SECHARD
Complete Zero Trust

# NIST Cybersecurity Framework

## (5 Core Functions)

www.sechard.com

# Components of the NIST Cybersecurity Framework

SECHARD
Complete Zero Trust

The NIST Cybersecurity Framework is a set of guidelines and best practices designed to help organizations improve their cybersecurity posture. The Framework consists of five core functions that organizations should focus on to manage and reduce cybersecurity risk. In this post, we will delve into each core function and their subcategories, along with example scenarios for each function.

Components of the NIST Cybersecurity Framework. The Framework consists of five core functions that organizations should focus on:

- Identify: This involves identifying assets and data that require protection and assessing their associated risks.
- Protect: This involves implementing safeguards to protect assets and data from potential threats.
- Detect: This involves detecting potential cybersecurity events that could impact the organization.
- Respond: This involves having a plan to respond to potential cybersecurity events and mitigate any potential damage.
- Recover: This involves having a plan to recover from cybersecurity events and return to normal operations.

# Identify

SECHARD
Complete Zero Trust

The first core function of the NIST Cybersecurity Framework is to identify. This involves identifying and understanding assets and data that require protection and assessing their associated risks. The Identify function is divided into three subcategories: Asset Management, Business Environment, and Governance.

Asset Management involves identifying and managing assets essential to an organization's operations, such as hardware, software, and data. This subcategory includes identifying the location of assets, understanding the value and importance of assets, and establishing and maintaining an inventory of assets. Organizations should also classify assets based on their criticality and confidentiality and develop a plan to protect them.

The Business Environment subcategory involves understanding the internal and external factors influencing an organization's cybersecurity risk management strategy. This includes understanding the organization's business objectives, legal and regulatory requirements, risk tolerance, and organizational structure. Organizations should also identify the stakeholders involved in cybersecurity risk management and ensure they are engaged and informed.

Governance involves establishing and maintaining a framework for managing cybersecurity risk. This includes developing policies and procedures, assigning roles and responsibilities, and ensuring clear accountability for cybersecurity risk management. Organizations should also establish a process for ongoing risk assessment and ensure that cybersecurity risk management is integrated into their overall risk management strategy.

## Example Scenario:

A financial institution has identified its critical assets as its customer data and its financial systems. The Asset Management subcategory would involve classifying these assets based on their criticality and confidentiality, and developing a plan to protect them. The Business Environment subcategory would involve understanding the legal and regulatory requirements that apply to the institution, as well as the risk tolerance of its stakeholders. The Governance subcategory would involve developing policies and procedures for managing cybersecurity risk, assigning roles and responsibilities, and ensuring ongoing risk assessment.

# Protect

SECHARD
Complete Zero Trust

The second core function of the NIST Cybersecurity Framework is to protect. This involves implementing safeguards to protect assets and data from potential threats. The Protect function comprises five subcategories: Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, and Maintenance.

Access Control ensures only authorized individuals can access an organization's assets and data. This includes implementing password policies, two-factor authentication, and role-based access controls. Organizations should also limit access to assets and data to those who need it and implement controls to prevent unauthorized access.

Awareness and Training ensure that employees and stakeholders know the organization's cybersecurity policies and procedures and are trained to follow them. This includes providing training on identifying and reporting potential cybersecurity threats and protecting sensitive information.

Data Security involves protecting data from unauthorized access, disclosure, and modification. This includes implementing encryption, firewalls, and intrusion detection systems. Organizations should also develop and implement policies and procedures for data backup and recovery.

Information Protection Processes and Procedures involve establishing and maintaining policies and procedures for protecting information throughout its lifecycle. This includes data retention policies, secure data disposal, and incident response. Organizations should also develop and implement procedures for incident response and recovery.

Maintenance involves implementing procedures for the secure configuration, testing, and maintenance of hardware, software, and firmware. This includes implementing patches and updates in a timely manner and ensuring that all systems and devices are secure and up-to-date.

## Example Scenario:

A healthcare provider wants to protect its patient data. The Access Control subcategory would involve implementing password policies, two-factor authentication, and role-based access controls to ensure that only authorized individuals have access to the data. The Awareness and Training subcategory would involve providing training to employees on how to identify and report potential cybersecurity threats and how to protect sensitive patient information. The Data Security subcategory would involve implementing encryption and firewalls to protect patient data from unauthorized access. The Information Protection Processes and Procedures subcategory would involve establishing policies and procedures for data retention, secure disposal of data, and incident response. Finally, the Maintenance subcategory would involve implementing procedures for the secure configuration, testing, and maintenance of hardware, software, and firmware to ensure that all systems and devices are secure and up-to-date.

# Detect

SECHARD
Complete Zero Trust

The third core function of the NIST Cybersecurity Framework is to detect. This involves detecting any potential cybersecurity events that could impact the organization. The Detect function is divided into two subcategories: Anomalies and Events, and Continuous Monitoring.

