Federal Information Security Modernization Act (FISMA) Implementation

CIO-IT Security-04-26

Revision 3

August 10, 2022

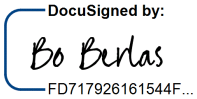
Office of the Chief Information Security Officer

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		Initial Version – June 13, 2016		
1	Henry/ Davis	Initial Guide to document revised process for collecting and reporting FISMA data.	Reflect FISMA Act of 2014 and changes in GSA processes.	All
2	Wilson/ Klemens	Multiple changes throughout the document.	Reformatted document to align with current ISP guide standards. Updated GSA FISMA data collection and reporting processes.	Multiple
		Revision 1 – April 28, 2017		
1	Feliksa/ Klemens	Inclusion of PMC process and information on ratings.	Included PMC self-assessment process and rating levels for PMC and FISMA reporting.	Multiple
		Revision 2 – April 16, 2019		
1	Dean	Formatting and style changes.	Biennial update.	Throughout
		Revision 2 – August 10, 2022		
1	Klemens	Formatting and style changes, updated references.	Scheduled update.	Throughout

Approval

IT Security Procedural Guide: Federal Information Security Modernization Act (FISMA) Implementation CIO-IT Security-04-26, Revision 3, is hereby approved for distribution.



Bo Berlas
GSA Chief Information Security Officer

Contact: GSA Office of the Chief Information Security Officer (OCISO), Policy and Compliance Division (ISP) at ispcompliance@gsa.gov.

Table of Contents

List of Tables

Notes:

- Hyperlinks in running text will be provided if they link to a location within this document (i.e., a different section or an appendix). Hyperlinks will be provided for external sources unless the hyperlink is to a web page or document listed in Section 1.4.
- It may be necessary to copy and paste hyperlinks in this document (Right-Click, Select Copy Hyperlink) directly into a web browser rather than using Ctrl-Click to access them within the document.

1 Introduction

The Federal Information Security Modernization Act (FISMA) of 2014 provides a comprehensive framework for ensuring the effectiveness of information security controls across Federal agencies. FISMA focuses on the program management, implementation, and evaluation aspects of the security of federal information systems. It codifies existing security policies, including Office of Management and Budget (OMB) Circular A-130, Revised, and reiterates security responsibilities provided for in the Computer Security Act of 1987, the Paperwork Reduction Act (PRA) of 1995, and the Clinger-Cohen Act (CCA) of 1996.

FISMA requires the General Services Administration (GSA) to provide quarterly and annual reports on its cybersecurity posture using CyberScope, a Department of Homeland Security (DHS) hosted web application. Specific reporting requirements (e.g., FISMA metrics, Cross Agency Priority [CAP] goals, Risk Management Assessment [RMA] metrics) are contained within the OMB Annual FISMA Report Memorandum and instructions provided by DHS on CyberScope and MAX, the Federal Community website.

1.1 Purpose

The purpose of this guide is to provide GSA Federal employees and contractors with FISMA related responsibilities, as identified in the current GSA Order CIO 2100.1, "GSA Information Technology (IT) Security Policy," specific procedures for completing FISMA tasks.

1.2 Scope

The requirements outlined within this guide apply to all GSA information systems, GSA Federal employees and contractors who have FISMA related responsibilities.

1.3 Policy

Through a combination of FISMA and OMB mandates, GSA is required to collect cybersecurity related data and provide this data to DHS and OMB on a quarterly basis and develop and provide an annual report which also must be provided to the Congressional Committees mentioned in Section 3.4.2.6 and the Government Accountability Office (GAO).

