NIST Cybersecurity Framework

1 Indentify (ID)

Asset Management (ID.AM)

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

Business Environment (ID.BE)

- ID.BE-1: The organization's role in the supply chain is identified and communicated
- ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated
- ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated
- ID.BE-4: Dependencies and critical functions for delivery of critical services are established
- ID.BE-5: Resilience requirements to support delivery of critical services are established

Governance (ID.GV)

- ID.GV-1: Organizational information security policy is established
- ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners
- ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
- ID.GV-4: Governance and risk management processes address cybersecurity risks

Risk Assessment (ID.RA)

- ID.RA-1: Asset vulnerabilities are identified and documented
- ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources
- ID.RA-3: Threats, both internal and external, are identified and documented
- ID.RA-4: Potential business impacts and likelihoods are identified
- ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
- ID.RA-6: Risk responses are identified and prioritized

Risk Management Strategy (ID.RM)

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

2 Protect (PR)

Access Control (PR.AC)

- PR.AC-1: Identities and credentials are managed for authorized devices and users
- PR.AC-2: Physical access to assets is managed and protected
- PR.AC-3: Remote access is managed
- PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties
- PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate

Awareness & Training (PR.AT)

- PR.AT-1: All users are informed and trained
- PR.AT-2: Privileged users understand roles & responsibilities
- PR.AT-3: Third-party stakeholders understand roles & responsibilities
- PR.AT-4: Senior executives understand roles & responsibilities
- PR.AT-5: Physical and information security personnel understand roles & responsibilities

Data Security (PR.DS)

- PR.DS-1: Data-at-rest is protected
- PR.DS-2: Data-in-transit is protected
- PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition
- PR.DS-4: Adequate capacity to ensure availability is maintained
- PR.DS-5: Protections against data leaks are implemented
- PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity
- PR.DS-7: The development and testing environment(s) are separate from the production environment

Info Protection Processes and Procedures (PR.IP)

- PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained
- PR.IP-2: A System Development Life Cycle to manage systems is implemented
- PR.IP-3: Configuration change control processes are in place
- PR.IP-4: Backups of information are conducted, maintained, and tested periodically
- PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met
- PR.IP-6: Data is destroyed according to policy
  - Use SP 800-88r1
- PR.IP-7: Protection processes are continuously improved
- PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties
- PR.IP-9: Response plans (IR and BCP) and recovery plans (IR and DR) are in place and managed
- PR.IP-10: Response and recovery plans are tested
- PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)
- PR.IP-12: A vulnerability management plan is developed and implemented

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

Protective Technology (PR.PT)

- PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
- PR.PT-2: Removable media is protected and its use restricted according to policy
- PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality
- PR.PT-4: Communications and control networks are protected

3 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
- DE.AE-2: Detected events are analyzed to understand attack targets and methods
- DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors
- DE.AE-4: Impact of events is determined
- DE.AE-5: Incident alert thresholds are established

Security Continuous Monitoring (DE.CM)

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

Detection Process (DE.DP)

- DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability
- DE.DP-2: Detection activities comply with all applicable requirements
- DE.DP-3: Detection processes are tested
- DE.DP-4: Event detection information is communicated to appropriate parties
- DE.DP-5: Detection processes are continuously improved

4 Respond (RS)

Analysis (RS.AN)

- RS.AN-1: Notifications from detection systems are investigated
- RS.AN-2: The impact of the incident is understood
- RS.AN-3: Forensics are performed
- RS.AN-4: Incidents are categorized consistent with response plans

Communication (RS.CO)

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

Mitigation (RS.MI)

- RS.MI-1: Incidents are contained
- RS.MI-2: Incidents are mitigated
- RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks

Improvements (RS.IM)

- RS.IM-1: Response plans incorporate lessons learned
- RS.IM-2: Response strategies are updated

Response Planning (RS.RP)

- RS.RP-1: Response plan is executed during or after an event

5 Recover (RC)

Communications (RC.CO)

- RC.CO-1: Public relations are managed
- RC.CO-2: Reputation after an event is repaired
- RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams

Improvements (RC.IM)

- RC.IM-1: Recovery plans incorporate lessons learned
- RC.IM-2: Recovery strategies are updated

Recovery Planning (RC.RP)

- RC.RP-1: Recovery plan is executed during or after an event