Memorandum from the Office of the Inspector General

September 9, 2025

Aaron P. Melda

REQUEST FOR MANAGEMENT DECISION – AUDIT 2025-17548 – FEDERAL INFORMATION SECURITY MANAGEMENT ACT

Attached is the subject final report for your review and management decision. You are responsible for determining the necessary actions to take in response to our findings. Please advise us of your management decision within 60 days from the date of this report. In accordance with the Inspector General Act of 1978, as amended, the Office of the Inspector General is required to report to Congress semiannually regarding audits that remain unresolved after 6 months from the date of report issuance.

If you have any questions or wish to discuss our findings, please contact Sarah E. Huffman, Director, Information Technology Audits, at (865) 633-7345. We appreciate the courtesy and cooperation received from your staff during the audit.

Greg Stinson

Greg Stinson
Assistant Inspector General
(Audits and Evaluations)

MLC:KDS
Attachment
cc (Attachment):

TVA Board of Directors
Brett A. Atkins
Kaitlyn R. Bennett
Collins Bishop
Kenneth C. Carnes II
Hannah S. Clements
Sherri R. Collins
Melissa R. Crane
Jessica Dufner
Gregory G. Jackson
Joshua Linville
Melissa A. Livesey
Jill M. Matthews
Todd E. McCarter
Jeannette Mills
Donald A. Moul
Dustin C. Pate
Ronald R. Sanders II
Francisco J. Soutuyo
Kevin L. Tarver
Josh Thomas
Rebecca C. Tolene
William M. Trumm
Ben R. Wagner
OIG File No. 2025-17548

Office of the Inspector General

Audit Report

To the Vice President and Chief Information and Digital Officer, Technology and Innovation

FEDERAL INFORMATION SECURITY MODERNIZATION ACT

Audit Team
Melissa L. Conforti

Audit 2025-17548
September 9, 2025

ABBREVIATIONS

CDM	Continuous Diagnostics and Mitigation
DHS	Department of Homeland Security
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
IG	Inspector General
ISCM	Information Security Continuous Monitoring
ISP	Information Security Program
OMB	Office of Management and Budget
TVA	Tennessee Valley Authority

TABLE OF CONTENTS

APPENDICES

Audit 2025-17548 – Federal Information Security Modernization Act

EXECUTIVE SUMMARY

Why the OIG Did This Audit

The Federal Information Security Modernization Act of 2014 (FISMA) requires each agency's Inspector General (IG) to conduct an annual independent evaluation to determine the effectiveness of the information security program (ISP) and practices of its respective agency.

Our objective was to determine the effectiveness of the Tennessee Valley Authority's (TVA) ISP and practices as defined by the *FY 2025 IG FISMA Reporting Metrics*. Our audit scope was limited to answering the fiscal year (FY) 2025 IG metrics, which include 20 core and 5 supplemental IG metrics (within Appendix B). The 20 core IG metrics were chosen based on alignment with Executive Order 14028, *Improving the Nation's Cybersecurity*,[i] as well as recent Office of Management and Budget guidance to agencies in furtherance of the modernization of federal cybersecurity.

What the OIG Found

During the course of this audit, we utilized the methodology and metrics in the FY 2025 IG metrics (within Appendix B) in our annual independent evaluation to determine the effectiveness of TVA's ISP and practices. The FISMA methodology considers metrics at a maturity level 4 (managed and measurable) or higher to be at an effective level of security. Each metric was assessed to determine its maturity level, as described in Table 1 below.

FY 2025 IG FISMA Maturity Definitions	
Maturity Level	**Maturity Level Description**
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.

Table 1

[i] United States, Executive Order of the President [Joseph Biden] Compilation of Presidential Documents, *Executive Order 14028 - Improving the Nation's Cybersecurity*, May 17, 2021, < https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity>, accessed on July 25, 2022.

For FY 2025, IGs were required to test 20 core and 5 supplemental IG metrics that were aligned with the following six function areas in the National Institute of Standards and Technology's *Cybersecurity Framework 2.0*: Govern, Identify, Protect, Detect, Respond, and Recover. Our analysis of the metric results was used to determine the overall function maturity levels in Table 2 below.

Function	FY 2025 Core Assessed Maturity Level	FY 2025 Supplemental Assessed Maturity Level*	Overall Assessed Maturity Level	FY 2025 Rating
Govern	5.00	4.33	4.50	Effective
Identify	4.40	3.00	4.17	Effective
Protect	3.25	-	3.25	Ineffective
Detect	5.00	4.00	4.67	Effective
Respond	4.00	-	4.00	Effective
Recover	4.50	-	4.50	Effective
Average of Functions	**4.36**	**3.78**	**4.15**	**Effective**
* The five supplemental metrics did not cover the Protect, Respond, or Recover functions.				

Table 2

Based on our analysis of the FY 2025 IG metrics and associated maturity models, we determined TVA's ISP and practices were operating in an effective manner as defined by the *FY 2025 IG FISMA Reporting Metrics*. However, we identified areas for improvement in both the core and supplemental metrics to further improve TVA's ISP and practices.

What the OIG Recommends

We made five recommendations to TVA management to further increase the effectiveness of TVA's ISP and practices as defined by the *FY 2025 IG FISMA Reporting Metrics*. Our specific recommendations are included within the report.

TVA Management's Comments

In response to our draft audit report, TVA management agreed with the recommendations. See Appendix C for TVA management's complete response.

BACKGROUND

The Federal Information Security Modernization Act of 2014 (FISMA) requires each agency's Inspector General (IG) to conduct an annual independent evaluation to determine the effectiveness of the information security program (ISP) and practices of its respective agency. FISMA shifted to a continuous assessment process in fiscal year (FY) 2022. As a result, the Office of Management and Budget (OMB) and the Council of the Inspectors General on Integrity and Efficiency transitioned the IG metrics process to a multi-year cycle beginning in FY 2022. Specifically, 20 core IG metrics were selected to be evaluated annually, and the remaining IG metrics will be evaluated on a two-year cycle. The 20 core IG metrics were chosen based on alignment with Executive Order 14028, *Improving the Nation's Cybersecurity*,[1] as well as recent OMB guidance to agencies in furtherance of the modernization of federal cybersecurity.

In FY 2025, the IG metrics were organized into ten domains and aligned with the six function areas in the National Institute of Standards and Technology's *Cybersecurity Framework 2.0*: Govern, Identify, Protect, Detect, Respond, and Recover. This framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise and provides IGs with guidance for assessing the maturity of controls to address those risks.

The *FY 2025 IG FISMA Reporting Metrics* (Appendix B) were developed by OMB and the Council of the Inspectors General on Integrity and Efficiency, in consultation with the Federal Chief Information Officer Council and other stakeholders. For FY 2025, IGs were required to test 20 core and 5 supplemental IG metrics.

The results of our review were provided to OMB and Department of Homeland Security (DHS) through the use of their online reporting tool on July 17, 2025.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine the effectiveness of the Tennessee Valley Authority's (TVA) ISP and practices as defined by the *FY 2025 IG FISMA Reporting Metrics*. Our audit scope was limited to answering the FY 2025 IG metrics, which included the 20 core and 5 supplemental IG metrics (within Appendix B); therefore, the results of this audit are based on assessing these 25 IG metrics only. A complete discussion of our objective, scope, and methodology is included in Appendix A.

[1] United States, Executive Order of the President [Joseph Biden] Compilation of Presidential Documents, *Executive Order 14028 - Improving the Nation's Cybersecurity*, May 17, 2021, <https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity>, accessed on July 25, 2022.

FINDINGS

The FISMA methodology considers metrics at a maturity level 4 (managed and measurable) or higher to be at an effective level of security. Based on our analysis of the FY 2025 IG metrics and associated maturity models, we determined TVA's ISP and practices were operating in an effective manner as defined by the *FY 2025 IG FISMA Reporting Metrics.* Specifically, as shown in Table 1, we determined five of the six functions and the overall assessed maturity level were effective for FY 2025.

Function	FY 2025 Core Assessed Maturity Level	FY 2025 Supplemental Assessed Maturity Level*	Overall Assessed Maturity Level	FY 2025 Rating
Govern	5.00	4.33	4.50	Effective
Identify	4.40	3.00	4.17	Effective
Protect	3.25	-	3.25	Ineffective
Detect	5.00	4.00	4.67	Effective
Respond	4.00	-	4.00	Effective
Recover	4.50	-	4.50	Effective
Average of Functions	**4.36**	**3.78**	**4.15**	**Effective**

* The five supplemental metrics did not cover the Protect, Respond, or Recover functions.

Table 1

While we determined TVA's ISP and practices were operating in an effective manner as defined by the *FY 2025 IG FISMA Reporting Metrics*, we identified areas for improvement in both the core and FY 2025 supplemental metrics to further improve TVA's ISP and practices. Specifically, eight (six core and two supplemental) of the 25 IG metrics were not effective.

- Four core metrics had actions in progress to improve their maturity, which included Executive Order 14028, *Improving the Nation's Cybersecurity,* requirements and ongoing multi-year projects in progress. Completion of these actions in progress could further improve the effectiveness of TVA's ISP and practices, specifically in the Protect and Respond functions.
- Two core IG metrics had weaknesses that should be addressed by TVA management, including:
  - Information system inventory and system components.
  - Common secure configurations.
- Two supplemental metrics had weaknesses that should be addressed by TVA management, including:
  - Cybersecurity profiles.
  - Data and corresponding metadata inventories.

The following provides a detailed discussion of the areas identified for improvement to further increase the effectiveness of TVA's ISP and practices as defined by the FISMA Reporting Metrics.

CORE INSPECTOR GENERAL METRICS

Based on our analysis of the 20 core IG metrics, we identified weaknesses in two metrics that should be addressed to further improve the effectiveness of TVA's ISP and practices. Specifically, the weaknesses include information system inventory and system components in the Identify function and common secure configurations in the Protect function. Our FY 2024 FISMA audit[2] found weaknesses in these same areas that TVA management completed actions to address; however, we identified additional improvements that are needed.

Information System Inventory and System Components

TVA has defined policies, procedures, and processes for developing and maintaining a comprehensive and accurate inventory of information systems, including cloud systems, public-facing websites, third-party systems, and system interconnections. In response to our FY 2024 FISMA audit, TVA management (1) implemented automated monitoring via the DHS Continuous Diagnostics and Mitigation (CDM) program for components applicable to TVA's information security continuous monitoring strategy and (2) updated processes for developing and maintaining an accurate and complete inventory of TVA's information systems to include automation and near real-time updates. However, TVA has not consistently implemented these policies, procedures, and processes for its public-facing website inventory. In a recent audit,[3] we also identified TVA does not maintain an accurate and complete cloud inventory. In that audit report, we made recommendations to TVA management to address the issue. Without maintaining a comprehensive and accurate inventory of its information systems and system interconnections, TVA cannot ensure that the information systems are subject to the monitoring processes defined within the organization's Information Security Continuous Monitoring (ISCM) strategy.

Common Secure Configurations

TVA has defined policies and procedures for secure configurations, including documenting common secure configurations. In response to our FY 2024 FISMA audit, TVA management implemented, assessed, and maintained common secure configuration settings for the information systems we previously found to be noncompliant. However, TVA has not consistently implemented, assessed, and maintained secure configuration settings for other information systems. Additionally, TVA does not incorporate vulnerability scanning into the DHS CDM dashboard in accordance with Binding Operational Directive 23-01. Without consistent implementation, assessment, and maintenance of secure configuration settings for all its information systems and consistent usage of scanning capabilities against all systems on the network, TVA cannot adequately

[2] Audit Report 2024-17494, *Federal Information Security Modernization Act*, August 30, 2024.

[3] Audit Report 2024-17521, *Cloud Inventory*, June 17, 2025.

employ automation to help maintain an up-to-date, complete, accurate, and readily available view of the security configurations.

SUPPLEMENTAL INSPECTOR GENERAL METRICS

Based on our analysis of the five FY 2025 supplemental IG metrics, we identified weaknesses in two metrics that should be addressed to further improve the effectiveness of TVA's ISP and practices. Specifically, the weaknesses include (1) cybersecurity profiles and (2) data and corresponding metadata inventories in the Govern and Identify functions, respectively.

Cybersecurity Profiles

TVA has defined policies and procedures for developing and maintaining cybersecurity profiles. TVA has developed a current and target profile, considered changes to cybersecurity, and created and implemented an action plan. However, TVA's current and target profiles are not (1) refined periodically based on known risk exposure and residual risk, (2) aligned with TVA's risk strategy, or (3) monitored and progress was not reported in reaching its target profile.

Data and Corresponding Metadata Inventories

TVA has defined and consistently implemented policies, procedures, processes, and roles and responsibilities to maintain a comprehensive and accurate inventory of data and corresponding metadata for data types, as appropriate. Additionally, TVA has assigned data classifications to designated data types and implemented role-based access controls and encryption as security controls. However, TVA has not ensured the data and corresponding metadata in its data inventories are subject to the monitoring processes defined within the ISCM strategy.

RECOMMENDATIONS

We recommend the Vice President, Chief Information and Digital Officer, Information Technology:

1. Consistently implement the defined policies, procedures, and processes for developing and maintaining a comprehensive and accurate inventory for public-facing websites.

2. Implement, assess, and maintain common secure configuration settings for all information systems.

3. Incorporate vulnerability scanning into the CDM dashboard in accordance with Binding Operational Directive 23-01, in coordination with DHS as necessary.

4. Refine the profiles periodically based on known risk exposure and residual risk, align cybersecurity profiles with risk strategy, and periodically monitor and report on progress in reaching TVA's target profile.

5. Verify the data and corresponding metadata in the data inventories are subject to the monitoring processes defined within TVA's ISCM strategy.

TVA Management's Comments – In response to our draft audit report, TVA management agreed with the recommendations. See Appendix C for TVA management's complete response.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine the effectiveness of the Tennessee Valley Authority's (TVA) information security program (ISP) and practices as defined by the *FY 2025 IG Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* (Appendix B). Our audit scope was limited to answering the FY 2025 Inspector General (IG) metrics, which included 20 core and 5 supplemental IG metrics (within Appendix B) and excludes TVA Transmission, Generation, and Nuclear. The security controls significant to the objective were incorporated into the FY 2025 IG metrics and associated maturity models.

To accomplish our objective, we:

- Reviewed TVA documentation to corroborate our understanding and assess the current state of TVA's ISP, including:
  - Relevant TVA agency-wide and business unit specific policies, procedures, and documents (such as Standard Programs and Processes and Work Instructions).
  - Information Technology organizational chart.
- Reviewed previous Office of Inspector General audit reports to include TVA's (1) compliance with the FISMA in FY 2022,[1] FY 2023,[2] and FY 2024;[3] (2) corporate wi-fi security;[4] (3) privacy program;[5] (4) SharePoint access management;[6] (5) cybersecurity vulnerability management;[7] and (6) cloud inventory[8] for relevant findings.
- Inquired with TVA Information Technology personnel as necessary to gain an understanding and clarification of the policies, processes, and current state of TVA's ISP.
- Reviewed a list of TVA's information systems and judgmentally selected six based on risk of data loss to determine whether TVA consistently implements and maintains a comprehensive and accurate inventory of its data and corresponding metadata for its data types.
- Assessed the maturity level for 20 core and 5 supplemental IG metrics contained in the *FY 2025 IG FISMA Reporting Metrics.*
- Calculated an average of the FY 2025 metrics for each function and corresponding domains included in Table 1 below.

[1] Audit Report 2022-17370, *Federal Information Security Modernization Act*, September 19, 2022.

[2] Audit Report 2023-17423, *Federal Information Security Modernization Act*, September 26, 2023.

[3] Audit Report 2024-17494, *Federal Information Security Modernization Act*, August 30, 2024.

[4] Audit Report 2023-17434, *Corporate Wi-Fi Security*, April 29, 2024.

[5] Audit Report 2024-17478, *TVA's Privacy Program*, November 7, 2024.

[6] Audit Report 2023-17423, *SharePoint Access Management*, August 7, 2024.

[7] Audit Report 2024-17508, *Cybersecurity Vulnerability Management*, January 30, 2025.

[8] Audit Report 2024-17521, *Cloud Inventory*, June 17, 2025.

FY 2025 FISMA Functions and Corresponding Domains	
Function	**Domain**
Govern	Cybersecurity Governance Cybersecurity Supply Chain Risk Management
Identify	Risk and Asset 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

Table 1

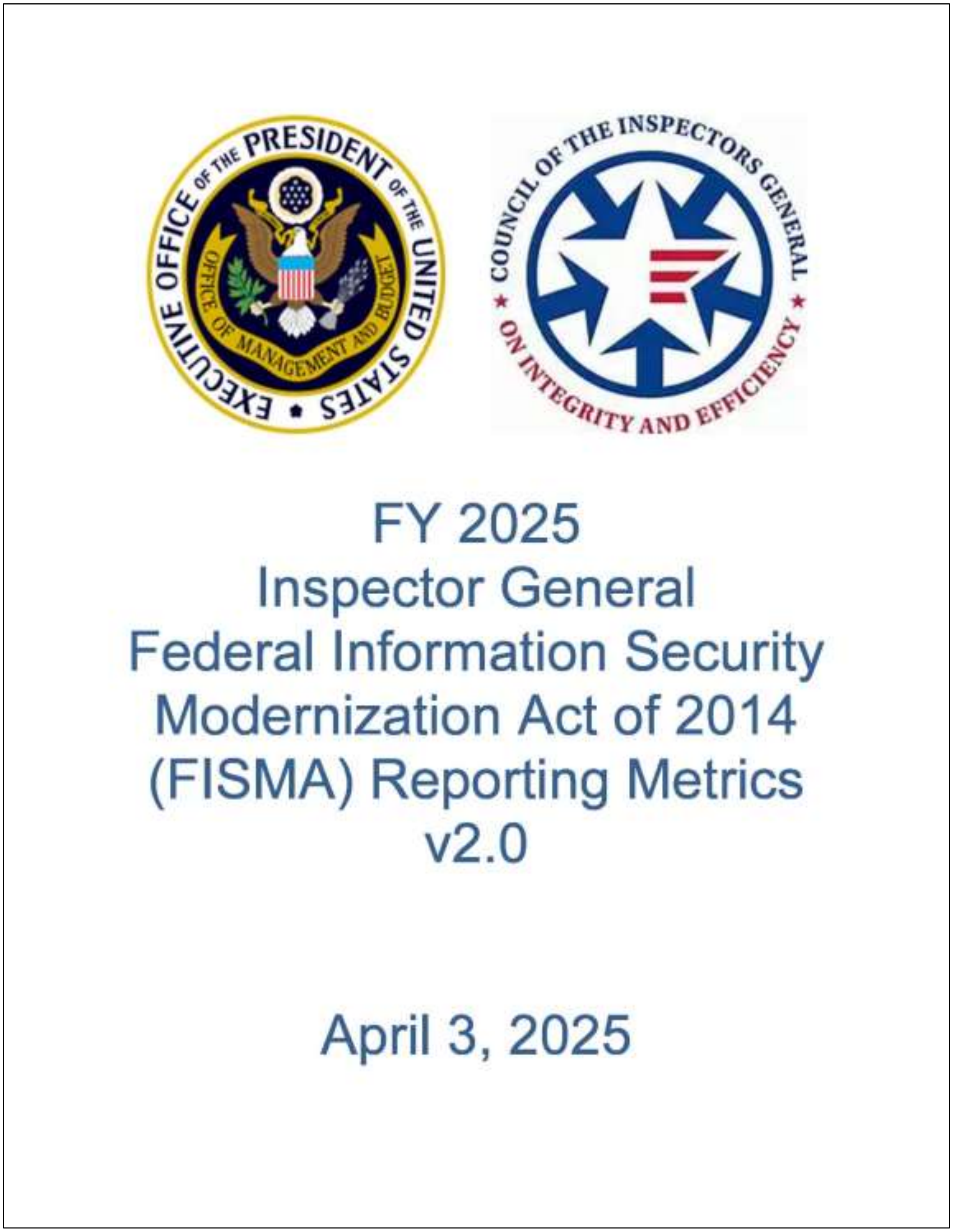
During the course of this audit, we determined the overall effectiveness of TVA's ISP and practices by assessing the 25 IG metrics (within Appendix B) on a maturity model spectrum. Table 2 below details the five maturity model levels.

FY 2025 IG FISMA Maturity Definitions	
Maturity Level	**Maturity Level Description**
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.

Table 2

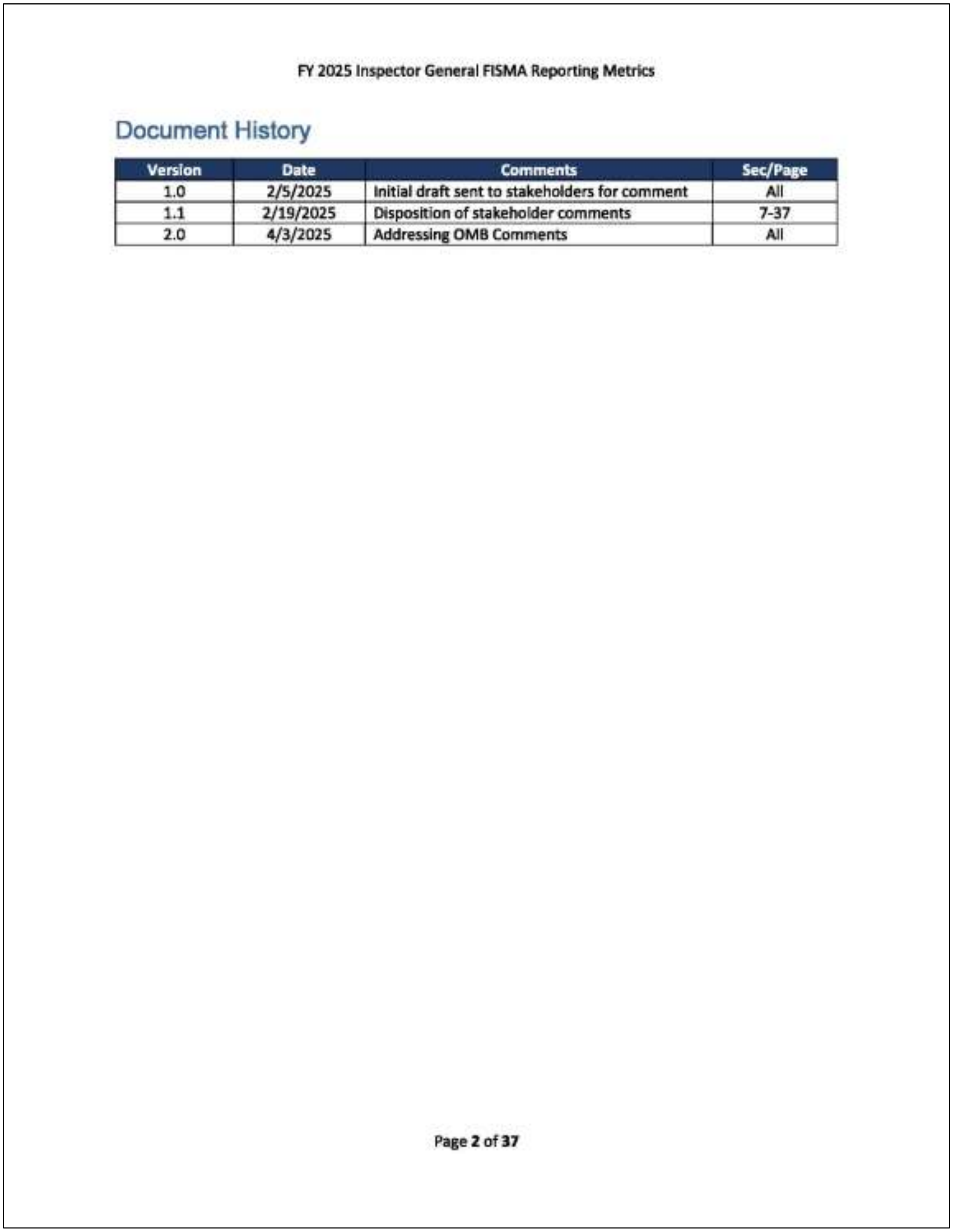
The maturity level was determined by answering the related FY 2025 IG metrics, which included 20 core and 5 supplemental IG metrics and using the average of the metrics in a particular domain to determine the effectiveness of individual function areas and the overall program. The FISMA methodology considers metrics at a maturity level 4 (managed and measurable) or higher to be at an effective level of security.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.



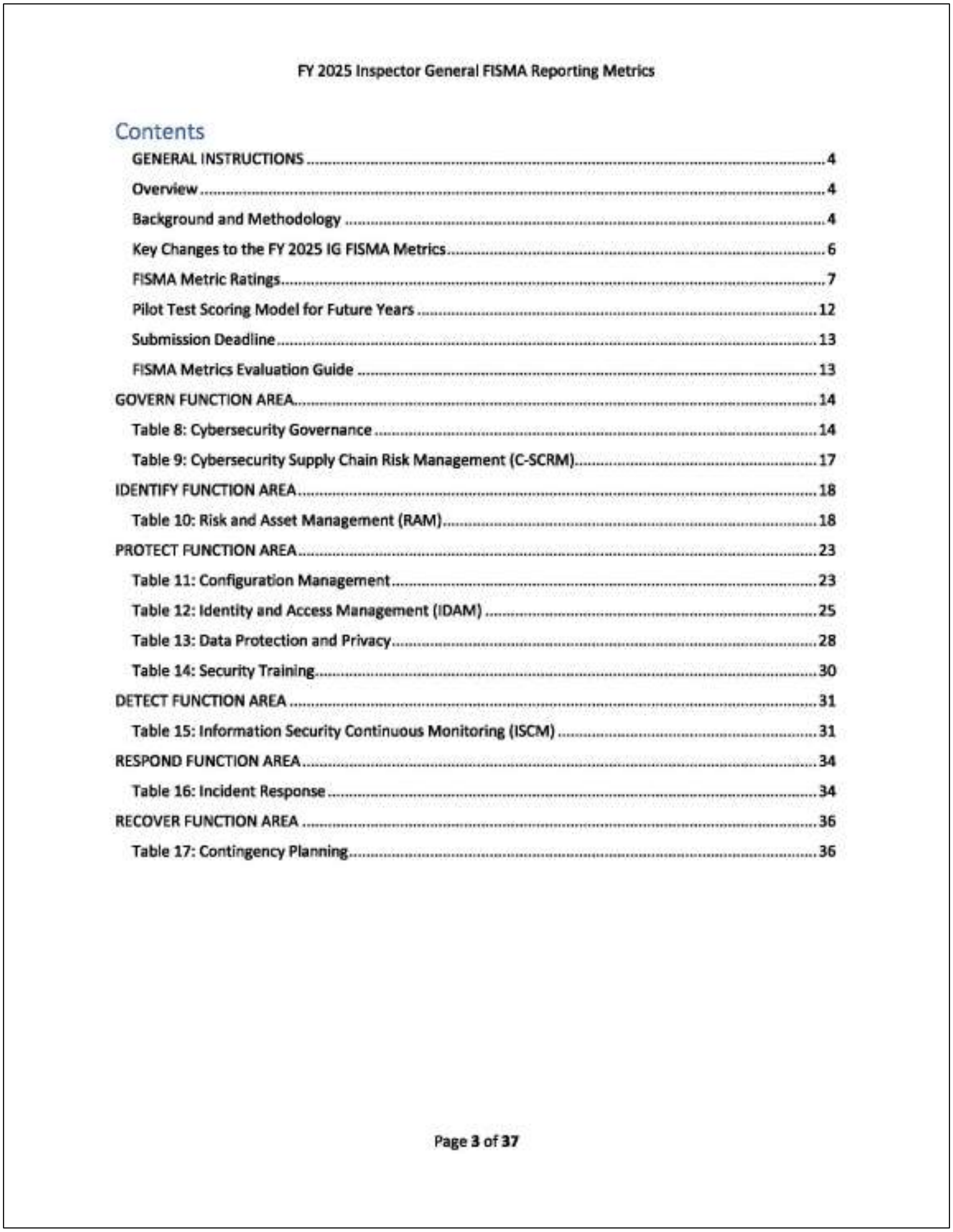
FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics v2.0

April 3, 2025

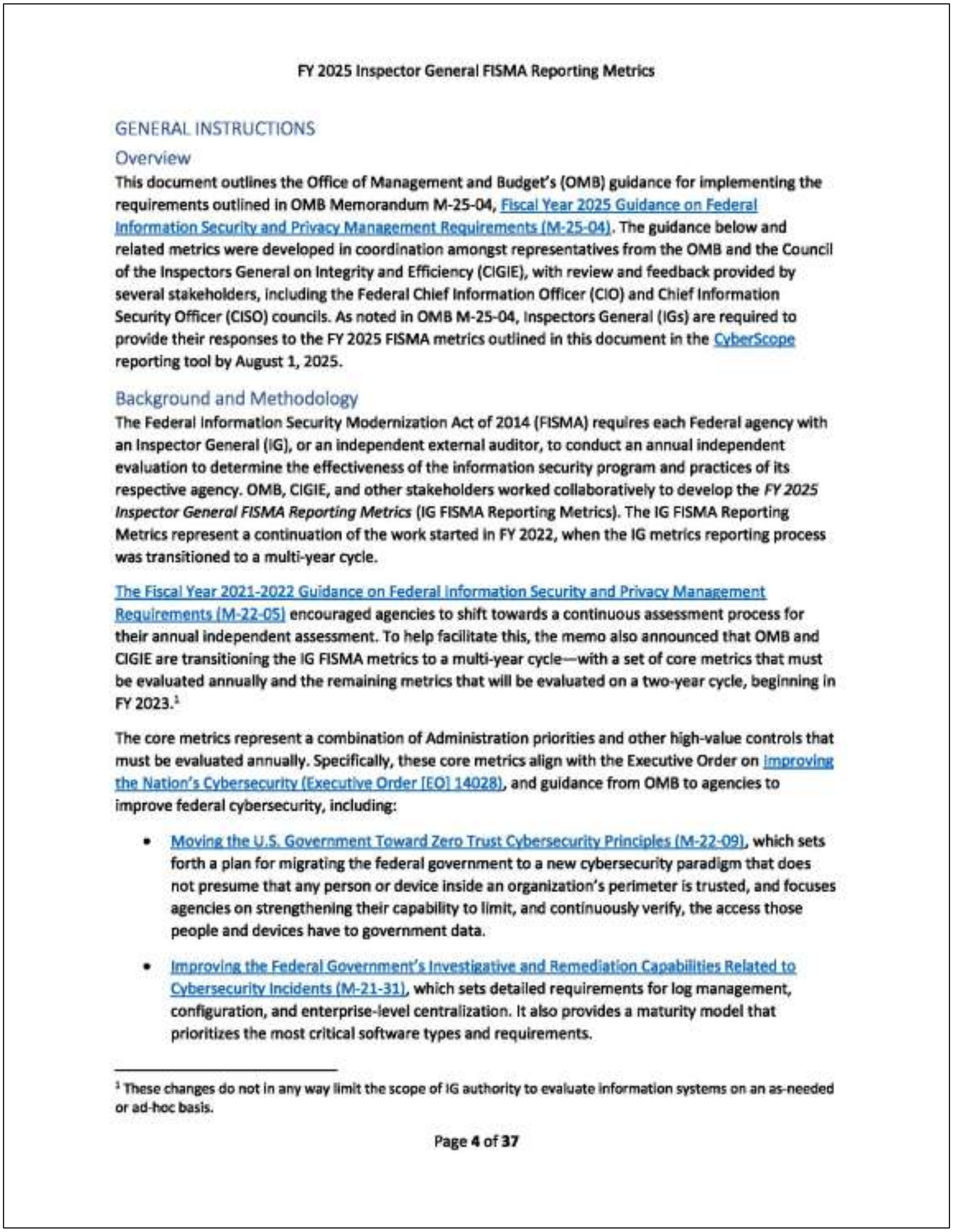


Document History

Version	Date	Comments	Sec/Page
1.0	2/5/2025	Initial draft sent to stakeholders for comment	All
1.1	2/19/2025	Disposition of stakeholder comments	7-37
2.0	4/3/2025	Addressing OMB Comments	All



Contents



GENERAL INSTRUCTIONS

Overview

This document outlines the Office of Management and Budget's (OMB) guidance for implementing the requirements outlined in OMB Memorandum M-25-04, Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements (M-25-04). The guidance below and related metrics were developed in coordination amongst representatives from the OMB and the Council of the Inspectors General on Integrity and Efficiency (CIGIE), with review and feedback provided by several stakeholders, including the Federal Chief Information Officer (CIO) and Chief Information Security Officer (CISO) councils. As noted in OMB M-25-04, Inspectors General (IGs) are required to provide their responses to the FY 2025 FISMA metrics outlined in this document in the CyberScope reporting tool by August 1, 2025.