1.4 References

Federal Laws, Standards, Regulations, and Publications:

- Executive Order 14028, "Improving the Nation's Cybersecurity"
- Public Law 104-13, "Paperwork Reduction Act of 1995"
- Public Law 113-283, "Federal Information Security Modernization Act (FISMA) of 2014"
- Public Law 100-235, "Computer Security Act of 1987"
- 40 US Code 11101, "Clinger-Cohen Act of 1996"

- Current Fiscal Year OMB Memorandum, "Fiscal Year xxxx-xxxx Guidance on Federal Information Security and Privacy Management Requirements"
- OMB Circular A-130 (revised), "Managing Federal Information as a Strategic Resource"
- OMB M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information"
- OMB M-19-03, "Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program"
- Cybersecurity Framework (CSF), Version 1.1, "Framework for Improving Critical Infrastructure Cybersecurity"
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations"

GSA Policies, Procedures, Guidance:

- GSA Order CIO 9297.2C, CHGE1, "GSA Information Breach Notification Policy"
- GSA Order CIO 2100.1M, "GSA Information Technology (IT) Security Policy"

The GSA CIO-IT Security Procedural Guides listed below are available on the GSA.gov IT Security Procedural Guides page.

- CIO-IT Security-01-02, "Incident Response (IR)"
- CIO-IT Security-06-30, "Managing Enterprise Cybersecurity Risk"
- CIO-IT Security-09-44, "Plan of Action and Milestones (POA&M)"

2 Roles and Responsibilities

The roles and responsibilities provided in this section have been extracted from GSA CIO 2100.1 and summarized based upon various OMB guidance/memoranda. The roles have direct responsibility to ensure effective implementation of annual FISMA reporting review requirements. Text in brackets [] has been added for clarity where appropriate.

2.1 GSA Administrator

The GSA Administrator is responsible for:

- Ensuring that the CIO, in coordination with the other senior agency officials, reports annually to the GSA Deputy Administrator on the effectiveness of the agency information security program, including the progress of remedial actions.
- Ensuring that the agency has trained personnel to support compliance with information security policies, processes, standards, and guidelines.
- Submitting an annual report to OMB, DHS, GAO, and the appropriate committees. [Including] An official letter, signed by the head of the agency, which provides their comprehensive assessment of the adequacy and effectiveness of their agency's information security policies, procedures, and practices, must be submitted to OMB.

2.2 GSA Chief Information Officer (CIO)

The GSA CIO is responsible for:

- Establishing reporting requirements within GSA to assess GSA's IT security posture, verifying compliance with Federal requirements and approved policies, and identifying agency-wide IT security needs.
- Reporting annually, in coordination with the other senior agency officials, to the GSA Deputy Administrator on the effectiveness of the agency information security program, including progress of remedial actions.
- Approving the CIO and Senior Agency Official for Privacy (SAOP) portions of the annual FISMA report.

2.3 GSA Chief Information Security Officer (CISO)

The GSA CISO is responsible for:

- Supporting the GSA CIO in annual reporting to the GSA Administrator on the effectiveness of the agency information security program, including progress of remedial actions.
- Administering FISMA requirements and coordinating GSA's annual FISMA security program review and Plan of Action and Milestones (POA&M) implementations.
- Preparing and submitting FISMA reports after approval by the Chief Information Officer/Senior Agency Official for Privacy.
- Supporting the GSA CIO in annual FISMA OIG audit process and submission.

2.4 GSA Senior Agency Official for Privacy (GSA's Deputy CIO is designated as the SAOP)

The GSA SAOP is responsible for:

- Reporting periodically to OMB on GSA Privacy Act activities, as required by law and OMB information requests, including the Privacy section for the annual FISMA report.

2.5 Authorizing Official (AO)

The GSA AO is responsible for:

- Ensuring all systems under their purview have a current ATO issued IAW A&A processes defined in GSA CIO-IT Security-06-30.
- Ensuring all incidents involving data breaches which could result in identity theft are coordinated through GSA IT's Office of the Chief Information Security Officer (OCISO) and the GSA Management Incident Response Team (MIRT) using the GSA breach notification plan per OMB M-17-12, "Preparing for and Responding to a Breach of

Personally Identifiable Information", CIO-IT Security-01-02, "Incident Response (IR)", and GSA Order 9297.2C, "GSA Information Breach Notification Policy."

- AOs, System Owners, ISSMs, and ISSOs shall support the collection and reporting of FISMA metrics/measures in data calls by the deadlines established by the OCISO.

