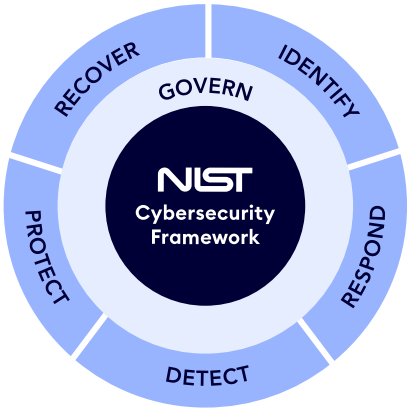
XM Cyber

NIST 2.0
Framework Checklist

The NIST Cybersecurity Framework (CSF) 2.0 is an updated version of NIST Cybersecurity Framework (NIST CSF), which was released in 2023. All versions of NIST aim to grant organizations a flexible set of guidelines to reduce risk and improve security posture. NIST 1.0 was introduced in 2014 and its update, NIST 1.1 was released in 2018, with a stronger focus on risk management in the supply chain, among other issues. Both have been widely adopted and have been instrumental in helping organizations build strong security programs. While it's not mandatory, in some cases, compliance with NIST guidelines may be required by law or regulation, such as in the case of federal agencies, or by contractual obligations with customers or partners

NIST 2.0 was officially released in 2024 and has a newly added Govern function, to ensure the framework keeps pace with the cybersecurity challenges organizations face today. The idea behind this function, which was partially present in previous versions but has now been formalized into its own "step", is to help organizations align their cybersecurity efforts with business objectives. This is accomplished by providing IT and security teams with the tools to design security strategies driven by risk priorities, expand organizational risk awareness and responsibility, and develop compelling justifications for additional program resources.



Steps for Creating & Using a CSF Organizational Profile

1. Scope the organizational profile.
2. Gather needed information.
3. Create the organizational profile.
4. Analyze gops and create an action plan.
5. Implement action plan and update profile.

...Repeat

GOVERNANCE (GV) - New in NIST 2.0

Cybersecurity Governance Structure (GV.ST)

- [ ] Establish governance structure with defined roles and responsibilities
- [ ] Ensure executive-level oversight of cybersecurity program
- [ ] Create governance committees with appropriate representation

Cybersecurity Strategy (GV.SG)

- [ ] Develop comprehensive cybersecurity strategy aligned with business objectives
- [ ] Establish strategic cybersecurity goals and objectives
- [ ] Allocate resources according to strategic priorities

Risk Management Program (GV.RM)

- [ ] Implement enterprise-wide risk management program
- [ ] Define risk appetite and tolerance levels
- [ ] Establish risk assessment methodology

Compliance and Obligations (GV.CO)

- [ ] Identify all applicable regulatory requirements
- [ ] Establish compliance monitoring and reporting processes
- [ ] Maintain documentation of compliance activities

IDENTIFY (ID)

Risk Management Strategy (ID.RM)

- [ ] Establish organizational risk management processes
- [ ] Determine risk tolerance
- [ ] Document risk management strategy

Asset Management (ID.AM)

- [ ] Inventory all physical devices and systems
- [ ] Inventory software platforms and applications
- [ ] Map communication and data flows
- [ ] Catalog external information systems
- [ ] Prioritize resources based on classification and criticality

Business Environment (ID.BE)

- [ ] Identify and prioritize critical business functions
- [ ] Document dependencies and critical functions for service delivery
- [ ] Establish resilience requirements for critical functions

Governance (ID.GV)

- [ ] Establish and communicate cybersecurity policies
- [ ] Align cybersecurity roles and responsibilities
- [ ] Understand legal and regulatory requirements
- [ ] Govern and manage cybersecurity risks

Risk Assessment (ID.RA)

- [ ] Identify and document asset vulnerabilities
- [ ] Collect and evaluate threat intelligence
- [ ] Identify potential business impacts and likelihoods
- [ ] Determine risk responses based on risk factors
- [ ] Update risk assessment processes regularly

Supply Chain Risk Management (ID.SC)

- [ ] Identify, prioritize, and assess suppliers and partners
- [ ] Implement supply chain risk management processes
- [ ] Include cybersecurity requirements in contracts
- [ ] Assess suppliers and third-party partners regularly