Background and Methodology

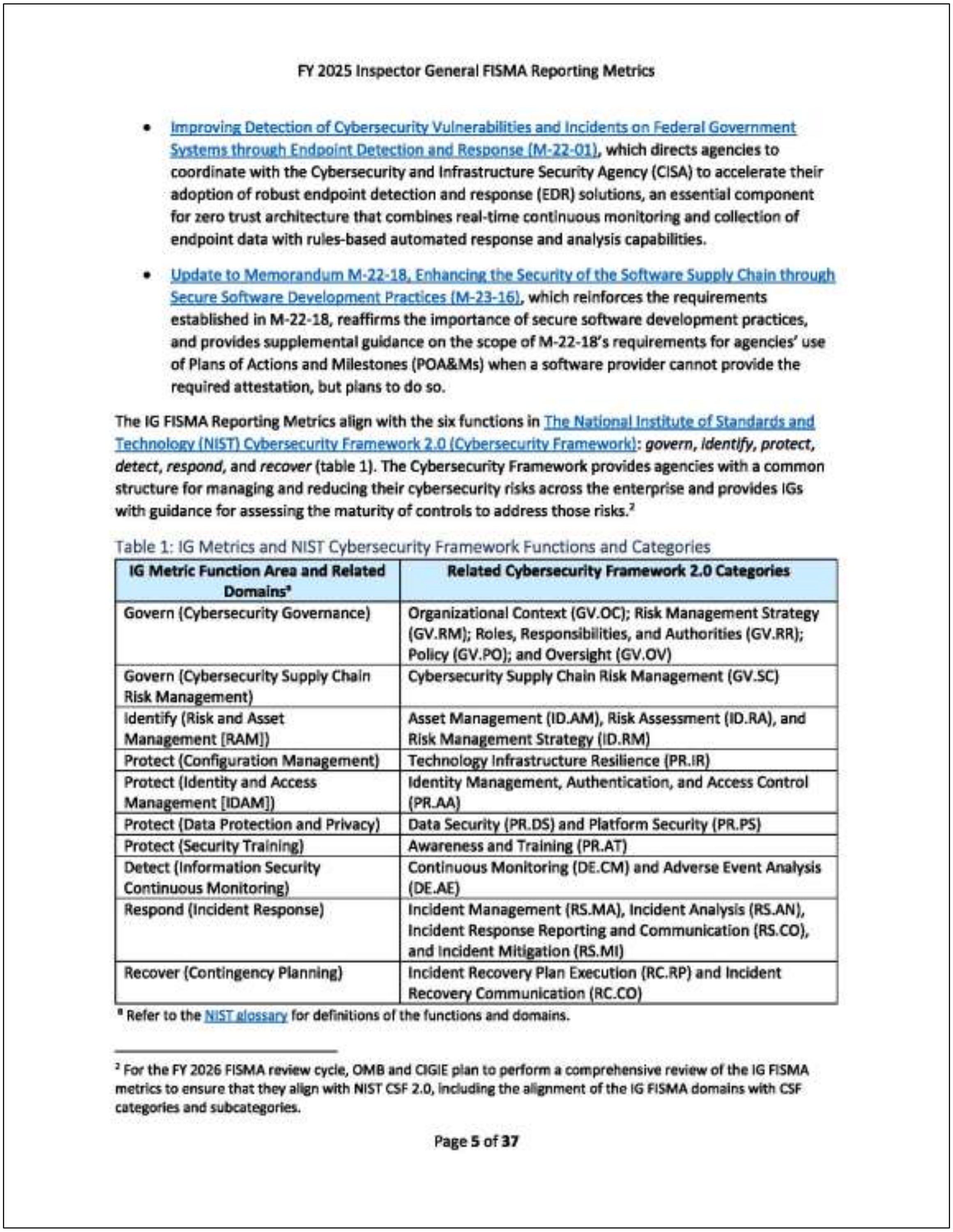
The Federal Information Security Modernization Act of 2014 (FISMA) requires each Federal agency with an Inspector General (IG), or an independent external auditor, to conduct an annual independent evaluation to determine the effectiveness of the information security program and practices of its respective agency. OMB, CIGIE, and other stakeholders worked collaboratively to develop the *FY 2025 Inspector General FISMA Reporting Metrics* (IG FISMA Reporting Metrics). The IG FISMA Reporting Metrics represent a continuation of the work started in FY 2022, when the IG metrics reporting process was transitioned to a multi-year cycle.

The Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements (M-22-05) encouraged agencies to shift towards a continuous assessment process for their annual independent assessment. To help facilitate this, the memo also announced that OMB and CIGIE are transitioning the IG FISMA metrics to a multi-year cycle—with a set of core metrics that must be evaluated annually and the remaining metrics that will be evaluated on a two-year cycle, beginning in FY 2023.[1]

The core metrics represent a combination of Administration priorities and other high-value controls that must be evaluated annually. Specifically, these core metrics align with the Executive Order on Improving the Nation's Cybersecurity (Executive Order [EO] 14028), and guidance from OMB to agencies to improve federal cybersecurity, including:

- Moving the U.S. Government Toward Zero Trust Cybersecurity Principles (M-22-09), which sets forth a plan for migrating the federal government to a new cybersecurity paradigm that does not presume that any person or device inside an organization's perimeter is trusted, and focuses agencies on strengthening their capability to limit, and continuously verify, the access those people and devices have to government data.
- Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents (M-21-31), which sets detailed requirements for log management, configuration, and enterprise-level centralization. It also provides a maturity model that prioritizes the most critical software types and requirements.

[1] 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.



- Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response (M-22-01), which directs agencies to coordinate with the Cybersecurity and Infrastructure Security Agency (CISA) to accelerate their adoption of robust endpoint detection and response (EDR) solutions, an essential component for zero trust architecture that combines real-time continuous monitoring and collection of endpoint data with rules-based automated response and analysis capabilities.
- Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices (M-23-16), which reinforces the requirements established in M-22-18, reaffirms the importance of secure software development practices, and provides supplemental guidance on the scope of M-22-18's requirements for agencies' use of Plans of Actions and Milestones (POA&Ms) when a software provider cannot provide the required attestation, but plans to do so.

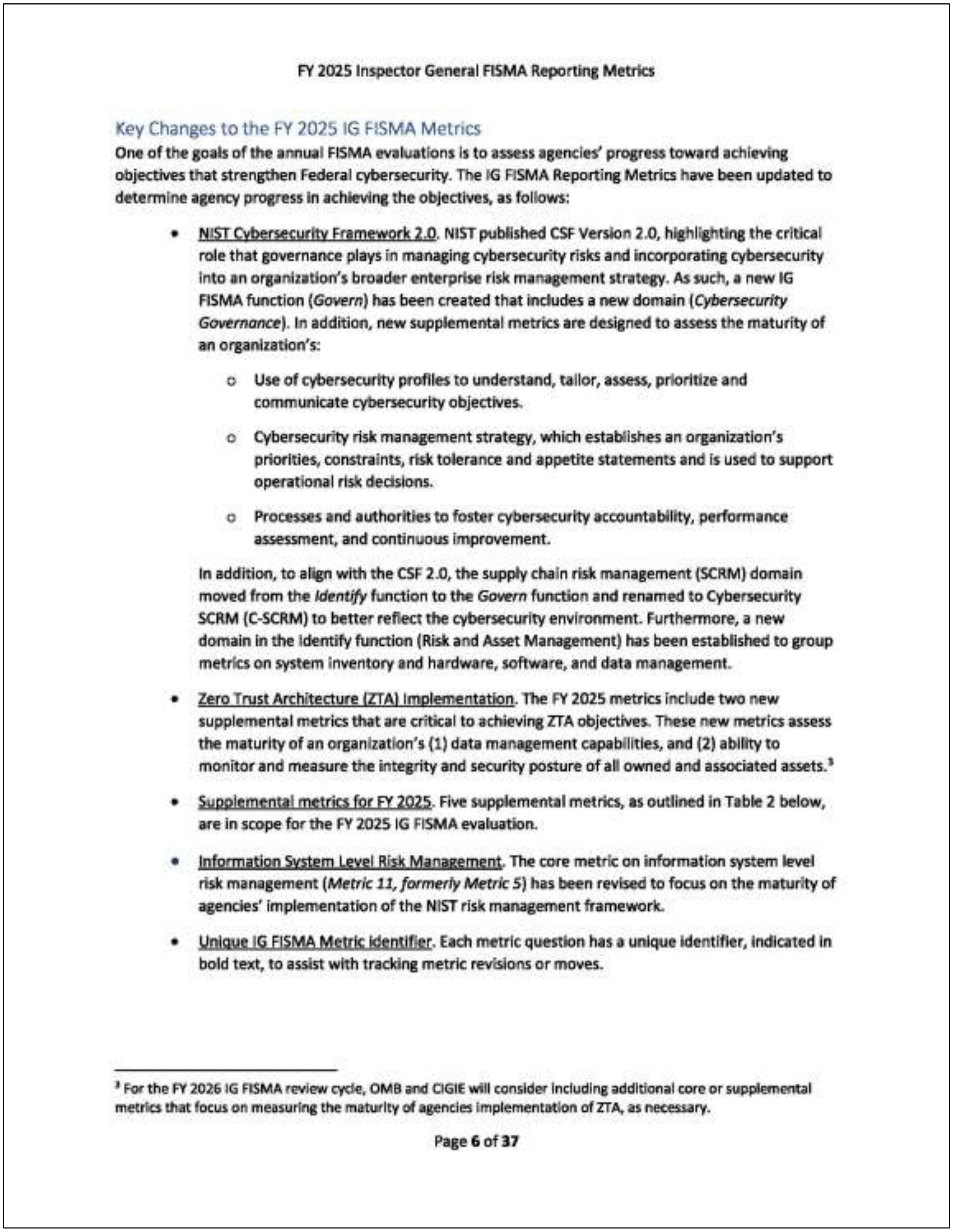
The IG FISMA Reporting Metrics align with the six functions in The National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0 (Cybersecurity Framework): *govern*, *identify*, *protect*, *detect*, *respond*, and *recover* (table 1). The Cybersecurity Framework provides agencies with a common structure for managing and reducing their cybersecurity risks across the enterprise and provides IGs with guidance for assessing the maturity of controls to address those risks.[2]

Table 1: IG Metrics and NIST Cybersecurity Framework Functions and Categories

IG Metric Function Area and Related Domains[a]	Related Cybersecurity Framework 2.0 Categories
Govern (Cybersecurity Governance)	Organizational Context (GV.OC); Risk Management Strategy (GV.RM); Roles, Responsibilities, and Authorities (GV.RR); Policy (GV.PO); and Oversight (GV.OV)
Govern (Cybersecurity Supply Chain Risk Management)	Cybersecurity Supply Chain Risk Management (GV.SC)
Identify (Risk and Asset Management [RAM])	Asset Management (ID.AM), Risk Assessment (ID.RA), and Risk Management Strategy (ID.RM)
Protect (Configuration Management)	Technology Infrastructure Resilience (PR.IR)
Protect (Identity and Access Management [IDAM])	Identity Management, Authentication, and Access Control (PR.AA)
Protect (Data Protection and Privacy)	Data Security (PR.DS) and Platform Security (PR.PS)
Protect (Security Training)	Awareness and Training (PR.AT)
Detect (Information Security Continuous Monitoring)	Continuous Monitoring (DE.CM) and Adverse Event Analysis (DE.AE)
Respond (Incident Response)	Incident Management (RS.MA), Incident Analysis (RS.AN), Incident Response Reporting and Communication (RS.CO), and Incident Mitigation (RS.MI)
Recover (Contingency Planning)	Incident Recovery Plan Execution (RC.RP) and Incident Recovery Communication (RC.CO)

[a] Refer to the NIST glossary for definitions of the functions and domains.

[2] For the FY 2026 FISMA review cycle, OMB and CIGIE plan to perform a comprehensive review of the IG FISMA metrics to ensure that they align with NIST CSF 2.0, including the alignment of the IG FISMA domains with CSF categories and subcategories.



Key Changes to the FY 2025 IG FISMA Metrics

One of the goals of the annual FISMA evaluations is to assess agencies' progress toward achieving objectives that strengthen Federal cybersecurity. The IG FISMA Reporting Metrics have been updated to determine agency progress in achieving the objectives, as follows:

- NIST Cybersecurity Framework 2.0. NIST published CSF Version 2.0, highlighting the critical role that governance plays in managing cybersecurity risks and incorporating cybersecurity into an organization's broader enterprise risk management strategy. As such, a new IG FISMA function (*Govern*) has been created that includes a new domain (*Cybersecurity Governance*). In addition, new supplemental metrics are designed to assess the maturity of an organization's:
  - Use of cybersecurity profiles to understand, tailor, assess, prioritize and communicate cybersecurity objectives.
  - Cybersecurity risk management strategy, which establishes an organization's priorities, constraints, risk tolerance and appetite statements and is used to support operational risk decisions.
  - Processes and authorities to foster cybersecurity accountability, performance assessment, and continuous improvement.

  In addition, to align with the CSF 2.0, the supply chain risk management (SCRM) domain moved from the *Identify* function to the *Govern* function and renamed to Cybersecurity SCRM (C-SCRM) to better reflect the cybersecurity environment. Furthermore, a new domain in the Identify function (Risk and Asset Management) has been established to group metrics on system inventory and hardware, software, and data management.
- Zero Trust Architecture (ZTA) Implementation. The FY 2025 metrics include two new supplemental metrics that are critical to achieving ZTA objectives. These new metrics assess the maturity of an organization's (1) data management capabilities, and (2) ability to monitor and measure the integrity and security posture of all owned and associated assets.[3]
- Supplemental metrics for FY 2025. Five supplemental metrics, as outlined in Table 2 below, are in scope for the FY 2025 IG FISMA evaluation.
- Information System Level Risk Management. The core metric on information system level risk management (*Metric 11, formerly Metric 5*) has been revised to focus on the maturity of agencies' implementation of the NIST risk management framework.
- Unique IG FISMA Metric Identifier. Each metric question has a unique identifier, indicated in bold text, to assist with tracking metric revisions or moves.

[3] For the FY 2026 IG FISMA review cycle, OMB and CIGIE will consider including additional core or supplemental metrics that focus on measuring the maturity of agencies implementation of ZTA, as necessary.

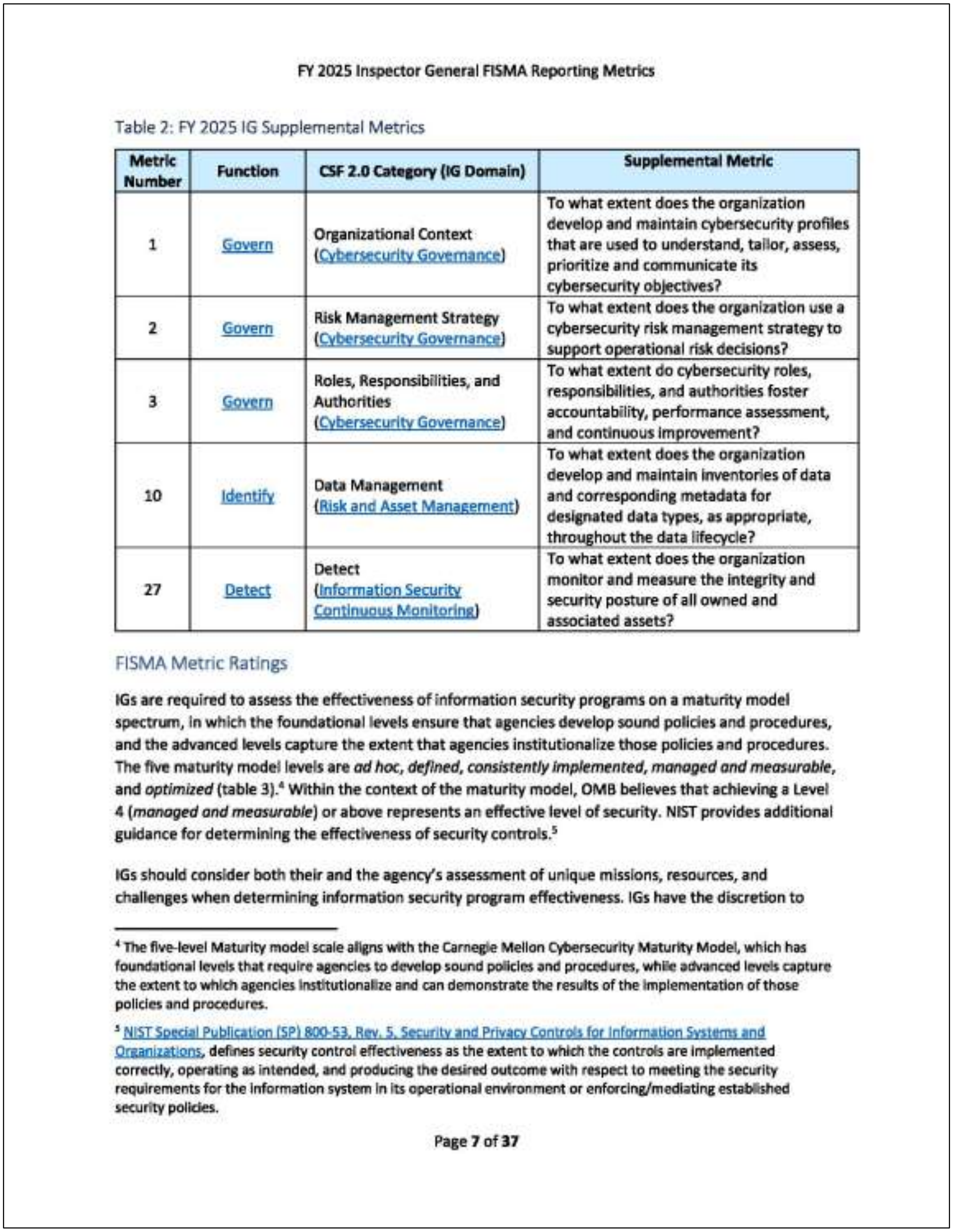


Table 2: FY 2025 IG Supplemental Metrics

Metric Number	Function	CSF 2.0 Category (IG Domain)	Supplemental Metric
1	Govern	Organizational Context (Cybersecurity Governance)	To what extent does the organization develop and maintain cybersecurity profiles that are used to understand, tailor, assess, prioritize and communicate its cybersecurity objectives?
2	Govern	Risk Management Strategy (Cybersecurity Governance)	To what extent does the organization use a cybersecurity risk management strategy to support operational risk decisions?
3	Govern	Roles, Responsibilities, and Authorities (Cybersecurity Governance)	To what extent do cybersecurity roles, responsibilities, and authorities foster accountability, performance assessment, and continuous improvement?
10	Identify	Data Management (Risk and Asset Management)	To what extent does the organization develop and maintain inventories of data and corresponding metadata for designated data types, as appropriate, throughout the data lifecycle?
27	Detect	Detect (Information Security Continuous Monitoring)	To what extent does the organization monitor and measure the integrity and security posture of all owned and associated assets?

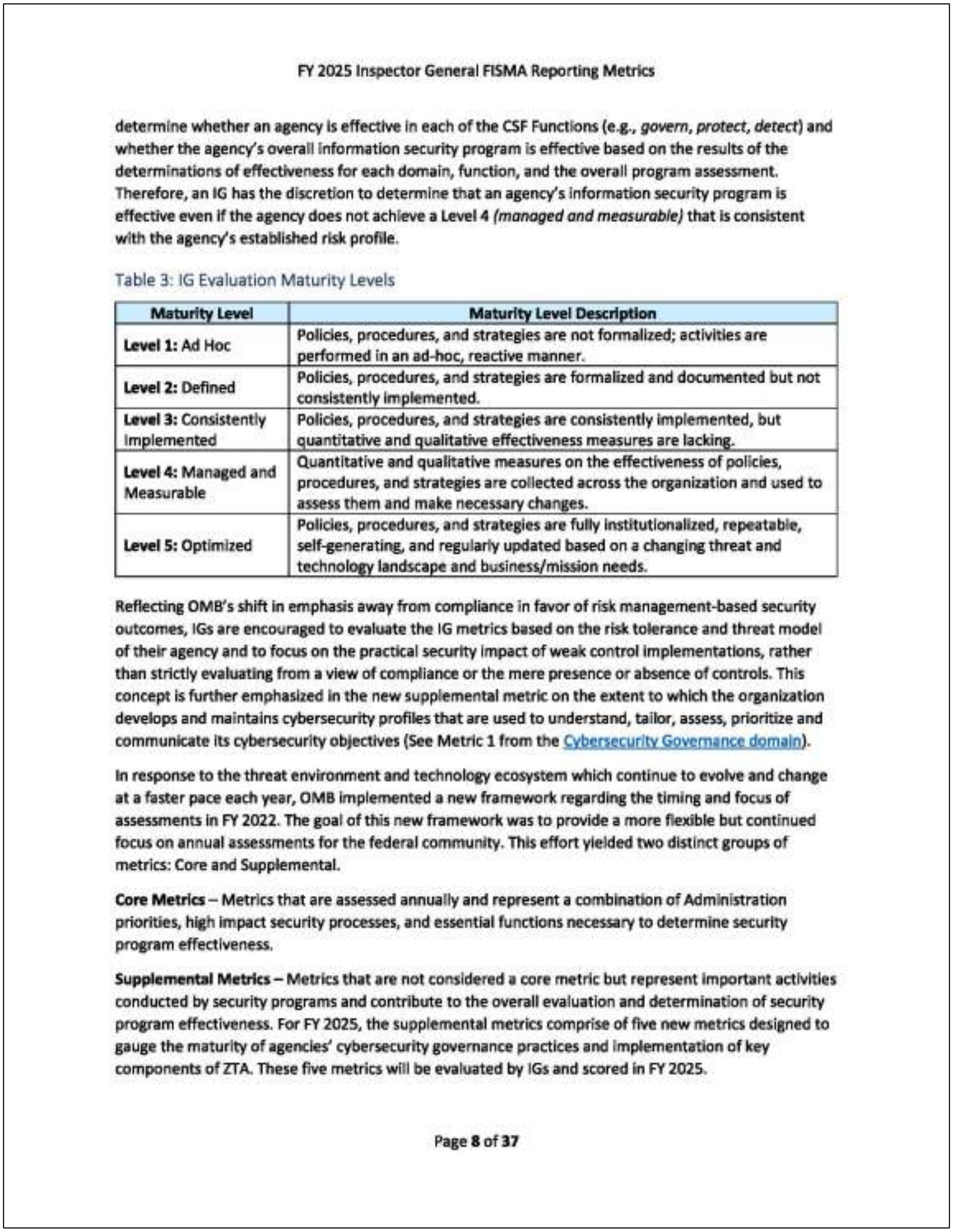
FISMA Metric Ratings

IGs are required to assess the effectiveness of information security programs on a maturity model spectrum, in which the foundational levels ensure that agencies develop sound policies and procedures, and the advanced levels capture the extent that agencies institutionalize those policies and procedures. The five maturity model levels are *ad hoc*, *defined*, *consistently implemented*, *managed and measurable*, and *optimized* (table 3).[4] Within the context of the maturity model, OMB believes that achieving a Level 4 (*managed and measurable*) or above represents an effective level of security. NIST provides additional guidance for determining the effectiveness of security controls.[5]

IGs should consider both their and the agency's assessment of unique missions, resources, and challenges when determining information security program effectiveness. IGs have the discretion to

[4] The five-level Maturity model scale aligns with the Carnegie Mellon Cybersecurity Maturity Model, which has foundational levels that require agencies to develop sound policies and procedures, while advanced levels capture the extent to which agencies institutionalize and can demonstrate the results of the implementation of those policies and procedures.

[5] NIST Special Publication (SP) 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations, defines security control effectiveness as the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment or enforcing/mediating established security policies.



determine whether an agency is effective in each of the CSF Functions (e.g., *govern*, *protect*, *detect*) and whether the agency's overall information security program is effective based on the results of the determinations of effectiveness for each domain, function, and the overall program assessment. Therefore, an IG has the discretion to determine that an agency's information security program is effective even if the agency does not achieve a Level 4 *(managed and measurable)* that is consistent with the agency's established risk profile.

