CYBERGEN®

NIST 2.0 FRAMEWORK CHECKLIST

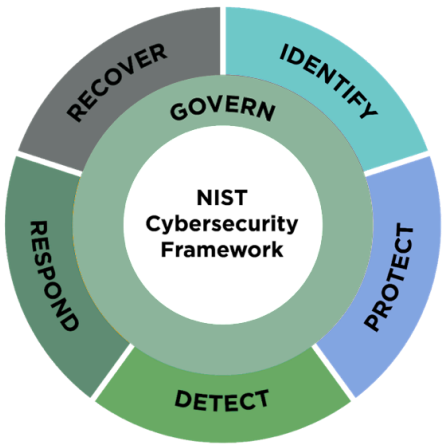
NIST

CYBERGEN®

The NIST Cybersecurity Framework (CSF) 2.0, released in 2024, is the latest update to a widely adopted framework originally introduced in 2014. Its purpose, consistent across all versions, is to provide organisations with flexible guidelines to reduce cyber risk and improve their overall security posture.

The original version (1.0) focused on foundational security practices, while the 2018 update (1.1) expanded on areas such as supply chain risk management. Although the framework is not legally mandatory for most organisations, compliance may be required in certain cases, such as for U.S. federal agencies, or through contractual obligations with customers or partners. Across industries, NIST has proven to be an essential reference for building structured, effective cybersecurity programs.

CSF 2.0 introduces a key enhancement: the addition of a sixth core function, Govern, which reflects the growing need to align cybersecurity with broader business strategy. While governance concepts were touched on in previous versions, this new function formalises the role of leadership and oversight in managing cyber risk. Its goal is to help organisations design security programs that are driven by risk priorities, increase accountability across departments, and equip IT and security teams to better advocate for resources and strategic support. By doing so, CSF 2.0 addresses modern cybersecurity challenges with a more integrated, enterprise-wide approach.



Steps for Creating & Using a CSF Organisational Profile

1. Scope the organisational profile.
2. Gather needed information.
3. Create the organisational profile.
4. Analyse gaps and create an action plan.
5. Implement action plan and update profile.

. . . Repeat

GOVERNANCE - New in NIST 2.0

Cybersecurity Governance Structure

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

Cybersecurity Strategy

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

Risk Management Program

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

Compliance and Obligations

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

IDENTIFY

Risk Management Strategy

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

Asset Management

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

Business Environment

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

Governance

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

Risk Assessment

- [ ] 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

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

PROTECT

Identity Management & Access Control

- [ ] 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

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

Data Security

- [ ] 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

- [ ] 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

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

Protective Technology

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

DETECT

Anomalies and Events

- [ ] 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

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

Detection Processes

- [ ] 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

Response Planning

- [ ] Execute and maintain response plan during incidents
- [ ] Ensure planning for Information Security controls

Communications

- [ ] 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

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

Mitigation

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

Improvements

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

RECOVER

Recovery Planning

- [ ] Execute and maintain recovery plan during incidents

Improvements

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

Communications

- [ ] 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 organisation, though it should be tailored to fit your specific industry, size, and regulatory requirements. NIST CSF 2.0 offers a best practice-based approach to managing cyber risk, and Cybergen makes it easier to demonstrate compliance and communicate your security posture to stakeholders and auditors.

Want to find out how Cybergen can help your organisation get started with NIST CSF 2.0? Get in touch with us today for a consultation.

Cybergen is a UK-based global cybersecurity consultancy helping organisations build resilience against today's evolving threats. With a focus on strategy, compliance, and hands-on technical expertise, Cybergen works closely with businesses to identify risks, strengthen defences, and respond effectively to incidents. Whether supporting internal teams or acting as a trusted external partner, Cybergen delivers tailored solutions that align with each client's industry, infrastructure, and regulatory environment. Our mission is to make enterprise-grade cybersecurity accessible, actionable, and aligned with business goals, so that security becomes an enabler, not a barrier, to growth.

www.cybergensecurity.co.uk **sales@cybergensecurity.co.uk** **+44 (0) 1865 950 828**

© 2025 Cybergen | All Rights Reserved