



NIST Cybersecurity Framework 1.1

EVALUATION SCORING REPORT



DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

Copyright © 2024 Axio Global, Inc. All rights reserved.

Axio is a registered trademark of Axio Global, Inc.



NO WARRANTY: THIS AXIO GLOBAL MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. AXIO GLOBAL MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM THE USE OF THE MATERIAL. AXIO GLOBAL DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Internal use: Permission to reproduce this material and to prepare derivative works from this material for use inside your organization is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

External use: This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other external and/or commercial use. Requests for such permission should be directed to info@axio.com.

Taren Vijayan prepared this report.

NOTE

For further information about Axio, visit <https://axio.com> or email info@axio.com.

About Axio

Cyber risk is the peril of our generation, but organizations struggle to get actionable visibility to their risk. While technology can be part of the solution, it is not a silver bullet. Minimizing and managing cyber risk requires a comprehensive, continuous evaluation across processes, people, balance sheet controls, and technology.

Axio believes that everyone should have the means to solve their unique cyber risk challenges. We are a passionate team of cybersecurity, cyber risk, and business leaders who developed a unique and holistic methodology and software platform to deliver on that belief.

Our innovative and proprietary approach gives companies visibility to their cyber risk and cyber posture in a manner that enables the prioritization of investments to optimize the protection of their business, customers, and employees.

Report Specifications

This report represents the results of an evaluation using the The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). The Framework provides a common organizing structure for multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively today.

This report was created on: **April 04, 2024**

The owner of this assessment is: **Taren Vijayan**

The scope defined for this assessment is: **Taren Vijayan**

The results presented in this report are based on participant input. For the purposes of this assessment, input is considered valid and accurate. The process did not include document reviews, observation of work, or an examination of security controls in place to support the evaluated scenarios.

Table of Contents

NIST Cybersecurity Framework	7
IDENTIFY(ID)	8
ID. AM : Asset Management.....	8
ID. BE : Business Environment.....	8
ID. GV : Governance.....	8
ID. RA : Risk Assessment.....	9
ID. RM : Risk Management Strategy.....	9
ID. SC : Supply Chain Risk Management.....	9
PROTECT(PR)	11
PR. AC : Identity Management, Authentication and Access Control.....	11
PR. AT : Awareness and Training.....	11
PR. DS : Data Security.....	11
PR. IP : Information Protection Processes and Procedures.....	12
PR. MA : Maintenance.....	12
PR. PT : Protective Technology.....	13
DETECT(DE)	14
DE. AE : Anomalies and Events.....	14
DE. CM : Security Continuous Monitoring.....	14
DE. DP : Detection Processes.....	14
RESPOND(RS)	16
RS. RP : Response Planning.....	16
RS. CO : Communications.....	16
RS. AN : Analysis.....	16
RS. MI : Mitigation.....	16
RS. IM : Improvements.....	17
RECOVER(RC)	18
RC. RP : Recovery Planning.....	18
RC. IM : Improvements.....	18
RC. CO : Communications.....	18
Notes	19
Evidence	20
Open Action Items	21

CSF Overview

The Framework for Improving Critical Infrastructure Cybersecurity¹(CSF) was developed by the National Institute of Standards and Technology in collaboration with the private sector. It is a set of industry standards and best practices for managing cybersecurity and privacy risks. It is technology neutral, while also referencing a variety of existing standards, guidelines, and practices that evolve with technology.

CSF is organized into five Functions:

- Identify – Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
- Protect – Develop and implement appropriate safeguards to ensure delivery of critical services.
- Detect – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
- Respond – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
- Recover – 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.

Each Function contains Categories and Subcategories, which are sets of activities to achieve specific cybersecurity outcomes. Each Subcategory has an associated set of Informative References, which are selected sections of standards, guidelines, and practices that illustrate a method to achieve the outcomes associated with the Subcategory.²

1. National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, NIST, April 16, 2018. <https://doi.org/10.6028/NIST.CSWP.04162016>






2. The Informative References for each Subcategory are shown on the Help tab in Axio360 when the Subcategory is selected.

Detailed Assessment Results

Assessment scores are derived from responses entered into Axio360. Each Subcategory includes a four-point answer scale: Fully Implemented (FI), Largely Implemented (LI), Partially Implemented (PI), and Not Implemented (NI). The answers of FI or LI are required for a Subcategory to be considered implemented for scoring. Credit is not applied for answers of PI or NI.

The assessment answer options are explained in more detail in Table 2.1. The answer options are used for Subcategory targets as well as current state. The colors for Fully Implemented and Largely Implemented vary by Function.

