust architecture

OMB Memoranda - encryption, cyber incident mgt, endpoint detection and response, software supply chain security

# New FY 2023 IG Evaluation Areas

- Reporting of government furnished equipment via the DHS' Continuous Diagnostics and Mitigation (CDM) program
- Asset visibility and vulnerability detection
- Security measures for EO critical software
- Software producer self-attestations
- Audit logging for privileged accounts
- Endpoint detection and response

# Sample IG FISMA Results - FY 23 and FY 24

FY 23

| Function | Core Metrics | FY23 Supp. Metrics | FY23 Assessed Maturity | FY23 Justification |
|---|---|---|---|---|
| Identify | 3.6 | 3.3 | Effective | Ipsum lorem. |
| Protect | 4.0 | 3.7 | Effective | Ipsum lorem. |
| Detect | 3.0 | 3.1 | Not Effective | Ipsum lorem. |
| Respond | 4.0 | 4.0 | Effective | Ipsum lorem. |
| Recover | 3.4 | 3.1 | Not Effective | Ipsum lorem. |
| Overall Maturity | 3.6 | 3.4 | Not Effective | Ipsum lorem. |

FY 24

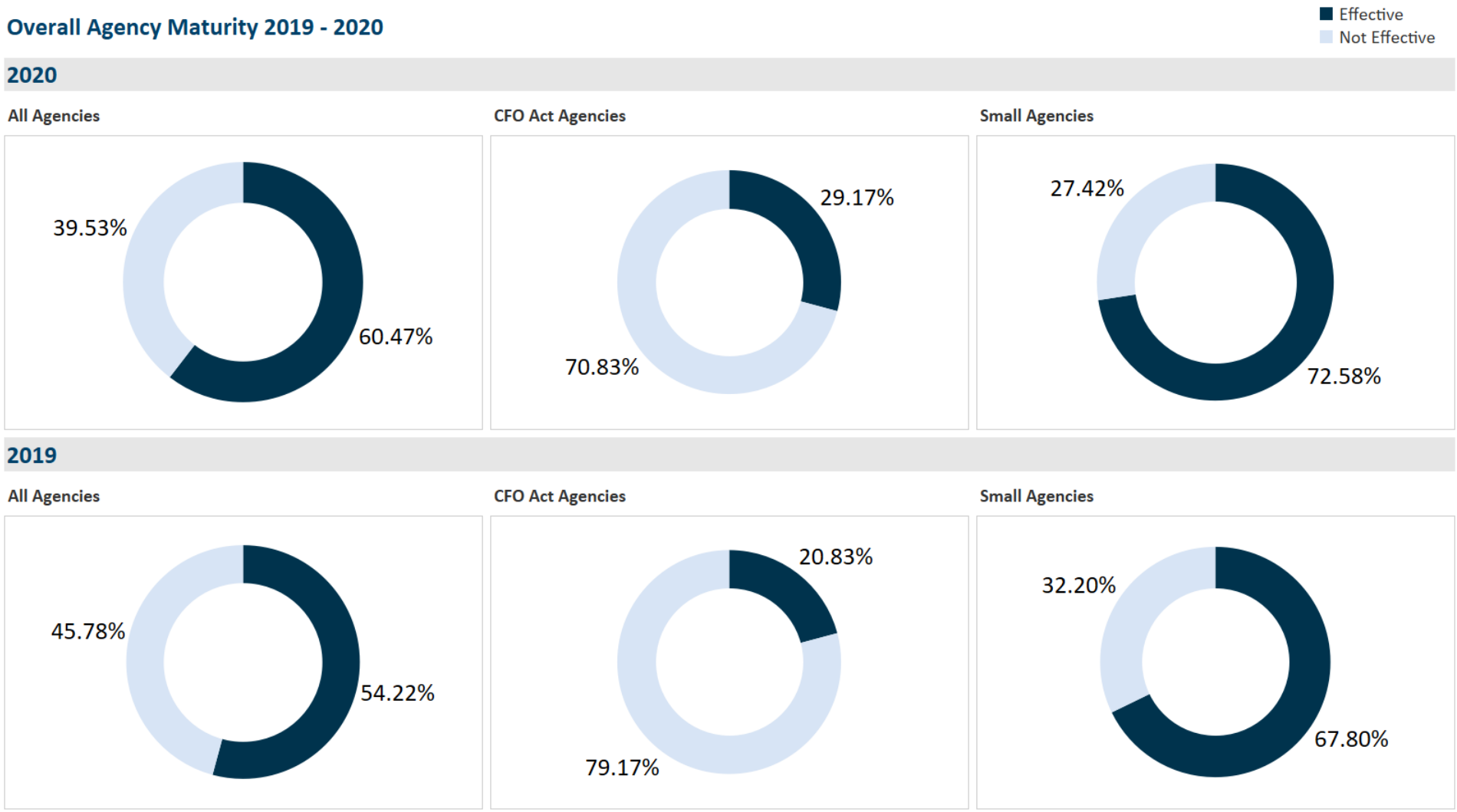
| Function | Core Metrics | FY23 Supp. Metrics | FY24 Supp. Metrics | FY24 Assessed Maturity | FY24 Justification |
|---|---|---|---|---|---|
| Identify | 3.7 | 3.3 | 3.5 | Effective | Ipsum lorem. |
| Protect | 4.0 | 3.7 | 3.6 | Effective | Ipsum lorem. |
| Detect | 3.2 | 3.1 | 3.2 | Not Effective | Ipsum lorem. |
| Respond | 4.0 | 4.0 | 3.9 | Effective | Ipsum lorem. |
| Recover | 3.4 | 3.1 | 3.2 | Not Effective | Ipsum lorem. |
| Overall Maturity | 3.7 | 3.4 | 3.5 | Not Effective | Ipsum lorem. |