Anomalies and Events involves identifying and monitoring potential cybersecurity events, such as malware infections and unauthorized access attempts. Organizations should also develop and implement procedures for reporting and responding to potential cybersecurity events.

Continuous Monitoring involves continuously monitoring assets and data for potential cybersecurity threats. This includes implementing intrusion detection and prevention systems, as well as performing regular vulnerability scans and penetration testing.

## Example Scenario:

A retail company wants to detect potential cybersecurity threats to its point-of-sale systems. The Anomalies and Events subcategory would involve identifying and monitoring potential cybersecurity events, such as malware infections and unauthorized access attempts to the point-of-sale systems.

The Continuous Monitoring subcategory would involve implementing intrusion detection and prevention systems and performing regular vulnerability scans and penetration testing to monitor the point-of-sale systems for potential cybersecurity threats continuously.

# Respond

SECHARD
Complete Zero Trust

The fourth core function of the NIST Cybersecurity Framework is to respond. This involves having a plan in place to respond to potential cybersecurity events and mitigate any potential damage. The Respond function is divided into three subcategories: Response Planning, Communications, and Analysis.

Response Planning involves developing and implementing a plan to respond to potential cybersecurity events. This includes establishing roles and responsibilities for incident response, identifying potential cybersecurity events, and developing procedures for responding to those events.

Communications involves establishing and maintaining communication channels for incident response. This includes establishing a reporting process for potential cybersecurity events and ensuring that all stakeholders are informed of potential cybersecurity threats and the status of incident response efforts.

Analysis involves analyzing potential cybersecurity events and assessing the impact of those events on the organization. This includes performing root cause analysis to identify the cause of the event and developing a plan to prevent similar events from occurring in the future.

## Example Scenario:

A manufacturing company experiences a ransomware attack. The Response Planning subcategory would involve developing and implementing a plan to respond to the ransomware attack, including identifying roles and responsibilities for incident response and developing response procedures. The Communications subcategory would involve establishing communication channels for incident response and ensuring that all stakeholders know the attack and the status of incident response efforts.

The Analysis subcategory would involve analyzing the ransomware attack and assessing the impact on the organization, performing root cause analysis to identify the cause of the attack, and developing a plan to prevent similar attacks from occurring in the future.

# Recover

SECHARD
Complete Zero Trust

The fifth and final core function of the NIST Cybersecurity Framework is to recover. This involves having a plan to recover from cybersecurity events and return to normal operations. The Recover function is divided into two subcategories: Recovery Planning and Improvements.

Recovery Planning involves developing and implementing a plan to recover from potential cybersecurity events. This includes developing procedures for restoring assets and data and testing those procedures to ensure they are effective.

Improvements involve reviewing and improving the organization's cybersecurity posture based on the lessons learned from cybersecurity events. This includes identifying and addressing weaknesses in the organization's cybersecurity infrastructure and processes and implementing improvements to prevent similar cybersecurity events from occurring in the future.

## Example Scenario:

A financial institution experiences a distributed denial-of-service (DDoS) attack that disrupts its online banking services. The Recovery Planning subcategory would involve developing and implementing a plan to recover from the DDoS attack, including developing procedures for restoring online banking services and testing those procedures to ensure they are effective.

The Improvements subcategory would involve reviewing and improving the financial institution's cybersecurity posture based on the lessons learned from the DDoS attack, such as strengthening its defenses against DDoS attacks and implementing additional redundancy measures to prevent similar disruptions to online banking services in the future.

SECHARD
Complete Zero Trust

# Implementing the NIST Cybersecurity Framework can seem daunting, but with the right software, it can be a manageable and effective way to manage cybersecurity risks. This is where Sechard comes in.

# SecHard Zero Trust Orchestrator

SECHARD
Complete Zero Trust

SecHard Zero Trust Orchestrator is a multi-module software for implementing Zero Trust Architecture that can help you implement the NIST Cybersecurity Framework. Our software is designed to facilitate compliance with the guidelines and best practices of the framework and provides a comprehensive set of tools for managing cybersecurity risks.

The SecHard Zero Trust Orchestrator modules, such as Security Hardening, Privileged Access Manager, Asset Manager, Vulnerability Manager, Risk Manager, Device Manager, Performance Monitor, Key Manager, TACACS+ Server, and Syslog Server, work together seamlessly to provide a comprehensive set of tools that facilitate compliance with the NIST Cybersecurity Framework.

With SecHard Zero Trust Orchestrator, you can easily implement the five core functions of the NIST Cybersecurity Framework. Our software provides a centralized platform for identifying potential cybersecurity risks, implementing safeguards, detecting potential cyber threats, responding to cybersecurity incidents, and recovering from cybersecurity incidents.

Contact us today to learn more about how Sechard can help you achieve your cybersecurity goals!

**sales@sechard.com**