2.6 Information Systems Security Manager (ISSM)

The GSA ISSM is responsible for:

- Reporting to the OCISO Director for the systems under their authority.
- AOs, System Owners, ISSMs, and ISSOs shall support the collection and reporting of FISMA metrics/measures in data calls by the deadlines established by the GSA OCISO.
- Working with the ISSO and System Owner to develop, implement, and manage POA&Ms for assigned systems IAW CIO IT Security-09-44, "Plan of Action and Milestones (POA&M)".

2.7 Information System Security Officer (ISSO)

The GSA ISSO is responsible for:

- The ISSO shall maintain accurate system inventories for information systems for which they have responsibility.
- Working with the ISSM and System Owners to develop, implement, and manage POA&Ms for assigned systems IAW CIO-IT Security-09-44, "Plan of Action and Milestones (POA&M)."
- AOs, System Owners, ISSMs, and ISSOs shall support the collection and reporting of FISMA metrics/measures in data calls by the deadlines established by the OCISO.

2.8 System Owners (SO)

The GSA SO is responsible for:

- Reviewing the security controls for their systems and networks annually as part of the FISMA self-assessment, when significant changes are made to the system and network, and at least every three years or via continuous monitoring if the system is in GSA's information security continuous monitoring (ISCM) program
- Working with the ISSO and ISSM to develop, implement, and manage POA&Ms for their respective systems IAW CIO-IT Security-09-44.
- AOs, System Owners, ISSMs, and ISSOs shall support the collection and reporting of FISMA metrics/measures in data calls by the deadlines established by the OCISO.

2.9 Office of the Inspector General (OIG)

The GSA OIG is responsible for:

- Performing annual independent FISMA evaluations.

- Preparing the OIG portion of the annual FISMA report.

3 FISMA Reporting

This section describes the quarterly and annual reporting requirements mandated by FISMA, OMB Memoranda, and instructions provided by OMB and DHS on using CyberScope.

The FISMA metrics have been aligned to the five functions outlined in the NIST CSF: Identify, Protect, Detect, Respond, and Recover. GSA reports its FISMA data aligned with this structure, as required by OMB and DHS reporting processes.

3.1 Reporting Requirements

Each year FISMA reporting requirements may change as well as the format and structure of reporting. Therefore, on an annual basis, OMB releases a memorandum establishing FISMA reporting guidance and deadlines. Additional details are provided via CyberScope and MAX. The OMB memorandum typically addresses the following topics:

- Reporting deadlines/timelines
- Reporting requirements
  - Performance metrics (e.g., CAP goals])
  - Instructions on reporting and report content
  - Details for the development of annual agency FISMA reports (e.g., High Value Asset (HVA) List, RMA data and metrics)
- New or modified requirements/definitions/goals established by OMB

The goals and metrics requested by OMB change from year to year, however typical areas covered are:

- Information Security Continuous Monitoring
- Inventory of Systems and Assets
  - Hardware Asset Management
  - Software Asset Management
- Management of Systems and Assets
  - Vulnerability and Weakness Management
  - Configuration Management
- Identity and Credential Access Management
  - Multi-factor Authentication of Users
  - Use and Management of Passwords
  - Anti-Phishing Defenses
- Protection of Data
  - Encryption of Data in Transit
  - Encryption of Data at Rest
  - Other Defenses

- Resiliency
  - Contingency Planning/Disaster Recovery
  - Incident Handling/Response

3.2 Report Preparation and Data Calls

The GSA OCISO downloads the latest FISMA reporting instructions from the MAX website and based upon these instructions, determines the enterprise and system related data that will be needed to satisfy the quarterly and annual FISMA reporting metrics. The GSA OCISO prepares data collection forms (e.g., spreadsheets, questionnaires, etc.) to assist in gathering the data throughout GSA. These forms are then uploaded to a central location (i.e., Google drive folder) for the appropriate GSA points of contact (POCs) to complete. An announcement of the data collection effort with instructions for completing the data call forms is prepared and sent to the POCs along with reporting deadlines and an OCISO POC for answering any questions.

3.3 Quarterly FISMA Reporting

OMB staff have mandated a quarterly cybersecurity assessment to assess agency-level cybersecurity performance. To meet these requirements, GSA is required to collect FISMA performance metrics data and upload the results of that FISMA data collection into CyberScope.

