



FISMA Oversight: Past, Present, and Future

CIGIE/GAO Financial Statement Audit Conference

Khalid Hasan

May 22, 2023

1

NONCONFIDENTIAL // EXTERNAL

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

2

2

NONCONFIDENTIAL // EXTERNAL

Agenda

- Evolution of Inspector General (IG) evaluations under the Federal Information Security Modernization Act of 2014 (FISMA)
- OMB's FY22 – FY24 FISMA guidance to IGs
 - Core IG FISMA metrics
- Relationship between the IG FISMA metrics & FISCAM
- Looking ahead and next steps

3

3

Evolution of IG FISMA Reporting

4

4

NONCONFIDENTIAL // EXTERNAL

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...”

5

5

NONCONFIDENTIAL // EXTERNAL

IG FISMA Reporting Process

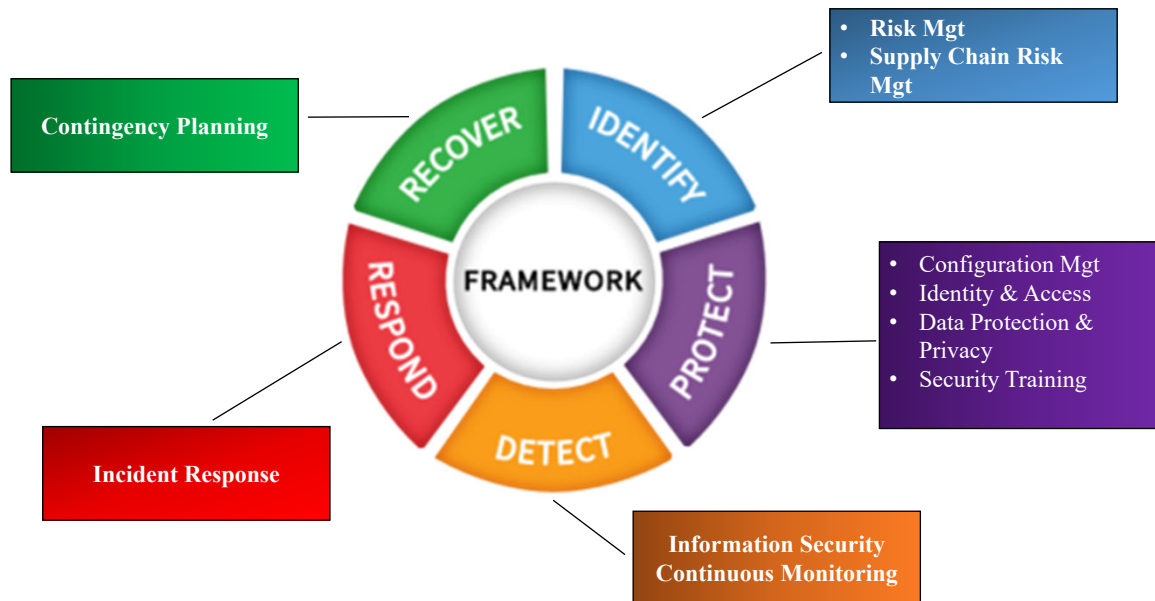
- The Office of Management and Budget (OMB) consults with the Department of Homeland Security (DHS), CIGIE, and other parties on the development of annual FISMA reporting guidance for IGs
 - CIGIE FISMA metrics working group coordinates with federal partners
- IG FISMA results are reported in DHS’s CyberScope application
- GAO and Congress utilize publicly posted IG reports to evaluate and report on agency performance

