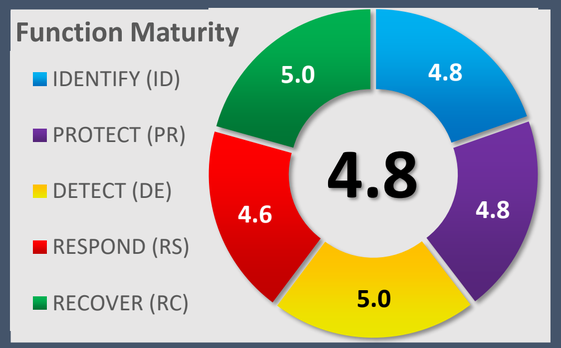
cipher
we secure your business

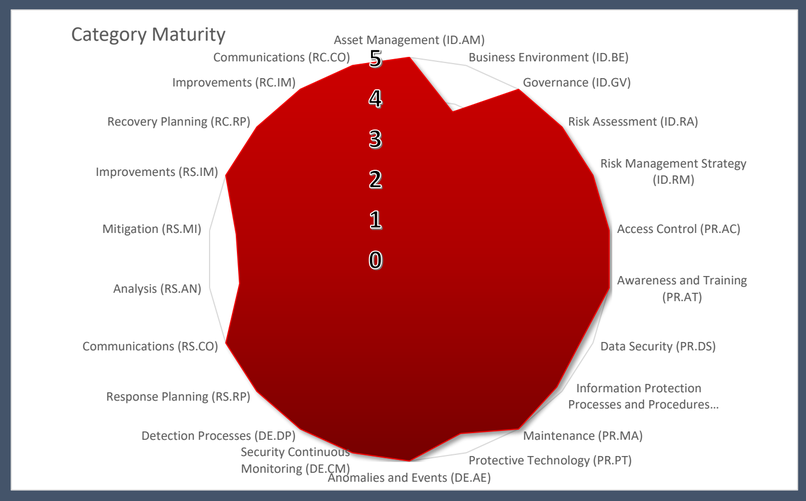
NIST Maturity Dashboard

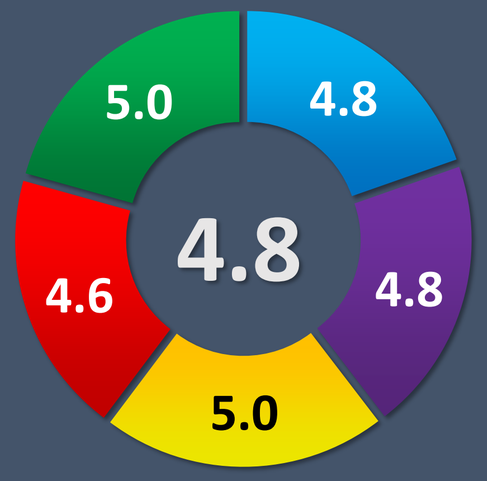
Overall Maturity:	4.8 Managed

Function	Maturity	Rating
IDENTIFY (ID)	4.8	Optimized
PROTECT (PR)	4.8	Optimized
DETECT (DE)	5.0	Optimized
RESPOND (RS)	4.6	Optimized
RECOVER (RC)	5.0	Optimized

	Category	Maturity	Rating
IDENTIFY (ID)	Asset Management (ID.AM)	5.0	Optimized
	Business Environment (ID.BE)	3.8	Managed
	Governance (ID.GV)	5.0	Optimized
	Risk Assessment (ID.RA)	5.0	Optimized
	Risk Management Strategy (ID.RM)	5.0	Optimized
PROTECT (PR)	Access Control (PR.AC)	5.0	Optimized
	Awareness and Training (PR.AT)	5.0	Optimized
	Data Security (PR.DS)	4.7	Optimized
	Information Protection Processes and Procedures (PR.IP)	4.8	Optimized
	Maintenance (PR.MA)	5.0	Optimized
	Protective Technology (PR.PT)	4.5	Optimized
DETECT (DE)	Anomalies and Events (DE.AE)	5.0	Optimized
	Security Continuous Monitoring (DE.CM)	5.0	Optimized
	Detection Processes (DE.DP)	5.0	Optimized
RESPOND (RS)	Response Planning (RS.RP)	5.0	Optimized
	Communications (RS.CO)	5.0	Optimized
	Analysis (RS.AN)	4.3	Managed
	Mitigation (RS.MI)	4.3	Managed
	Improvements (RS.IM)	5.0	Optimized
RECOVER (RC	Recovery Planning (RC.RP)	5.0	Optimized
	Improvements (RC.IM)	5.0	Optimized
	Communications (RC.CO)	5.0	Optimized