Table 3: IG Evaluation Maturity Levels

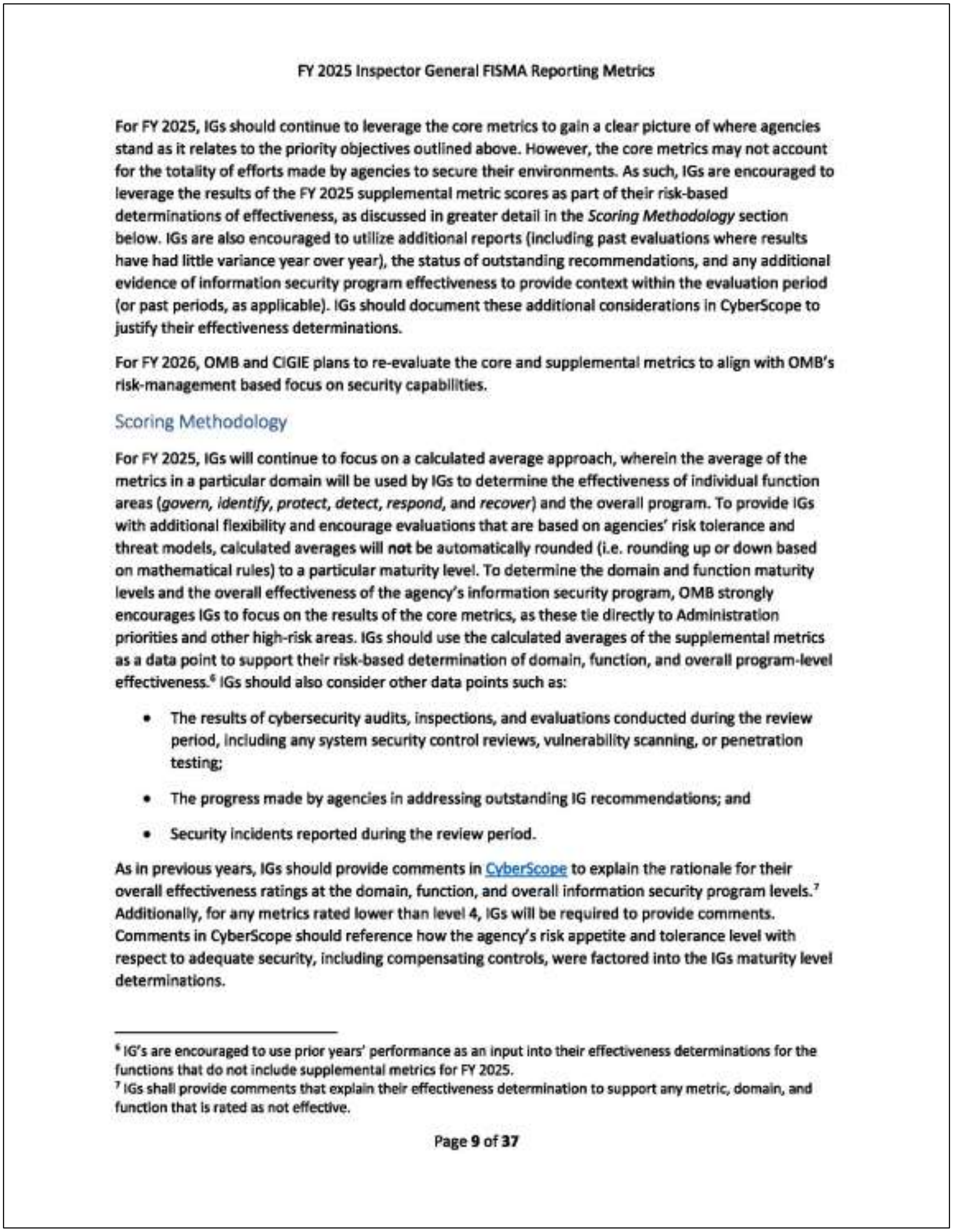
Maturity Level	Maturity Level Description
Level 1: Ad Hoc	Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategies are formalized and documented but not consistently implemented.
Level 3: Consistently 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, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Reflecting OMB's shift in emphasis away from compliance in favor of risk management-based security outcomes, IGs are encouraged to evaluate the IG metrics based on the risk tolerance and threat model of their agency and to focus on the practical security impact of weak control implementations, rather than strictly evaluating from a view of compliance or the mere presence or absence of controls. This concept is further emphasized in the new supplemental metric on the extent to which the organization develops and maintains cybersecurity profiles that are used to understand, tailor, assess, prioritize and communicate its cybersecurity objectives (See Metric 1 from the Cybersecurity Governance domain).

In response to the threat environment and technology ecosystem which continue to evolve and change at a faster pace each year, OMB implemented a new framework regarding the timing and focus of assessments in FY 2022. The goal of this new framework was to provide a more flexible but continued focus on annual assessments for the federal community. This effort yielded two distinct groups of metrics: Core and Supplemental.

Core Metrics – Metrics that are assessed annually and represent a combination of Administration priorities, high impact security processes, and essential functions necessary to determine security program effectiveness.

Supplemental Metrics – Metrics that are not considered a core metric but represent important activities conducted by security programs and contribute to the overall evaluation and determination of security program effectiveness. For FY 2025, the supplemental metrics comprise of five new metrics designed to gauge the maturity of agencies' cybersecurity governance practices and implementation of key components of ZTA. These five metrics will be evaluated by IGs and scored in FY 2025.



For FY 2025, IGs should continue to leverage the core metrics to gain a clear picture of where agencies stand as it relates to the priority objectives outlined above. However, the core metrics may not account for the totality of efforts made by agencies to secure their environments. As such, IGs are encouraged to leverage the results of the FY 2025 supplemental metric scores as part of their risk-based determinations of effectiveness, as discussed in greater detail in the *Scoring Methodology* section below. IGs are also encouraged to utilize additional reports (including past evaluations where results have had little variance year over year), the status of outstanding recommendations, and any additional evidence of information security program effectiveness to provide context within the evaluation period (or past periods, as applicable). IGs should document these additional considerations in CyberScope to justify their effectiveness determinations.

For FY 2026, OMB and CIGIE plans to re-evaluate the core and supplemental metrics to align with OMB's risk-management based focus on security capabilities.

Scoring Methodology

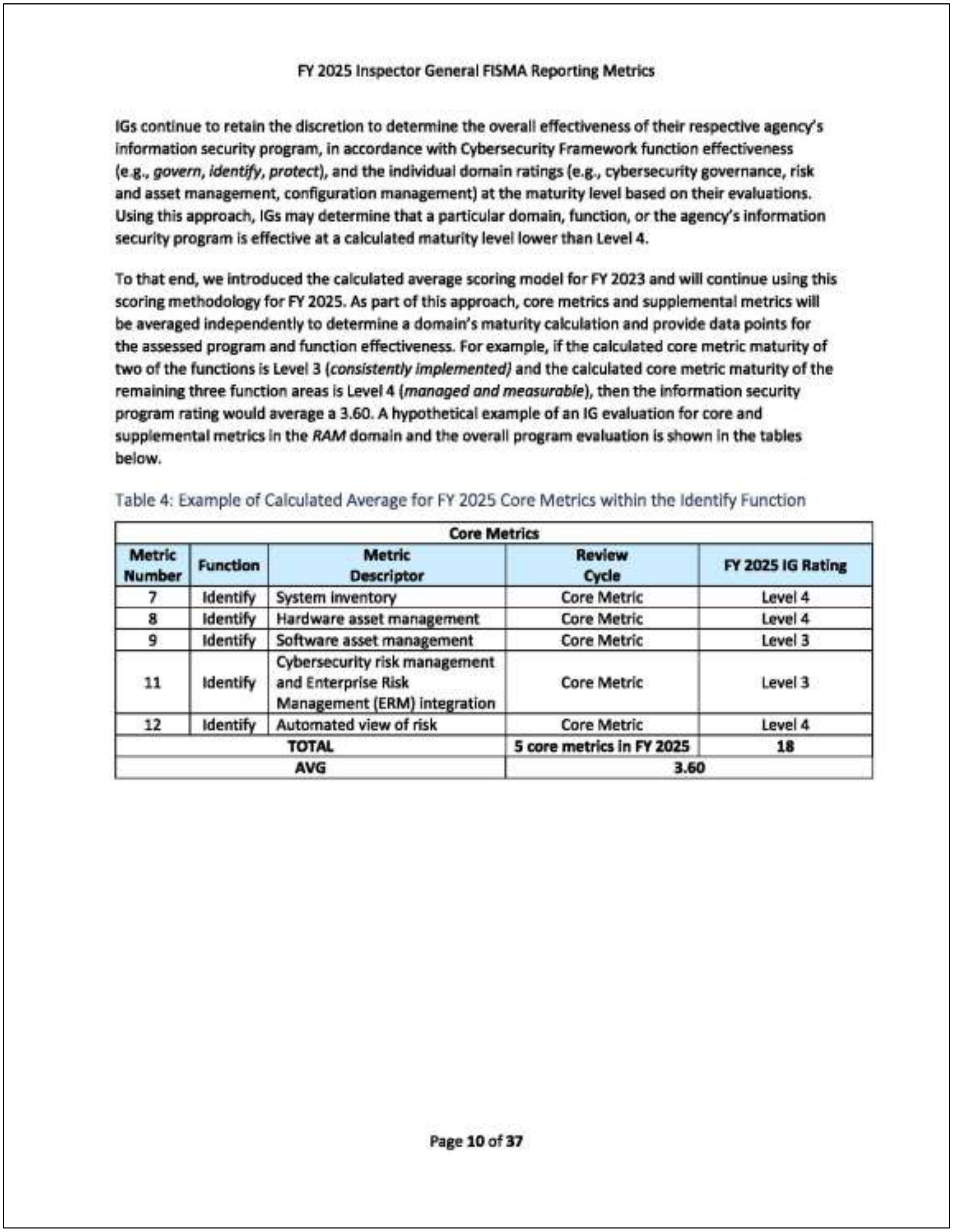
For FY 2025, IGs will continue to focus on a calculated average approach, wherein the average of the metrics in a particular domain will be used by IGs to determine the effectiveness of individual function areas (*govern*, *identify*, *protect*, *detect*, *respond*, and *recover*) and the overall program. To provide IGs with additional flexibility and encourage evaluations that are based on agencies' risk tolerance and threat models, calculated averages will **not** be automatically rounded (i.e. rounding up or down based on mathematical rules) to a particular maturity level. To determine the domain and function maturity levels and the overall effectiveness of the agency's information security program, OMB strongly encourages IGs to focus on the results of the core metrics, as these tie directly to Administration priorities and other high-risk areas. IGs should use the calculated averages of the supplemental metrics as a data point to support their risk-based determination of domain, function, and overall program-level effectiveness.[6] IGs should also consider other data points such as:

- The results of cybersecurity audits, inspections, and evaluations conducted during the review period, including any system security control reviews, vulnerability scanning, or penetration testing;
- The progress made by agencies in addressing outstanding IG recommendations; and
- Security incidents reported during the review period.

As in previous years, IGs should provide comments in CyberScope to explain the rationale for their overall effectiveness ratings at the domain, function, and overall information security program levels.[7] Additionally, for any metrics rated lower than level 4, IGs will be required to provide comments. Comments in CyberScope should reference how the agency's risk appetite and tolerance level with respect to adequate security, including compensating controls, were factored into the IGs maturity level determinations.

[6] IG's are encouraged to use prior years' performance as an input into their effectiveness determinations for the functions that do not include supplemental metrics for FY 2025.

[7] IGs shall provide comments that explain their effectiveness determination to support any metric, domain, and function that is rated as not effective.



IGs continue to retain the discretion to determine the overall effectiveness of their respective agency's information security program, in accordance with Cybersecurity Framework function effectiveness (e.g., *govern*, *identify*, *protect*), and the individual domain ratings (e.g., cybersecurity governance, risk and asset management, configuration management) at the maturity level based on their evaluations. Using this approach, IGs may determine that a particular domain, function, or the agency's information security program is effective at a calculated maturity level lower than Level 4.

To that end, we introduced the calculated average scoring model for FY 2023 and will continue using this scoring methodology for FY 2025. As part of this approach, core metrics and supplemental metrics will be averaged independently to determine a domain's maturity calculation and provide data points for the assessed program and function effectiveness. For example, if the calculated core metric maturity of two of the functions is Level 3 (*consistently implemented)* and the calculated core metric maturity of the remaining three function areas is Level 4 (*managed and measurable*), then the information security program rating would average a 3.60. A hypothetical example of an IG evaluation for core and supplemental metrics in the *RAM* domain and the overall program evaluation is shown in the tables below.

Table 4: Example of Calculated Average for FY 2025 Core Metrics within the Identify Function

Core Metrics				
Metric Number	**Function**	**Metric Descriptor**	**Review Cycle**	**FY 2025 IG Rating**
7	Identify	System inventory	Core Metric	Level 4
8	Identify	Hardware asset management	Core Metric	Level 4
9	Identify	Software asset management	Core Metric	Level 3
11	Identify	Cybersecurity risk management and Enterprise Risk Management (ERM) integration	Core Metric	Level 3
12	Identify	Automated view of risk	Core Metric	Level 4
TOTAL			**5 core metrics in FY 2025**	**18**
AVG			**3.60**	

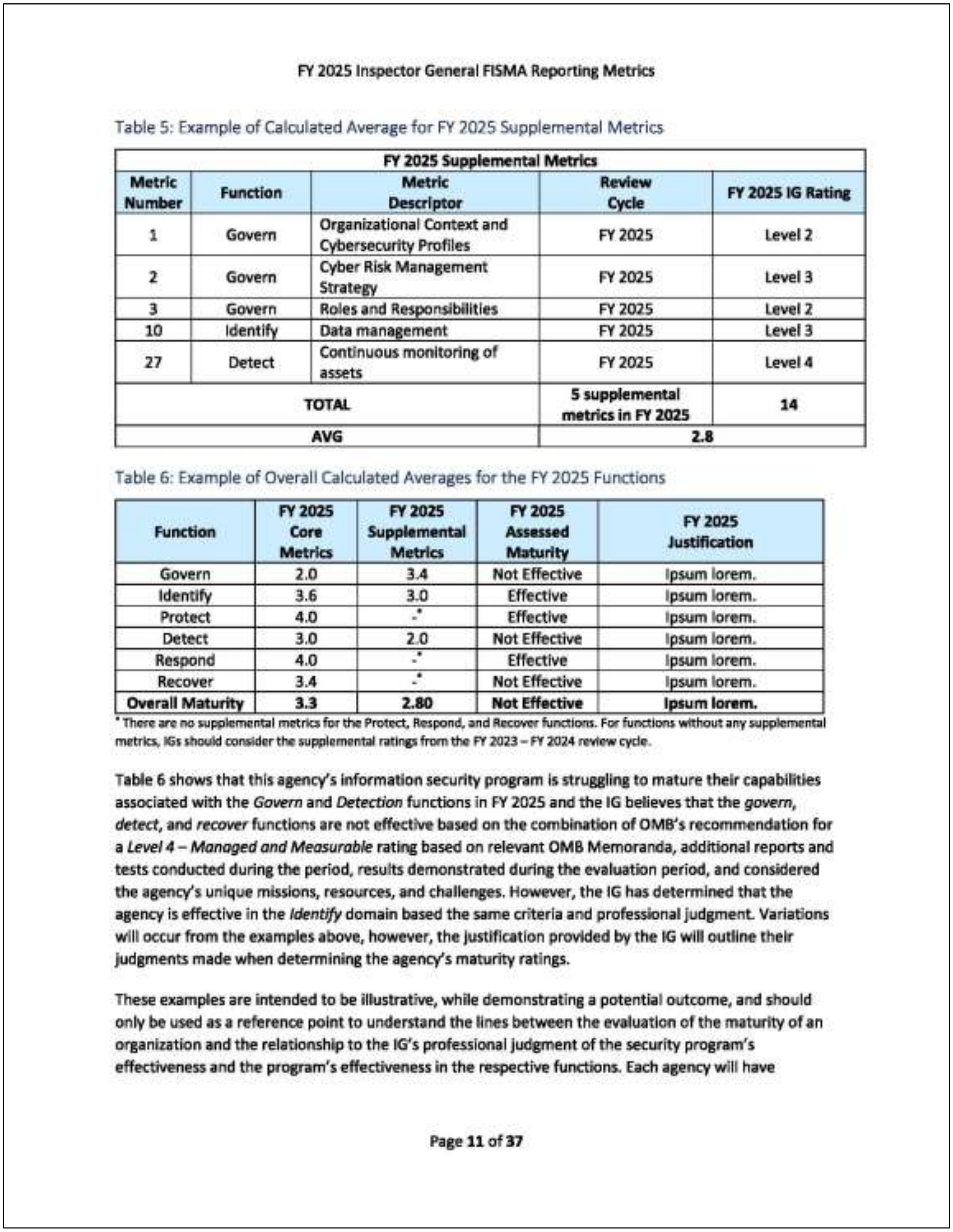


Table 5: Example of Calculated Average for FY 2025 Supplemental Metrics

FY 2025 Supplemental Metrics				
Metric Number	Function	Metric Descriptor	Review Cycle	FY 2025 IG Rating
1	Govern	Organizational Context and Cybersecurity Profiles	FY 2025	Level 2
2	Govern	Cyber Risk Management Strategy	FY 2025	Level 3
3	Govern	Roles and Responsibilities	FY 2025	Level 2
10	Identify	Data management	FY 2025	Level 3
27	Detect	Continuous monitoring of assets	FY 2025	Level 4
TOTAL			5 supplemental metrics in FY 2025	14
AVG			2.8	

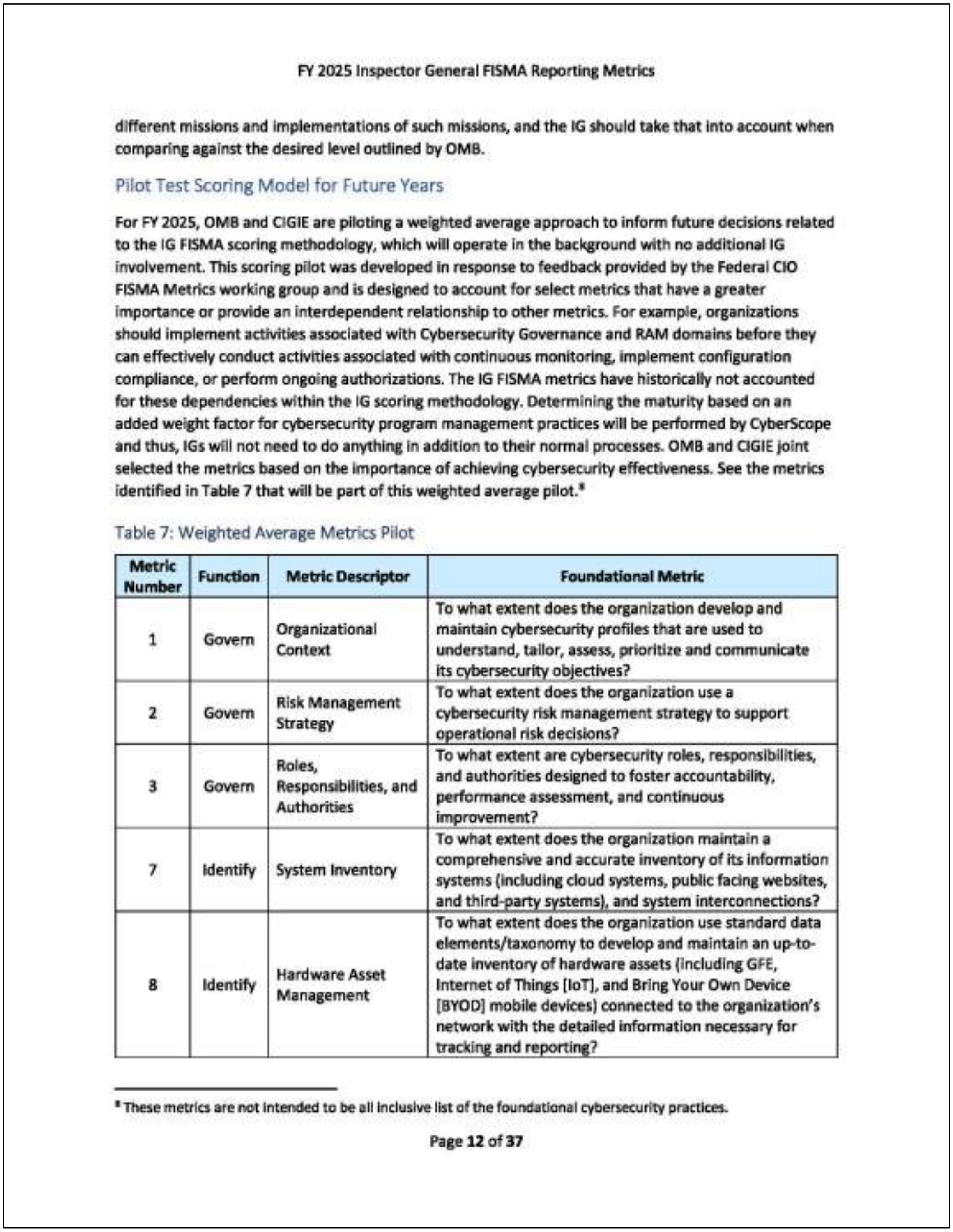
Table 6: Example of Overall Calculated Averages for the FY 2025 Functions

Function	FY 2025 Core Metrics	FY 2025 Supplemental Metrics	FY 2025 Assessed Maturity	FY 2025 Justification
Govern	2.0	3.4	Not Effective	Ipsum lorem.
Identify	3.6	3.0	Effective	Ipsum lorem.
Protect	4.0	-*	Effective	Ipsum lorem.
Detect	3.0	2.0	Not Effective	Ipsum lorem.
Respond	4.0	-*	Effective	Ipsum lorem.
Recover	3.4	-*	Not Effective	Ipsum lorem.
Overall Maturity	**3.3**	**2.80**	**Not Effective**	**Ipsum lorem.**

* There are no supplemental metrics for the Protect, Respond, and Recover functions. For functions without any supplemental metrics, IGs should consider the supplemental ratings from the FY 2023 – FY 2024 review cycle.

Table 6 shows that this agency's information security program is struggling to mature their capabilities associated with the *Govern* and *Detection* functions in FY 2025 and the IG believes that the *govern, detect*, and *recover* functions are not effective based on the combination of OMB's recommendation for a *Level 4 – Managed and Measurable* rating based on relevant OMB Memoranda, additional reports and tests conducted during the period, results demonstrated during the evaluation period, and considered the agency's unique missions, resources, and challenges. However, the IG has determined that the agency is effective in the *Identify* domain based the same criteria and professional judgment. Variations will occur from the examples above, however, the justification provided by the IG will outline their judgments made when determining the agency's maturity ratings.

These examples are intended to be illustrative, while demonstrating a potential outcome, and should only be used as a reference point to understand the lines between the evaluation of the maturity of an organization and the relationship to the IG's professional judgment of the security program's effectiveness and the program's effectiveness in the respective functions. Each agency will have



different missions and implementations of such missions, and the IG should take that into account when comparing against the desired level outlined by OMB.

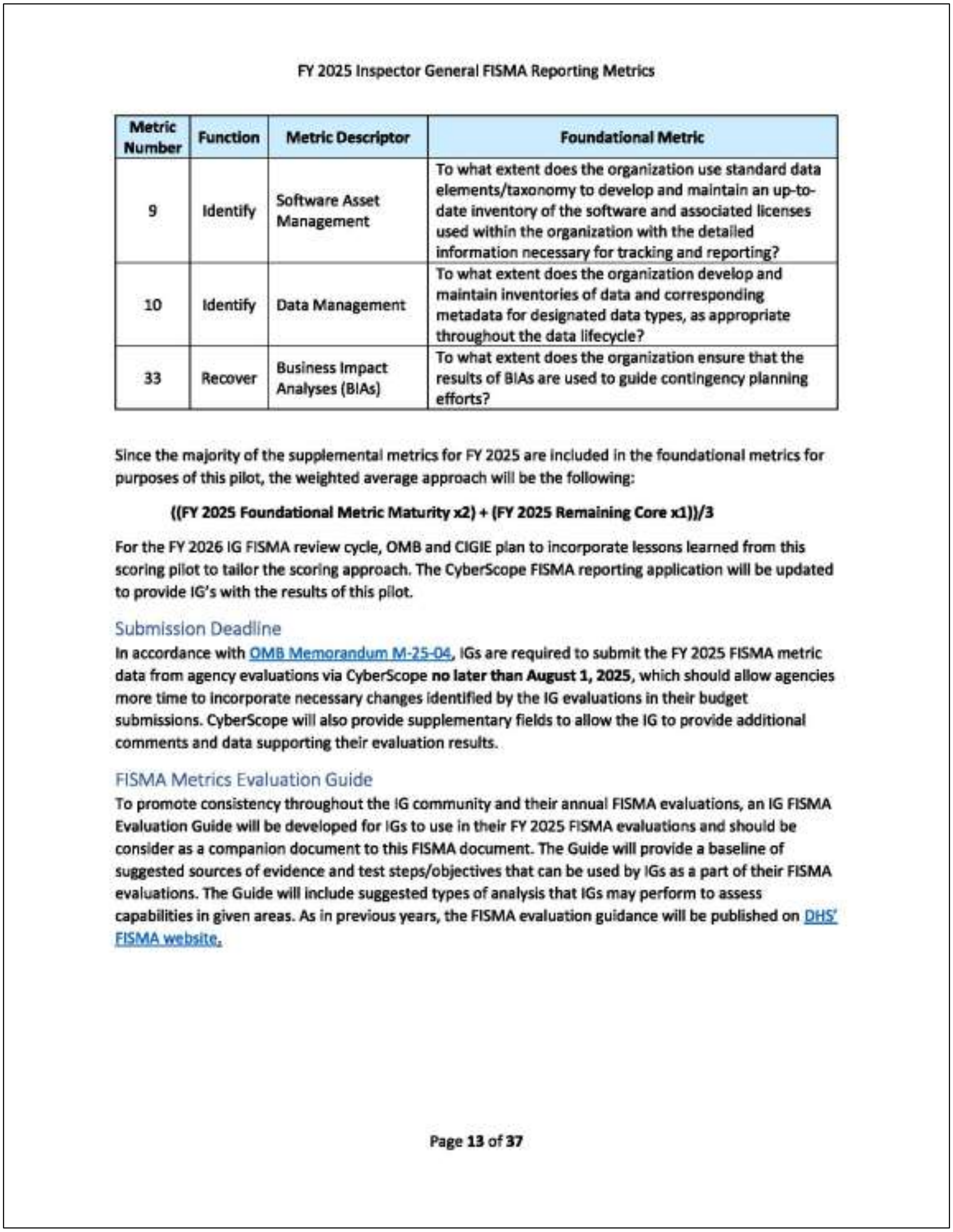
Pilot Test Scoring Model for Future Years

For FY 2025, OMB and CIGIE are piloting a weighted average approach to inform future decisions related to the IG FISMA scoring methodology, which will operate in the background with no additional IG involvement. This scoring pilot was developed in response to feedback provided by the Federal CIO FISMA Metrics working group and is designed to account for select metrics that have a greater importance or provide an interdependent relationship to other metrics. For example, organizations should implement activities associated with Cybersecurity Governance and RAM domains before they can effectively conduct activities associated with continuous monitoring, implement configuration compliance, or perform ongoing authorizations. The IG FISMA metrics have historically not accounted for these dependencies within the IG scoring methodology. Determining the maturity based on an added weight factor for cybersecurity program management practices will be performed by CyberScope and thus, IGs will not need to do anything in addition to their normal processes. OMB and CIGIE joint selected the metrics based on the importance of achieving cybersecurity effectiveness. See the metrics identified in Table 7 that will be part of this weighted average pilot.[8]

Table 7: Weighted Average Metrics Pilot

Metric Number	Function	Metric Descriptor	Foundational Metric
1	Govern	Organizational Context	To what extent does the organization develop and maintain cybersecurity profiles that are used to understand, tailor, assess, prioritize and communicate its cybersecurity objectives?
2	Govern	Risk Management Strategy	To what extent does the organization use a cybersecurity risk management strategy to support operational risk decisions?
3	Govern	Roles, Responsibilities, and Authorities	To what extent are cybersecurity roles, responsibilities, and authorities designed to foster accountability, performance assessment, and continuous improvement?
7	Identify	System Inventory	To what extent does the organization maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public facing websites, and third-party systems), and system interconnections?
8	Identify	Hardware Asset Management	To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets (including GFE, Internet of Things [IoT], and Bring Your Own Device [BYOD] mobile devices) connected to the organization's network with the detailed information necessary for tracking and reporting?

[8] These metrics are not intended to be all inclusive list of the foundational cybersecurity practices.



Metric Number	Function	Metric Descriptor	Foundational Metric
9	Identify	Software Asset Management	To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting?
10	Identify	Data Management	To what extent does the organization develop and maintain inventories of data and corresponding metadata for designated data types, as appropriate throughout the data lifecycle?
33	Recover	Business Impact Analyses (BIAs)	To what extent does the organization ensure that the results of BIAs are used to guide contingency planning efforts?