# CIGIE FISMA Capstone Report Project

# IG FISMA Capstone Report

- Earlier this year, the CIGIE Technology Committee established a working group to develop a FISMA capstone report
- The goal of this working group is to analyze IG FISMA data and identify trends and perform statistical analysis on the metrics
- Report will include the results of a survey on IG experiences with Cyberscope

# Historical Analysis of IG FISMA Data



# Historical Analysis of IG FISMA Data

## 2020 Top 10 Metric Analysis

| Rank | Question Theme | FISMA Domain | % Effective | |
|---|---|---|---|---|
| 1 | Stakeholder Collaboration | Incident Response | 65.1% | → |
| 2 | Security Awareness | Security Training | 59.3% | ↑ |
| 3 | Roles and Responsibilities | Incident Response | 58.1% | ↑ |
| 4 | Policies and Procedures | Security Training | 55.8% | ↓ |
| | Roles and Responsibilities | Security Training | 55.8% | ↑ |
| 6 | Security Training Strategy | Security Training | 54.7% | ↑ |
| 7 | Specialized Security Training | Security Training | 52.3% | ↓ |
| | Remote Access | Identity & Access Management | 52.3% | → |
| 9 | Incident Handling | Incident Response | 50.0% | ↑ |
| | System Inventory | Risk Management | 50.0% | → |

# Historical Analysis of IG FISMA Data

## 2020 Bottom 10 Metric Analysis

| Rank | Question Theme | FISMA Domain | % Not Consistently Implemented | |
|---|---|---|---|---|
| 1 | Policies and Procedures | Risk Management | 51.2% | ↑ |
| 2 | Automated View of Risks | Risk Management | 50.0% | ↓ |
| 3 | Information Security Architecture | Risk Management | 48.8% | ↑ |
| 4 | Least Privilege/Separation of Duties | Identity & Access Management | 47.7% | ↑ |
| 5 | Policies and Procedures | Identity & Access Management | 45.3% | ↑ |
| | Flaw Remediation | Configuration Management | 45.3% | → |
| 7 | Business Impact Analysis | Contingency Planning | 43.0% | ↓ |
| | Measuring ISCM Performance | ISCM | 43.0% | → |
| | Policies and Procedures | Configuration Management | 43.0% | ↑ |
| 10 | Config Mgmt Plan | Configuration Management | 40.7% | ↑ |

# Looking Ahead

# Next Steps and Thoughts

- Three-year continuous evaluation cycle should provide key data to identify improvements
- Challenge remains in finding the right balance amongst compliance, risk management, and effectiveness
- Target profiles may help IG's better evaluate effectiveness while taking into account agency specific factors

# Questions?

Khalid Hasan
Khalid.A.Hasan@Frb.Gov

COUNCIL OF THE INSPECTORS GENERAL
ON INTEGRITY AND EFFICIENCY

Office of Inspector General
Board of Governors of the Federal Reserve System
Consumer Financial Protection Bureau