3.3.1 FISMA Quarterly Metrics Participation

The FISMA quarterly metrics data collection will be completed by the responsible GSA POC who has the necessary knowledge of the GSA's operation and security posture. The quarterly metrics collection may involve multiple persons working in concert with the responsible POC on an as needed basis. For example, system level metrics may involve the ISSM, ISSOs, Program Managers and other knowledgeable POCs. Enterprise level metrics may involve representatives/POCs from GSA OCISO divisions of Security Engineering and Security Operations, members/POCs from various Infrastructure Operations Divisions of Network Operations, Server Services, Active Directory, Client Engineering, Remote Access team, etc. Based on the current implementation of security capabilities, the responsible POC will collect data and complete the data call forms, as necessary. Following the completion of quarterly metrics collection activities, an analysis/review will be performed by the GSA OCISO to ensure they are complete and accurate.

3.3.2 Draft Quarterly Metrics Response Review and Submittal

The GSA OCISO will compile the provided metrics to address the requirements of the FISMA quarterly report. OCISO will follow up with system POCs, as required, to address any questions or gaps in the information provided. The CISO reviews the finalized collected/compiled metrics

for upload into CyberScope. After review and approval by the CISO/CIO, the metrics data and any required documentation will be uploaded into CyberScope by OCISO.

3.3.3 Risk Management Assessment (RMA)

Each year OMB publishes guidance on how they will use the submission of CIO and IG FISMA metrics to compile agency-specific or government-wide RMA scorecards. The scorecard is used as one of the primary mechanisms to manage enterprise cyber risks. The RMA is grouped by the FISMA metrics and Cyber Security Framework domains with associated risk ratings (e.g., Managing Risk, At Risk, High Risk, or Not Applicable) for the individual groups and summarized at the group and overall agency level. Based on the OMB guidance, this data is included in FISMA reporting and is used to guide the remediation of risks based on OMB/DHS guidance/requirements.

3.3.4 Quarterly High Value Assets List Updates

DHS and OMB have mandated quarterly submissions of agency's High Value asset (HVA) list to ensure effective management of cybersecurity risk. To meet these requirements GSA is required to review their agency HVA list on a quarterly basis and provide updates and modifications via the Homeland Security Information Network (HSIN) if there are any changes.

3.4 Annual FISMA Report

The GSA OCISO will coordinate the completion of GSA's annual FISMA report. The OMB-required report consists of multiple parts:

- CIO – Answers to questions and data metrics on GSA's implementation of FISMA CAP measures and base measures.
- SAOP – Answers to questions and data metrics on GSA's progress in implementing a Privacy Program in compliance with the Privacy Act.
- OIG – Answers to questions independently prepared by the OIG regarding GSA's security and privacy programs.

3.4.1 Annual (4th Quarter) Metrics

Annual metrics are the 4th Quarter metrics. The GSA OCISO will coordinate with the responsible GSA POCs who have the necessary knowledge of each system's operation and security posture, however metrics collection may involve multiple persons working in concert with the responsible POC, as needed. For example, system level metrics may involve the ISSM, ISSOs, Program Managers and other knowledgeable POCs. Enterprise level metrics may involve representatives/POCs from OCISO divisions of Security Engineering and Security Operations, members/POCs from various Infrastructure Operations Divisions of Network Operations, Server Services, Active Directory, Client Engineering, Remote Access team, etc. The OCISO will analyze and review data, and coordinate on any follow-up action required.

3.4.2 Final Annual Report Development

3.4.2.1 CIO Report

The GSA OCISO will prepare the CIO portion of the Annual FISMA Report based on the instructions contained in the OMB Annual FISMA Report Memorandum, as well as OMB and DHS instructions provided in CyberScope/MAX.

3.4.2.2 SAOP Report

The Privacy team within OCISO prepares the Privacy portion of the Annual FISMA Report based on the instructions contained in the OMB Annual FISMA Report Memorandum, as well as, OMB and DHS instructions provided in CyberScope/MAX, and instructions in the Annual FISMA Data Call email.