Since the majority of the supplemental metrics for FY 2025 are included in the foundational metrics for purposes of this pilot, the weighted average approach will be the following:

((FY 2025 Foundational Metric Maturity x2) + (FY 2025 Remaining Core x1))/3

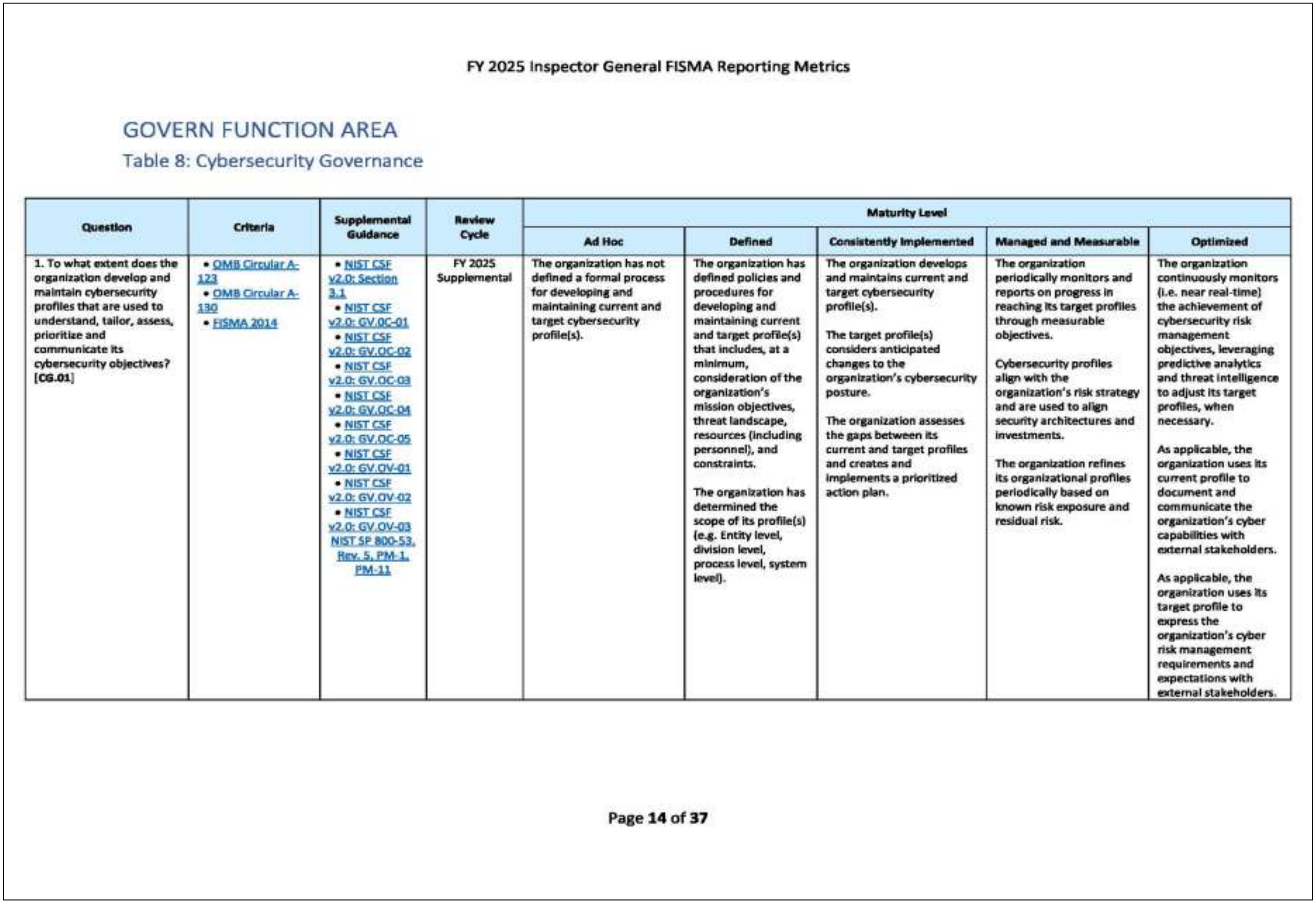
For the FY 2026 IG FISMA review cycle, OMB and CIGIE plan to incorporate lessons learned from this scoring pilot to tailor the scoring approach. The CyberScope FISMA reporting application will be updated to provide IG's with the results of this pilot.

Submission Deadline

In accordance with OMB Memorandum M-25-04, IGs are required to submit the FY 2025 FISMA metric data from agency evaluations via CyberScope **no later than August 1, 2025**, which should allow agencies more time to incorporate necessary changes identified by the IG evaluations in their budget submissions. CyberScope will also provide supplementary fields to allow the IG to provide additional comments and data supporting their evaluation results.

FISMA Metrics Evaluation Guide

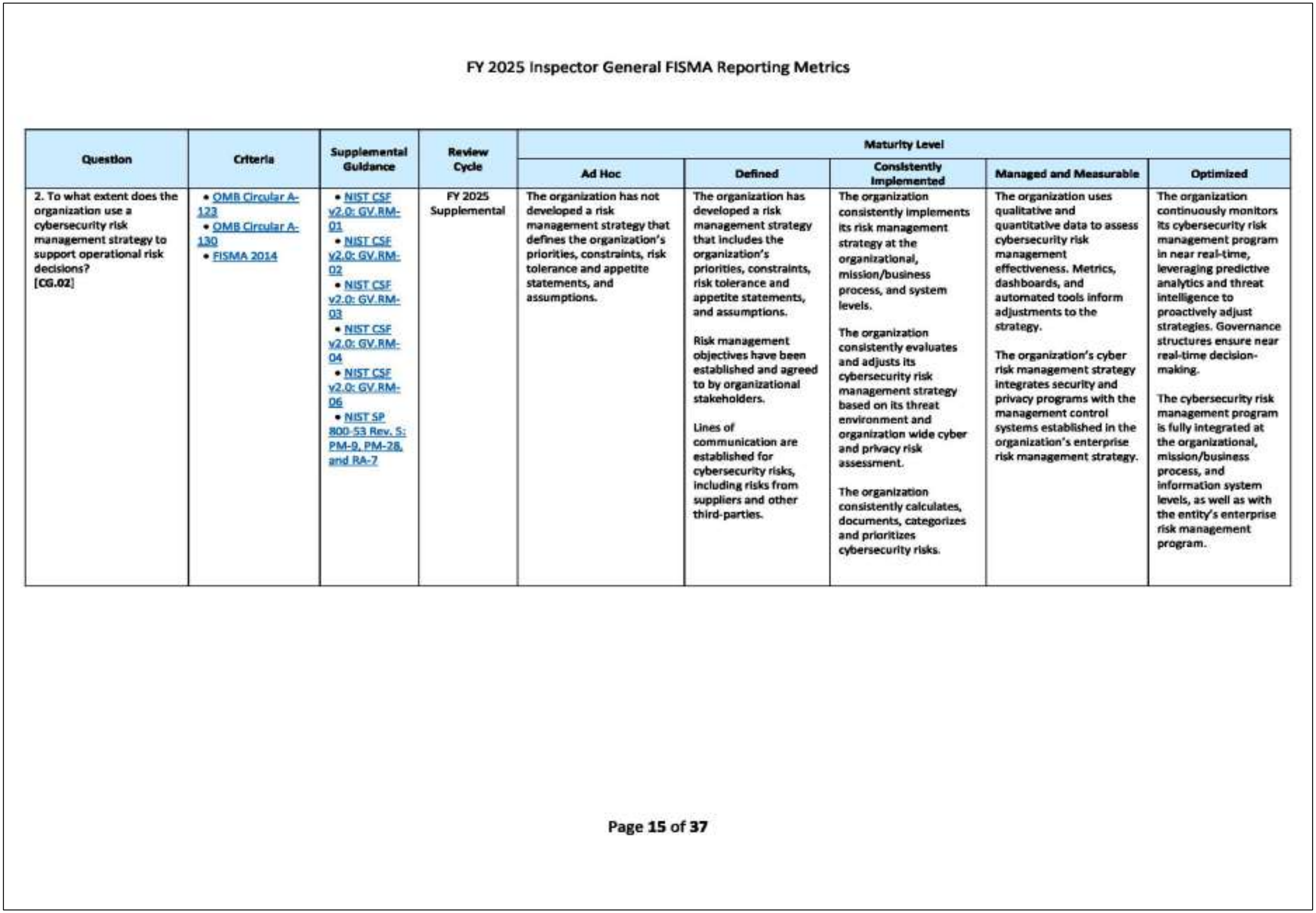
To promote consistency throughout the IG community and their annual FISMA evaluations, an IG FISMA Evaluation Guide will be developed for IGs to use in their FY 2025 FISMA evaluations and should be consider as a companion document to this FISMA document. The Guide will provide a baseline of suggested sources of evidence and test steps/objectives that can be used by IGs as a part of their FISMA evaluations. The Guide will include suggested types of analysis that IGs may perform to assess capabilities in given areas. As in previous years, the FISMA evaluation guidance will be published on DHS' FISMA website.



GOVERN FUNCTION AREA

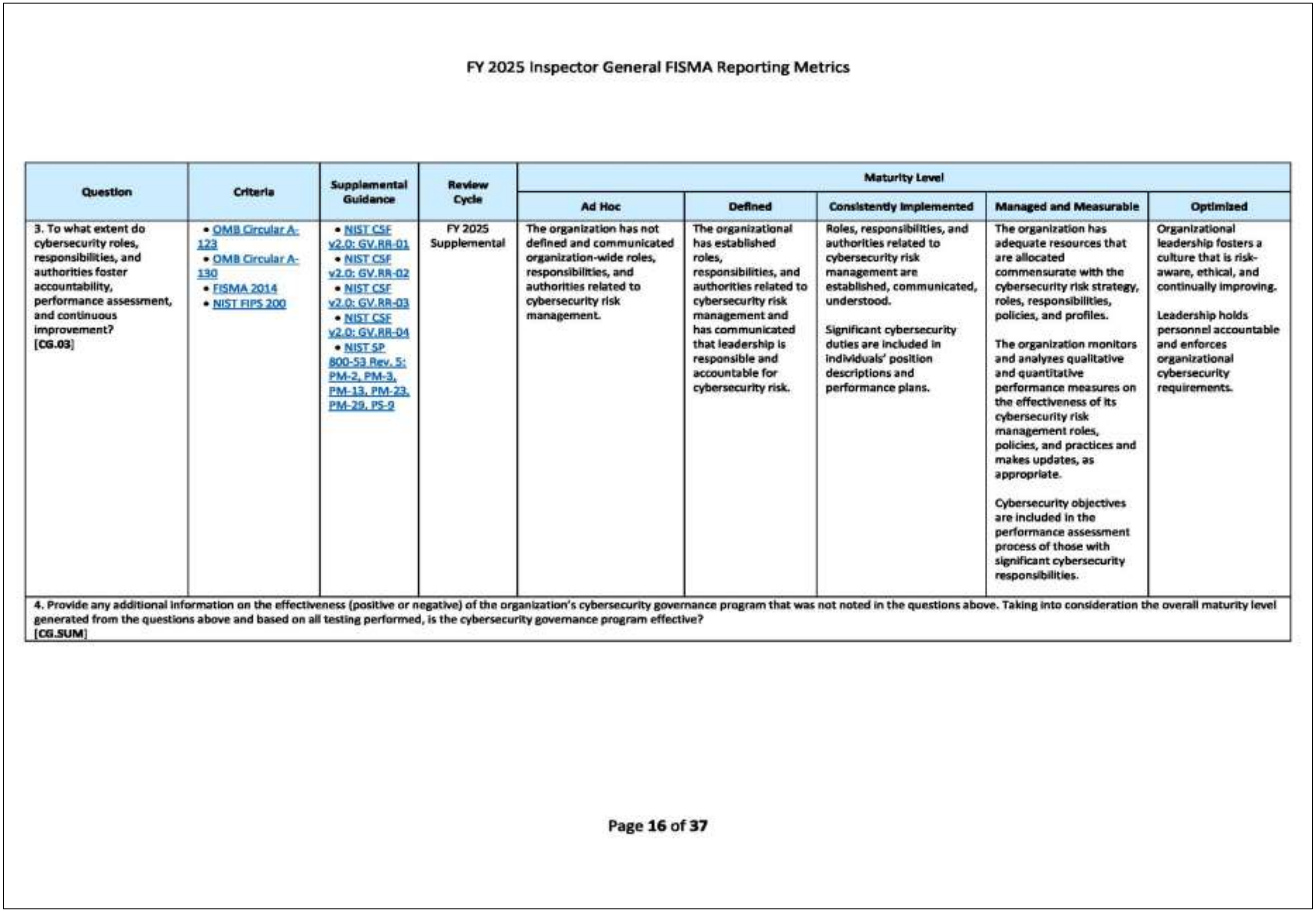
Table 8: Cybersecurity Governance

Question	Criteria	Supplemental Guidance	Review Cycle	Maturity Level				
				Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
1. To what extent does the organization develop and maintain cybersecurity profiles that are used to understand, tailor, assess, prioritize and communicate its cybersecurity objectives? [CG.01]	• OMB Circular A-123 • OMB Circular A-130 • FISMA 2014	• NIST CSF v2.0: Section 3.1 • NIST CSF v2.0: GV.OC-01 • NIST CSF v2.0: GV.OC-02 • NIST CSF v2.0: GV.OC-03 • NIST CSF v2.0: GV.OC-04 • NIST CSF v2.0: GV.OC-05 • NIST CSF v2.0: GV.OV-01 • NIST CSF v2.0: GV.OV-02 • NIST CSF v2.0: GV.OV-03 NIST SP 800-53, Rev. 5, PM-1, PM-11	FY 2025 Supplemental	The organization has not defined a formal process for developing and maintaining current and target cybersecurity profile(s).	The organization has defined policies and procedures for developing and maintaining current and target profile(s) that includes, at a minimum, consideration of the organization's mission objectives, threat landscape, resources (including personnel), and constraints. The organization has determined the scope of its profile(s) (e.g. Entity level, division level, process level, system level).	The organization develops and maintains current and target cybersecurity profile(s). The target profile(s) considers anticipated changes to the organization's cybersecurity posture. The organization assesses the gaps between its current and target profiles and creates and implements a prioritized action plan.	The organization periodically monitors and reports on progress in reaching its target profiles through measurable objectives. Cybersecurity profiles align with the organization's risk strategy and are used to align security architectures and investments. The organization refines its organizational profiles periodically based on known risk exposure and residual risk.	The organization continuously monitors (i.e. near real-time) the achievement of cybersecurity risk management objectives, leveraging predictive analytics and threat intelligence to adjust its target profiles, when necessary. As applicable, the organization uses its current profile to document and communicate the organization's cyber capabilities with external stakeholders. As applicable, the organization uses its target profile to express the organization's cyber risk management requirements and expectations with external stakeholders.

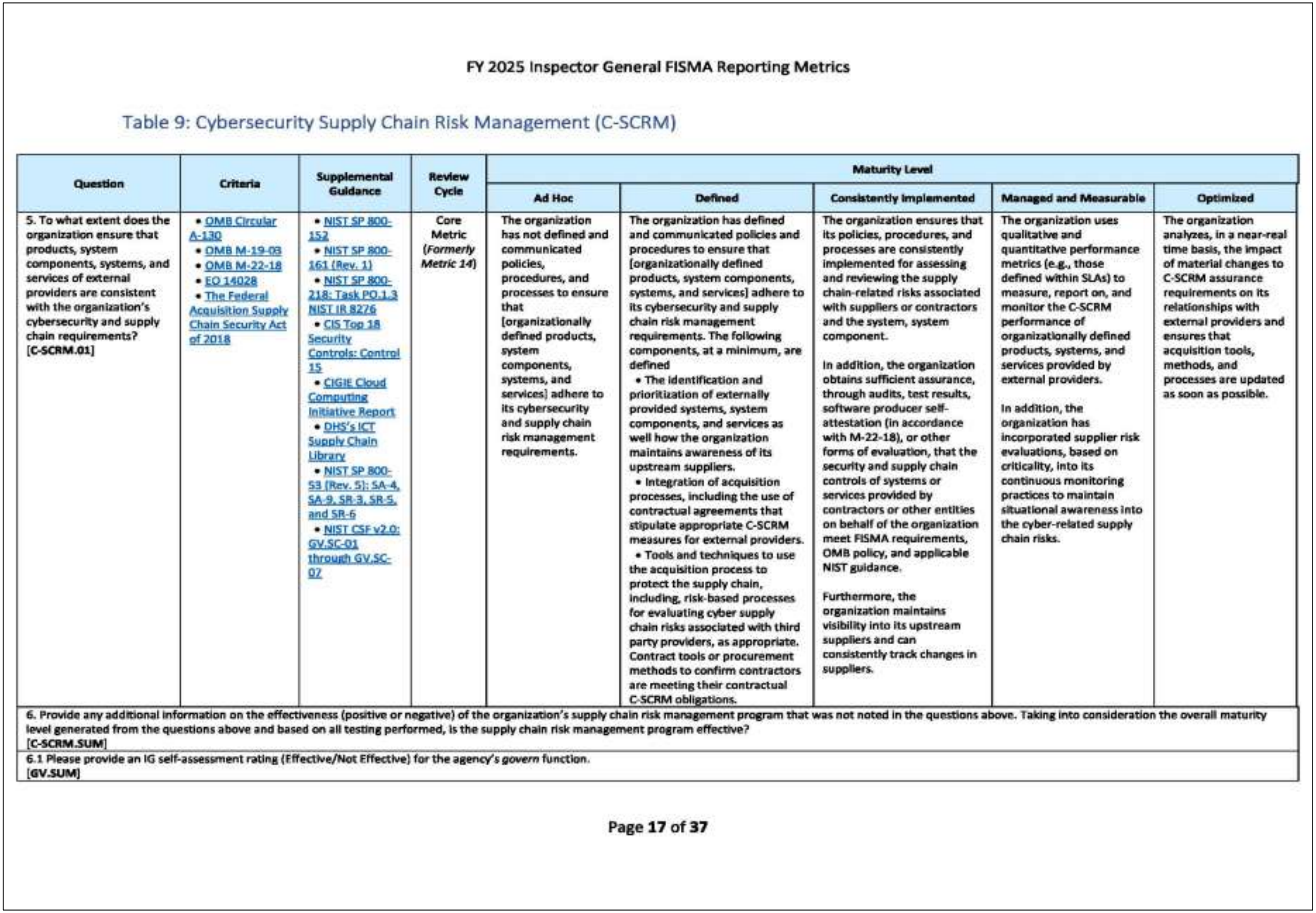


FY 2025 Inspector General FISMA Reporting Metrics

Question	Criteria	Supplemental Guidance	Review Cycle	Maturity Level				
				Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
2. To what extent does the organization use a cybersecurity risk management strategy to support operational risk decisions? [CG.02]	• OMB Circular A-123 • OMB Circular A-130 • FISMA 2014	• NIST CSF v2.0: GV.RM-01 • NIST CSF v2.0: GV.RM-02 • NIST CSF v2.0: GV.RM-03 • NIST CSF v2.0: GV.RM-04 • NIST CSF v2.0: GV.RM-06 • NIST SP 800-53 Rev. 5: PM-9, PM-28, and RA-7	FY 2025 Supplemental	The organization has not developed a risk management strategy that defines the organization's priorities, constraints, risk tolerance and appetite statements, and assumptions.	The organization has developed a risk management strategy that includes the organization's priorities, constraints, risk tolerance and appetite statements, and assumptions. Risk management objectives have been established and agreed to by organizational stakeholders. Lines of communication are established for cybersecurity risks, including risks from suppliers and other third-parties.	The organization consistently implements its risk management strategy at the organizational, mission/business process, and system levels. The organization consistently evaluates and adjusts its cybersecurity risk management strategy based on its threat environment and organization wide cyber and privacy risk assessment. The organization consistently calculates, documents, categorizes and prioritizes cybersecurity risks.	The organization uses qualitative and quantitative data to assess cybersecurity risk management effectiveness. Metrics, dashboards, and automated tools inform adjustments to the strategy. The organization's cyber risk management strategy integrates security and privacy programs with the management control systems established in the organization's enterprise risk management strategy.	The organization continuously monitors its cybersecurity risk management program in near real-time, leveraging predictive analytics and threat intelligence to proactively adjust strategies. Governance structures ensure near real-time decision-making. The cybersecurity risk management program is fully integrated at the organizational, mission/business process, and information system levels, as well as with the entity's enterprise risk management program.



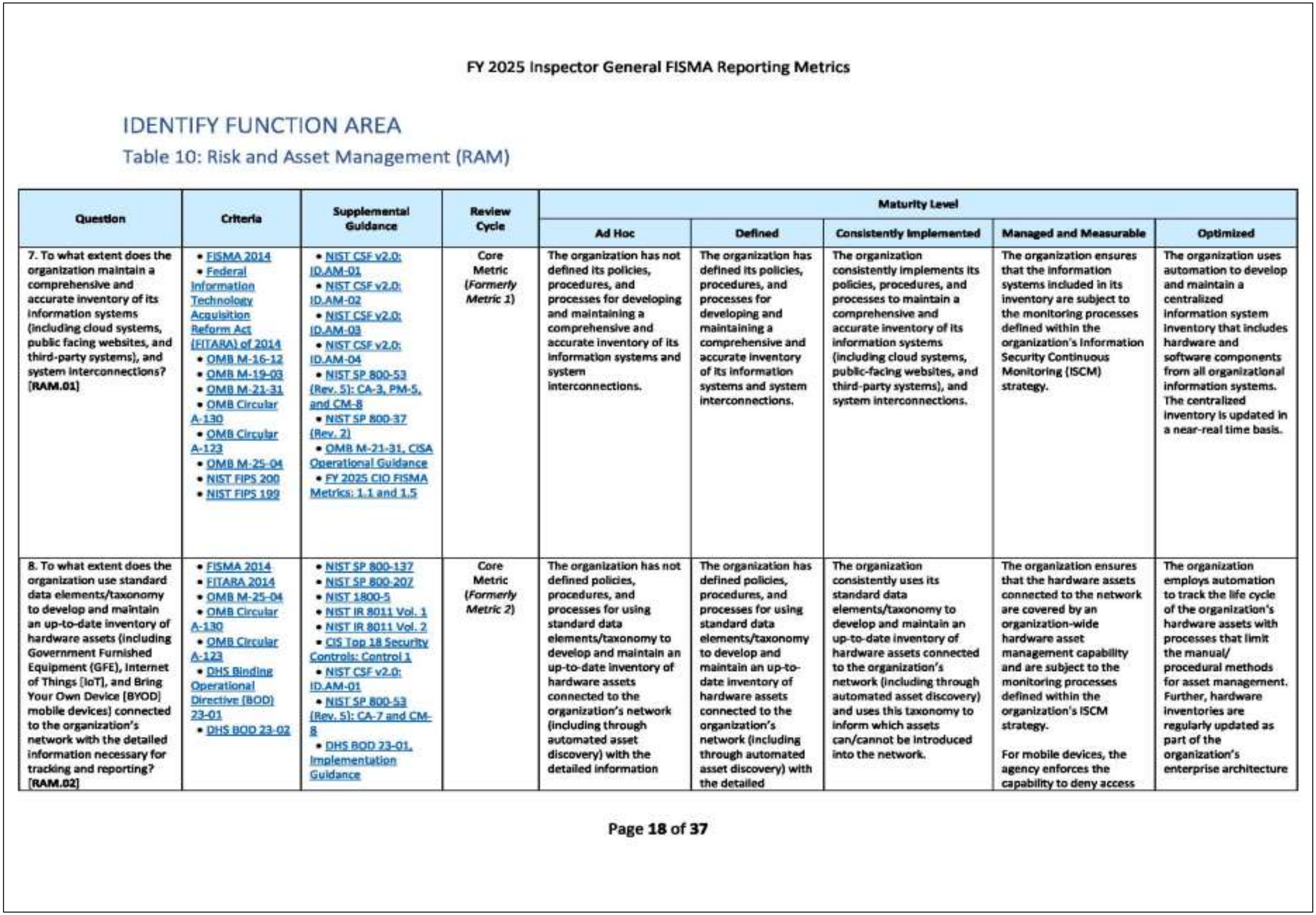
Question	Criteria	Supplemental Guidance	Review Cycle	Maturity Level				
				Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
3. To what extent do cybersecurity roles, responsibilities, and authorities foster accountability, performance assessment, and continuous improvement? **[CG.03]**	• OMB Circular A-123 • OMB Circular A-130 • FISMA 2014 • NIST FIPS 200	• NIST CSF v2.0: GV.RR-01 • NIST CSF v2.0: GV.RR-02 • NIST CSF v2.0: GV.RR-03 • NIST CSF v2.0: GV.RR-04 • NIST SP 800-53 Rev. 5: PM-2, PM-3, PM-13, PM-23, PM-29, PS-9	FY 2025 Supplemental	The organization has not defined and communicated organization-wide roles, responsibilities, and authorities related to cybersecurity risk management.	The organizational has established roles, responsibilities, and authorities related to cybersecurity risk management and has communicated that leadership is responsible and accountable for cybersecurity risk.	Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood. Significant cybersecurity duties are included in individuals' position descriptions and performance plans.	The organization has adequate resources that are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, policies, and profiles. The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its cybersecurity risk management roles, policies, and practices and makes updates, as appropriate. Cybersecurity objectives are included in the performance assessment process of those with significant cybersecurity responsibilities.	Organizational leadership fosters a culture that is risk-aware, ethical, and continually improving. Leadership holds personnel accountable and enforces organizational cybersecurity requirements.
4. Provide any additional information on the effectiveness (positive or negative) of the organization's cybersecurity governance program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the cybersecurity governance program effective? **[CG.SUM]**								



FY 2025 Inspector General FISMA Reporting Metrics

Table 9: Cybersecurity Supply Chain Risk Management (C-SCRM)

Question	Criteria	Supplemental Guidance	Review Cycle	Maturity Level				
				Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
5. To what extent does the organization ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain requirements? **[C-SCRM.01]**	• OMB Circular A-130 • OMB M-19-03 • OMB M-22-18 • EO 14028 • The Federal Acquisition Supply Chain Security Act of 2018	• NIST SP 800-152 • NIST SP 800-161 (Rev. 1) • NIST SP 800-218: Task PO.1.3 NIST IR 8276 • CIS Top 18 Security Controls: Control 15 • CIGIE Cloud Computing Initiative Report • DHS's ICT Supply Chain Library • NIST SP 800-53 (Rev. 5): SA-4, SA-9, SR-3, SR-5, and SR-6 • NIST CSF v2.0: GV.SC-01 through GV.SC-07	Core Metric (*Formerly Metric 14*)	The organization has not defined and communicated policies, procedures, and processes to ensure that [organizationally defined products, system components, systems, and services] adhere to its cybersecurity and supply chain risk management requirements.	The organization has defined and communicated policies and procedures to ensure that [organizationally defined products, system components, systems, and services] adhere to its cybersecurity and supply chain risk management requirements. The following components, at a minimum, are defined • The identification and prioritization of externally provided systems, system components, and services as well how the organization maintains awareness of its upstream suppliers. • Integration of acquisition processes, including the use of contractual agreements that stipulate appropriate C-SCRM measures for external providers. • Tools and techniques to use the acquisition process to protect the supply chain, including, risk-based processes for evaluating cyber supply chain risks associated with third party providers, as appropriate. Contract tools or procurement methods to confirm contractors are meeting their contractual C-SCRM obligations.	The organization ensures that its policies, procedures, and processes are consistently implemented for assessing and reviewing the supply chain-related risks associated with suppliers or contractors and the system, system component. In addition, the organization obtains sufficient assurance, through audits, test results, software producer self-attestation (in accordance with M-22-18), or other forms of evaluation, that the security and supply chain controls of systems or services provided by contractors or other entities on behalf of the organization meet FISMA requirements, OMB policy, and applicable NIST guidance. Furthermore, the organization maintains visibility into its upstream suppliers and can consistently track changes in suppliers.	The organization uses qualitative and quantitative performance metrics (e.g., those defined within SLAs) to measure, report on, and monitor the C-SCRM performance of organizationally defined products, systems, and services provided by external providers. In addition, the organization has incorporated supplier risk evaluations, based on criticality, into its continuous monitoring practices to maintain situational awareness into the cyber-related supply chain risks.	The organization analyzes, in a near-real time basis, the impact of material changes to C-SCRM assurance requirements on its relationships with external providers and ensures that acquisition tools, methods, and processes are updated as soon as possible.
6. Provide any additional information on the effectiveness (positive or negative) of the organization's supply chain risk management program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the supply chain risk management program effective? **[C-SCRM.SUM]**								
6.1 Please provide an IG self-assessment rating (Effective/Not Effective) for the agency's *govern* function. **[GV.SUM]**								