6

6

NONCONFIDENTIAL // EXTERNAL

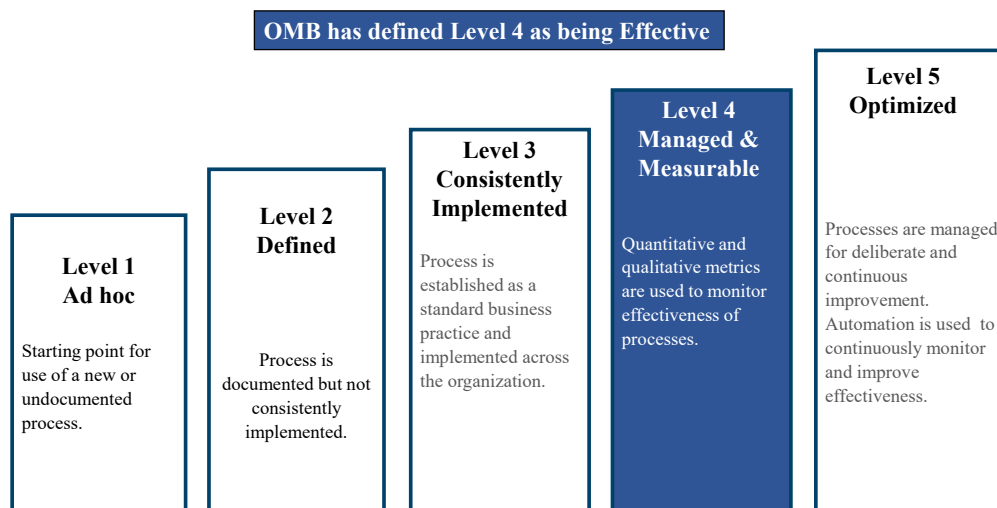
Components of IG FISMA Evaluations



7

NONCONFIDENTIAL // EXTERNAL

IG FISMA Maturity Model

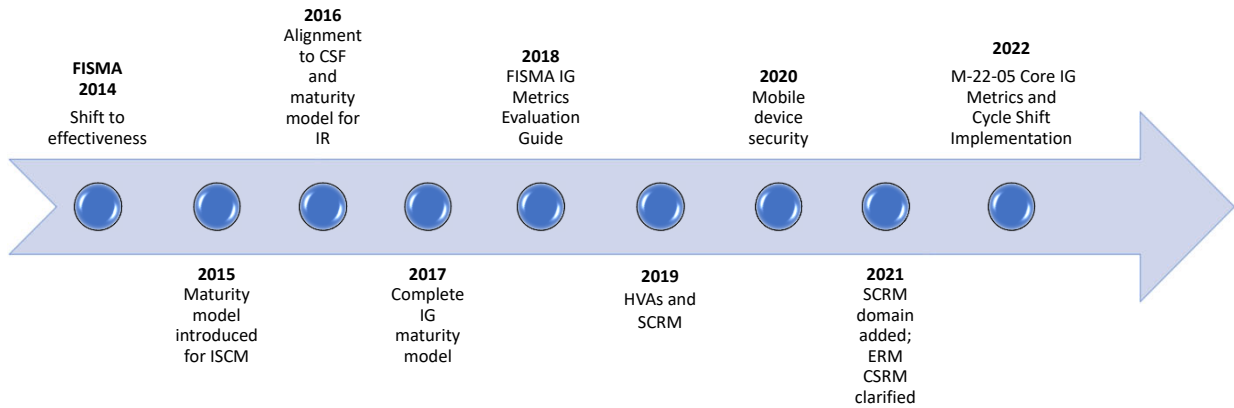


8

8

NONCONFIDENTIAL // EXTERNAL

IG FISMA Reporting Evolution



9

9

OMB's FY22 - FY24 FISMA Guidance to IGs

10

10

NONCONFIDENTIAL // EXTERNAL

IG FISMA Reporting Process Shift (FY 22-24)

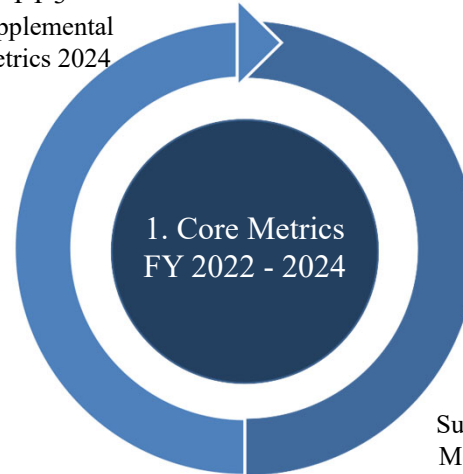
M-22-05 FISMA Guidance on IG Reporting for FY22

"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."

FY 3
Supplemental
Metrics 2024



FY 2
Supplemental
Metrics 2023

11

11

NONCONFIDENTIAL // EXTERNAL

IG FISMA Metrics Working Group

- Established for January 2022 – March 2022
- Volunteers worked with OMB to develop Core IG Metrics for FY22 – FY24
- OMB evaluated suggestions provided by the working group to develop Core IG Metrics
- OMB published FY22 IG FISMA Implementation Guidance and Analysis which included Core IG Metrics in April 2022
- OMB published FY23 – FY24 IG FISMA Guidance which included Core IG Metrics and Supplemental Metrics in February 2023

12

12

NONCONFIDENTIAL // EXTERNAL

FY 23-24 Scoring Evaluation

- IG FISMA Metrics Working Group developed multiple approaches for updating the scoring methodology
- Status Quo calculation led to multiple issues
 - Rounding questions, errors, and disagreements
 - Presentation of evaluation conducted by IG community was inconsistent
- GAO-22-104364: OMB Should Update Inspector General Reporting Guidance to Increase Rating Consistency and Precision
 - 2 Open Recommendations
 - Collaboration and clarify when to use methodologies
 - Create a more precise overall effectiveness rating scale

13

13

NONCONFIDENTIAL // EXTERNAL

Sample IG FISMA Results - FY 23 and FY 24

	Function	Core Metrics	FY23 Supp. Metrics	FY23 Assessed Maturity	FY23 Justification
FY 23	Identify	3.6	3.3	Effective	Ipssum lorem.
	Protect	4.0	3.7	Effective	Ipssum lorem.
	Detect	3.0	3.1	Not Effective	Ipssum lorem.
	Respond	4.0	4.0	Effective	Ipssum lorem.
	Recover	3.4	3.1	Not Effective	Ipssum lorem.
	Overall Maturity	3.6	3.4	Not Effective	Ipssum lorem.