3.4.2.3 OIG Report

FISMA requires federal agencies, including GSA, to have an annual independent evaluation performed of their information security programs and practices and to report the results of the evaluations to the OMB. FISMA states that the independent evaluation is to be performed by the agency OIG or an independent external auditor as determined by the OIG.

The OIG performs an independent evaluation of GSA's information security program and practices. The GSA OIG conducts their independent evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency Quality Standards for Inspection and Evaluation and prepares the OIG portion of the Annual FISMA Report based on the results of the independent evaluation.

The GSA OCISO facilitates OIG audits by providing OIG with enterprise-wide policies and procedures and system level documentation as required to support the review of GSA's security program. The GSA OCISO will coordinate with OIG and provide additional support, as requested.

3.4.2.4 Decision Paper and Administrator's Letter

The OCISO will prepare a draft Decision Paper providing an overview of:

- Current FISMA reporting requirements
- Summary of the CIO, OIG, and SAOP FISMA reviews/reports
- Summary of other FISMA metrics
- Details on the total number of incidents reported to DHS US-CERT
- Description of each major incident
- Progress on the Cross-Agency Priority (CAP) Questions/Metrics
- Recommendation for Administrator Signature

Along with the decision paper, a draft GSA Administrator's transmittal letter to OMB will be prepared.

3.4.2.5 Final Coordination and Approval

A Google drive will be leveraged as a repository to store metrics and associated artifacts. Access to the Google drive will be configured to limit access to only those personnel with an explicit need to know. Once all metrics data has been completed, GSA OCISO, GSA Privacy Office and OIG representatives will upload their specific metrics into CyberScope. They will also upload supporting artifacts/attachments or other documentation, as necessary. Once the CyberScope upload is complete, an OCISO representative will generate and download Portable Document Format (PDF) versions of the CIO, SAOP and OIG reports along with the associated attachments and prepare the final FISMA Package for internal GSA coordination and approval.

The Final Annual FISMA Package, consisting of the following, will be assembled and uploaded into the Salesforce Control Document Tracker (CDT) application:

- CIO Report
- SAOP Report
- OIG Report
- Decision paper
- OMB transmittal letter
- Any required supporting documentation

The Final Annual FISMA package will be coordinated for required approvals via CDT through the following offices:

1) Office of Congressional & Intergovernmental Affairs (OCIA)
2) Office of the General Counsel
3) Office of Administrative Services (OAS) Executive Secretariat Division

All approvals and comments will be tracked via CDT. An OCISO or OAS representative will update and upload new versions of the documents, as review comments dictate. Once the package has been fully coordinated and approved, the decision paper will be signed by the CIO and the OMB transmittal letter will be signed by the GSA Administrator. Copies of the signed decision paper and OMB transmittal letter will be uploaded to CyberScope by an OCISO representative. The Final Annual FISMA Package will be submitted by the CISO to OMB via CyberScope.

3.4.2.6 Congressional Notification

FISMA (section 3544(c)(1)) and the current year OMB Memo require that annual agency reports also be sent to GAO, the Comptroller General, and the following Congressional Committees:

- House Committee on Oversight and Government Reform;
- House Committee on Homeland Security;
- House Committee on Science, Space, and Technology;
- Senate Committee on Homeland Security and Government Affairs;
- Senate Committee on Commerce, Science, and Transportation; and
- The appropriate authorization and appropriations committees of the House and Senate

Similar to the FISMA Annual report submission to OMB, GSA OCISO prepares Transmittal letters for the Congressional Committees mentioned above and seeks Administrator approval and signature through the Salesforce CDT application. Upon notification from OMB, the GSA OCISO coordinates with the GSA Office of Congressional Affairs to forward GSA's FISMA Report to the appropriate Congressional Committees after OMB has reviewed and approved the annual FISMA reports. The GSA OCISO sends the OMB-approved GSA FISMA report to GAO via email.