Ref	Function	Category	Subcategory	Maturity	Evidence Reviewed
1	IDENTIFY (ID)	Asset Management (ID.AM)	ID.AM-1: Physical devices and systems within the organization are inventoried	5 - Optimized	All physical devices and systems are inventoried
2	IDENTIFY (ID)	Asset Management (ID.AM)	ID.AM-2: Software platforms and applications within the organization are inventoried	5 - Optimized	All software platforms and applications are inventoried
3	IDENTIFY (ID)	Asset Management (ID.AM)	ID.AM-3: Organizational communication and data flows are mapped	5 - Optimized	Organizational communication and data flows are mapped
4	IDENTIFY (ID)	Asset Management (ID.AM)	ID.AM-4: External information systems are catalogued	5 - Optimized	External information systems are cataloged
5	IDENTIFY (ID)	Asset Management (ID.AM)	ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	5 - Optimized	Resources are prioritized
6	IDENTIFY (ID)	Asset Management (ID.AM)	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	5 - Optimized	Roles and responsibilities are established
7	IDENTIFY (ID)	Business Environment (ID.BE)	ID.BE-1: The organization's role in the supply chain is identified and communicated	5 - Optimized	Yes
8	IDENTIFY (ID)	Business Environment (ID.BE)	ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	5 - Optimized	Yes
9	IDENTIFY (ID)	Business Environment (ID.BE)	ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	3 - Defined	Yes
10	IDENTIFY (ID)	Business Environment (ID.BE)	ID.BE-4: Dependencies and critical functions for delivery of critical services are established	3 - Defined	No critical services provided but dependencies are in place.
11	IDENTIFY (ID)	Business Environment (ID.BE)	ID.BE-5: Resilience requirements to support delivery of critical services are established	3 - Defined	No critical services provided but resilliences requirements are in place.
12	IDENTIFY (ID)	Governance (ID.GV)	ID.GV-1: Organizational information security policy is established	5 - Optimized	Yes, an information security policy is in place.
13	IDENTIFY (ID)	Governance (ID.GV)	ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	5 - Optimized	Yes
14	IDENTIFY (ID)	Governance (ID.GV)	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	5 - Optimized	Yes

15	IDENTIFY (ID)	Governance (ID.GV)	ID.GV-4: Governance and risk management processes address cybersecurity risks	5 - Optimized	Yes
16	IDENTIFY (ID)	Risk Assessment (ID.RA)	ID.RA-1: Asset vulnerabilities are identified and documented	5 - Optimized	Yes
17	IDENTIFY (ID)	Risk Assessment (ID.RA)	ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	5 - Optimized	Yes
18	IDENTIFY (ID)	Risk Assessment (ID.RA)	ID.RA-3: Threats, both internal and external, are identified and documented	5 - Optimized	Yes
19	IDENTIFY (ID)	Risk Assessment (ID.RA)	ID.RA-4: Potential business impacts and likelihoods are identified	5 - Optimized	Yes
20	IDENTIFY (ID)	Risk Assessment (ID.RA)	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	5 - Optimized	Yes
21	IDENTIFY (ID)	Risk Assessment (ID.RA)	ID.RA-6: Risk responses are identified and prioritized	5 - Optimized	Yes
22	IDENTIFY (ID)	Risk Management Strategy (ID.RM)	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	5 - Optimized	Yes
23	IDENTIFY (ID)	Risk Management Strategy (ID.RM)	ID.RM-2: Organizational risk tolerance is determined and clearly expressed	5 - Optimized	Yes
24	IDENTIFY (ID)	Risk Management Strategy (ID.RM)	ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	5 - Optimized	Yes
25	PROTECT (PR)	Access Control (PR.AC)	PR.AC-1: Identities and credentials are managed for authorized devices and users	5 - Optimising	Yes
26	PROTECT (PR)	Access Control (PR.AC)	PR.AC-2: Physical access to assets is managed and protected	5 - Optimized	Security cameras are in place for physical security. There is also an alarm system.
27	PROTECT (PR)	Access Control (PR.AC)	PR.AC-3: Remote access is managed	5 - Optimized	Remote access is limited to pre-approved IP addresses.
28	PROTECT (PR)	Access Control (PR.AC)	PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	5 - Optimising	Remote access is limited to pre-approved IP addresses with roles in place for all users.
29	PROTECT (PR)	Access Control (PR.AC)	PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	5 - Optimized	Yes
30	PROTECT (PR)	Awareness and Training (PR.AT)	PR.AT-1: All users are informed and trained	5 - Optimized	Yes - the IT Manager briefs all users of cybersecurity.