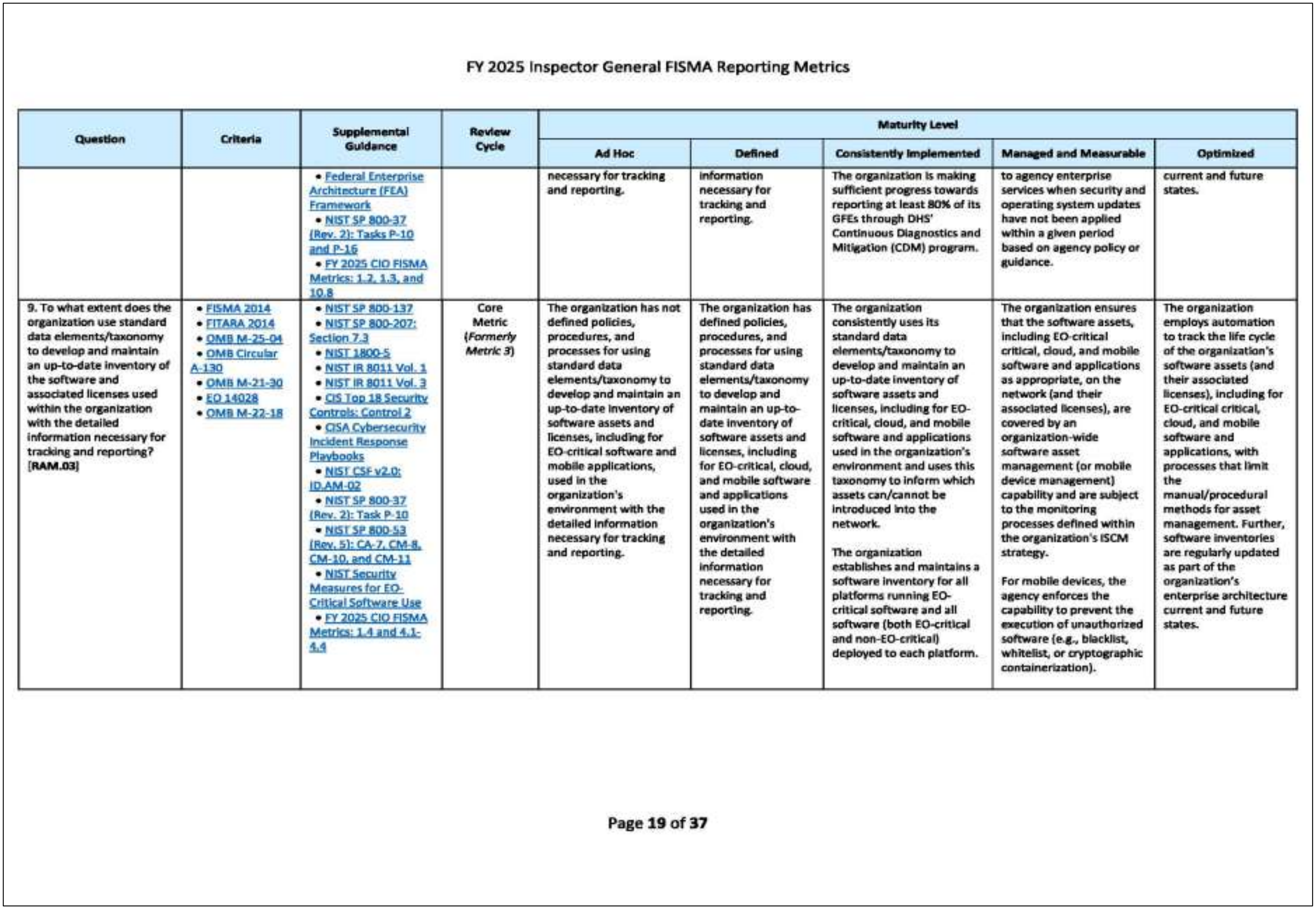


FY 2025 Inspector General FISMA Reporting Metrics

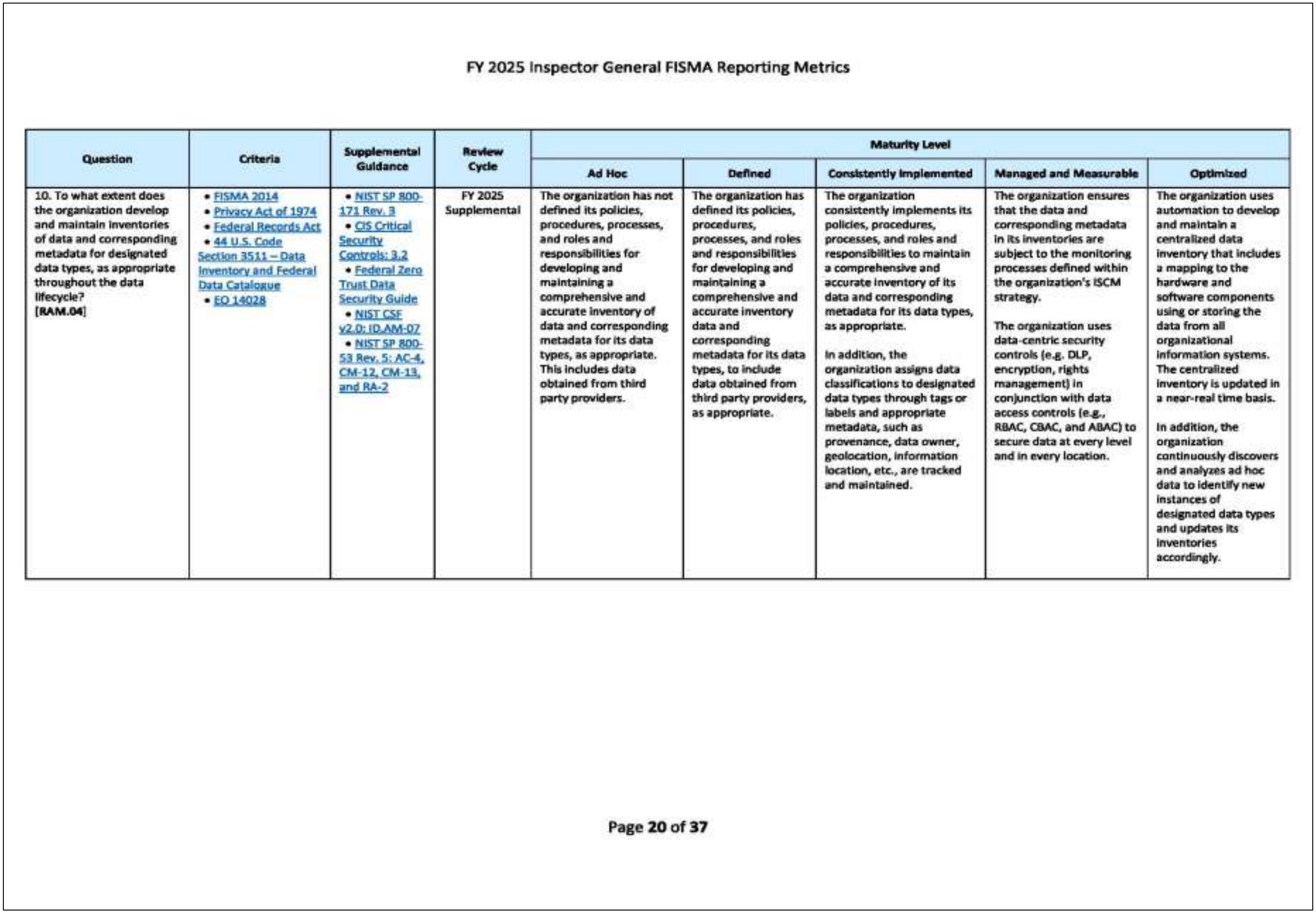
IDENTIFY FUNCTION AREA

Table 10: Risk and Asset Management (RAM)

Question	Criteria	Supplemental Guidance	Review Cycle	Maturity Level				
				Ad Hoc	**Defined**	**Consistently Implemented**	**Managed and Measurable**	**Optimized**
7. To what extent does the organization maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public facing websites, and third-party systems), and system interconnections? [**RAM.01**]	• FISMA 2014 • Federal Information Technology Acquisition Reform Act (FITARA) of 2014 • OMB M-16-12 • OMB M-19-03 • OMB M-21-31 • OMB Circular A-130 • OMB Circular A-123 • OMB M-25-04 • NIST FIPS 200 • NIST FIPS 199	• NIST CSF v2.0: ID.AM-01 • NIST CSF v2.0: ID.AM-02 • NIST CSF v2.0: ID.AM-03 • NIST CSF v2.0: ID.AM-04 • NIST SP 800-53 (Rev. 5): CA-3, PM-5, and CM-8 • NIST SP 800-37 (Rev. 2) • OMB M-21-31, CISA Operational Guidance • FY 2025 CIO FISMA Metrics: 1.1 and 1.5	Core Metric (*Formerly Metric 1*)	The organization has not defined its policies, procedures, and processes for developing and maintaining a comprehensive and accurate inventory of its information systems and system interconnections.	The organization has defined its policies, procedures, and processes for developing and maintaining a comprehensive and accurate inventory of its information systems and system interconnections.	The organization consistently implements its policies, procedures, and processes to maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public-facing websites, and third-party systems), and system interconnections.	The organization ensures that the information systems included in its inventory are subject to the monitoring processes defined within the organization's Information Security Continuous Monitoring (ISCM) strategy.	The organization uses automation to develop and maintain a centralized information system inventory that includes hardware and software components from all organizational information systems. The centralized inventory is updated in a near-real time basis.
8. To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets (including Government Furnished Equipment (GFE), Internet of Things [IoT], and Bring Your Own Device [BYOD] mobile devices) connected to the organization's network with the detailed information necessary for tracking and reporting? [**RAM.02**]	• FISMA 2014 • FITARA 2014 • OMB M-25-04 • OMB Circular A-130 • OMB Circular A-123 • DHS Binding Operational Directive (BOD) 23-01 • DHS BOD 23-02	• NIST SP 800-137 • NIST SP 800-207 • NIST 1800-5 • NIST IR 8011 Vol. 1 • NIST IR 8011 Vol. 2 • CIS Top 18 Security Controls: Control 1 • NIST CSF v2.0: ID.AM-01 • NIST SP 800-53 (Rev. 5): CA-7 and CM-8 • DHS BOD 23-01, Implementation Guidance	Core Metric (*Formerly Metric 2*)	The organization has not defined policies, procedures, and processes for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network (including through automated asset discovery) with the detailed information	The organization has defined policies, procedures, and processes for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network (including through automated asset discovery) with the detailed	The organization consistently uses its standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network (including through automated asset discovery) and uses this taxonomy to inform which assets can/cannot be introduced into the network.	The organization ensures that the hardware assets connected to the network are covered by an organization-wide hardware asset management capability and are subject to the monitoring processes defined within the organization's ISCM strategy. For mobile devices, the agency enforces the capability to deny access	The organization employs automation to track the life cycle of the organization's hardware assets with processes that limit the manual/ procedural methods for asset management. Further, hardware inventories are regularly updated as part of the organization's enterprise architecture

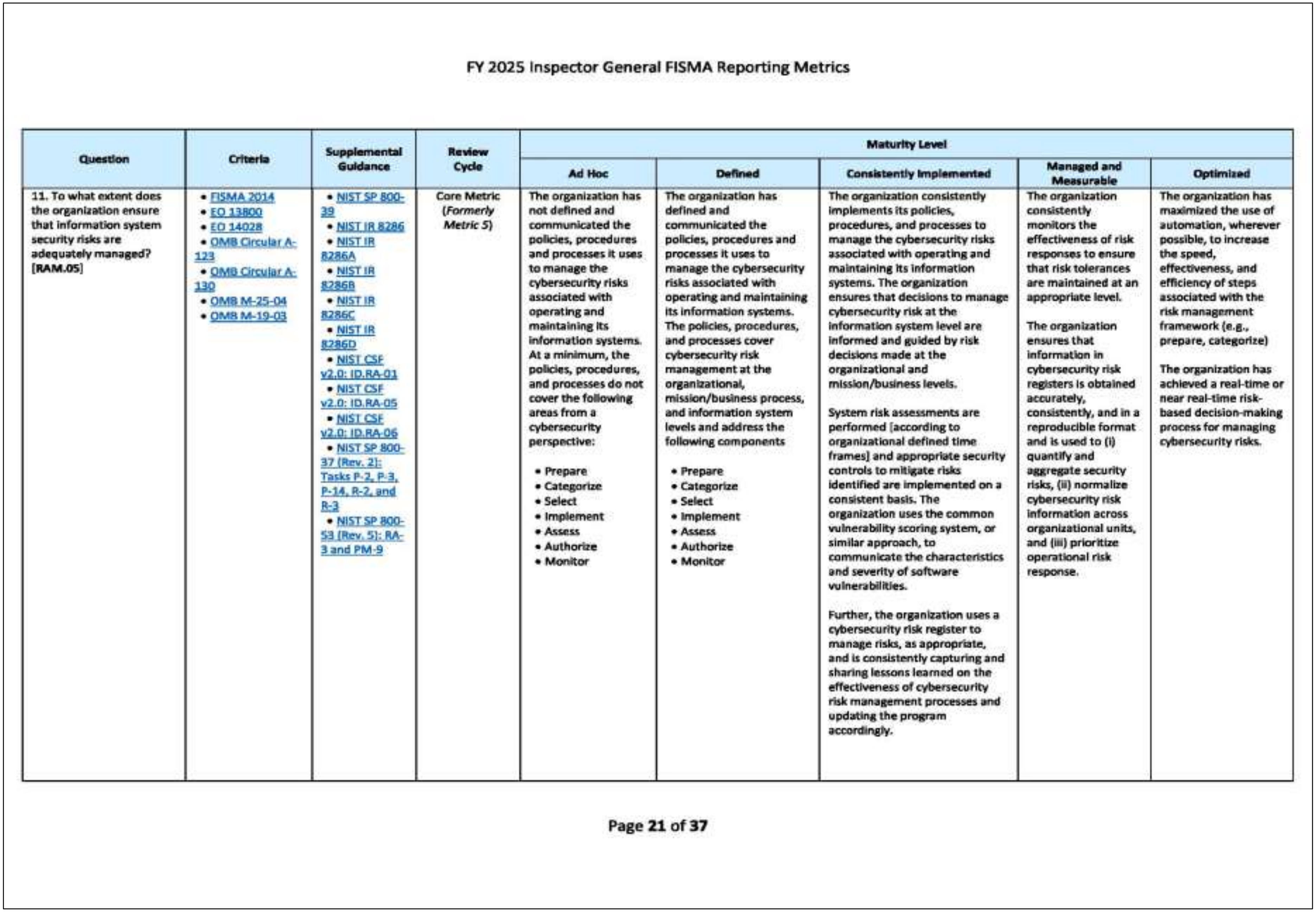


Question	Criteria	Supplemental Guidance	Review Cycle	Maturity Level				
				Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
		• Federal Enterprise Architecture (FEA) Framework • NIST SP 800-37 (Rev. 2): Tasks P-10 and P-16 • FY 2025 CIO FISMA Metrics: 1.2, 1.3, and 10.8		necessary for tracking and reporting.	information necessary for tracking and reporting.	The organization is making sufficient progress towards reporting at least 80% of its GFEs through DHS' Continuous Diagnostics and Mitigation (CDM) program.	to agency enterprise services when security and operating system updates have not been applied within a given period based on agency policy or guidance.	current and future states.
9. To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting? [**RAM.03**]	• FISMA 2014 • FITARA 2014 • OMB M-25-04 • OMB Circular A-130 • OMB M-21-30 • EO 14028 • OMB M-22-18	• NIST SP 800-137 • NIST SP 800-207: Section 7.3 • NIST 1800-5 • NIST IR 8011 Vol. 1 • NIST IR 8011 Vol. 3 • CIS Top 18 Security Controls: Control 2 • CISA Cybersecurity Incident Response Playbooks • NIST CSF v2.0: ID.AM-02 • NIST SP 800-37 (Rev. 2): Task P-10 • NIST SP 800-53 (Rev. 5): CA-7, CM-8, CM-10, and CM-11 • NIST Security Measures for EO-Critical Software Use • FY 2025 CIO FISMA Metrics: 1.4 and 4.1-4.4	Core Metric (*Formerly Metric 3*)	The organization has not defined policies, procedures, and processes for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of software assets and licenses, including for EO-critical software and mobile applications, used in the organization's environment with the detailed information necessary for tracking and reporting.	The organization has defined policies, procedures, and processes for using standard data elements/taxonomy to develop and maintain an up-to-date inventory of software assets and licenses, including for EO-critical, cloud, and mobile software and applications used in the organization's environment with the detailed information necessary for tracking and reporting.	The organization consistently uses its standard data elements/taxonomy to develop and maintain an up-to-date inventory of software assets and licenses, including for EO-critical, cloud, and mobile software and applications used in the organization's environment and uses this taxonomy to inform which assets can/cannot be introduced into the network. The organization establishes and maintains a software inventory for all platforms running EO-critical software and all software (both EO-critical and non-EO-critical) deployed to each platform.	The organization ensures that the software assets, including EO-critical critical, cloud, and mobile software and applications as appropriate, on the network (and their associated licenses), are covered by an organization-wide software asset management (or mobile device management) capability and are subject to the monitoring processes defined within the organization's ISCM strategy. For mobile devices, the agency enforces the capability to prevent the execution of unauthorized software (e.g., blacklist, whitelist, or cryptographic containerization).	The organization employs automation to track the life cycle of the organization's software assets (and their associated licenses), including for EO-critical critical, cloud, and mobile software and applications, with processes that limit the manual/procedural methods for asset management. Further, software inventories are regularly updated as part of the organization's enterprise architecture current and future states.



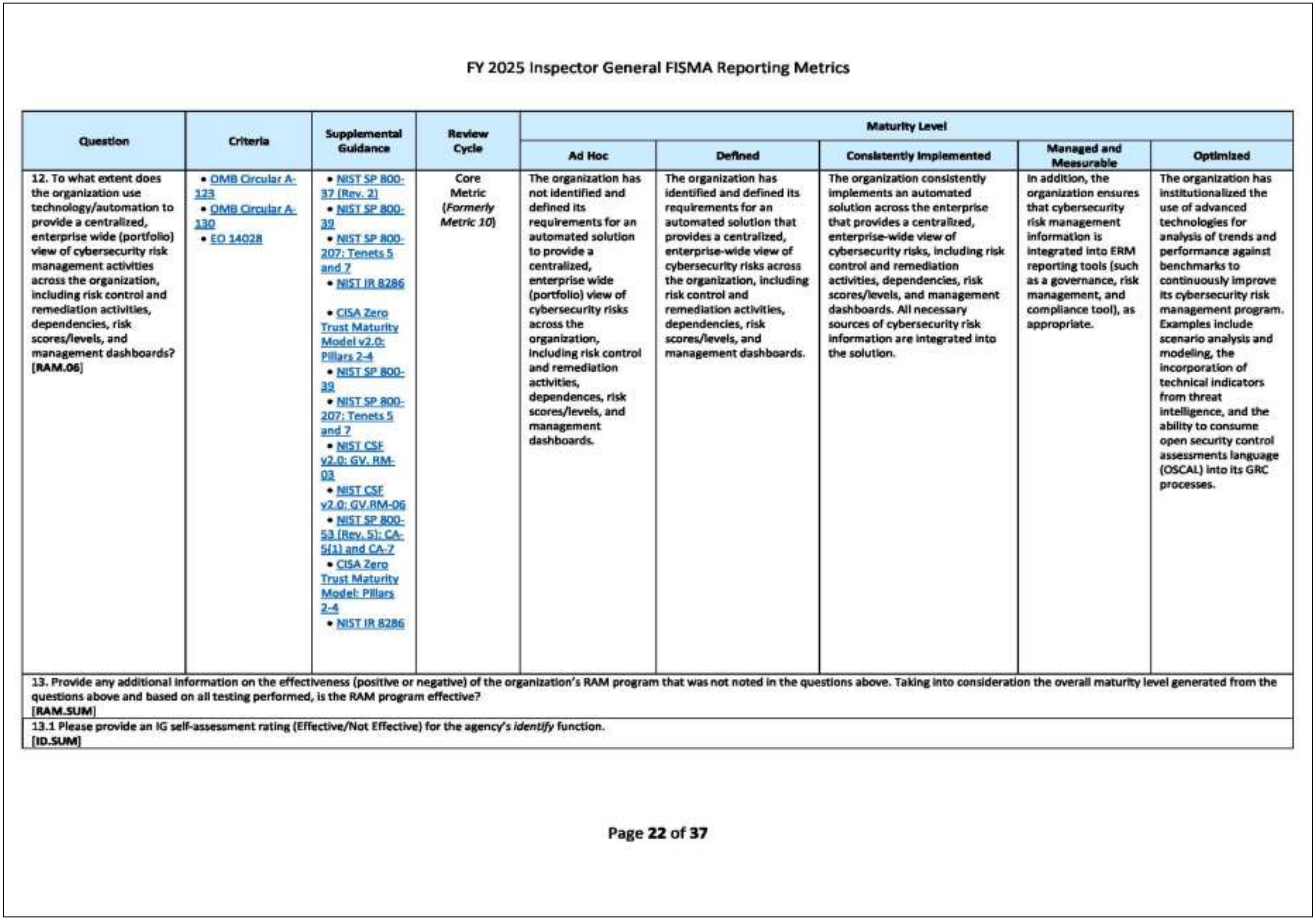
FY 2025 Inspector General FISMA Reporting Metrics

Question	Criteria	Supplemental Guidance	Review Cycle	Maturity Level				
				Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
10. To what extent does the organization develop and maintain inventories of data and corresponding metadata for designated data types, as appropriate throughout the data lifecycle? [RAM.04]	• FISMA 2014 • Privacy Act of 1974 • Federal Records Act • 44 U.S. Code Section 3511 – Data Inventory and Federal Data Catalogue • EO 14028	• NIST SP 800-171 Rev. 3 • CIS Critical Security Controls: 3.2 • Federal Zero Trust Data Security Guide • NIST CSF v2.0: ID.AM-07 • NIST SP 800-53 Rev. 5: AC-4, CM-12, CM-13, and RA-2	FY 2025 Supplemental	The organization has not defined its policies, procedures, processes, and roles and responsibilities for developing and maintaining a comprehensive and accurate inventory of data and corresponding metadata for its data types, as appropriate. This includes data obtained from third party providers.	The organization has defined its policies, procedures, processes, and roles and responsibilities for developing and maintaining a comprehensive and accurate inventory data and corresponding metadata for its data types, to include data obtained from third party providers, as appropriate.	The organization consistently implements its policies, procedures, processes, and roles and responsibilities to maintain a comprehensive and accurate inventory of its data and corresponding metadata for its data types, as appropriate. In addition, the organization assigns data classifications to designated data types through tags or labels and appropriate metadata, such as provenance, data owner, geolocation, information location, etc., are tracked and maintained.	The organization ensures that the data and corresponding metadata in its inventories are subject to the monitoring processes defined within the organization's ISCM strategy. The organization uses data-centric security controls (e.g. DLP, encryption, rights management) in conjunction with data access controls (e.g., RBAC, CBAC, and ABAC) to secure data at every level and in every location.	The organization uses automation to develop and maintain a centralized data inventory that includes a mapping to the hardware and software components using or storing the data from all organizational information systems. The centralized inventory is updated in a near-real time basis. In addition, the organization continuously discovers and analyzes ad hoc data to identify new instances of designated data types and updates its inventories accordingly.



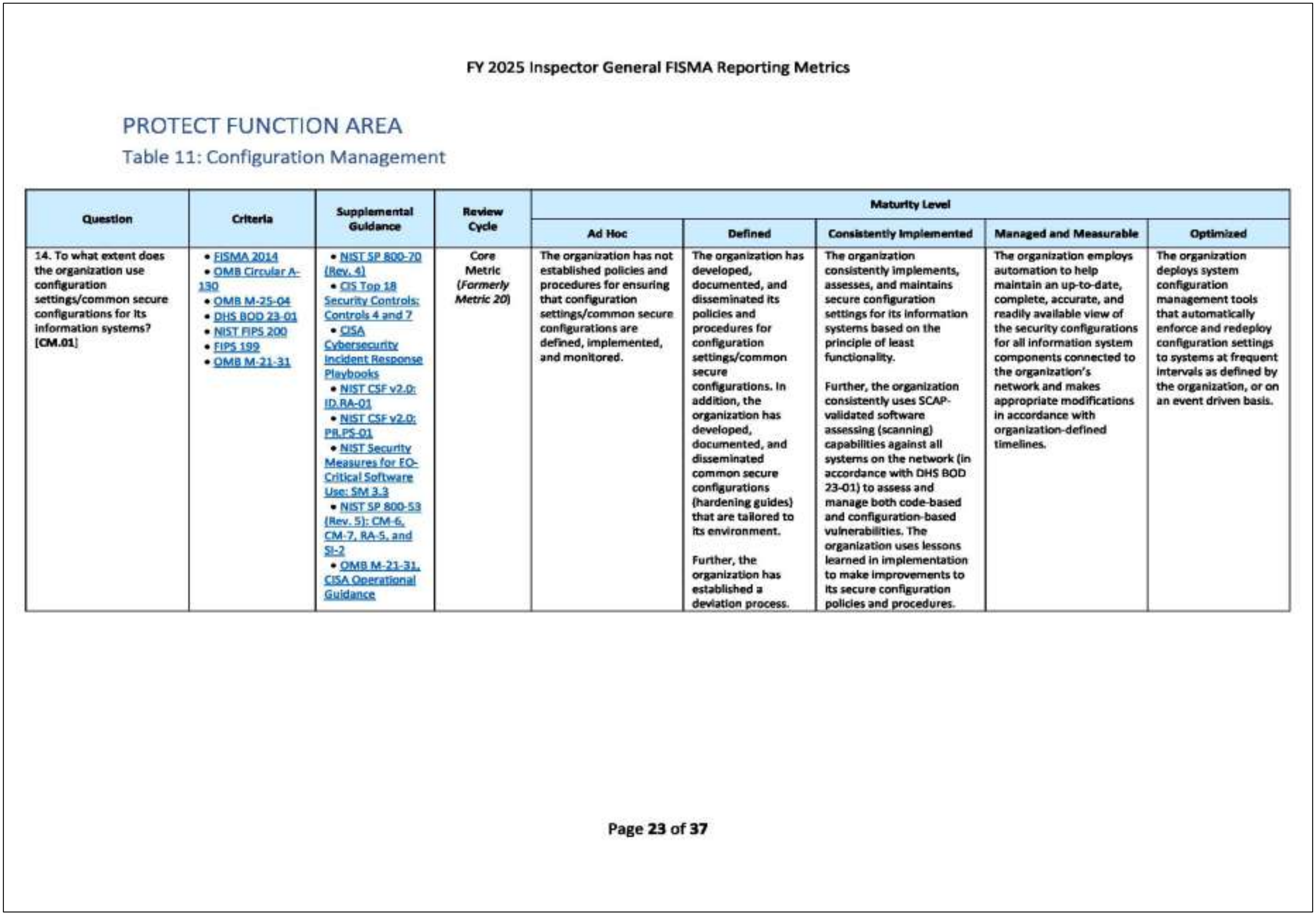
FY 2025 Inspector General FISMA Reporting Metrics

Question	Criteria	Supplemental Guidance	Review Cycle	Maturity Level				
				Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
11. To what extent does the organization ensure that information system security risks are adequately managed? [RAM.05]	• FISMA 2014 • EO 13800 • EO 14028 • OMB Circular A-123 • OMB Circular A-130 • OMB M-25-04 • OMB M-19-03	• NIST SP 800-39 • NIST IR 8286 • NIST IR 8286A • NIST IR 8286B • NIST IR 8286C • NIST IR 8286D • NIST CSF v2.0: ID.RA-01 • NIST CSF v2.0: ID.RA-05 • NIST CSF v2.0: ID.RA-06 • NIST SP 800-37 (Rev. 2): Tasks P-2, P-3, P-14, R-2, and R-3 • NIST SP 800-53 (Rev. 5): RA-3 and PM-9	Core Metric (*Formerly Metric 5*)	The organization has not defined and communicated the policies, procedures and processes it uses to manage the cybersecurity risks associated with operating and maintaining its information systems. At a minimum, the policies, procedures, and processes do not cover the following areas from a cybersecurity perspective: • Prepare • Categorize • Select • Implement • Assess • Authorize • Monitor	The organization has defined and communicated the policies, procedures and processes it uses to manage the cybersecurity risks associated with operating and maintaining its information systems. The policies, procedures, and processes cover cybersecurity risk management at the organizational, mission/business process, and information system levels and address the following components • Prepare • Categorize • Select • Implement • Assess • Authorize • Monitor	The organization consistently implements its policies, procedures, and processes to manage the cybersecurity risks associated with operating and maintaining its information systems. The organization ensures that decisions to manage cybersecurity risk at the information system level are informed and guided by risk decisions made at the organizational and mission/business levels. System risk assessments are performed [according to organizational defined time frames] and appropriate security controls to mitigate risks identified are implemented on a consistent basis. The organization uses the common vulnerability scoring system, or similar approach, to communicate the characteristics and severity of software vulnerabilities. Further, the organization uses a cybersecurity risk register to manage risks, as appropriate, and is consistently capturing and sharing lessons learned on the effectiveness of cybersecurity risk management processes and updating the program accordingly.	The organization consistently monitors the effectiveness of risk responses to ensure that risk tolerances are maintained at an appropriate level. The organization ensures that information in cybersecurity risk registers is obtained accurately, consistently, and in a reproducible format and is used to (i) quantify and aggregate security risks, (ii) normalize cybersecurity risk information across organizational units, and (iii) prioritize operational risk response.	The organization has maximized the use of automation, wherever possible, to increase the speed, effectiveness, and efficiency of steps associated with the risk management framework (e.g., prepare, categorize) The organization has achieved a real-time or near real-time risk-based decision-making process for managing cybersecurity risks.