4 FISMA Self-Assessment

The GSA OCISO will select a number of NIST SP 800-53 controls for the current Fiscal Year's FISMA self-assessment. The control selection is based upon an analysis of the following:

- The previous year's POA&M items and identified weaknesses
- OIG/other Audit findings
- Previous year's security breaches that were caused by a failure in a control implementation
- Volatility of specific security controls and/or key technical controls that have been identified by GSA as needing to be tested on a more frequent basis

The GSA OCISO will prepare and upload the appropriate test cases for assessment of those controls to a central location. An announcement of the data collection effort with instructions for completing the data call forms and self-assessments is prepared and sent to the POCs along with a deadline and the OCISO POC to answer any questions.

Prior to the commencement of the self-assessments, GSA OCISO will conduct FISMA Self-Assessment Training. This training will be provided to personnel responsible for FISMA-related activities and will cover, at a minimum, the following topics:

- Anything new in the current year FISMA requirements
- Identification of systems requiring a FISMA Self-Assessment for the current year
- Guidance on how control testing is to be completed
- Identification of the controls selected for the FISMA Self-Assessment
- Location for uploading FISMA Self-Assessments

The completion of a FISMA self-assessment applies to all systems within GSA. It can be completed by satisfying one of the following:

- Completing the self-assessment test cases
- Submitting a completed Security Assessment Report (SAR)

Note: Systems may only submit a completed SAR if they have received (or will receive) an Authorization to Operate (ATO) within the fiscal year. The SAR must be dated within the current FISMA FY.

The ISSO/POC will coordinate with the ISSM, Program Manager, or others as needed to complete the self-assessments. Completed self-assessments along with any supporting documentation will be uploaded to the appropriate central location identified by the OCISO in the data call email. The OCISO will analyze/review the self-assessments and coordinate with the ISSO, ISSM, or others to ensure the assessments are completed.

Self-assessments must specify an appropriate test result (Fully Satisfied, Partially Satisfied, Not Satisfied, or Not Applicable) and observation. Adequate descriptions of compliance with a given control will allow anyone reviewing the assessment to understand the rationale for the selected implementation and test status. Providing sufficiently detailed descriptions and supporting evidence will accelerate the self-assessment process by reducing review and follow-up coordination.

5 Typical Quarterly and Annual FISMA Schedule

Table 5-1 depicts the typical FISMA Reporting timeline.

Table 5-1. Typical FISMA Reporting Schedule

Milestone	Due Date	Responsibility
FISMA Quarterly Reports HVA Quarterly Report	1. 15th of January 2. 15th of April 3. 15th of July	OCISO/Appropriate POCs
FISMA Self-Assessment Training	Prior to FISMA Self-Assessments	OCISO
Completed FISMA Annual Self-Assessment	31st of August	ISSOs/System POCs
CIO and SAOP Annual Reports completed	September	OCISO/Privacy Office
IG Draft Annual Report completed	September	OIG
GSA FISMA Annual Report Uploaded to Salesforce CDT	Beginning of October	OCISO
GSA FISMA Annual Report is due to OMB	End of October	OCISO
GSA FISMA Annual Report is due to Congress and GAO	1st of March	OCISO/Congressional Affairs

APPENDIX A: Additional Reference Information

Cybersecurity Framework

The five core function definitions for the Cybersecurity Framework are provided below.

- **Identify (ID)**
  Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
  - The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.
- **Protect (PR)**
  Develop and implement appropriate safeguards to ensure delivery of critical services.
  - The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.
- **Detect (DE)**
  Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
  - The Detect Function enables timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.
- **Respond (RS)**
  Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
  - The Respond Function supports the ability to contain the impact of a potential cybersecurity incident. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.
- **Recover (RC)**
  Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.
  - The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications.

IG Maturity Levels

Table A-1 lists summarized definitions of IG Maturity Levels.

Table A-1. IG Maturity Levels

Maturity Level	Definition
Ad Hoc (Level 1)	Policies, procedures, and processes are not formalized; activities are performed in an ad-hoc, reactive manner.
Defined (Level 2)	Policies, procedures, and processes are formalized and defined but are not consistently implemented.
Consistently Implemented (Level 3)	Policies, procedures, and processes are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Managed and Measurable (Level 4)	Quantitative and qualitative measures on the effectiveness of policies, procedures, and processes are collected across the organization and used to assess them and make necessary changes.
Optimized (Level 5)	Policies, procedures, and processes are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.