NIST CSF - Assessor Checklist

Requirement ID	Requirement Name	Requirement Description	In Compliance	References	Issues
ID.AM-1	Hardware inventory	ID.AM-1: Physical devices and systems within the organization are inventoried.	Yes	NIST CSF Assessment	
ID.AM-2	Software and Platform Inventory	ID.AM-2: Software platforms and applications within the organization are inventoried	Yes	NIST CSF Assessment	
ID.AM-3	Data Flows	ID.AM-3: Organizational communication and data flows are mapped	Yes	NIST CSF Assessment	
ID.AM-4	External Information Systems	ID.AM-4: External information systems are catalogued	Yes	NIST CSF Assessment	
ID.AM-5	Resource and Data Prioritization	ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	No	NIST CSF Assessment	Requirement not addressed.
ID.AM-6	Cybersecurity Roles and Responsibilities	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.	Yes	NIST CSF Assessment	
ID.BE-1	Supply Chain Role	ID.BE-1: The organization's role in the supply chain is identified and communicated	Yes	NIST CSF Assessment	
ID.BE-2	Critical Infrastructure Role	ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	Yes	NIST CSF Assessment	
ID.BE-3	Priorities	ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	Yes	NIST CSF Assessment	
ID.BE-4	Dependencies	ID.BE-4: Dependencies and critical functions for delivery of critical services are established	Yes	NIST CSF Assessment	
ID.BE-5	Resilience	ID.BE-5: Resilience requirements to support delivery of critical services are established	Yes	NIST CSF Assessment	
ID.GV-1	Security Policy	ID.GV-1: Organizational information security policy is established.	Yes	NIST CSF Assessment	
ID.GV-2	Coordination	ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	Yes	NIST CSF Assessment	
ID.GV-3	Legal and regulatory requirements	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.	Yes	NIST CSF Assessment	
ID.GV-4	Governance and risk management processes	ID.GV-4: Governance and risk management processes address cybersecurity risks.	Yes	NIST CSF Assessment	
ID.RA-1	Identify vulnerabilities	ID.RA-1: Asset vulnerabilities are identified and documented.	Yes	NIST CSF Assessment	
ID.RA-2	Information sharing forums	ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	Yes	NIST CSF Assessment	
ID.RA-3	Identify threats	ID.RA-3: Threats, both internal and external, are identified and documented.	Yes	NIST CSF Assessment	
ID.RA-4	Identify impacts	ID.RA-4: Potential business impacts and likelihoods are identified.	Yes	NIST CSF Assessment	
ID.RA-5	Determining risk	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.	Yes	NIST CSF Assessment	
ID.RA-6	Risk responses	ID.RA-6: Risk responses are identified and prioritized	Yes	NIST CSF Assessment	
ID.RM-1	Risk management processes	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders.	Yes	NIST CSF Assessment	
ID.RM-2	Organizational risk tolerance	ID.RM-2: Organizational risk tolerance is determined and clearly expressed.	Yes	NIST CSF Assessment	
ID.RM-3	Risk tolerance determination	ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis.	Yes	NIST CSF Assessment	
PR.AC-1	Identities and credentials	PR.AC-1: Identities and credentials are managedÂ for authorized devices and users.	Yes	NIST CSF Assessment	
PR.AC-2	Physical access	PR.AC-2: Physical access to assets is managed and protected.	Yes	NIST CSF Assessment	
PR.AC-3	Remote access	PR.AC-3: Remote access is managed.	Yes	NIST CSF Assessment	
PR.AC-4	Access permissions	PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	Yes	NIST CSF Assessment	
PR.AC-5	Network integrity	PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate.	No	NIST CSF Assessment	Requirement not addressed.
PR.AT-1	Training	PR.AT-1: All users are informed and trained.	No	NIST CSF Assessment	Requirement not addressed.