	Function	Core Metrics	FY23 Supp. Metrics	FY24 Supp. Metrics	FY24 Assessed Maturity	FY24 Justification
FY 24	Identify	3.7	3.3	3.5	Effective	Ipssum lorem.
	Protect	4.0	3.7	3.6	Effective	Ipssum lorem.
	Detect	3.2	3.1	3.2	Not Effective	Ipssum lorem.
	Respond	4.0	4.0	3.9	Effective	Ipssum lorem.
	Recover	3.4	3.1	3.2	Not Effective	Ipssum lorem.
	Overall Maturity	3.7	3.4	3.5	Not Effective	Ipssum lorem.

14

14

Core IG FISMA Metrics

15

15

NONCONFIDENTIAL // EXTERNAL

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%	↑

16

16

NONCONFIDENTIAL // EXTERNAL

Historical Analysis of IG FISMA Data

2020 Top 10 Metric Analysis

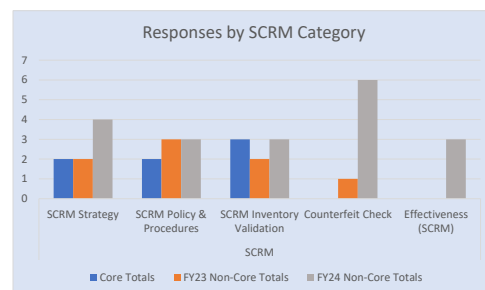
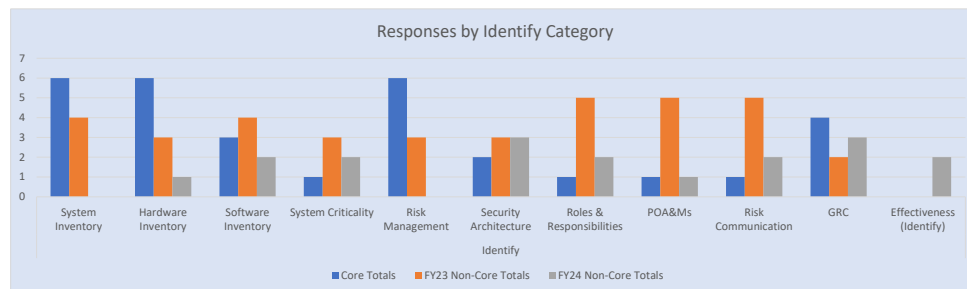
Rank	Question Theme	FISMA Domain	% Effective	
1	Stakeholder Collaboration	Incident Response	65.1%	➡
2	Security Awareness	Security Training	59.3%	⬆
3	Roles and Responsibilities	Incident Response	58.1%	⬆
4	Policies and Procedures	Security Training	55.8%	⬇
	Roles and Responsibilities	Security Training	55.8%	⬆
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%	➡

17

17

NONCONFIDENTIAL // EXTERNAL

Working Group Responses (Identify)

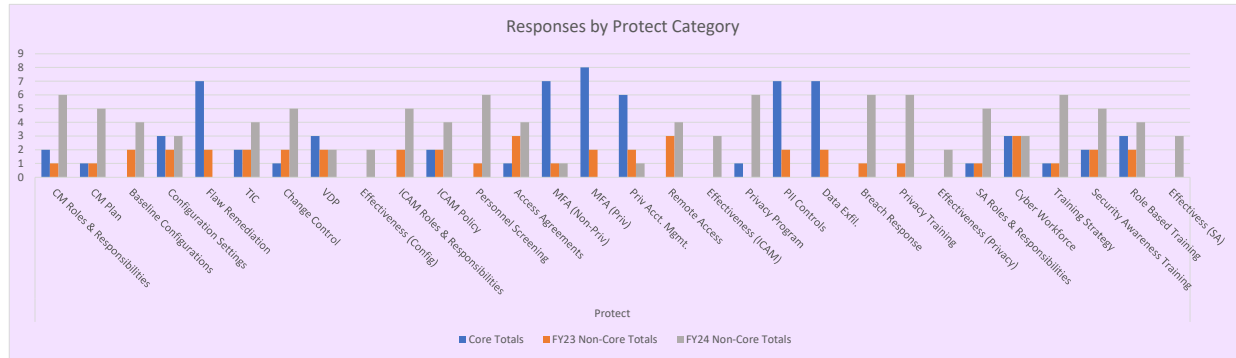


18

18

NONCONFIDENTIAL // EXTERNAL

Working Group Responses (Protect)