Table 2.1: Assessment Answer Scale

	Answer Scale	Implementation Description
	Fully Implemented	Complete
	Largely Implemented	Complete, but with a gap that is considered non-material
	Partially Implemented	Incomplete implementation; one or more material gaps are present
	Not Implemented	Absent; the practice is not performed by the organization or
	Not Targeted	The target and current levels are set to not implemented, indicating that the practice is not selected for implementation
	Level Not Set	A current or target level has not been selected for the practice

Presentation of Results

Scores and targets are shown in the report next to each Subcategory, and scores are also summarized in the form of donut charts and stripe charts. The donut charts and stripe charts show aggregate Subcategory-level results and use colors to give an overall view of Subcategory implementation completeness.

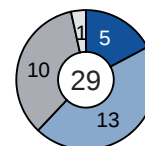
If any evidence or action items were entered in Axio360, they are displayed along with the Subcategory they pertain to or in the appendices at the end of the report, depending on which option was selected.

Interpretation of the donut charts and stripe charts is explained in detail below.

Donut Charts

Donut charts are used in the scoring summary to show the status of achievement of a Function. A circle that is entirely colored in the darkest shade for that Function indicates that all Subcategories in the Function are scored either FI or LI and achievement of the Function is complete.

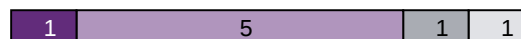
The Identify Function is used in the example. As shown in the center of the donut, there are 29 Subcategories in the Function. Five Subcategories are scored as Fully Implemented, 13 Subcategories are scored as Largely Implemented, 10 Subcategories are scored as Partially Implemented, and 1 Subcategory is scored as Not Implemented.



Stripe Charts

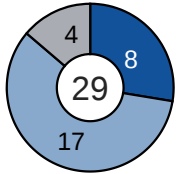
Stripe charts are used in the scoring summary to show the status of achievement by Category within a Function. In the example, in the Protect Function's Data Security Category, 1 Subcategory is scored as Fully Implemented, 5 Subcategories are scored as Largely Implemented, 1 Subcategory is scored as Partially Implemented, and 1 Subcategory is scored as Not Implemented.

PR.DS: Data Security

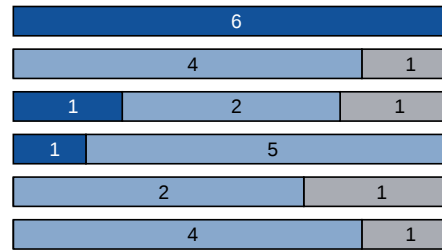


NIST Cybersecurity Framework

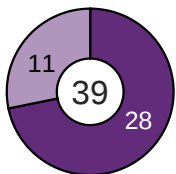
IDENTIFY (ID)



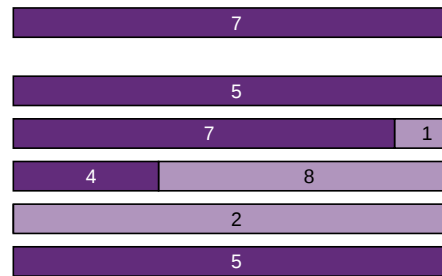
- ID.AM: Asset Management
- ID.BE: Business Environment
- ID.GV: Governance
- ID.RA: Risk Assessment
- ID.RM: Risk Management Strategy
- ID.SC: Supply Chain Risk Management



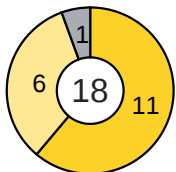
PROTECT (PR)



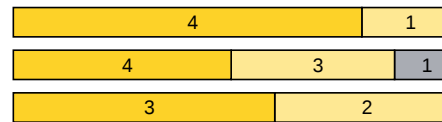
- PR.AC: Identity Management, Authentication and Access Control
- PR.AT: Awareness and Training
- PR.DS: Data Security
- PR.IP: Information Protection Processes and Procedures
- PR.MA: Maintenance
- PR.PT: Protective Technology



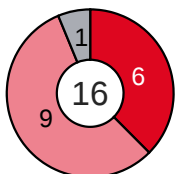
DETECT (DE)



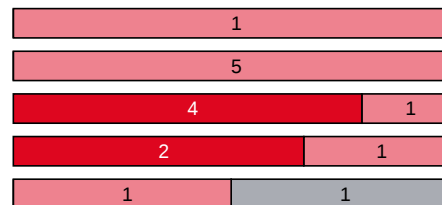
- DE.AE: Anomalies and Events
- DE.CM: Security Continuous Monitoring
- DE.DP: Detection Processes



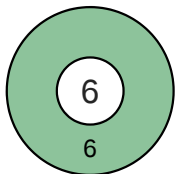
RESPOND (RS)



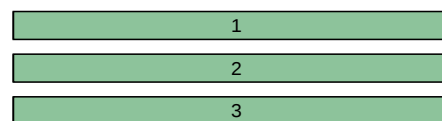
- RS.RP: Response Planning
- RS.CO: Communications
- RS.AN: Analysis
- RS.MI: Mitigation
- RS.IM: Improvements



RECOVER (RC)



- RC.RP: Recovery Planning
- RC.IM: Improvements
- RC.CO: Communications



Fully Implemented

Largely Implemented

Partially Implemented

Not Implemented

No Response

IDENTIFY (ID)

ID.AM: Asset Management

The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.

