
Secure Programs:
Cyber Security Frameworks &
Methodologies

What is a Cyber Security Framework?

A cybersecurity framework is a set of guidelines, best practices, and standards that organizations can use to manage and reduce their cybersecurity risks.

Why do businesses and organizations need a Cybersecurity Framework?

Having a cybersecurity framework is important because it helps organizations identify and prioritize their cybersecurity risks, implement controls to mitigate those risks, and continuously monitor and improve their cybersecurity posture.

What is NIST CSF?

This is the National Institute of Standards and Technology Cybersecurity Framework .

It is a set of guidelines, standards, and best practices developed by the National Institute of Standards and Technology (NIST) to help organizations manage and reduce their cybersecurity risk.

What does NIST CSF do for non-profit organizations?

The NIST CSF provides a common language and framework for organizations to manage cybersecurity risk across their entire enterprise, including people, processes, and technology.

It is designed to be flexible and adaptable to any organization, regardless of its size, industry, or sector.

The NIST Five: Understanding the Core Functions of the NIST Framework.

What are the core functions of the NIST CSF Framework?

- The framework is organized into five core functions: Identify, Protect, Detect, Respond, and Recover.
- These functions help organizations to develop and implement a cybersecurity program that is tailored to their specific needs and risk profile.
- The NIST CSF is widely used by organizations in the public and private sectors as a tool to improve their cybersecurity posture and reduce the risk of cyber attacks.

IDENTIFY

This function involves understanding and managing cybersecurity risks to systems, assets, data, and capabilities.

It includes:

- developing an inventory of all the assets that need to be protected
- understanding the potential threats and vulnerabilities
- assessing the impact of a cybersecurity incident on the organization's mission, reputation, and finances

IDENTIFY

The Identify function also involves establishing policies and procedures to manage cybersecurity risk, and ensuring that all stakeholders are aware of their roles and responsibilities.

PROTECT

This function involves developing and implementing safeguards to protect against cyber threats.

It includes:

- implementing access controls
- developing secure configurations for hardware and software
- implementing data security and encryption
- providing awareness and training programs for employees

PROTECT

The Protect function also involves managing third-party risks, such as those posed by vendors and partners.

DETECT

This function involves developing and implementing systems to detect cybersecurity events.
It includes:

- Monitoring networks and systems for signs of compromise
- Implementing threat intelligence programs
- Establishing procedures for incident reporting and response

DETECT

The Detect function also involves conducting regular security testing and vulnerability assessments.

RESPOND

This function involves developing and implementing procedures to respond to a cybersecurity incident.

It includes:

- Developing and testing incident response plans
- Establishing procedures for communicating with stakeholders
- Containing and eradicating the incident

RESPOND

The “response” function also involves conducting post-incident analysis and implementing measures to prevent similar incidents from occurring in the future.

RECOVER

This function involves developing and implementing procedures to recover from a cybersecurity incident.

It includes:

- Restoring systems and data
- conducting lessons learned exercises
- Implementing measures to improve the organization's overall cybersecurity posture

RECOVER

The Recover function also involves engaging with stakeholders to ensure that they are informed of the incident and its impact on the organization.

NIST 800-171: The Cybersecurity Framework for Your Growing Non-Profit Organization

What is NIST 800-171?

- A cybersecurity framework that provides guidelines for protecting controlled unclassified information (CUI)
- This framework outlines a set of security controls that organizations can use to secure CUI and mitigate cybersecurity risks
- Non-profit organizations such as yours can use the NIST 800-171 framework to implement effective cybersecurity controls that align with their mission, goals, and objectives.

How will NIST 800-171 work for your organization?

When building secure platforms and programs for non-profit organizations such as yours, we can effectively use the NIST 800-171 framework to implement effective cybersecurity controls that align with your mission, goals, and objectives.

What is NIST 800-171 comprised of?