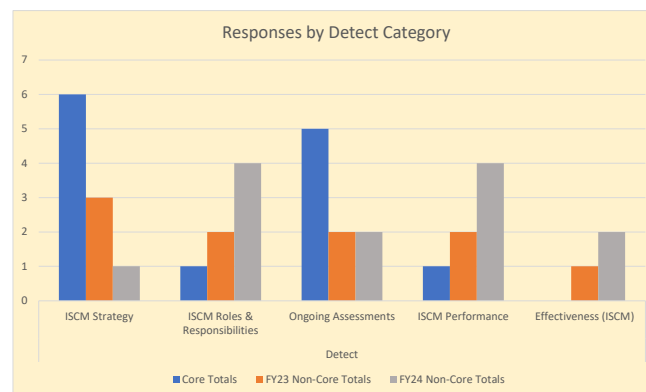


19

19

NONCONFIDENTIAL // EXTERNAL

Working Group Responses (Detect)

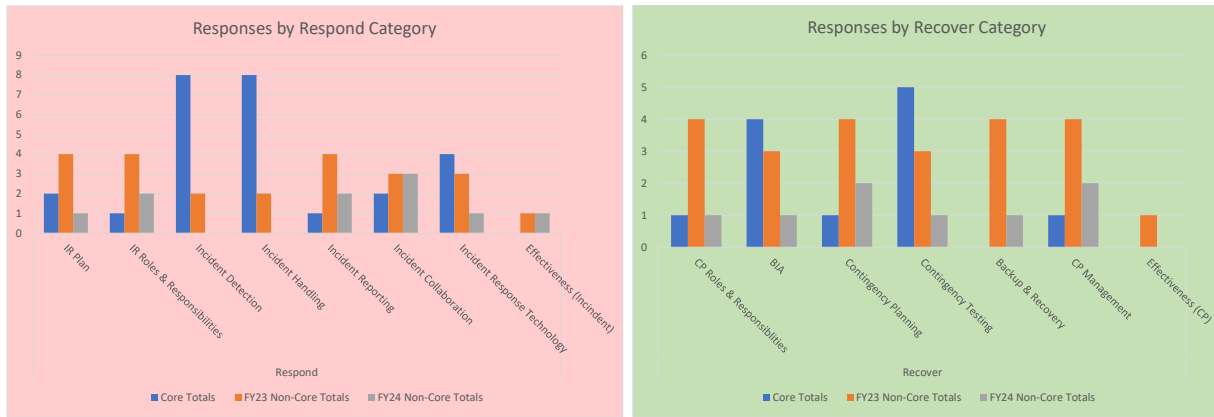


20

20

NONCONFIDENTIAL // EXTERNAL

Working Group Responses (Respond/Recover)



21

21

NONCONFIDENTIAL // EXTERNAL

Core IG Metrics

Function	Core Metrics Area
Identify	<ul style="list-style-type: none"> Inventory and asset mgt Cyber risk mgt Third party security risk mgt
Protect	<ul style="list-style-type: none"> Secure configurations and flaw remediation Multifactor authentication and privileged account mgt Encryption of data at rest and in transit Data exfiltration Cyber workforce assessment
Detect	<ul style="list-style-type: none"> Information security continuous monitoring strategy Ongoing assessments and authorizations
Respond	<ul style="list-style-type: none"> Incident detection, analysis, and handling
Recover	<ul style="list-style-type: none"> 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

22

22

NONCONFIDENTIAL // EXTERNAL

New FY 2023 - FY 2024 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

23

23

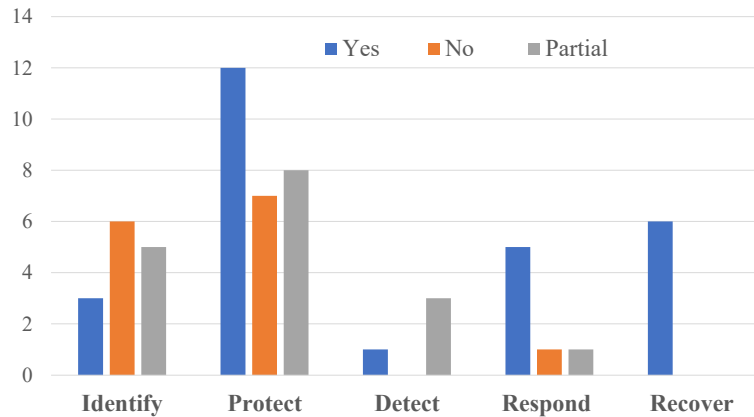
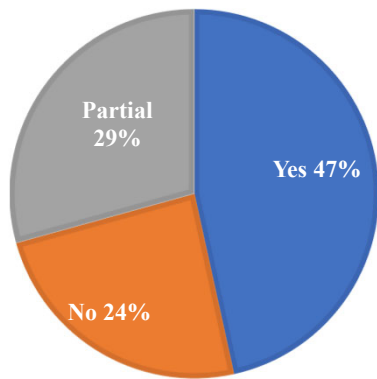
Relationship Between the IG FISMA Metrics & FISCAM