FY 2025 Inspector General FISMA Reporting Metrics

Question	Criteria	Supplemental Guidance	Review Cycle	Maturity Level				
				Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
12. To what extent does the organization use technology/automation to provide a centralized, enterprise wide (portfolio) view of cybersecurity risk management activities across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards? **[RAM.06]**	• OMB Circular A-123 • OMB Circular A-130 • EO 14028	• NIST SP 800-37 (Rev. 2) • NIST SP 800-39 • NIST SP 800-207: Tenets 5 and 7 • NIST IR 8286 • CISA Zero Trust Maturity Model v2.0: Pillars 2-4 • NIST SP 800-39 • NIST SP 800-207: Tenets 5 and 7 • NIST CSF v2.0: GV. RM-03 • NIST CSF v2.0: GV.RM-06 • NIST SP 800-53 (Rev. 5): CA-5(1) and CA-7 • CISA Zero Trust Maturity Model: Pillars 2-4 • NIST IR 8286	Core Metric (*Formerly Metric 10*)	The organization has not identified and defined its requirements for an automated solution to provide a centralized, enterprise wide (portfolio) view of cybersecurity risks across the organization, including risk control and remediation activities, dependences, risk scores/levels, and management dashboards.	The organization has identified and defined its requirements for an automated solution that provides a centralized, enterprise-wide view of cybersecurity risks across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards.	The organization consistently implements an automated solution across the enterprise that provides a centralized, enterprise-wide view of cybersecurity risks, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards. All necessary sources of cybersecurity risk information are integrated into the solution.	In addition, the organization ensures that cybersecurity risk management information is integrated into ERM reporting tools (such as a governance, risk management, and compliance tool), as appropriate.	The organization has institutionalized the use of advanced technologies for analysis of trends and performance against benchmarks to continuously improve its cybersecurity risk management program. Examples include scenario analysis and modeling, the incorporation of technical indicators from threat intelligence, and the ability to consume open security control assessments language (OSCAL) into its GRC processes.
13. Provide any additional information on the effectiveness (positive or negative) of the organization's RAM program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the RAM program effective? **[RAM.SUM]**								
13.1 Please provide an IG self-assessment rating (Effective/Not Effective) for the agency's *identify* function. **[ID.SUM]**								



PROTECT FUNCTION AREA

Table 11: Configuration Management

Question	Criteria	Supplemental Guidance	Review Cycle	Maturity Level				
				Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
14. To what extent does the organization use configuration settings/common secure configurations for its information systems? [**CM.01**]	• FISMA 2014 • OMB Circular A-130 • OMB M-25-04 • DHS BOD 23-01 • NIST FIPS 200 • FIPS 199 • OMB M-21-31	• NIST SP 800-70 (Rev. 4) • CIS Top 18 Security Controls: Controls 4 and 7 • CISA Cybersecurity Incident Response Playbooks • NIST CSF v2.0: ID.RA-01 • NIST CSF v2.0: PR.PS-01 • NIST Security Measures for EO-Critical Software Use: SM 3.3 • NIST SP 800-53 (Rev. 5): CM-6, CM-7, RA-5, and SI-2 • OMB M-21-31, CISA Operational Guidance	Core Metric (*Formerly Metric 20*)	The organization has not established policies and procedures for ensuring that configuration settings/common secure configurations are defined, implemented, and monitored.	The organization has developed, documented, and disseminated its policies and procedures for configuration settings/common secure configurations. In addition, the organization has developed, documented, and disseminated common secure configurations (hardening guides) that are tailored to its environment. Further, the organization has established a deviation process.	The organization consistently implements, assesses, and maintains secure configuration settings for its information systems based on the principle of least functionality. Further, the organization consistently uses SCAP-validated software assessing (scanning) capabilities against all systems on the network (in accordance with DHS BOD 23-01) to assess and manage both code-based and configuration-based vulnerabilities. The organization uses lessons learned in implementation to make improvements to its secure configuration policies and procedures.	The organization employs automation to help maintain an up-to-date, complete, accurate, and readily available view of the security configurations for all information system components connected to the organization's network and makes appropriate modifications in accordance with organization-defined timelines.	The organization deploys system configuration management tools that automatically enforce and redeploy configuration settings to systems at frequent intervals as defined by the organization, or on an event driven basis.

Question	Criteria	Supplemental Guidance	Review Cycle	Maturity Level				
				Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
15. To what extent does the organization use flaw remediation processes, including asset discovery, vulnerability scanning, analysis, and patch management, to manage software vulnerabilities on all network addressable IP-assets? [CM.02]	• OMB M-25-04 • OMB Circular A-130 • NIST FIPS 200 • DHS BOD 18-02 • DHS BOD 19-02 • DHS BOD 22-01 • DHS BOD 23-01	• NIST SP 800-40 (Rev. 4) • NIST SP 800-207: Section 2.1 • NIST Security Measures for EO-Critical Software Use: SM 3.2 • CIS Top 18 Security Controls: Controls 4 and 7 • CISA Cybersecurity Incident Response Playbooks • NIST CSF v2.0: ID.RA-01 • NIST SP 800-53 (Rev. 5): CM-3, RA-5, SI-2, and SI-3 • DHS BOD 23-01, Implementation Guidance • FY 2025 CIO FISMA Metrics: 8.1, 8.2, and 8.3	Core Metric (*Formerly Metric 21*)	The organization has not developed, documented, and disseminated its policies and procedures for flaw remediation, including for mobile devices (GFE and non-GFE).	The organization has developed, documented, and disseminated its policies and procedures for flaw remediation, including for mobile devices. Policies and procedures include processes for: identifying, validating, reporting, and correcting information system flaws, testing software and firmware updates prior to implementation, installing security relevant updates and patches within organizational-defined timeframes, and incorporating flaw remediation into the organization's configuration management processes.	The organization consistently implements its flaw remediation policies, procedures, and processes and ensures that patches, hotfixes, service packs, and anti-virus/malware software updates are identified, prioritized, tested, and installed in a timely manner. In addition, the organization patches critical vulnerabilities within 30 days and uses lessons learned in implementation to make improvements to its flaw remediation policies and procedures. Further, for EO-critical software platforms and all software deployed to those platforms, the organization uses supported software versions.	The organization centrally manages its flaw remediation process and uses automated patch management and software update tools for operating systems, where such tools are available and safe. The organization monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of flaw remediation processes and ensures that data supporting the metrics is obtained accurately, consistently, and in a reproducible format.	The organization uses automated patch management and software update tools for all applications and network devices (including mobile devices), as appropriate, where such tools are available and safe. As part its flaw remediation processes, the organization performs deeper analysis of software code, such as through patch sourcing and testing.
16. Provide any additional information (positive or negative) of the organization's configuration management program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the configuration management program effective? [CM.SUM]								

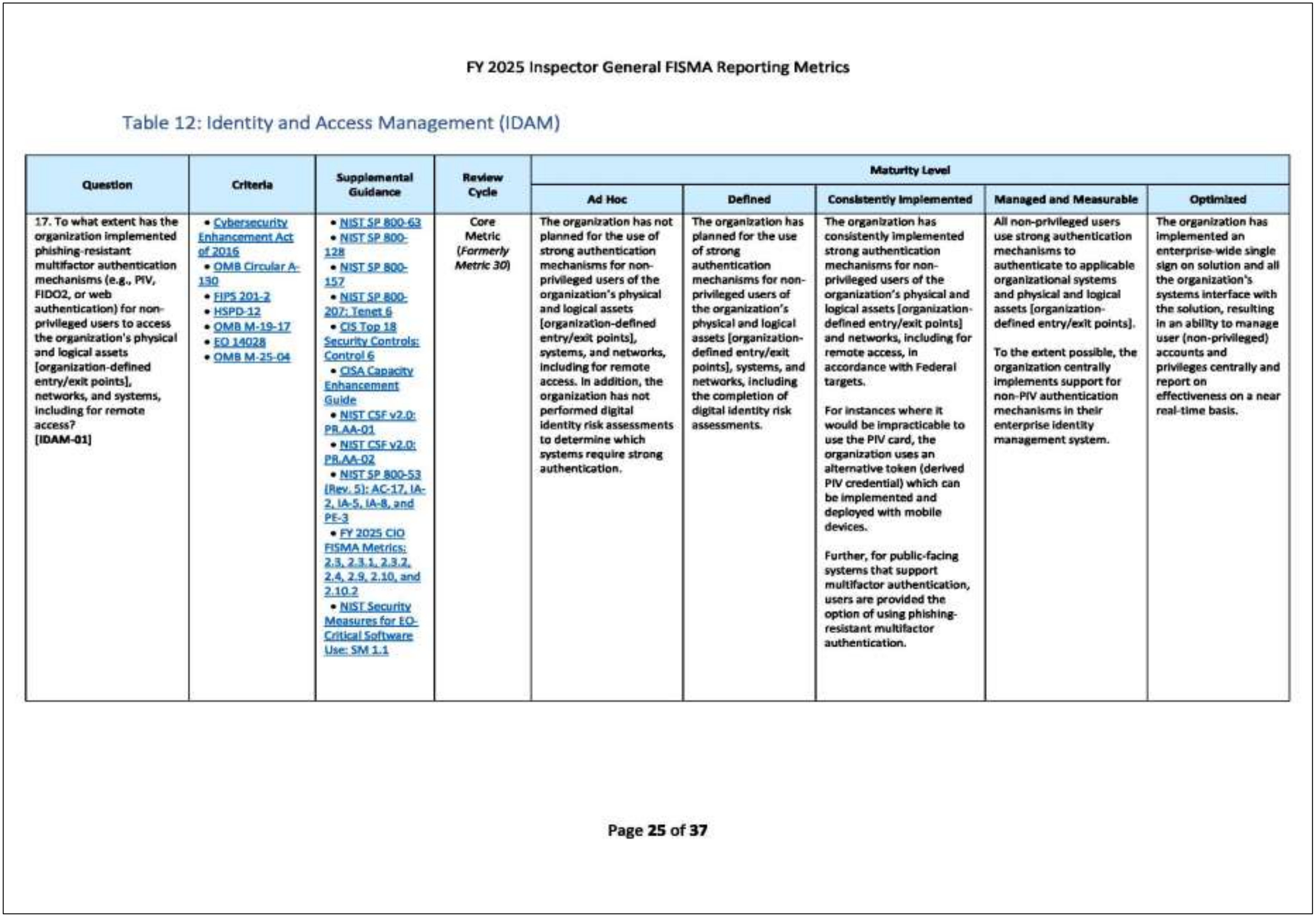
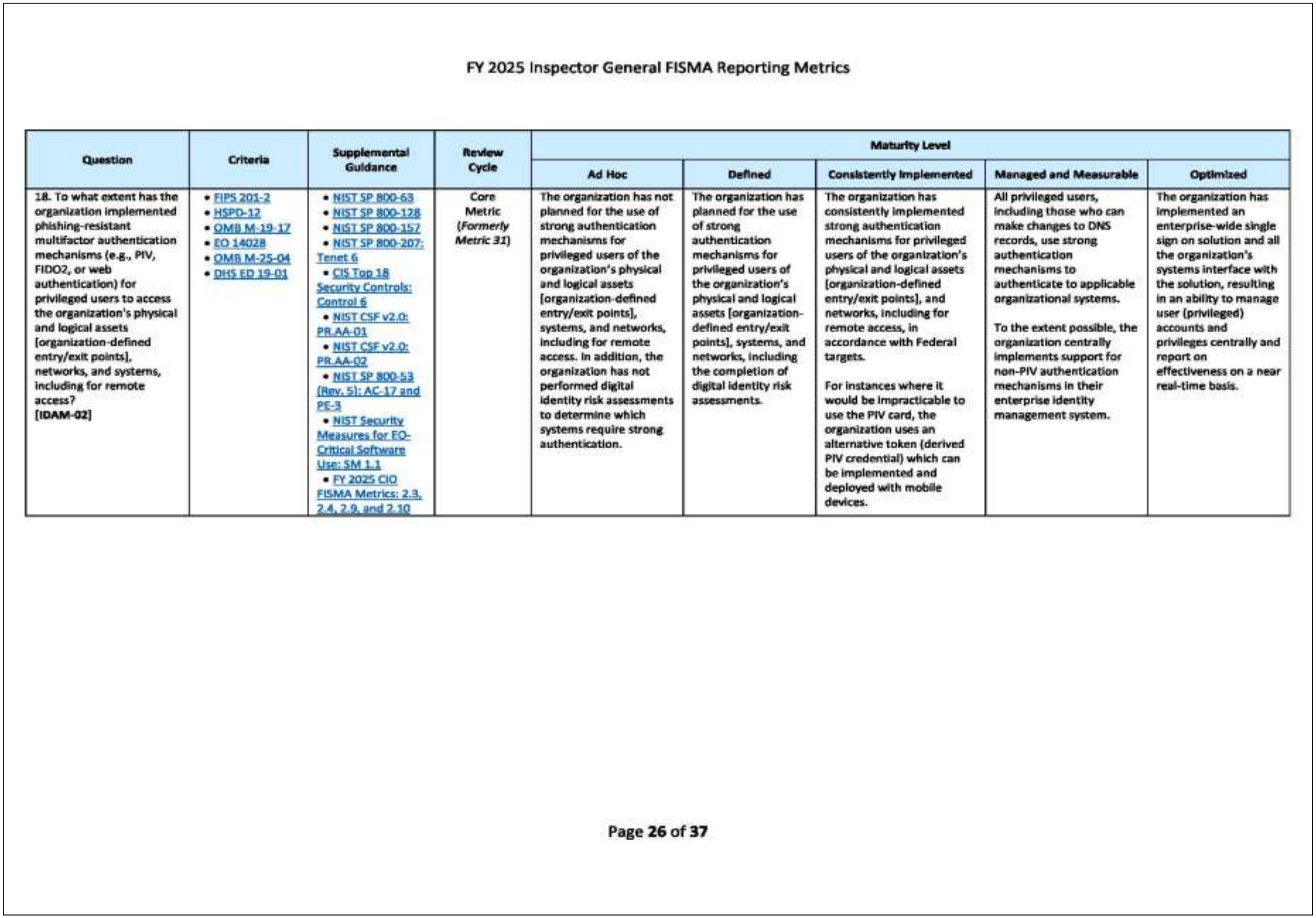


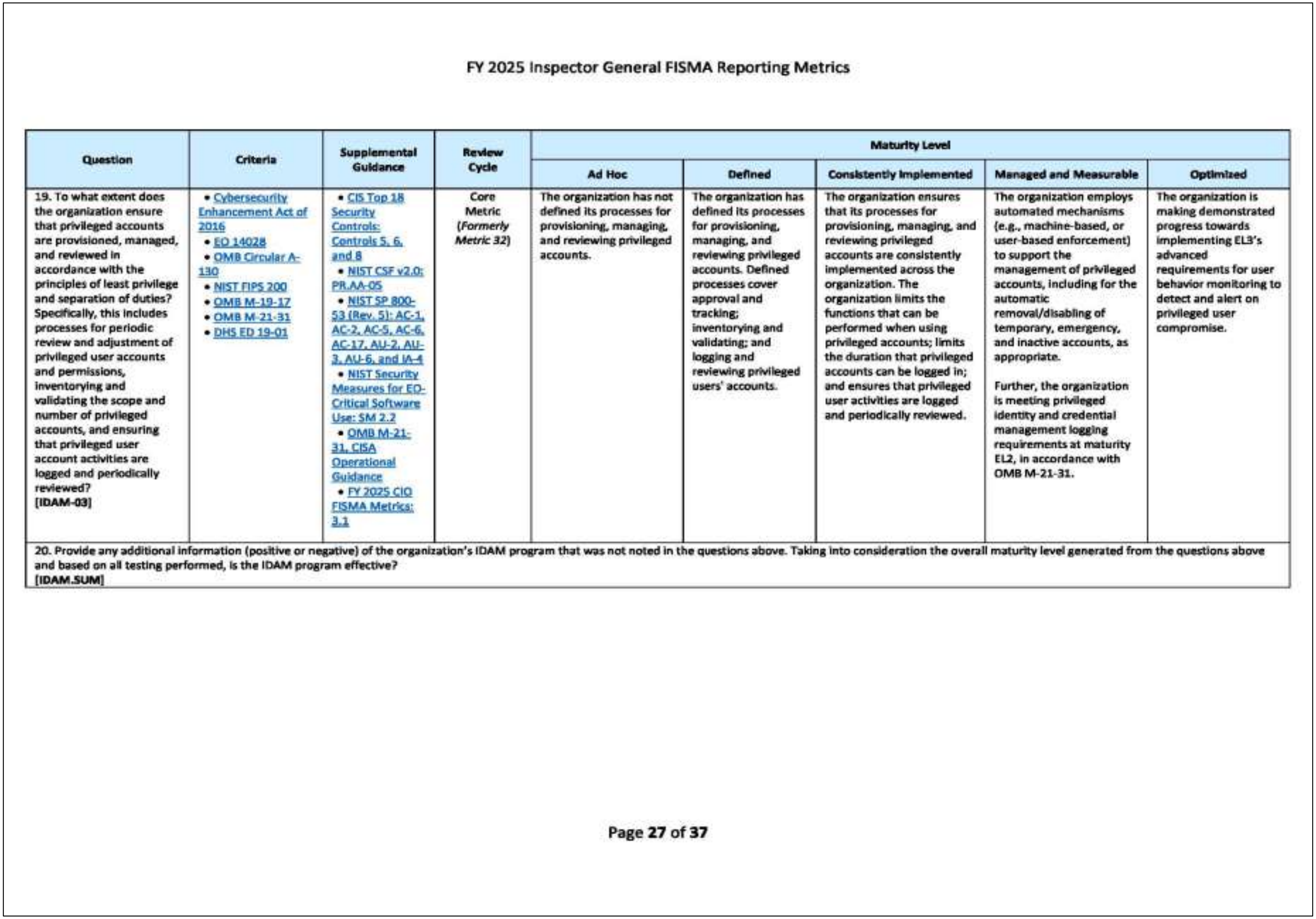
Table 12: Identity and Access Management (IDAM)

Question	Criteria	Supplemental Guidance	Review Cycle	Maturity Level				
				Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
17. To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms (e.g., PIV, FIDO2, or web authentication) for non-privileged users to access the organization's physical and logical assets [organization-defined entry/exit points], networks, and systems, including for remote access? **[IDAM-01]**	• Cybersecurity Enhancement Act of 2016 • OMB Circular A-130 • FIPS 201-2 • HSPD-12 • OMB M-19-17 • EO 14028 • OMB M-25-04	• NIST SP 800-63 • NIST SP 800-128 • NIST SP 800-157 • NIST SP 800-207: Tenet 6 • CIS Top 18 Security Controls: Control 6 • CISA Capacity Enhancement Guide • NIST CSF v2.0: PR.AA-01 • NIST CSF v2.0: PR.AA-02 • NIST SP 800-53 (Rev. 5): AC-17, IA-2, IA-5, IA-8, and PE-3 • FY 2025 CIO FISMA Metrics: 2.3, 2.3.1, 2.3.2, 2.4, 2.9, 2.10, and 2.10.2 • NIST Security Measures for EO-Critical Software Use: SM 1.1	Core Metric *(Formerly Metric 30)*	The organization has not planned for the use of strong authentication mechanisms for non-privileged users of the organization's physical and logical assets [organization-defined entry/exit points], systems, and networks, including for remote access. In addition, the organization has not performed digital identity risk assessments to determine which systems require strong authentication.	The organization has planned for the use of strong authentication mechanisms for non-privileged users of the organization's physical and logical assets [organization-defined entry/exit points], systems, and networks, including the completion of digital identity risk assessments.	The organization has consistently implemented strong authentication mechanisms for non-privileged users of the organization's physical and logical assets [organization-defined entry/exit points] and networks, including for remote access, in accordance with Federal targets. For instances where it would be impracticable to use the PIV card, the organization uses an alternative token (derived PIV credential) which can be implemented and deployed with mobile devices. Further, for public-facing systems that support multifactor authentication, users are provided the option of using phishing-resistant multifactor authentication.	All non-privileged users use strong authentication mechanisms to authenticate to applicable organizational systems and physical and logical assets [organization-defined entry/exit points]. To the extent possible, the organization centrally implements support for non-PIV authentication mechanisms in their enterprise identity management system.	The organization has implemented an enterprise-wide single sign on solution and all the organization's systems interface with the solution, resulting in an ability to manage user (non-privileged) accounts and privileges centrally and report on effectiveness on a near real-time basis.



FY 2025 Inspector General FISMA Reporting Metrics

Question	Criteria	Supplemental Guidance	Review Cycle	Maturity Level				
				Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
18. To what extent has the organization implemented phishing-resistant multifactor authentication mechanisms (e.g., PIV, FIDO2, or web authentication) for privileged users to access the organization's physical and logical assets [organization-defined entry/exit points], networks, and systems, including for remote access? **[IDAM-02]**	• FIPS 201-2 • HSPD-12 • OMB M-19-17 • EO 14028 • OMB M-25-04 • DHS ED 19-01	• NIST SP 800-63 • NIST SP 800-128 • NIST SP 800-157 • NIST SP 800-207: Tenet 6 • CIS Top 18 Security Controls: Control 6 • NIST CSF v2.0: PR.AA-01 • NIST CSF v2.0: PR.AA-02 • NIST SP 800-53 (Rev. 5): AC-17 and PE-3 • NIST Security Measures for EO-Critical Software Use: SM 1.1 • FY 2025 CIO FISMA Metrics: 2.3, 2.4, 2.9, and 2.10	Core Metric (*Formerly Metric 31*)	The organization has not planned for the use of strong authentication mechanisms for privileged users of the organization's physical and logical assets [organization-defined entry/exit points], systems, and networks, including for remote access. In addition, the organization has not performed digital identity risk assessments to determine which systems require strong authentication.	The organization has planned for the use of strong authentication mechanisms for privileged users of the organization's physical and logical assets [organization-defined entry/exit points], systems, and networks, including the completion of digital identity risk assessments.	The organization has consistently implemented strong authentication mechanisms for privileged users of the organization's physical and logical assets [organization-defined entry/exit points], and networks, including for remote access, in accordance with Federal targets. For instances where it would be impracticable to use the PIV card, the organization uses an alternative token (derived PIV credential) which can be implemented and deployed with mobile devices.	All privileged users, including those who can make changes to DNS records, use strong authentication mechanisms to authenticate to applicable organizational systems. To the extent possible, the organization centrally implements support for non-PIV authentication mechanisms in their enterprise identity management system.	The organization has implemented an enterprise-wide single sign on solution and all the organization's systems interface with the solution, resulting in an ability to manage user (privileged) accounts and privileges centrally and report on effectiveness on a near real-time basis.



FY 2025 Inspector General FISMA Reporting Metrics

Question	Criteria	Supplemental Guidance	Review Cycle	Maturity Level				
				Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
19. To what extent does the organization ensure that privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties? Specifically, this includes processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed? **[IDAM-03]**	• Cybersecurity Enhancement Act of 2016 • EO 14028 • OMB Circular A-130 • NIST FIPS 200 • OMB M-19-17 • OMB M-21-31 • DHS ED 19-01	• CIS Top 18 Security Controls: Controls 5, 6, and 8 • NIST CSF v2.0: PR.AA-05 • NIST SP 800-53 (Rev. 5): AC-1, AC-2, AC-5, AC-6, AC-17, AU-2, AU-3, AU-6, and IA-4 • NIST Security Measures for EO-Critical Software Use: SM 2.2 • OMB M-21-31, CISA Operational Guidance • FY 2025 CIO FISMA Metrics: 3.1	Core Metric (*Formerly Metric 32*)	The organization has not defined its processes for provisioning, managing, and reviewing privileged accounts.	The organization has defined its processes for provisioning, managing, and reviewing privileged accounts. Defined processes cover approval and tracking; inventorying and validating; and logging and reviewing privileged users' accounts.	The organization ensures that its processes for provisioning, managing, and reviewing privileged accounts are consistently implemented across the organization. The organization limits the functions that can be performed when using privileged accounts; limits the duration that privileged accounts can be logged in; and ensures that privileged user activities are logged and periodically reviewed.	The organization employs automated mechanisms (e.g., machine-based, or user-based enforcement) to support the management of privileged accounts, including for the automatic removal/disabling of temporary, emergency, and inactive accounts, as appropriate. Further, the organization is meeting privileged identity and credential management logging requirements at maturity EL2, in accordance with OMB M-21-31.	The organization is making demonstrated progress towards implementing EL3's advanced requirements for user behavior monitoring to detect and alert on privileged user compromise.
20. Provide any additional information (positive or negative) of the organization's IDAM program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the IDAM program effective? **[IDAM.SUM]**								

FY 2025 Inspector General FISMA Reporting Metrics

Table 13: Data Protection and Privacy

Question	Criteria	Supplemental Guidance	Review Cycle	Maturity Level				
				Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
21. To what extent has the organization implemented the following security controls to protect the confidentiality, integrity, and availability of its PII and other agency sensitive data, as appropriate, throughout the data lifecycle? • Encryption of data at rest • Encryption of data in transit • Limitation of transfer to removable media • Sanitization of digital media prior to disposal or reuse • Backups of data are created, protected, maintained, and tested •Access to personal email, external file sharing and storage sites, and personal communication applications are blocked, as appropriate. **[DPP.01]**	• OMB Circular A-130 • EO 14028 • DHS BOD 18-02	• NIST SP 800-207 • CIS Top 18 Security Controls: Control 3 • NIST CSF v2.0: PR.DS-01 • NIST CSF v2.0: PR.DS-02 • NIST CSF v2.0: PR.DS-11 • NIST CSF v2.0: ID.AM-08 • NIST SP 800-53 (Rev. 5): SC-8, SC-28, MP-3, MP-6, and SI-12(3) • NIST Security Measures for EO-Critical Software Use: SM 2.3 and SM 2.4 • NIST SP 800-37 (Rev. 2) • FY 2025 CIO FISMA Metrics: 2.1, 2.1.1 and 2.2	Core Metric *(Formerly Metric 36)*	The organization has not defined its policies and procedures in one or more of the specified areas.	The organization's policies and procedures have been defined and communicated for the specified areas. Further, the policies and procedures have been tailored to the organization's environment and include specific considerations based on data classification and sensitivity.	The organization's policies and procedures have been consistently implemented for the specified areas, including (i) use of FIPS-validated encryption of PII and other agency sensitive data, as appropriate, both at rest and in transit, (ii) prevention and detection of untrusted removable media, (iii) destruction or reuse of media containing PII or other sensitive agency data, (iv) backups of PII, including protection and testing of backups, and (v) access to personal email, external file sharing and storage sites, and personal communication applications are blocked, as appropriate.	The organization ensures that the security controls for protecting PII and other agency sensitive data, as appropriate, throughout the data lifecycle are subject to the monitoring processes defined within the organization's ISCM strategy.	The organization employs advanced capabilities to enhance protective controls, including: • Remote wiping • Dual authorization for sanitization of media devices • Exemption of media marking as long as the media remains within organizationally-defined control areas • Configuring systems to record the date the PII was collected, created, or updated and when the data is to be deleted or destroyed according to an approved data retention schedule Continuously backup critical data in near real-time.

