

What Is the NIST Cybersecurity Framework?

The NIST Cybersecurity Framework is a set of guidelines designed to help organizations secure their critical infrastructure and improve their ability to identify, prevent, detect, respond and recover from cyber incidents.

Today, it is embraced by many to help manage their organization's cybersecurity risks and provide a common language to leverage between technical and non-technical teams.



Identify

Protect

Detect

Respond

Recover

- Asset Inventory and Management
- Remote Monitoring and Management (RMM)
- Information Security Policy
- Governance, Risk Management and Compliance
- Vulnerability Management

- Security Awareness Training
- Antivirus (AV)
- Firewall(s)
- Multi-Factor Authentication (MFA)
- DNS Filtering
- Email Filtering
- Patch Management

- Threat Hunting
- Endpoint Detection and Response (EDR)
- Network Detection and Response (NDR)
- Security Information and Event Management (SIEM)
- Log Analysis
- Network Behavior Analysis
- Vulnerability Scanning

- Endpoint Detection and Response (EDR)
- Network Detection and Response (NDR)
- Global Threat Intelligence Feed
- Cyber Response Team/Personnel
- Incident Response Plan

- Backup and Disaster Recovery (BDR)
- Disaster Recovery Plan
- Business Continuity Plan
- Cyber Insurance

Identify

Protect

Detect

Respond

Recover



-
-
-
-
-

-
-
-
-
-

-
-
-
-
-

-
-
-
-
-

-
-
-
-
-