31	PROTECT (PR)	Awareness and Training (PR.AT)	PR.AT-2: Privileged users understand roles & responsibilities	5 - Optimized	Yes - the IT Manager briefs all users of cybersecurity.
32	PROTECT (PR)	Awareness and Training (PR.AT)	PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	5 - Optimized	Yes - the IT Manager briefs all users of cybersecurity.
33	PROTECT (PR)	Awareness and Training (PR.AT)	PR.AT-4: Senior executives understand roles & responsibilities	5 - Optimized	Yes - the IT Manager briefs all users of cybersecurity.
34	PROTECT (PR)	Awareness and Training (PR.AT)	PR.AT-5: Physical and information security personnel understand roles & responsibilities	5 - Optimized	Yes - the IT Manager briefs all users of cybersecurity.
35	PROTECT (PR)	Data Security (PR.DS)	PR.DS-1: Data-at-rest is protected	4 - Managed	Data-at-rest is protected by passwords to servers and to databases. Passwords are hashed for users of our web apps. Only PII on servers is first name, last name, and
36	PROTECT (PR)	Data Security (PR.DS)	PR.DS-2: Data-in-transit is protected	4 - Managed	Data-in-transit is protected by passwords to servers and to databases. Passwords are hashed for users of our web apps. Only PII on servers is first name, last name, and
37	PROTECT (PR)	Data Security (PR.DS)	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	5 - Optimized	Yes
38	PROTECT (PR)	Data Security (PR.DS)	PR.DS-4: Adequate capacity to ensure availability is maintained	5 - Optimized	Yes - through virtual servers.
39	PROTECT (PR)	Data Security (PR.DS)	PR.DS-5: Protections against data leaks are implemented	5 - Optimized	Yes
40	PROTECT (PR)	Data Security (PR.DS)	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	5 - Optimized	Yes
41	PROTECT (PR)	Data Security (PR.DS)	PR.DS-7: The development and testing environment(s) are separate from the production environment	5 - Optimized	Yes - all development and testing servers are separate from production servers
42	PROTECT (PR)	Information Protection Processes and Procedures (PR.IP)	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained	5 - Optimized	Yes
43	PROTECT (PR)	Information Protection Processes and Procedures (PR.IP)	PR.IP-2: A System Development Life Cycle to manage systems is implemented	5 - Optimized	Yes
44	PROTECT (PR)	Information Protection Processes and Procedures (PR.IP)	PR.IP-3: Configuration change control processes are in place	3 - Defined	Yes
45	PROTECT (PR)	Information Protection Processes and Procedures (PR.IP)	PR.IP-4: Backups of information are conducted, maintained, and tested periodically	5 - Optimized	Yes - there are three backups of all servers, databases, and internal files. One on the cloud, two physical (one on-site and one off-site)
46	PROTECT (PR)	Information Protection Processes and Procedures (PR.IP)	PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	5 - Optimized	Yes

47	PROTECT (PR)	Information Protection Processes and Procedures (PR.IP)	PR.IP-6: Data is destroyed according to policy	5 - Optimized	Yes
48	PROTECT (PR)	Information Protection Processes and Procedures (PR.IP)	PR.IP-7: Protection processes are continuously improved	5 - Optimized	Yes, annually
49	PROTECT (PR)	Information Protection Processes and Procedures (PR.IP)	PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	5 - Optimized	Yes
50	PROTECT (PR)	Information Protection Processes and Procedures (PR.IP)	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	5 - Optimized	Yes
51	PROTECT (PR)	Information Protection Processes and Procedures (PR.IP)	PR.IP-10: Response and recovery plans are tested	5 - Optimized	Yes, annually
52	PROTECT (PR)	Information Protection Processes and Procedures (PR.IP)	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	5 - Optimized	Yes
53	PROTECT (PR)	Information Protection Processes and Procedures (PR.IP)	PR.IP-12: A vulnerability management plan is developed and implemented	5 - Optimized	Yes
54	PROTECT (PR)	Maintenance (PR.MA)	PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	5 - Optimized	Yes
55	PROTECT (PR)	Maintenance (PR.MA)	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	5 - Optimized	Yes
56	PROTECT (PR)	Protective Technology (PR.PT)	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	4 - Managed	Yes, basic audit/logs
57	PROTECT (PR)	Protective Technology (PR.PT)	PR.PT-2: Removable media is protected and its use restricted according to policy	4 - Managed	Yes, basic restrictions and protections are in place
58	PROTECT (PR)	Protective Technology (PR.PT)	PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	5 - Optimized	Yes
59	PROTECT (PR)	Protective Technology (PR.PT)	PR.PT-4: Communications and control networks are protected	5 - Optimized	Yes
60	DETECT (DE)	Anomalies and Events (DE.AE)	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	5 - Optimized	Yes
61	DETECT (DE)	Anomalies and Events (DE.AE)	DE.AE-2: Detected events are analyzed to understand attack targets and methods	5 - Optimized	Yes