		Current Level	Target Level
ID.AM-1	Physical devices and systems within the organization are inventoried	FI	
ID.AM-2	Software platforms and applications within the organization are inventoried	FI	
ID.AM-3	Organizational communication and data flows are mapped	FI	
ID.AM-4	External information systems are catalogued	FI	
ID.AM-5	Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	FI	
ID.AM-6	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	FI	

ID.BE: Business Environment

The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.

		Current Level	Target Level
ID.BE-1	The organization's role in the supply chain is identified and communicated	LI	
ID.BE-2	The organization's place in critical infrastructure and its industry sector is identified and communicated	LI	
ID.BE-3	Priorities for organizational mission, objectives, and activities are established and communicated	LI	
ID.BE-4	Dependencies and critical functions for delivery of critical services are established	PI	
ID.BE-5	Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	LI	

ID.GV: Governance

The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.

		Current Level	Target Level
ID.GV-1	Organizational cybersecurity policy is established and communicated	LI	
ID.GV-2	Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	FI	
ID.GV-3	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	PI	

		Current Level	Target Level
ID.GV-4	Governance and risk management processes address cybersecurity risks	LI	

ID.RA: Risk Assessment

The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

		Current Level	Target Level
ID.RA-1	Asset vulnerabilities are identified and documented	LI	
ID.RA-2	Cyber threat intelligence is received from information sharing forums and sources	LI	
ID.RA-3	Threats, both internal and external, are identified and documented	LI	
ID.RA-4	Potential business impacts and likelihoods are identified	FI	
ID.RA-5	Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	LI	
ID.RA-6	Risk responses are identified and prioritized	LI	

ID.RM: Risk Management Strategy

The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

		Current Level	Target Level
ID.RM-1	Risk management processes are established, managed, and agreed to by organizational stakeholders	LI	
ID.RM-2	Organizational risk tolerance is determined and clearly expressed	LI	
ID.RM-3	The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	PI	

ID.SC: Supply Chain Risk Management

The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.

		Current Level	Target Level
ID.SC-1	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	LI	
ID.SC-2	Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	LI	

		Current Level	Target Level
ID.SC-3	Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	LI	
ID.SC-4	Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	PI	
ID.SC-5	Response and recovery planning and testing are conducted with suppliers and third-party providers	LI	

PROTECT (PR)

PR.AC: Identity Management, Authentication and Access Control

Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.

		Current Level	Target Level
PR.AC-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	FI	
PR.AC-2	Physical access to assets is managed and protected	FI	
PR.AC-3	Remote access is managed	FI	
PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	FI	
PR.AC-5	Network integrity is protected (e.g., network segregation, network segmentation)	FI	
PR.AC-6	Identities are proofed and bound to credentials and asserted in interactions	FI	
PR.AC-7	Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	FI	

PR.AT: Awareness and Training

The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.

		Current Level	Target Level
PR.AT-1	All users are informed and trained	FI	
PR.AT-2	Privileged users understand their roles and responsibilities	FI	
PR.AT-3	Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities	FI	
PR.AT-4	Senior executives understand their roles and responsibilities	FI	
PR.AT-5	Physical and cybersecurity personnel understand their roles and responsibilities	FI	

PR.DS: Data Security

Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

		Current Level	Target Level
PR.DS-1	Data-at-rest is protected	FI	
PR.DS-2	Data-in-transit is protected	FI	
PR.DS-3	Assets are formally managed throughout removal, transfers, and disposition	FI	

		Current Level	Target Level
PR.DS-4	Adequate capacity to ensure availability is maintained	FI	
PR.DS-5	Protections against data leaks are implemented	FI	
PR.DS-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity	LI	
PR.DS-7	The development and testing environment(s) are separate from the production environment	FI	
PR.DS-8	Integrity checking mechanisms are used to verify hardware integrity	FI	

PR.IP: Information Protection Processes and Procedures

Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

		Current Level	Target Level
PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	LI	
PR.IP-2	A System Development Life Cycle to manage systems is implemented	LI	
PR.IP-3	Configuration change control processes are in place	LI	
PR.IP-4	Backups of information are conducted, maintained, and tested	FI	
PR.IP-5	Policy and regulations regarding the physical operating environment for organizational assets are met	LI	
PR.IP-6	Data is destroyed according to policy	FI	
PR.IP-7	Protection processes are improved	FI	
PR.IP-8	Effectiveness of protection technologies is shared	LI	
PR.IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	LI	
PR.IP-10	Response and recovery plans are tested	FI	
PR.IP-11	Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	LI	
PR.IP-12	A vulnerability management plan is developed and implemented	LI	

PR.MA: Maintenance

Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.