NIST 800-171 are organized into 14 categories of security requirements

Access Control
Awareness and Training
Audit and Accountability
Configuration Management
Identification and Authentication
Incident Response
Maintenance
Media Protection
Personal Security
Physical Protection
Risk Assessment
Security Assessment
Systems and Communications Protection
Systems and Information Integrity

ACCESS CONTROL

Contains guidelines that limit access to information systems, applications, and data to authorized personnel only.

This includes requirements such as implementing multi-factor authentication, enforcing password policies, and maintaining an access control list.

AWARENESS TRAINING

Contains controls that ensure personnel are trained and aware of their security responsibilities.

This includes requirements such as providing security awareness training, reminding users to be vigilant when handling sensitive information, and conducting periodic security refresher training.

AUDIT & ACCOUNTABILITY

Contain controls ensures that security-related events are logged, monitored, and analyzed.

This includes requirements such as maintaining an audit trail, performing regular audits of information systems and data, and analyzing security-related data to identify potential security incidents.

CONFIGURATION MANAGEMENT

Contains controls that that ensure that information systems are configured and managed to protect against security threats.

This includes requirements such as implementing configuration baselines, managing system changes, and maintaining an up-to-date inventory of hardware and software limit access to information systems, applications, and data to authorized personnel only.

IDENTIFICATION & AUTHENTICATION

Contains guidelines that ensure that individuals are properly identified and authenticated before accessing information systems, applications or data.

This includes requirements such as implementing multi-factor authentication, enforcing password policies, and monitoring and managing user accounts.

INCIDENT RESPONSE

Includes guidelines that ensure that security incidents are detected, reported, and responded to in a timely and effective manner.

This includes requirements such as maintaining maintaining an incident response plan, conducting periodic exercises and drills, and implementing incident reporting procedures.

MAINTENANCE

Contains guidelines that ensure that information systems are maintained and updated to protect against security threats.

This includes requirements such as maintaining up-to-date patches and security updates, monitoring system health, and ensuring the availability and integrity of system backups.

MEDIA PROTECTION

Contains controls that ensure that information stored on physical media is protected against unauthorized access, theft, or damage.

This includes requirements such as encrypting sensitive data, securely disposing of media when no longer needed, and ensuring the physical security of media storage facilities.

PERSONAL SECURITY

Includes controls that ensure that personnel are trustworthy and have appropriate security clearances and access levels.

This includes requirements such as conducting background checks, implementing a security awareness program, and monitoring personnel for security violations.

PHYSICAL PROTECTION

Contains guidelines that ensure that physical assets such as equipment and facilities are protected against unauthorized access, theft, or damage

This includes requirements such as implementing access controls, maintaining secure facilities, and monitoring physical access to sensitive areas.

RISK ASSESSMENT

Contains guidelines that ensure that security risks are identified and assessed, and that appropriate mitigation strategies are implemented.

This includes requirements such as conducting regular risk assessments, developing a risk management plan, and implementing controls to mitigate identified risks.

SECURITY ASSESSMENT

Includes controls that ensure that information systems and applications are periodically assessed to identify potential vulnerabilities and weaknesses

This includes requirements such as conducting periodic security assessments, testing information systems for vulnerabilities, and implementing remediation plans to address identified weaknesses .

SYSTEM & COMMUNICATIONS PROTECTION

Contains controls that ensure that information systems and communications networks are protected against unauthorized access, theft, or damage.

This includes requirements such as implementing firewalls and intrusion detection systems, encrypting data in transit, and securing wireless networks.

SYSTEM & INFORMATION INTEGRITY

Contains guidelines that ensure that that information systems and applications are protected against unauthorized access, modification, or destruction.

This includes requirements such as conducting regular risk assessments, developing a risk management plan, and implementing controls to mitigate identified risks.

Thank you for your time!

Presentation Designers: Jane Pierre and Mishelly Sandoval

Contributors: Lucas Higgs and Elizabeth Bond

Research: Frederick Asante, Shemar Brown, Tianna Green
Jonathan Henao and Aaron Kaah