62	DETECT (DE)	Anomalies and Events (DE.AE)	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	5 - Optimized	Yes
63	DETECT (DE)	Anomalies and Events (DE.AE)	DE.AE-4: Impact of events is determined	5 - Optimized	Yes
64	DETECT (DE)	Anomalies and Events (DE.AE)	DE.AE-5: Incident alert thresholds are established	5 - Optimized	Yes
65	DETECT (DE)	Security Continuous Monitoring (DE.CM)	DE.CM-1: The network is monitored to detect potential cybersecurity events	5 - Optimized	Yes
66	DETECT (DE)	Security Continuous Monitoring (DE.CM)	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	5 - Optimized	Yes with security cameras and an alarm system.
67	DETECT (DE)	Security Continuous Monitoring (DE.CM)	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	5 - Optimized	Yes
68	DETECT (DE)	Security Continuous Monitoring (DE.CM)	DE.CM-4: Malicious code is detected	5 - Optimized	Yes
69	DETECT (DE)	Security Continuous Monitoring (DE.CM)	DE.CM-5: Unauthorized mobile code is detected	5 - Optimized	Yes
70	DETECT (DE)	Security Continuous Monitoring (DE.CM)	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	5 - Optimized	Yes
71	DETECT (DE)	Security Continuous Monitoring (DE.CM)	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	5 - Optimized	Yes
72	DETECT (DE)	Security Continuous Monitoring (DE.CM)	DE.CM-8: Vulnerability scans are performed	5 - Optimized	Yes
73	DETECT (DE)	Detection Processes (DE.DP)	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	5 - Optimized	Yes
74	DETECT (DE)	Detection Processes (DE.DP)	DE.DP-2: Detection activities comply with all applicable requirements	5 - Optimized	Yes
75	DETECT (DE)	Detection Processes (DE.DP)	DE.DP-3: Detection processes are tested	5 - Optimized	Yes
76	DETECT (DE)	Detection Processes (DE.DP)	DE.DP-4: Event detection information is communicated to appropriate parties	5 - Optimized	Yes
77	DETECT (DE)	Detection Processes (DE.DP)	DE.DP-5: Detection processes are continuously improved	5 - Optimized	Yes

78	RESPOND (RS)	Response Planning (RS.RP)	RS.RP-1: Response plan is executed during or after an event	5 - Optimized	Yes
79	RESPOND (RS)	Communications (RS.CO)	RS.CO-1: Personnel know their roles and order of operations when a response is needed	5 - Optimized	Yes
80	RESPOND (RS)	Communications (RS.CO)	RS.CO-2: Events are reported consistent with established criteria	5 - Optimized	Yes
81	RESPOND (RS)	Communications (RS.CO)	RS.CO-3: Information is shared consistent with response plans	5 - Optimized	Yes
82	RESPOND (RS)	Communications (RS.CO)	RS.CO-4: Coordination with stakeholders occurs consistent with response plans		N/A
83	RESPOND (RS)	Communications (RS.CO)	RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness		N/A
84	RESPOND (RS)	Analysis (RS.AN)	RS.AN-1: Notifications from detection systems are investigated	5 - Optimized	Yes
85	RESPOND (RS)	Analysis (RS.AN)	RS.AN-2: The impact of the incident is understood	5 - Optimized	Yes
86	RESPOND (RS)	Analysis (RS.AN)	RS.AN-3: Forensics are performed	2 - Managed	Basic forensics are performed
87	RESPOND (RS)	Analysis (RS.AN)	RS.AN-4: Incidents are categorized consistent with response plans	5 - Optimized	Yes
88	RESPOND (RS)	Mitigation (RS.MI)	RS.MI-1: Incidents are contained	4 - Managed	Yes
89	RESPOND (RS)	Mitigation (RS.MI)	RS.MI-2: Incidents are mitigated	4 - Managed	Yes
90	RESPOND (RS)	Mitigation (RS.MI)	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	5 - Optimized	Yes
91	RESPOND (RS)	Improvements (RS.IM)	RS.IM-1: Response plans incorporate lessons learned	5 - Optimized	Yes
92	RESPOND (RS)	Improvements (RS.IM)	RS.IM-2: Response strategies are updated	5 - Optimized	Yes
93	RECOVER (RC)	Recovery Planning (RC.RP)	RC.RP-1: Recovery plan is executed during or after an event	5 - Optimized	Yes

94	RECOVER (RC)	Improvements (RC.IM)	RC.IM-1: Recovery plans incorporate lessons learned	5 - Optimized	Yes
95	RECOVER (RC)	Improvements (RC.IM)	RC.IM-2: Recovery strategies are updated	5 - Optimized	Yes
96	RECOVER (RC)	Communications (RC.CO)	RC.CO-1: Public relations are managed	5 - Optimized	Yes
97	RECOVER (RC)	Communications (RC.CO)	RC.CO-2: Reputation after an event is repaired	5 - Optimized	Yes
98	RECOVER (RC)	Communications (RC.CO)	RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	5 - Optimized	Yes