FY 2025 Inspector General FISMA Reporting Metrics

Question	Criteria	Supplemental Guidance	Review Cycle	Maturity Level				
				Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
22. To what extent has the organization implemented security controls (e.g., DLP, IDPS, CASB, User and Entity Behavior Analytic tools, SIEM and EDR) to prevent data exfiltration and enhance network defenses? [**DPP.02**]	• DHS BOD 18-01 • DHS ED 19-01 • OMB M-21-07 • OMB M-22-01	• CIS Top 18 Security Controls: Controls 9 and 10 • NIST CSF v2.0: DE.CM-01 • NIST SP 800-53 (Rev. 5): SI-3, SI-7(8), SI-4(4)(18), SC-7(10), and SC-18 • NIST Security Measures for EO-Critical Software Use: SM 4.3 • FY2025 CIO FISMA Metrics: 10.8	Core Metric (*Formerly Metric 37*)	The organization has not defined its policies and procedures related to data exfiltration, endpoint detection and response, enhanced network defenses, email authentication processes, and mitigation against DNS infrastructure tampering.	The organization has defined and communicated its policies and procedures for data exfiltration, endpoint detection and response, enhanced network defenses, email authentication processes, and mitigation against DNS infrastructure tampering.	The organization consistently monitors inbound and outbound network traffic, ensuring that all traffic passes through a web content filter that protects against phishing, malware, and blocks against known malicious sites. Additionally, the organization checks outbound communications traffic to detect encrypted exfiltration of information, anomalous traffic patterns, and elements of PII. Also, suspected malicious traffic is quarantined or blocked. In addition, the organization uses email authentication technology and ensures the use of valid encryption certificates for its domains. The organization consistently implements EDR capabilities to support host-level visibility, attribution, and response for its information systems.	The organization analyzes qualitative and quantitative measures on the performance of its data exfiltration and enhanced network defenses. The organization also conducts exfiltration exercises to measure the effectiveness of its data exfiltration and enhanced network defenses. Further, the organization monitors its DNS infrastructure for potential tampering, in accordance with its ISCM strategy. In addition, the organization audits its DNS records. Further, the organization has assessed its current EDR capabilities, identified any gaps, and is coordinating with CISA for future EDR solution deployments.	The organization's data exfiltration and enhanced network defenses are fully integrated into the ISCM and incident response programs to provide near real-time monitoring of the data that is entering and exiting the network, and other suspicious inbound and outbound communications. The organization continuously runs device posture assessments (e.g., using EDR tools) to maintain visibility and analytics capabilities related to data exfiltration.
23. Provide any additional information (positive or negative) of the organization's data protection and privacy program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the data protection and privacy program effective? [**DPP.SUM**]								

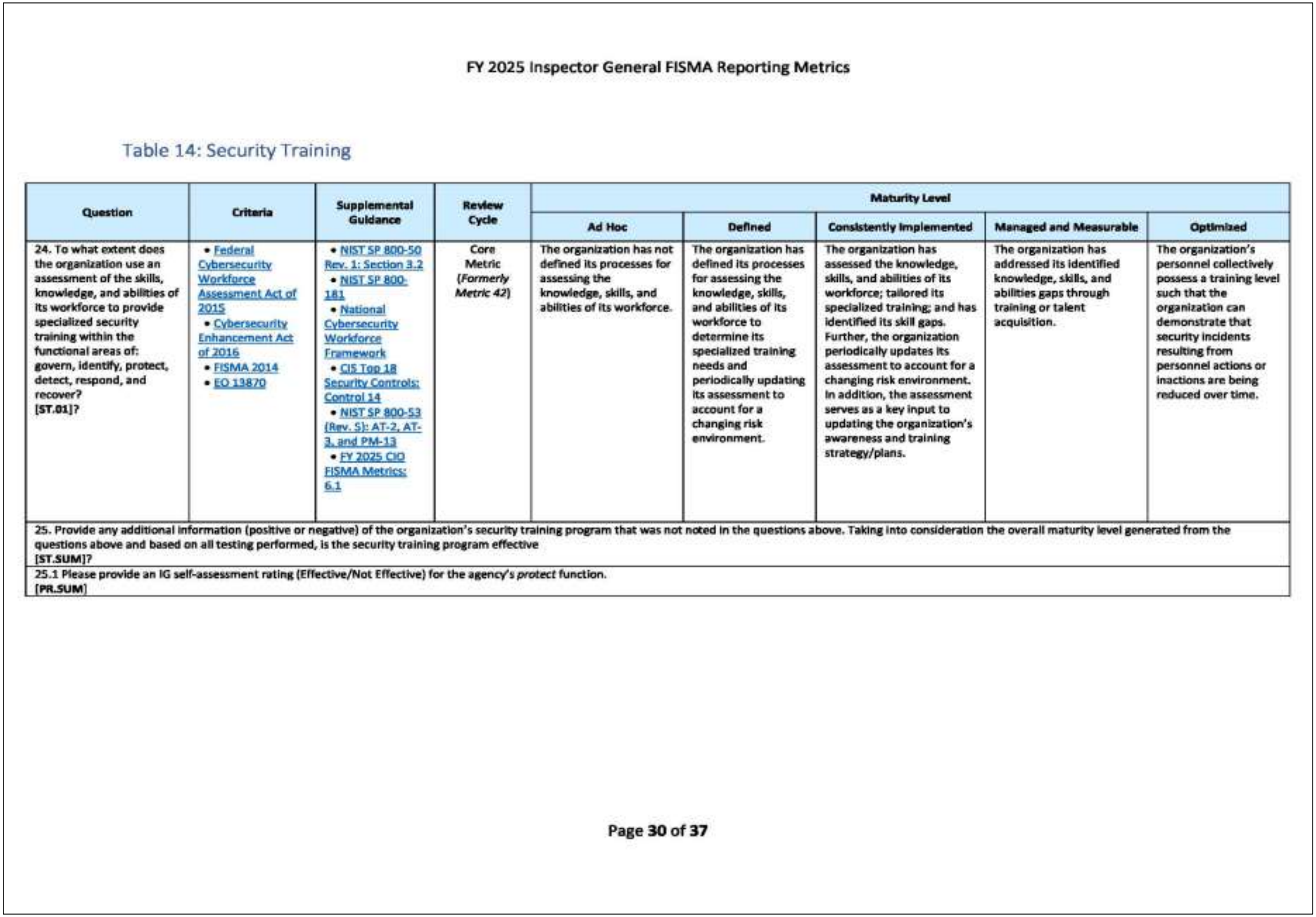
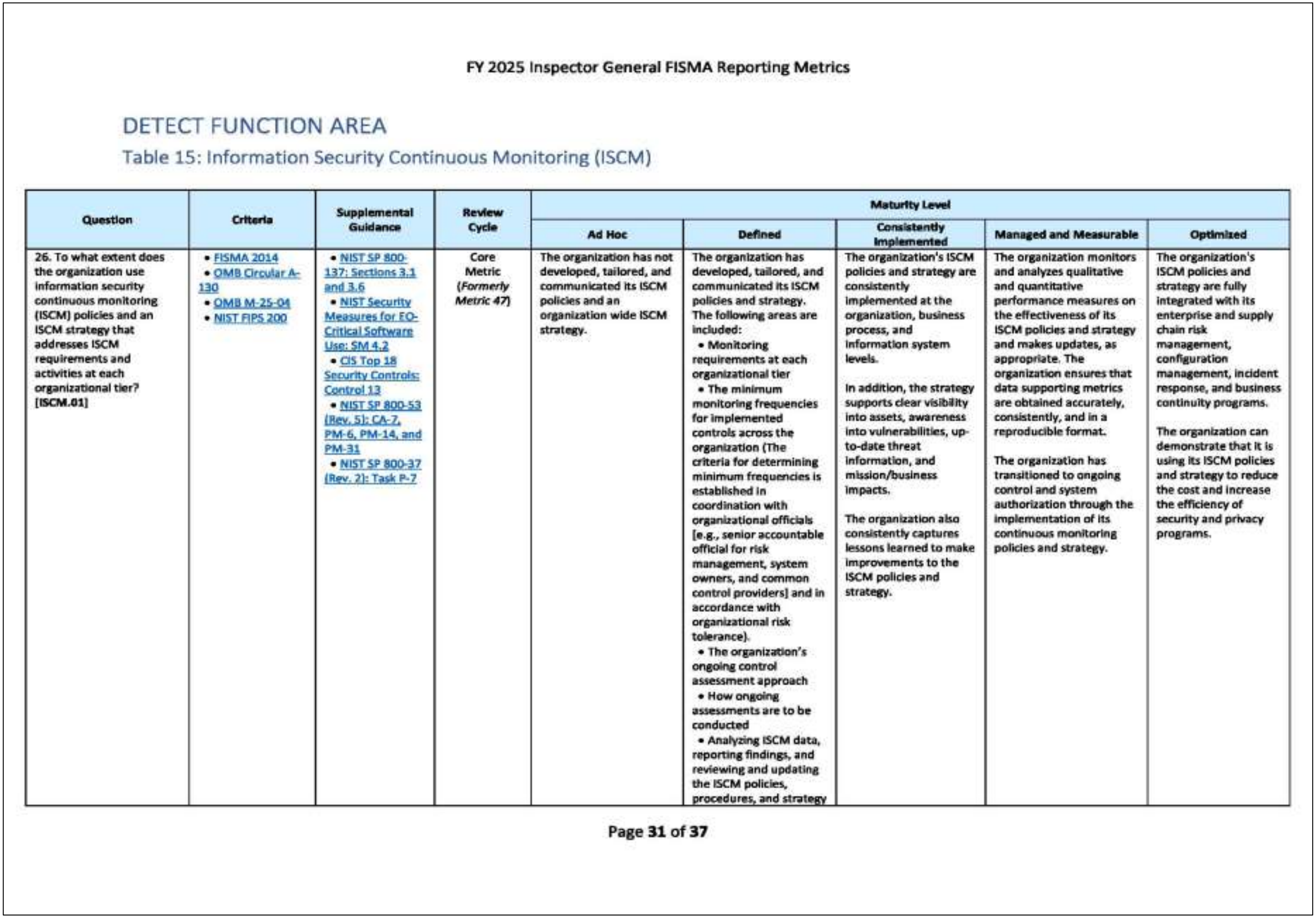


Table 14: Security Training

Question	Criteria	Supplemental Guidance	Review Cycle	Maturity Level				
				Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
24. To what extent does the organization use an assessment of the skills, knowledge, and abilities of its workforce to provide specialized security training within the functional areas of: govern, identify, protect, detect, respond, and recover? [ST.01]?	• Federal Cybersecurity Workforce Assessment Act of 2015 • Cybersecurity Enhancement Act of 2016 • FISMA 2014 • EO 13870	• NIST SP 800-50 Rev. 1: Section 3.2 • NIST SP 800-181 • National Cybersecurity Workforce Framework • CIS Top 18 Security Controls: Control 14 • NIST SP 800-53 (Rev. 5): AT-2, AT-3, and PM-13 • FY 2025 CIO FISMA Metrics: 6.1	Core Metric *(Formerly Metric 42)*	The organization has not defined its processes for assessing the knowledge, skills, and abilities of its workforce.	The organization has defined its processes for assessing the knowledge, skills, and abilities of its workforce to determine its specialized training needs and periodically updating its assessment to account for a changing risk environment.	The organization has assessed the knowledge, skills, and abilities of its workforce; tailored its specialized training; and has identified its skill gaps. Further, the organization periodically updates its assessment to account for a changing risk environment. In addition, the assessment serves as a key input to updating the organization's awareness and training strategy/plans.	The organization has addressed its identified knowledge, skills, and abilities gaps through training or talent acquisition.	The organization's personnel collectively possess a training level such that the organization can demonstrate that security incidents resulting from personnel actions or inactions are being reduced over time.
25. Provide any additional information (positive or negative) of the organization's security training program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the security training program effective [ST.SUM]?								
25.1 Please provide an IG self-assessment rating (Effective/Not Effective) for the agency's *protect* function. [PR.SUM]								

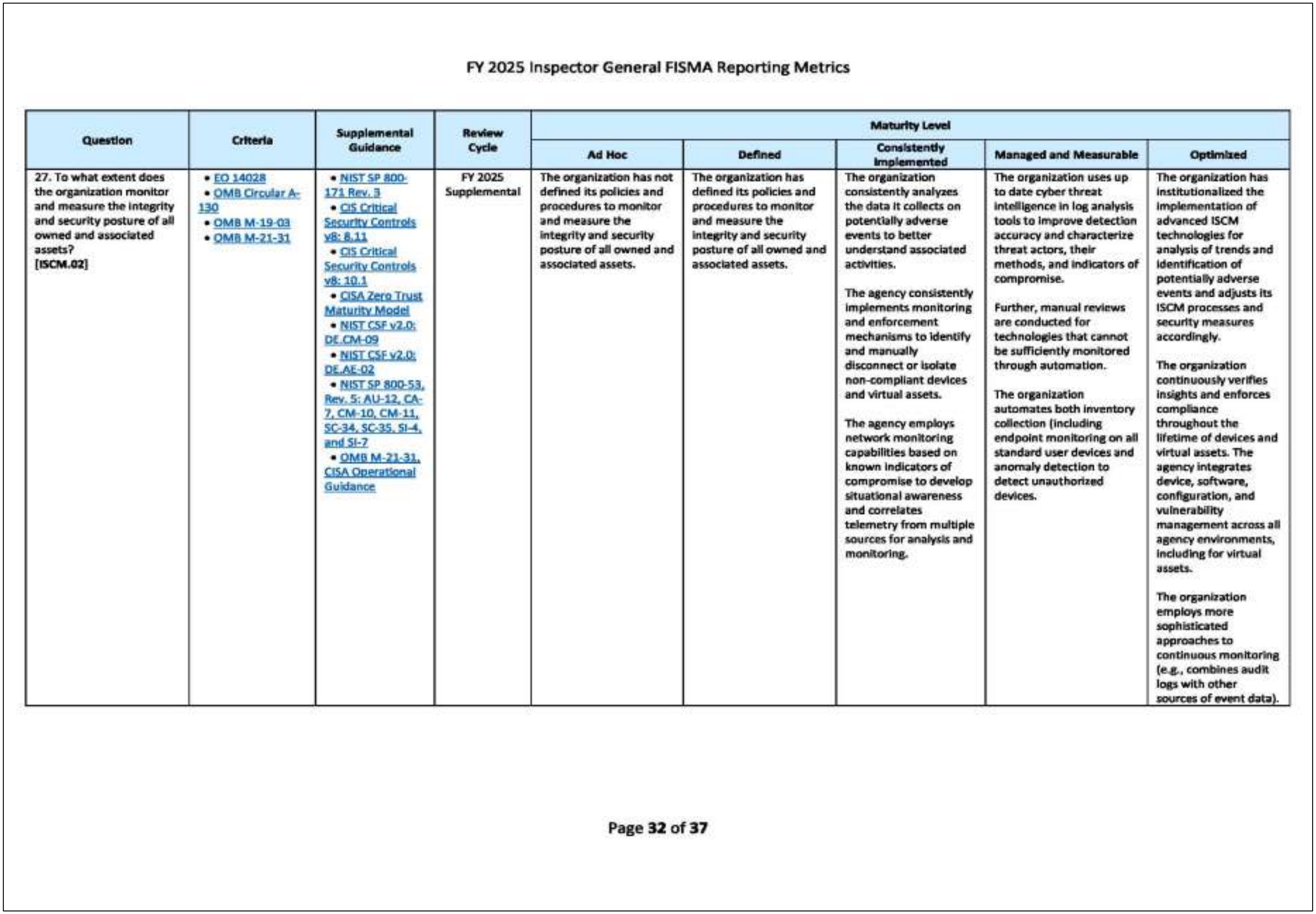


FY 2025 Inspector General FISMA Reporting Metrics

DETECT FUNCTION AREA

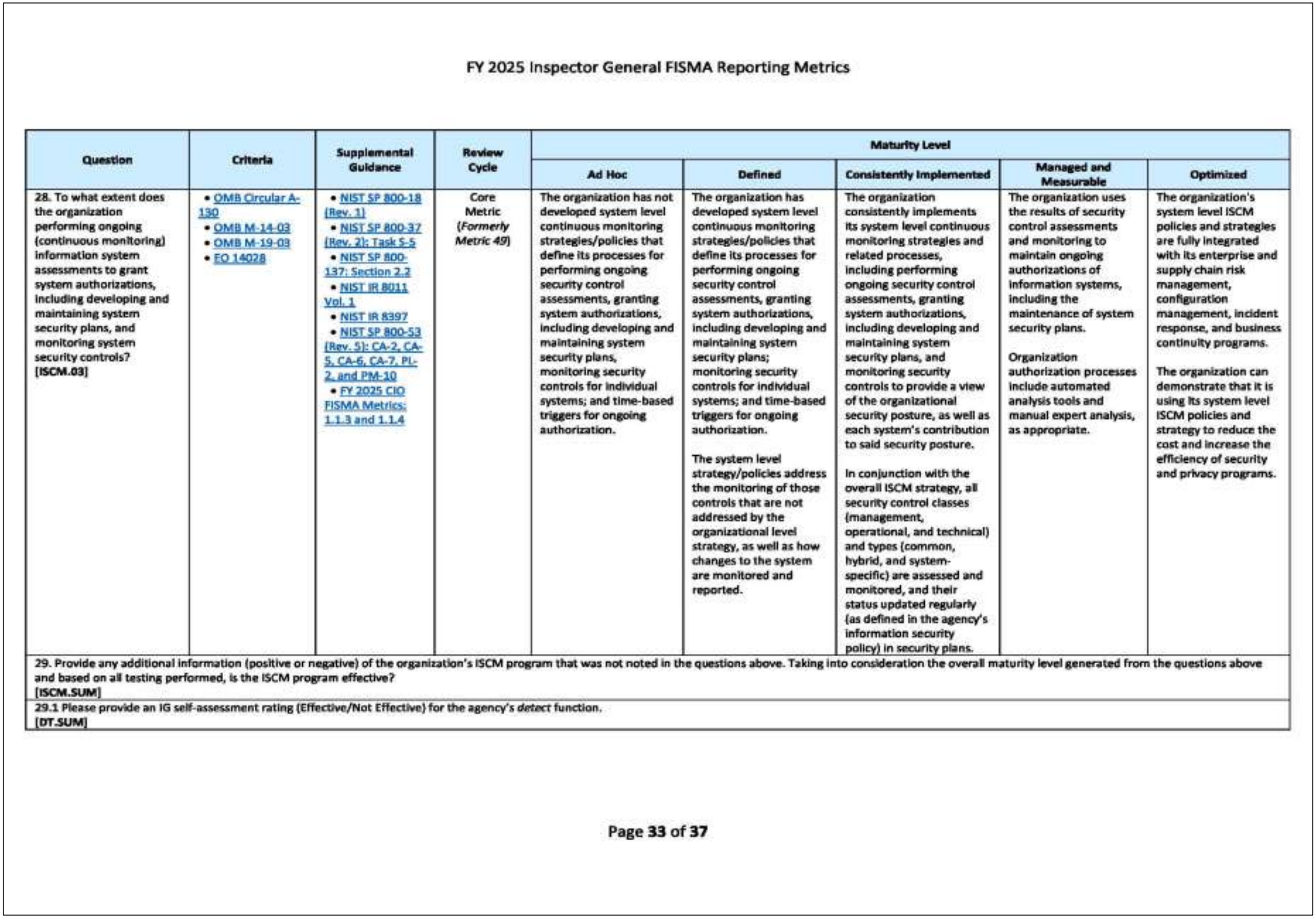
Table 15: Information Security Continuous Monitoring (ISCM)

Question	Criteria	Supplemental Guidance	Review Cycle	Maturity Level				
				Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
26. To what extent does the organization use information security continuous monitoring (ISCM) policies and an ISCM strategy that addresses ISCM requirements and activities at each organizational tier? **[ISCM.01]**	• FISMA 2014 • OMB Circular A-130 • OMB M-25-04 • NIST FIPS 200	• NIST SP 800-137: Sections 3.1 and 3.6 • NIST Security Measures for EO-Critical Software Use: SM 4.2 • CIS Top 18 Security Controls: Control 13 • NIST SP 800-53 (Rev. 5): CA-7, PM-6, PM-14, and PM-31 • NIST SP 800-37 (Rev. 2): Task P-7	Core Metric (*Formerly Metric 47*)	The organization has not developed, tailored, and communicated its ISCM policies and an organization wide ISCM strategy.	The organization has developed, tailored, and communicated its ISCM policies and strategy. The following areas are included: • Monitoring requirements at each organizational tier • The minimum monitoring frequencies for implemented controls across the organization (The criteria for determining minimum frequencies is established in coordination with organizational officials [e.g., senior accountable official for risk management, system owners, and common control providers] and in accordance with organizational risk tolerance). • The organization's ongoing control assessment approach • How ongoing assessments are to be conducted • Analyzing ISCM data, reporting findings, and reviewing and updating the ISCM policies, procedures, and strategy	The organization's ISCM policies and strategy are consistently implemented at the organization, business process, and information system levels. In addition, the strategy supports clear visibility into assets, awareness into vulnerabilities, up-to-date threat information, and mission/business impacts. The organization also consistently captures lessons learned to make improvements to the ISCM policies and strategy.	The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its ISCM policies and strategy and makes updates, as appropriate. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format. The organization has transitioned to ongoing control and system authorization through the implementation of its continuous monitoring policies and strategy.	The organization's ISCM policies and strategy are fully integrated with its enterprise and supply chain risk management, configuration management, incident response, and business continuity programs. The organization can demonstrate that it is using its ISCM policies and strategy to reduce the cost and increase the efficiency of security and privacy programs.



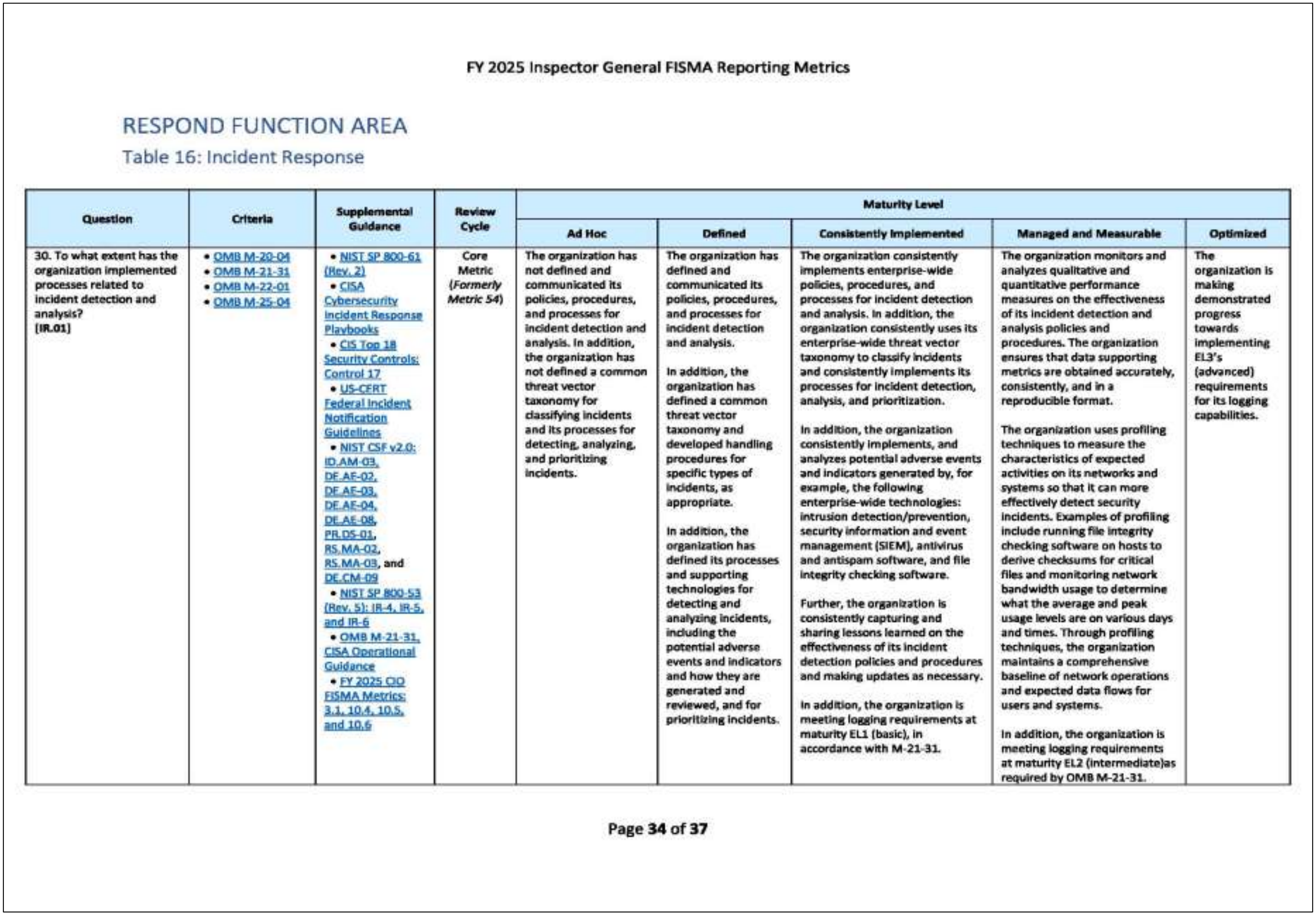
FY 2025 Inspector General FISMA Reporting Metrics

Question	Criteria	Supplemental Guidance	Review Cycle	Maturity Level				
				Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
27. To what extent does the organization monitor and measure the integrity and security posture of all owned and associated assets? **[ISCM.02]**	• EO 14028 • OMB Circular A-130 • OMB M-19-03 • OMB M-21-31	• NIST SP 800-171 Rev. 3 • CIS Critical Security Controls v8: 8.11 • CIS Critical Security Controls v8: 10.1 • CISA Zero Trust Maturity Model • NIST CSF v2.0: DE.CM-09 • NIST CSF v2.0: DE.AE-02 • NIST SP 800-53, Rev. 5: AU-12, CA-7, CM-10, CM-11, SC-34, SC-35, SI-4, and SI-7 • OMB M-21-31, CISA Operational Guidance	FY 2025 Supplemental	The organization has not defined its policies and procedures to monitor and measure the integrity and security posture of all owned and associated assets.	The organization has defined its policies and procedures to monitor and measure the integrity and security posture of all owned and associated assets.	The organization consistently analyzes the data it collects on potentially adverse events to better understand associated activities. The agency consistently implements monitoring and enforcement mechanisms to identify and manually disconnect or isolate non-compliant devices and virtual assets. The agency employs network monitoring capabilities based on known indicators of compromise to develop situational awareness and correlates telemetry from multiple sources for analysis and monitoring.	The organization uses up to date cyber threat intelligence in log analysis tools to improve detection accuracy and characterize threat actors, their methods, and indicators of compromise. Further, manual reviews are conducted for technologies that cannot be sufficiently monitored through automation. The organization automates both inventory collection (including endpoint monitoring on all standard user devices and anomaly detection to detect unauthorized devices.	The organization has institutionalized the implementation of advanced ISCM technologies for analysis of trends and identification of potentially adverse events and adjusts its ISCM processes and security measures accordingly. The organization continuously verifies insights and enforces compliance throughout the lifetime of devices and virtual assets. The agency integrates device, software, configuration, and vulnerability management across all agency environments, including for virtual assets. The organization employs more sophisticated approaches to continuous monitoring (e.g., combines audit logs with other sources of event data).