24

24

NONCONFIDENTIAL // EXTERNAL

FISCAM Coverage of IG FISMA Metrics

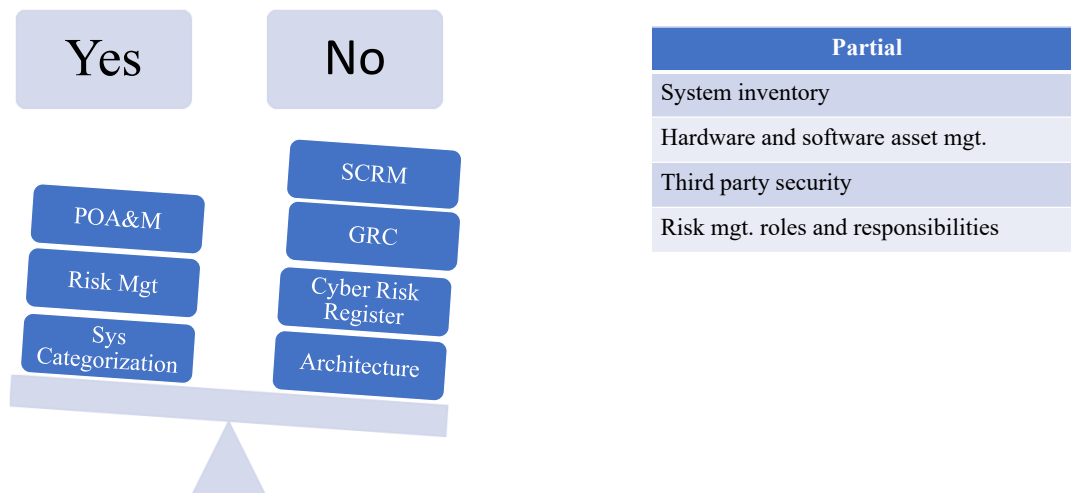


25

25

NONCONFIDENTIAL // EXTERNAL

FISCAM VS. Identify Function

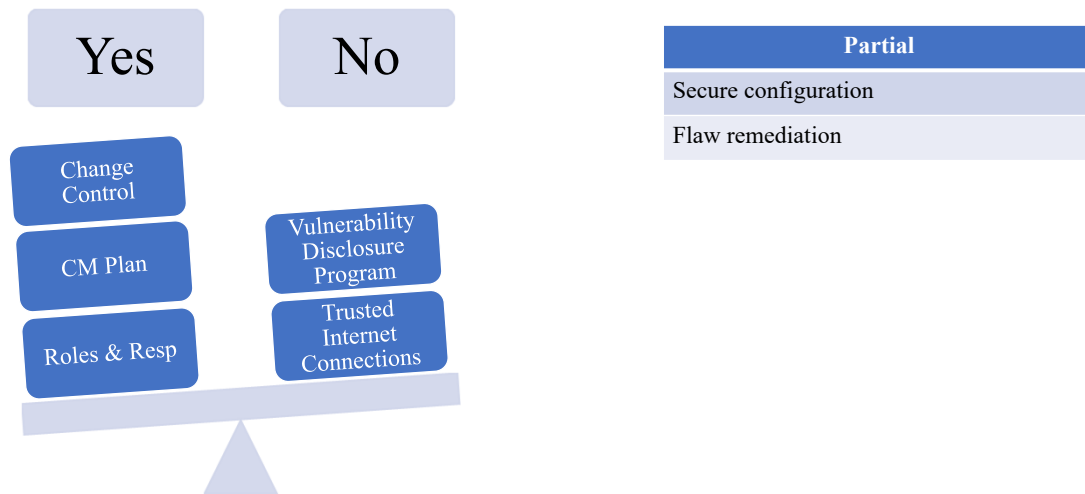


26

26

NONCONFIDENTIAL // EXTERNAL

FISCAM Vs. Protect (Config Mgt)