PROTECT (PR)

Identity Management & Access Control (PR.AC)

- [ ] Establish identity management for users and devices
- [ ] Manage and protect physical and remote access
- [ ] Implement least privilege and separation of duties
- [ ] Protect network integrity through segregation

Awareness and Training (PR.AT)

- [ ] Conduct cybersecurity awareness training
- [ ] Ensure users understand roles and responsibilities
- [ ] Provide specialized cybersecurity training for specific roles
- [ ] Educate senior executives and third parties on their responsibilities

Data Security (PR.DS)

- [ ] Protect data-at-rest, in-transit, and in-use
- [ ] Implement data security controls (encryption, integrity checking)
- [ ] Implement formal data destruction procedures
- [ ] Ensure adequate capacity for system availability
- [ ] Implement data leak protection mechanisms

Information Protection Processes and Procedures (PR.IP)

- [ ] Create and maintain baseline configurations
- [ ] Implement system development life cycle
- [ ] Establish configuration change control processes
- [ ] Perform regular backups
- [ ] Establish and test incident response and business continuity plans
- [ ] Update response and recovery plans based on lessons learned

Maintenance (PR.MA)

- [ ] Perform and log maintenance activities
- [ ] Approve and control remote maintenance activities

Protective Technology (PR.PT)

- [ ] Implement audit/log records
- [ ] Protect removable media
- [ ] Configure systems according to security principles
- [ ] Implement communications and control network protection

DETECT (DE)

Anomalies and Events (DE.AE)

- [ ] Establish baseline network operations and data flows
- [ ] Analyze detected events to understand attack targets and methods
- [ ] Aggregate and correlate event data from multiple sources
- [ ] Determine event impact and thresholds for action

Security Continuous Monitoring (DE.CM)

- [ ] Monitor networks, physical environment, and personnel activity
- [ ] Perform vulnerability scans
- [ ] Deploy monitoring systems at strategic locations
- [ ] Monitor for unauthorized devices, software, and code
- [ ] Monitor for unauthorized external service provider activity

Detection Processes (DE.DP)

- [ ] Define detection process roles and responsibilities
- [ ] Ensure detection activities comply with requirements
- [ ] Test detection processes regularly
- [ ] Communicate detection information to appropriate parties
- [ ] Continuously improve detection processes

RESPOND (RS)

Response Planning (RS.RP)

- [ ] Execute and maintain response plan during incidents

Communications (RS.CO)

- [ ] Establish personnel for response coordination
- [ ] Report incidents according to established criteria
- [ ] Share incident information consistent with response plans
- [ ] Coordinate with stakeholders according to response plans
- [ ] Share incident information voluntarily with external stakeholders

Analysis (RS.AN)

- [ ] Investigate notifications from detection systems
- [ ] Understand the impact of incidents
- [ ] Perform forensics analysis
- [ ] Categorize incidents according to response plans

Mitigation (RS.MI)

- [ ] Contain incidents to minimize impact
- [ ] Mitigate incidents to prevent expansion
- [ ] Document newly identified vulnerabilities

Improvements (RS.IM)

- [ ] Incorporate lessons learned into response plans
- [ ] Update response strategies based on lessons learned

RECOVER (RC)

Recovery Planning (RC.RP)

- [ ] Execute and maintain recovery plan during incidents

Improvements (RC.IM)

- [ ] Incorporate lessons learned into recovery plans
- [ ] Update recovery strategies based on lessons learned

Communications (RC.CO)

- [ ] Manage public relations during and after incidents
- [ ] Repair reputation after incidents
- [ ] Communicate recovery activities to stakeholders

Communications (RC.CO)

- [ ] Manage public relations during and after incidents
- [ ] Repair reputation after incidents
- [ ] Communicate recovery activities to stakeholders

This checklist provides a comprehensive framework for implementing NIST CSF 2.0 in your organization, although you may need to adapt it to your specific industry, size, and regulatory requirements.

NIST CSF 2.0 is a comprehensive best practice-based approach to managing cyber risk and XM Cyber makes it easy and effective to communicate alignment to stakeholders and auditors.

Want to find out how XM Cyber can help your organization get started with NIST 2?

Get a demo today!