FY 2025 Inspector General FISMA Reporting Metrics

Question	Criteria	Supplemental Guidance	Review Cycle	Maturity Level				
				Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
28. To what extent does the organization performing ongoing (continuous monitoring) information system assessments to grant system authorizations, including developing and maintaining system security plans, and monitoring system security controls? **[ISCM.03]**	• OMB Circular A-130 • OMB M-14-03 • OMB M-19-03 • EO 14028	• NIST SP 800-18 (Rev. 1) • NIST SP 800-37 (Rev. 2): Task S-5 • NIST SP 800-137: Section 2.2 • NIST IR 8011 Vol. 1 • NIST IR 8397 • NIST SP 800-53 (Rev. 5): CA-2, CA-5, CA-6, CA-7, PL-2, and PM-10 • FY 2025 CIO FISMA Metrics: 1.1.3 and 1.1.4	Core Metric (*Formerly Metric 49*)	The organization has not developed system level continuous monitoring strategies/policies that define its processes for performing ongoing security control assessments, granting system authorizations, including developing and maintaining system security plans, monitoring security controls for individual systems; and time-based triggers for ongoing authorization.	The organization has developed system level continuous monitoring strategies/policies that define its processes for performing ongoing security control assessments, granting system authorizations, including developing and maintaining system security plans; monitoring security controls for individual systems; and time-based triggers for ongoing authorization. The system level strategy/policies address the monitoring of those controls that are not addressed by the organizational level strategy, as well as how changes to the system are monitored and reported.	The organization consistently implements its system level continuous monitoring strategies and related processes, including performing ongoing security control assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring security controls to provide a view of the organizational security posture, as well as each system's contribution to said security posture. In conjunction with the overall ISCM strategy, all security control classes (management, operational, and technical) and types (common, hybrid, and system-specific) are assessed and monitored, and their status updated regularly (as defined in the agency's information security policy) in security plans.	The organization uses the results of security control assessments and monitoring to maintain ongoing authorizations of information systems, including the maintenance of system security plans. Organization authorization processes include automated analysis tools and manual expert analysis, as appropriate.	The organization's system level ISCM policies and strategies are fully integrated with its enterprise and supply chain risk management, configuration management, incident response, and business continuity programs. The organization can demonstrate that it is using its system level ISCM policies and strategy to reduce the cost and increase the efficiency of security and privacy programs.
29. Provide any additional information (positive or negative) of the organization's ISCM program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the ISCM program effective? **[ISCM.SUM]**								
29.1 Please provide an IG self-assessment rating (Effective/Not Effective) for the agency's *detect* function. **[DT.SUM]**								

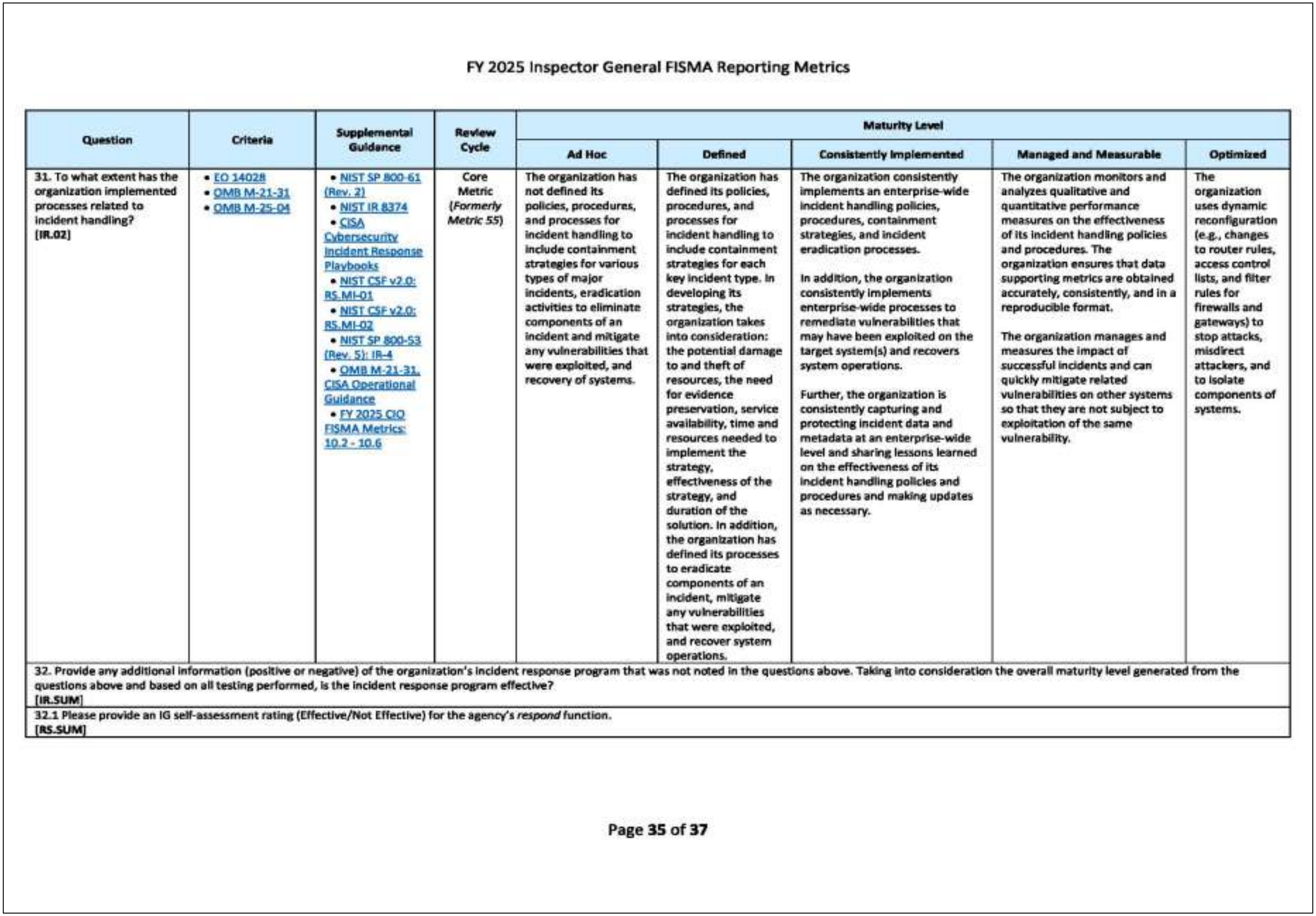


FY 2025 Inspector General FISMA Reporting Metrics

RESPOND FUNCTION AREA

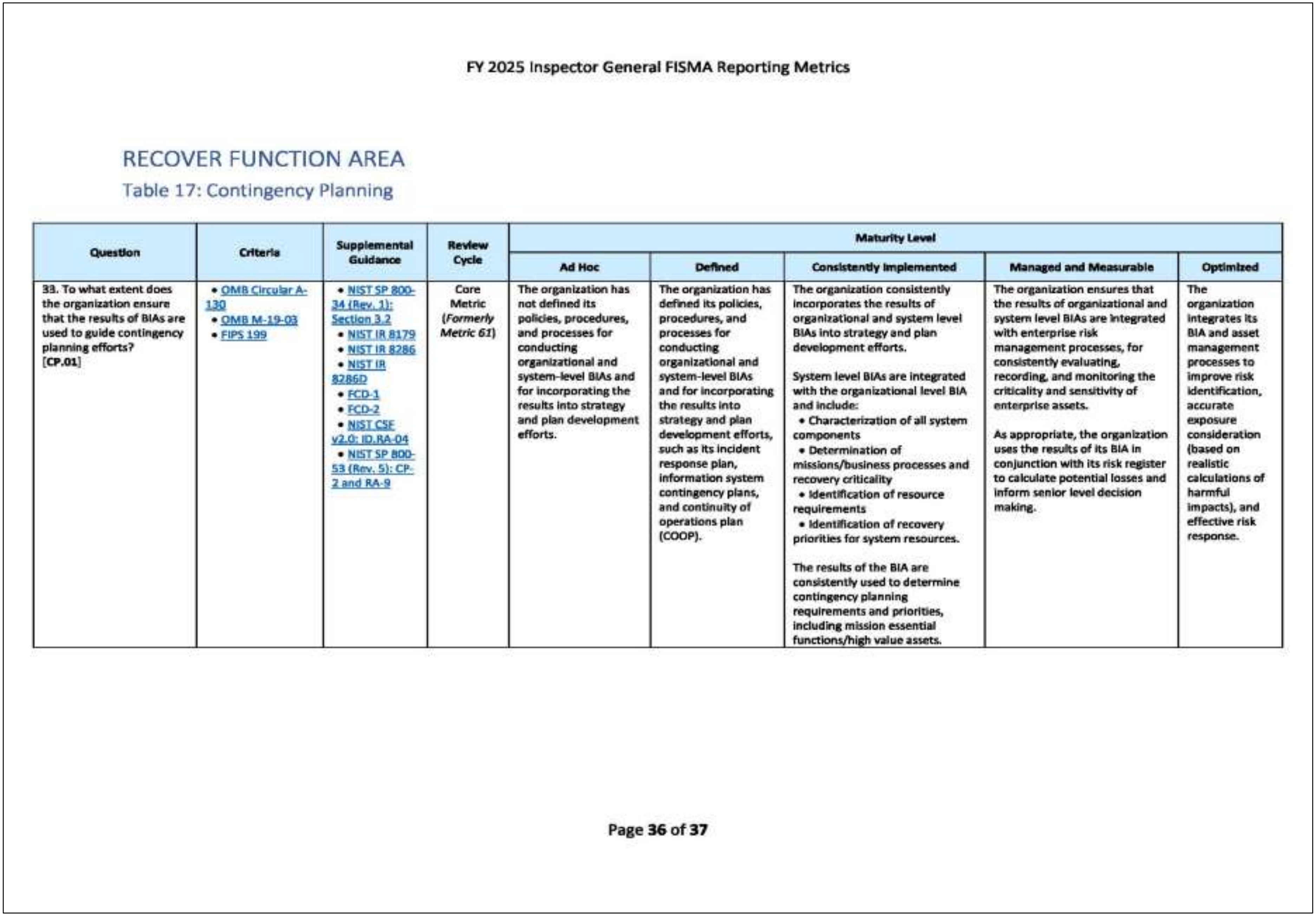
Table 16: Incident Response

Question	Criteria	Supplemental Guidance	Review Cycle	Maturity Level				
				Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
30. To what extent has the organization implemented processes related to incident detection and analysis? (IR.01)	• OMB M-20-04 • OMB M-21-31 • OMB M-22-01 • OMB M-25-04	• NIST SP 800-61 (Rev. 2) • CISA Cybersecurity Incident Response Playbooks • CIS Top 18 Security Controls: Control 17 • US-CERT Federal Incident Notification Guidelines • NIST CSF v2.0: ID.AM-03, DE.AE-02, DE.AE-03, DE.AE-04, DE.AE-08, PR.DS-01, RS.MA-02, RS.MA-03, and DE.CM-09 • NIST SP 800-53 (Rev. 5): IR-4, IR-5, and IR-6 • OMB M-21-31, CISA Operational Guidance • FY 2025 CIO FISMA Metrics: 3.1, 10.4, 10.5, and 10.6	Core Metric (*Formerly Metric 54*)	The organization has not defined and communicated its policies, procedures, and processes for incident detection and analysis. In addition, the organization has not defined a common threat vector taxonomy for classifying incidents and its processes for detecting, analyzing, and prioritizing incidents.	The organization has defined and communicated its policies, procedures, and processes for incident detection and analysis. In addition, the organization has defined a common threat vector taxonomy and developed handling procedures for specific types of incidents, as appropriate. In addition, the organization has defined its processes and supporting technologies for detecting and analyzing incidents, including the potential adverse events and indicators and how they are generated and reviewed, and for prioritizing incidents.	The organization consistently implements enterprise-wide policies, procedures, and processes for incident detection and analysis. In addition, the organization consistently uses its enterprise-wide threat vector taxonomy to classify incidents and consistently implements its processes for incident detection, analysis, and prioritization. In addition, the organization consistently implements, and analyzes potential adverse events and indicators generated by, for example, the following enterprise-wide technologies: intrusion detection/prevention, security information and event management (SIEM), antivirus and antispam software, and file integrity checking software. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of its incident detection policies and procedures and making updates as necessary. In addition, the organization is meeting logging requirements at maturity EL1 (basic), in accordance with M-21-31.	The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its incident detection and analysis policies and procedures. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format. The organization uses profiling techniques to measure the characteristics of expected activities on its networks and systems so that it can more effectively detect security incidents. Examples of profiling include running file integrity checking software on hosts to derive checksums for critical files and monitoring network bandwidth usage to determine what the average and peak usage levels are on various days and times. Through profiling techniques, the organization maintains a comprehensive baseline of network operations and expected data flows for users and systems. In addition, the organization is meeting logging requirements at maturity EL2 (intermediate)as required by OMB M-21-31.	The organization is making demonstrated progress towards implementing EL3's (advanced) requirements for its logging capabilities.



FY 2025 Inspector General FISMA Reporting Metrics

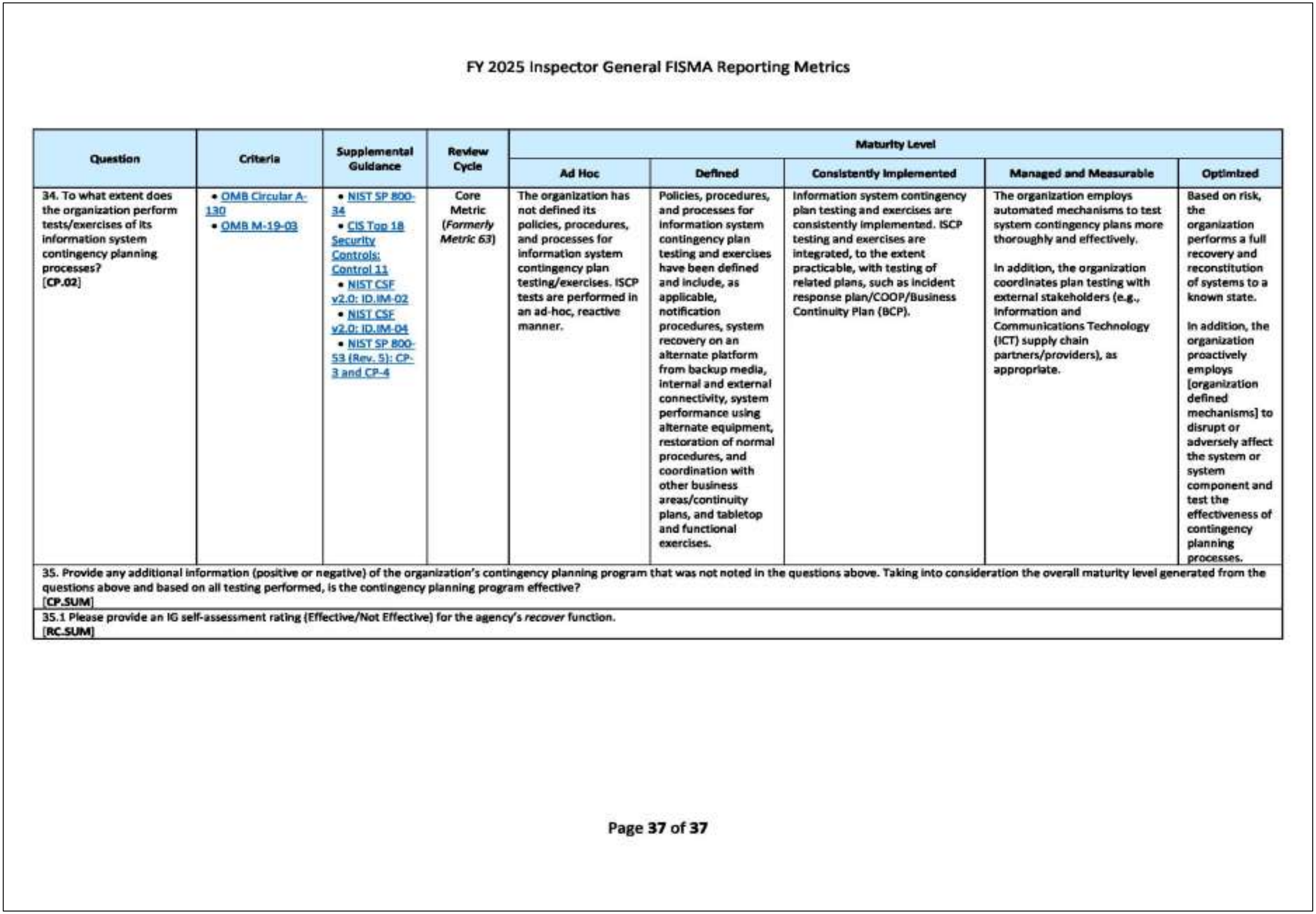
Question	Criteria	Supplemental Guidance	Review Cycle	Maturity Level				
				Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
31. To what extent has the organization implemented processes related to incident handling? **[IR.02]**	• EO 14028 • OMB M-21-31 • OMB M-25-04	• NIST SP 800-61 (Rev. 2) • NIST IR 8374 • CISA Cybersecurity Incident Response Playbooks • NIST CSF v2.0: RS.MI-01 • NIST CSF v2.0: RS.MI-02 • NIST SP 800-53 (Rev. 5): IR-4 • OMB M-21-31, CISA Operational Guidance • FY 2025 CIO FISMA Metrics: 10.2 - 10.6	Core Metric (*Formerly Metric 55*)	The organization has not defined its policies, procedures, and processes for incident handling to include containment strategies for various types of major incidents, eradication activities to eliminate components of an incident and mitigate any vulnerabilities that were exploited, and recovery of systems.	The organization has defined its policies, procedures, and processes for incident handling to include containment strategies for each key incident type. In developing its strategies, the organization takes into consideration: the potential damage to and theft of resources, the need for evidence preservation, service availability, time and resources needed to implement the strategy, effectiveness of the strategy, and duration of the solution. In addition, the organization has defined its processes to eradicate components of an incident, mitigate any vulnerabilities that were exploited, and recover system operations.	The organization consistently implements an enterprise-wide incident handling policies, procedures, containment strategies, and incident eradication processes. In addition, the organization consistently implements enterprise-wide processes to remediate vulnerabilities that may have been exploited on the target system(s) and recovers system operations. Further, the organization is consistently capturing and protecting incident data and metadata at an enterprise-wide level and sharing lessons learned on the effectiveness of its incident handling policies and procedures and making updates as necessary.	The organization monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its incident handling policies and procedures. The organization ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format. The organization manages and measures the impact of successful incidents and can quickly mitigate related vulnerabilities on other systems so that they are not subject to exploitation of the same vulnerability.	The organization uses dynamic reconfiguration (e.g., changes to router rules, access control lists, and filter rules for firewalls and gateways) to stop attacks, misdirect attackers, and to isolate components of systems.
32. Provide any additional information (positive or negative) of the organization's incident response program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the incident response program effective? **[IR.SUM]**								
32.1 Please provide an IG self-assessment rating (Effective/Not Effective) for the agency's *respond* function. **[RS.SUM]**								



RECOVER FUNCTION AREA

Table 17: Contingency Planning

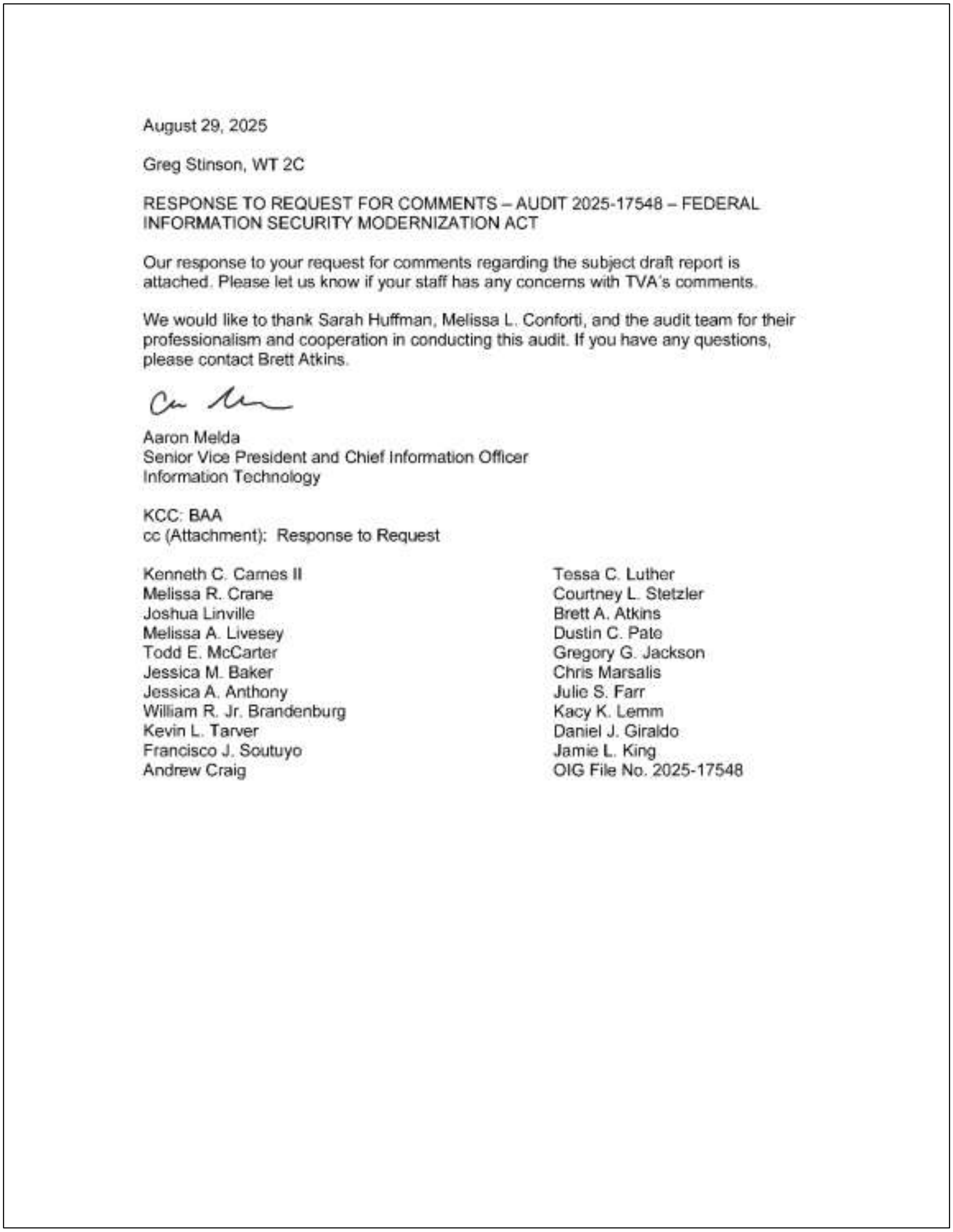
Question	Criteria	Supplemental Guidance	Review Cycle	Maturity Level				
				Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
33. To what extent does the organization ensure that the results of BIAs are used to guide contingency planning efforts? [**CP.01**]	• OMB Circular A-130 • OMB M-19-03 • FIPS 199	• NIST SP 800-34 (Rev. 1): Section 3.2 • NIST IR 8179 • NIST IR 8286 • NIST IR 8286D • FCD-1 • FCD-2 • NIST CSF v2.0: ID.RA-04 • NIST SP 800-53 (Rev. 5): CP-2 and RA-9	Core Metric (*Formerly Metric 61*)	The organization has not defined its policies, procedures, and processes for conducting organizational and system-level BIAs and for incorporating the results into strategy and plan development efforts.	The organization has defined its policies, procedures, and processes for conducting organizational and system-level BIAs and for incorporating the results into strategy and plan development efforts, such as its incident response plan, information system contingency plans, and continuity of operations plan (COOP).	The organization consistently incorporates the results of organizational and system level BIAs into strategy and plan development efforts. System level BIAs are integrated with the organizational level BIA and include: • Characterization of all system components • Determination of missions/business processes and recovery criticality • Identification of resource requirements • Identification of recovery priorities for system resources. The results of the BIA are consistently used to determine contingency planning requirements and priorities, including mission essential functions/high value assets.	The organization ensures that the results of organizational and system level BIAs are integrated with enterprise risk management processes, for consistently evaluating, recording, and monitoring the criticality and sensitivity of enterprise assets. As appropriate, the organization uses the results of its BIA in conjunction with its risk register to calculate potential losses and inform senior level decision making.	The organization integrates its BIA and asset management processes to improve risk identification, accurate exposure consideration (based on realistic calculations of harmful impacts), and effective risk response.



FY 2025 Inspector General FISMA Reporting Metrics

Question	Criteria	Supplemental Guidance	Review Cycle	Maturity Level				
				Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
34. To what extent does the organization perform tests/exercises of its information system contingency planning processes? [CP.02]	• OMB Circular A-130 • OMB M-19-03	• NIST SP 800-34 • CIS Top 18 Security Controls: Control 11 • NIST CSF v2.0: ID.IM-02 • NIST CSF v2.0: ID.IM-04 • NIST SP 800-53 (Rev. 5): CP-3 and CP-4	Core Metric *(Formerly Metric 63)*	The organization has not defined its policies, procedures, and processes for information system contingency plan testing/exercises. ISCP tests are performed in an ad-hoc, reactive manner.	Policies, procedures, and processes for information system contingency plan testing and exercises have been defined and include, as applicable, notification procedures, system recovery on an alternate platform from backup media, internal and external connectivity, system performance using alternate equipment, restoration of normal procedures, and coordination with other business areas/continuity plans, and tabletop and functional exercises.	Information system contingency plan testing and exercises are consistently implemented. ISCP testing and exercises are integrated, to the extent practicable, with testing of related plans, such as incident response plan/COOP/Business Continuity Plan (BCP).	The organization employs automated mechanisms to test system contingency plans more thoroughly and effectively. In addition, the organization coordinates plan testing with external stakeholders (e.g., Information and Communications Technology (ICT) supply chain partners/providers), as appropriate.	Based on risk, the organization performs a full recovery and reconstitution of systems to a known state. In addition, the organization proactively employs [organization defined mechanisms] to disrupt or adversely affect the system or system component and test the effectiveness of contingency planning processes.
35. Provide any additional information (positive or negative) of the organization's contingency planning program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the contingency planning program effective? [CP.SUM]								
35.1 Please provide an IG self-assessment rating (Effective/Not Effective) for the agency's *recover* function. [RC.SUM]								

APPENDIX C
Page 1 of 2



August 29, 2025

Greg Stinson, WT 2C

RESPONSE TO REQUEST FOR COMMENTS – AUDIT 2025-17548 – FEDERAL INFORMATION SECURITY MODERNIZATION ACT

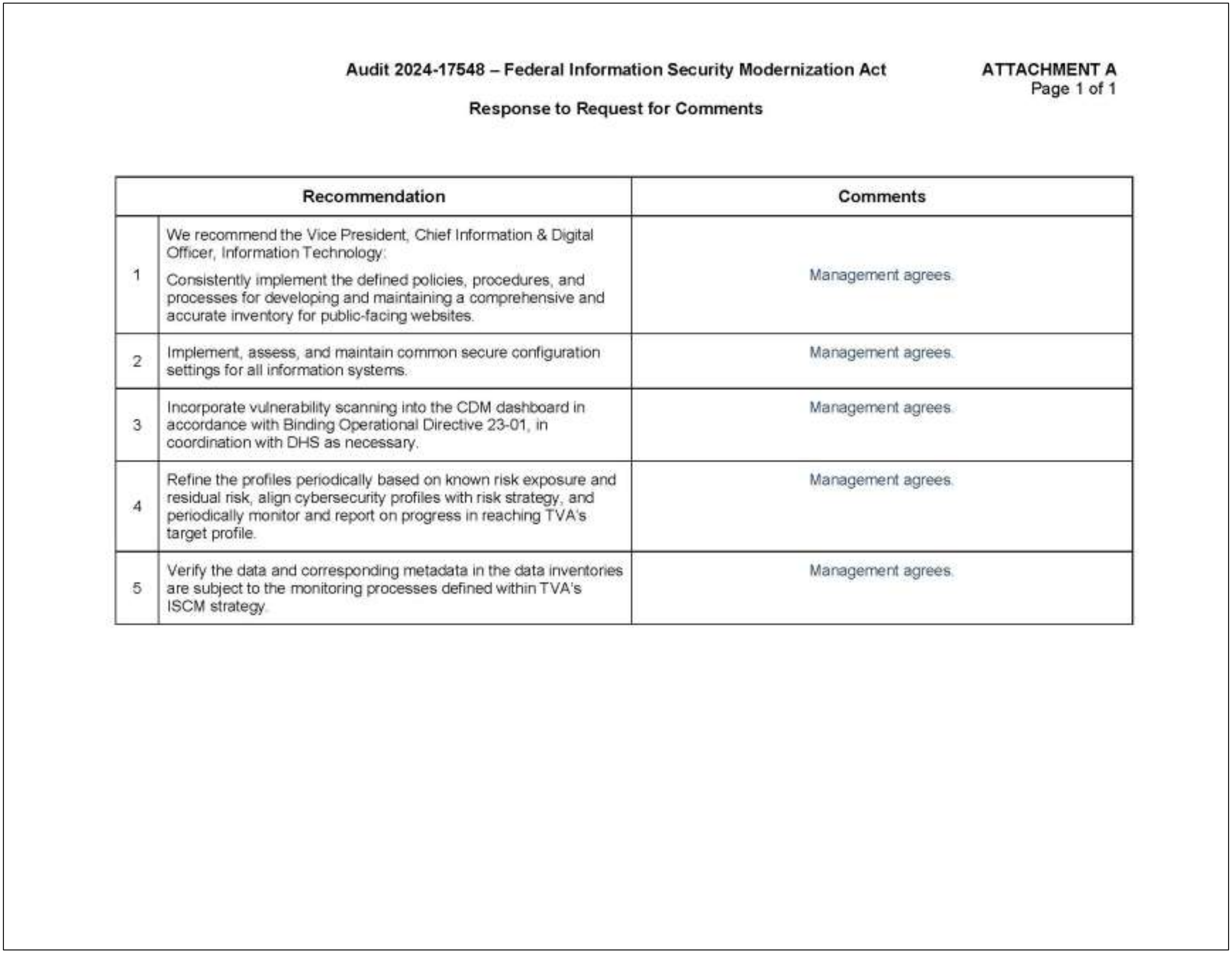
Our response to your request for comments regarding the subject draft report is attached. Please let us know if your staff has any concerns with TVA's comments.

We would like to thank Sarah Huffman, Melissa L. Conforti, and the audit team for their professionalism and cooperation in conducting this audit. If you have any questions, please contact Brett Atkins.

Aaron Melda
Senior Vice President and Chief Information Officer
Information Technology

KCC: BAA
cc (Attachment): Response to Request

Kenneth C. Carnes II
Melissa R. Crane
Joshua Linville
Melissa A. Livesey
Todd E. McCarter
Jessica M. Baker
Jessica A. Anthony
William R. Jr. Brandenburg
Kevin L. Tarver
Francisco J. Soutuyo
Andrew Craig
Tessa C. Luther
Courtney L. Stetzler
Brett A. Atkins
Dustin C. Pate
Gregory G. Jackson
Chris Marsalis
Julie S. Farr
Kacy K. Lemm
Daniel J. Giraldo
Jamie L. King
OIG File No. 2025-17548



Audit 2024-17548 – Federal Information Security Modernization Act

ATTACHMENT A
Page 1 of 1

Response to Request for Comments

	Recommendation	Comments
1	We recommend the Vice President, Chief Information & Digital Officer, Information Technology: Consistently implement the defined policies, procedures, and processes for developing and maintaining a comprehensive and accurate inventory for public-facing websites.	Management agrees.
2	Implement, assess, and maintain common secure configuration settings for all information systems.	Management agrees.
3	Incorporate vulnerability scanning into the CDM dashboard in accordance with Binding Operational Directive 23-01, in coordination with DHS as necessary.	Management agrees.
4	Refine the profiles periodically based on known risk exposure and residual risk, align cybersecurity profiles with risk strategy, and periodically monitor and report on progress in reaching TVA's target profile.	Management agrees.
5	Verify the data and corresponding metadata in the data inventories are subject to the monitoring processes defined within TVA's ISCM strategy.	Management agrees.