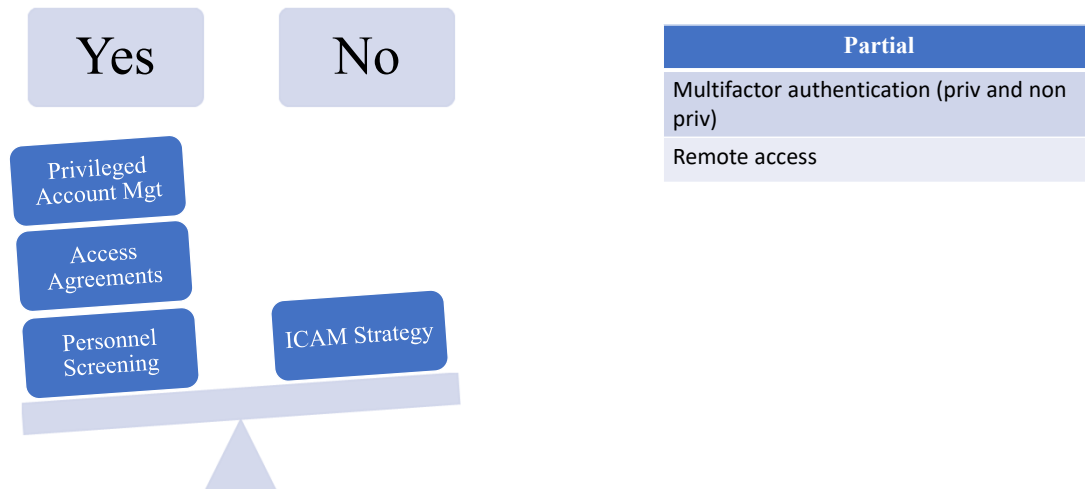


27

27

NONCONFIDENTIAL // EXTERNAL

FISCAM Vs. Protect (I&A)

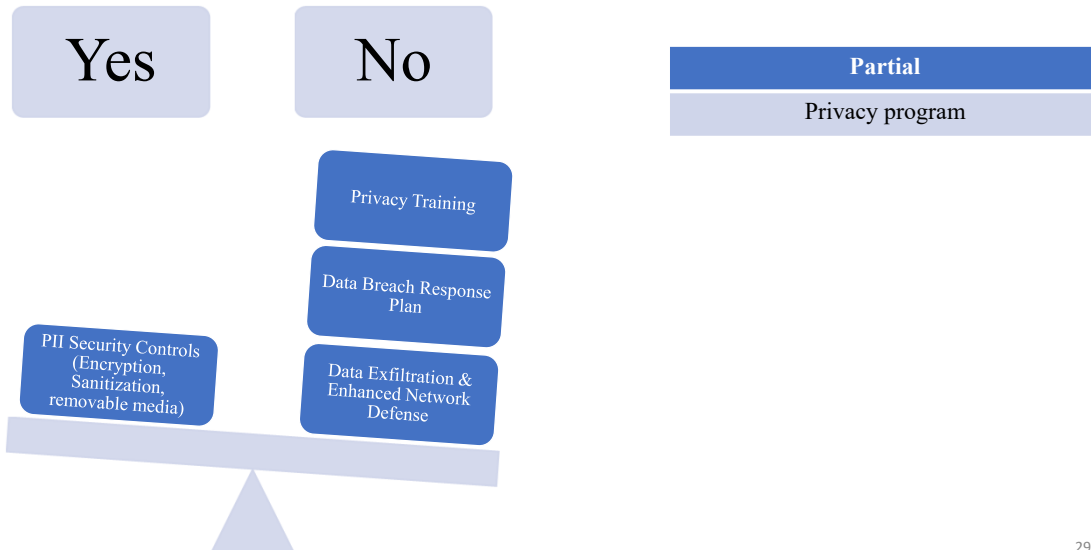


28

28

NONCONFIDENTIAL // EXTERNAL

FISCAM VS. Protect (DP &P)