PR.AT-2	Privileged users	PR.AT-2: Privileged users understand roles & responsibilities.	Yes	NIST CSF Assessment	
PR.AT-3	Third-party stakeholders	PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	Yes	NIST CSF Assessment	
PR.AT-4	Senior executives	PR.AT-4: Senior executives understand roles & responsibilities.	Yes	NIST CSF Assessment	
PR.AT-5	Physical and information security personnel	PR.AT-5: Physical and information security personnel understand roles & responsibilities.	Yes	NIST CSF Assessment	
PR.DS-1	Data-at-rest	PR.DS-1: Data-at-rest is protected	Yes	NIST CSF Assessment	
PR.DS-2	Data-in-transit	PR.DS-2: Data-in-transit is protected.	Yes	NIST CSF Assessment	
PR.DS-3	Asset management	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition.	No	NIST CSF Assessment	Requirement not addressed.
PR.DS-4	Capacity	PR.DS-4: Adequate capacity to ensure availability is maintained	No	NIST CSF Assessment	Requirement not addressed.
PR.DS-5	Data leak protection	PR.DS-5: Protections against data leaks are implemented	No	NIST CSF Assessment	Requirement not addressed.
PR.DS-6	Integrity checking	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	Yes	NIST CSF Assessment	
PR.DS-7	Development & testing environments	PR.DS-7: The development and testing environment(s) are separate from the production environment	No	NIST CSF Assessment	Requirement not addressed.
PR.IP-1	Baseline configurations	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained.	Yes	NIST CSF Assessment	
PR.IP-2	System Development Life Cycle	PR.IP-2: A System Development Life Cycle to manage systems is implemented	Yes	NIST CSF Assessment	
PR.IP-3	Configuration change control	PR.IP-3: Configuration change control processes are in place.	Yes	NIST CSF Assessment	
PR.IP-4	Backups	PR.IP-4: Backups of information are conducted, maintained, and tested periodically	No	NIST CSF Assessment	Requirement not addressed.

PR.IP-5	Physical operating environment	PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met.	Yes	NIST CSF Assessment	
PR.IP-6	Data destruction	PR.IP-6: Data is destroyed according to policy.	No	NIST CSF Assessment	Requirement not addressed.
PR.IP-7	Continuous improvement	PR.IP-7: Protection processes are continuously improved.	No	NIST CSF Assessment	Requirement not addressed.
PR.IP-8	Sharing information	PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties.	Yes	NIST CSF Assessment	
PR.IP-9	Incident Response and Business Continuity Plans	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.	No	NIST CSF Assessment	Supporting controls not fully implemented.
PR.IP-10	Incident response and recovery plan testing	PR.IP-10: Response and recovery plans are tested.	No	NIST CSF Assessment	Supporting controls not fully implemented.
PR.IP-11	Human Resource practices	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	No	NIST CSF Assessment	Requirement not addressed.
PR.IP-12	Vulnerability management	PR.IP-12: A vulnerability management plan is developed and implemented	Yes	NIST CSF Assessment	
PR.MA-1	Maintenance	PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	Yes	NIST CSF Assessment	
PR.MA-2	Remote maintenance	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	Yes	NIST CSF Assessment	
PR.PT-1	Logging & Audit Controls	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	Yes	NIST CSF Assessment	
PR.PT-2	Removable media	PR.PT-2: Removable media is protected and its use restricted according to policy.	Yes	NIST CSF Assessment	
PR.PT-3	Least functionality	PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality.	Yes	NIST CSF Assessment	
PR.PT-4	Communications protection	PR.PT-4: Communications and control networks are protected	Yes	NIST CSF Assessment	
DE.AE-1	Network operations baseline	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.	Yes	NIST CSF Assessment	
DE.AE-2	Analyze events	DE.AE-2: Detected events are analyzed to understand attack targets and methods.	Yes	NIST CSF Assessment	
DE.AE-3	Data aggregation and correlation	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	Yes	NIST CSF Assessment	
DE.AE-4	Event impact	DE.AE-4: Impact of events is determined.	Yes	NIST CSF Assessment	
DE.AE-5	Incident alerts	DE.AE-5: Incident alert thresholds are established.	Yes	NIST CSF Assessment	
DE.CM-1	Network monitoring	DE.CM-1: The network is monitored to detect potential cybersecurity events	Yes	NIST CSF Assessment	
DE.CM-2	Physical environment monitoring	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	Yes	NIST CSF Assessment	
DE.CM-3	Personnel monitoring	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	Yes	NIST CSF Assessment	
DE.CM-4	Malicious code detection	DE.CM-4: Malicious code is detected	No	NIST CSF Assessment	Requirement not addressed.