		Current Level	Target Level
PR.MA-1	Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	LI	

		Current Level	Target Level
PR.MA-2	Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	LI	

PR.PT: Protective Technology

Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

		Current Level	Target Level
PR.PT-1	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	FI	
PR.PT-2	Removable media is protected and its use restricted according to policy	FI	
PR.PT-3	The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	FI	
PR.PT-4	Communications and control networks are protected	FI	
PR.PT-5	Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	FI	

DETECT (DE)

DE.AE: Anomalies and Events

Anomalous activity is detected and the potential impact of events is understood.

		Current Level	Target Level
DE.AE-1	A baseline of network operations and expected data flows for users and systems is established and managed	FI	
DE.AE-2	Detected events are analyzed to understand attack targets and methods	FI	
DE.AE-3	Event data are collected and correlated from multiple sources and sensors	FI	
DE.AE-4	Impact of events is determined	FI	
DE.AE-5	Incident alert thresholds are established	LI	

DE.CM: Security Continuous Monitoring

The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.

		Current Level	Target Level
DE.CM-1	The network is monitored to detect potential cybersecurity events	FI	
DE.CM-2	The physical environment is monitored to detect potential cybersecurity events	PI	
DE.CM-3	Personnel activity is monitored to detect potential cybersecurity events	LI	
DE.CM-4	Malicious code is detected	FI	
DE.CM-5	Unauthorized mobile code is detected	FI	
DE.CM-6	External service provider activity is monitored to detect potential cybersecurity events	LI	
DE.CM-7	Monitoring for unauthorized personnel, connections, devices, and software is performed	LI	
DE.CM-8	Vulnerability scans are performed	FI	

DE.DP: Detection Processes

Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.

		Current Level	Target Level
DE.DP-1	Roles and responsibilities for detection are well defined to ensure accountability	LI	
DE.DP-2	Detection activities comply with all applicable requirements	FI	
DE.DP-3	Detection processes are tested	FI	
DE.DP-4	Event detection information is communicated	FI	

		Current Level	Target Level
DE.DP-5	Detection processes are continuously improved	LI	

RESPOND (RS)

RS.RP: Response Planning

Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.

		Current Level	Target Level
RS.RP-1	Response plan is executed during or after an incident	LI	

RS.CO: Communications

Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).

		Current Level	Target Level
RS.CO-1	Personnel know their roles and order of operations when a response is needed	LI	
RS.CO-2	Incidents are reported consistent with established criteria	LI	
RS.CO-3	Information is shared consistent with response plans	LI	
RS.CO-4	Coordination with stakeholders occurs consistent with response plans	LI	
RS.CO-5	Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	LI	

RS.AN: Analysis

Analysis is conducted to ensure effective response and support recovery activities.

		Current Level	Target Level
RS.AN-1	Notifications from detection systems are investigated	FI	
RS.AN-2	The impact of the incident is understood	FI	
RS.AN-3	Forensics are performed	FI	
RS.AN-4	Incidents are categorized consistent with response plans	LI	
RS.AN-5	Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	FI	

RS.MI: Mitigation

Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.

		Current Level	Target Level
--	--	---------------	--------------

		Current Level	Target Level
RS.MI-1	Incidents are contained	FI	
RS.MI-2	Incidents are mitigated	FI	
RS.MI-3	Newly identified vulnerabilities are mitigated or documented as accepted risks	LI	

RS.IM: Improvements

Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

		Current Level	Target Level
RS.IM-1	Response plans incorporate lessons learned	LI	
RS.IM-2	Response strategies are updated	PI	

RECOVER (RC)

RC.RP: Recovery Planning

Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.

		Current Level	Target Level
RC.RP-1	Recovery plan is executed during or after a cybersecurity incident	LI	

RC.IM: Improvements

Recovery planning and processes are improved by incorporating lessons learned into future activities.

		Current Level	Target Level
RC.IM-1	Recovery plans incorporate lessons learned	LI	
RC.IM-2	Recovery strategies are updated	LI	

RC.CO: Communications

Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).

		Current Level	Target Level
RC.CO-1	Public relations are managed	LI	
RC.CO-2	Reputation is repaired after an incident	LI	
RC.CO-3	Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	LI	

Notes

No notes provided for this assessment.

Evidence

No evidence provided for this assessment.

Open Action Items

No open action items provided for this assessment.