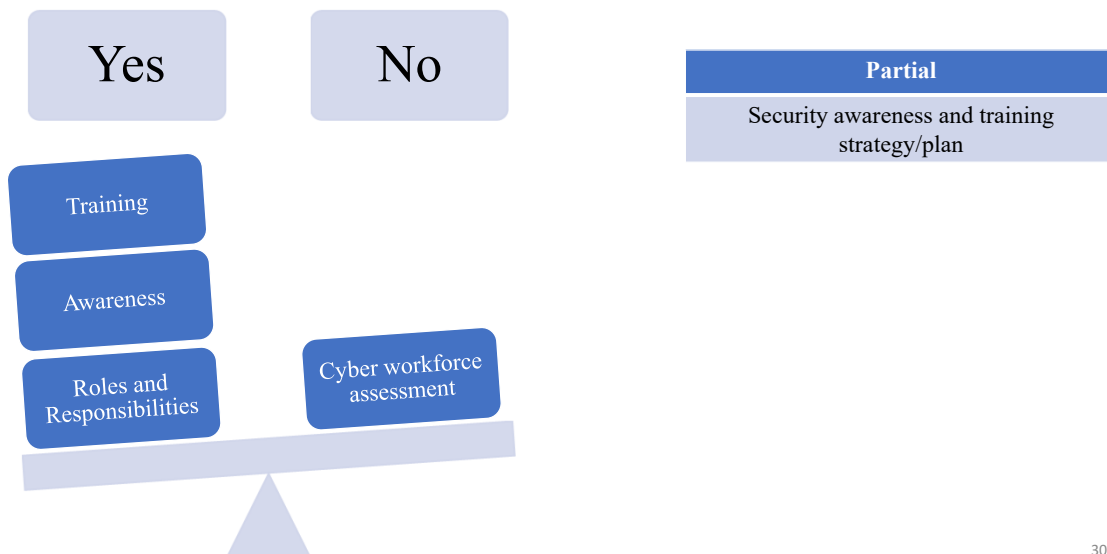


29

29

NONCONFIDENTIAL // EXTERNAL

FISCAM VS. Protect (Security Training)

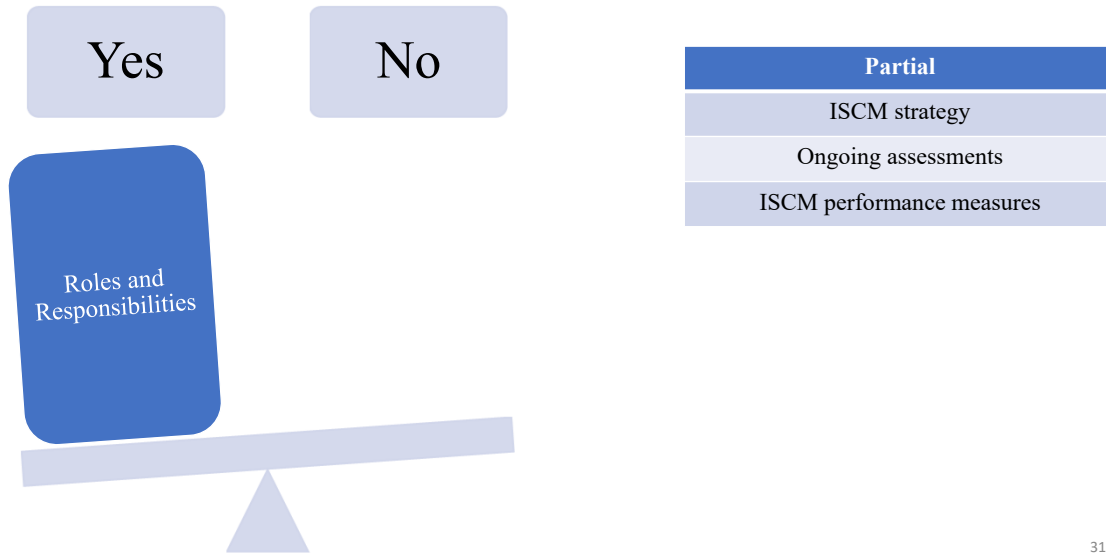


30

30

NONCONFIDENTIAL // EXTERNAL

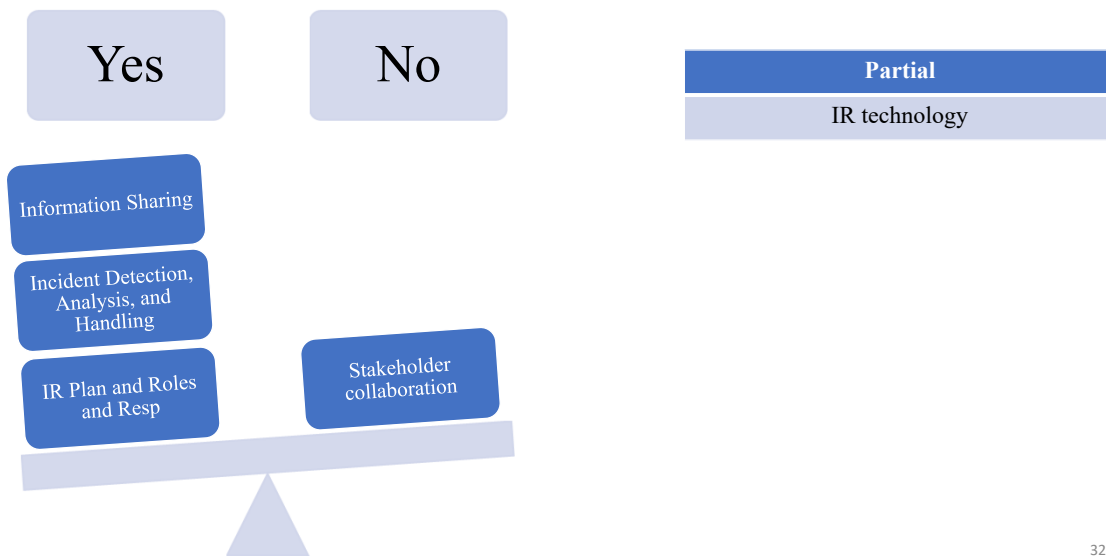
FISCAM VS. Detect (ISCM)