DE.CM-5	Mobile code	DE.CM-5: Unauthorized mobile code is detected	Yes	NIST CSF Assessment	
DE.CM-6	External service provider monitoring	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events.	Yes	NIST CSF Assessment	
DE.CM-7	Unauthorized activity monitoring	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	Yes	NIST CSF Assessment	
DE.CM-8	Vulnerability scans	DE.CM-8: Vulnerability scans are performed	No	NIST CSF Assessment	Supporting controls not fully implemented.
DE.DP-1	Detection roles and responsibilities	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability.	Yes	NIST CSF Assessment	
DE.DP-2	Detection compliance	DE.DP-2: Detection activities comply with all applicable requirements.	Yes	NIST CSF Assessment	
DE.DP-3	Test detection processes	DE.DP-3: Detection processes are tested	Yes	NIST CSF Assessment	
DE.DP-4	Communicate detections	DE.DP-4: Event detection information is communicated to appropriate parties.	Yes	NIST CSF Assessment	
DE.DP-5	Detection continuous improvement	DE.DP-5: Detection processes are continuously improved.	Yes	NIST CSF Assessment	
RS.RP-1	Execute response plans	RS.RP-1: Response plan is executed during or after an event.	Yes	NIST CSF Assessment	
RS.CO-1	Response roles and responsibilities.	RS.CO-1: Personnel know their roles and order of operations when a response is needed.	Yes	NIST CSF Assessment	
RS.CO-2	Event reporting	RS.CO-2: Events are reported consistent with established criteria.	No	NIST CSF Assessment	Requirement not addressed.
RS.CO-3	Response information sharing	RS.CO-3: Information is shared consistent with response plans.	Yes	NIST CSF Assessment	
RS.CO-4	Response coordination	RS.CO-4: Coordination with stakeholders occurs consistent with response plans	Yes	NIST CSF Assessment	
RS.CO-5	Voluntary information sharing	RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	No	NIST CSF Assessment	Requirement not addressed.
RS.AN-1	Investigate notifications	RS.AN-1: Notifications from detection systems are investigated.Â	Yes	NIST CSF Assessment	
RS.AN-2	Incident impact	RS.AN-2: The impact of the incident is understood.	Yes	NIST CSF Assessment	
RS.AN-3	Perform forensics	RS.AN-3: Forensics are performed.	Yes	NIST CSF Assessment	
RS.AN-4	Categorize incidents	RS.AN-4: Incidents are categorized consistent with response plans.	No	NIST CSF Assessment	Requirement not addressed.
RS.MI-1	Contain incidents	RS.MI-1: Incidents are contained	Yes	NIST CSF Assessment	
RS.MI-2	Mitigate incidents	RS.MI-2: Incidents are mitigated	Yes	NIST CSF Assessment	
RS.MI-3	Newly identified vulnerabilities	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks.	Yes	NIST CSF Assessment	
RS.IM-1	Response lessons learned	RS.IM-1: Response plans incorporate lessons learned.	No	NIST CSF Assessment	Requirement not addressed.
RS.IM-2	Update response strategies	RS.IM-2: Response strategies are updated	Yes	NIST CSF Assessment	
RC.RP-1	Execute recovery plan	RC.RP-1: Recovery plan is executed during or after an event	Yes	NIST CSF Assessment	
RC.IM-1	Recovery lessons learned	RC.IM-1: Recovery plans incorporate lessons learned.	Yes	NIST CSF Assessment	
RC.IM-2	Update recovery strategies	RC.IM-2: Recovery strategies are updated.	Yes	NIST CSF Assessment	
RC.CO-1	Manage public relations	RC.CO-1: Public relations are managed.	Yes	NIST CSF Assessment	
RC.CO-2	Reputation repair	RC.CO-2: Reputation after an event is repaired	Yes	NIST CSF Assessment	
RC.CO-3	Communicate recovery activities	RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	Yes	NIST CSF Assessment	