31

NONCONFIDENTIAL // EXTERNAL

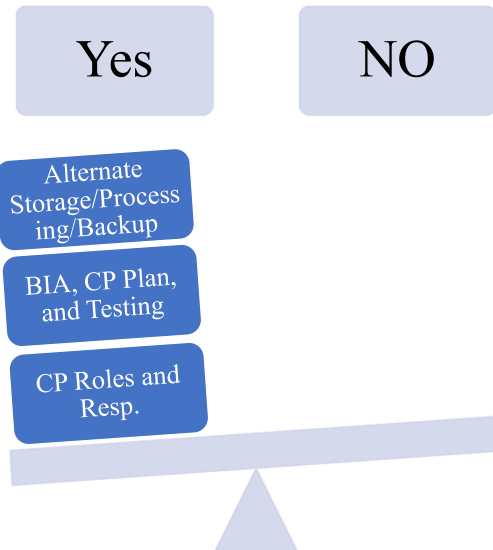
FISCAM VS. Response (Incident Response)



32

NONCONFIDENTIAL // EXTERNAL

FISCAM VS. Recover (Contingency Planning)



33

33

Looking Ahead

34

34

NONCONFIDENTIAL // EXTERNAL

NIST CSF 2.0 (Draft)

CSF 2.0 Function	CSF 2.0 Category	CSF 2.0 Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles and Responsibilities	GV.RR
	Policies and Procedures	GV.PO
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Supply Chain Risk Management	ID.SC
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Adverse Event Analysis	DE.AE
	Continuous Monitoring	DE.CM
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover	Incident Recovery Plan Execution	RC.RP

35

35

NONCONFIDENTIAL // EXTERNAL

FISMA of 2023 (Draft) - Key Agency Updates

- Designation of a Chief Privacy Officer
- Focus on ongoing and continuous risk assessments
- GAO review of OMB guidance
- Penetration testing requirements

36

36

NONCONFIDENTIAL // EXTERNAL

FISMA of 2023 (Draft) – Key IG Updates

- Changes the annual IG evaluation requirement to biennial
- IGs required to perform, or review the results of the agency's, penetration testing
- CIGIE tasked with developing a dashboard of information security recommendations

37

37

NONCONFIDENTIAL // EXTERNAL

IG FISMA Capstone Report

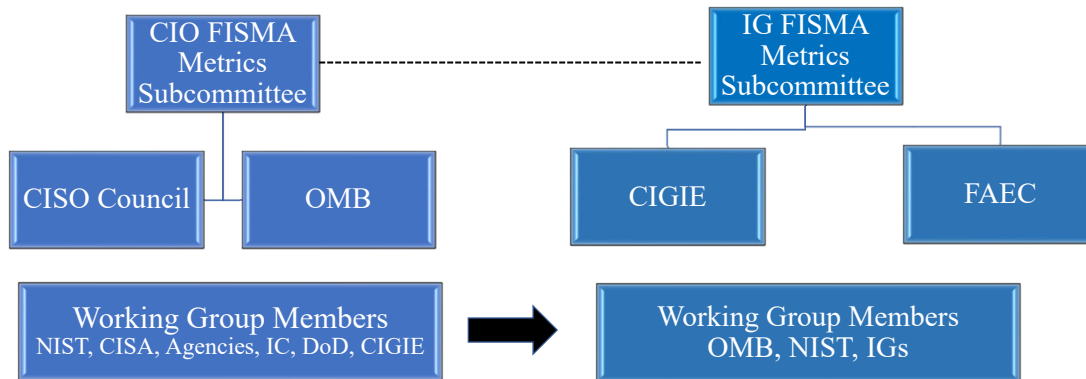
- Earlier this year, the CIGIE Technology Committee established a working group to develop a FISMA capstone report
- The goal of this working group is to analyze IG FISMA data and identify trends and perform statistical analysis on the metrics
- Report will include the results of a survey on IG experiences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

38

38

NONCONFIDENTIAL // EXTERNAL

CIO & IG FISMA Metrics Committees



39

39

NONCONFIDENTIAL // EXTERNAL

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

40

40

NONCONFIDENTIAL // EXTERNAL

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