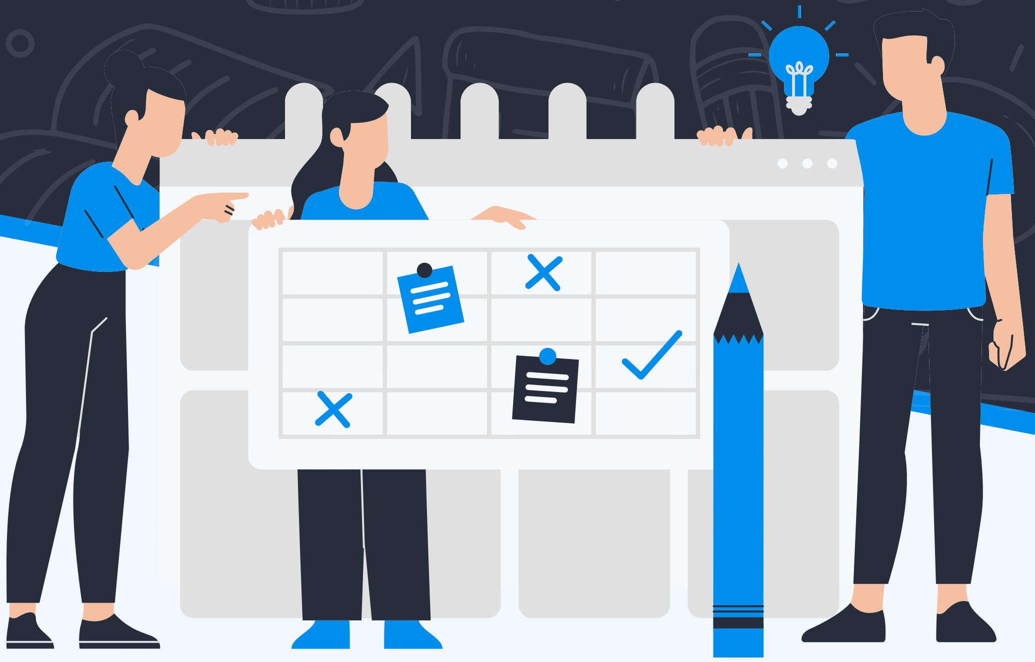
Quick Start E-book:

Building Your Security Program with NIST CSF 2.0



Pivotalogic

Table of Contents

Pivotalogic

Pivotalogic

Introduction

Ready to build a stronger, more secure organization? Our NIST CSF 2.0 E-book gives you a clear, actionable guide to create an effective security program—fast. Avoid the costly risks of inaction and the frustration of doing it alone. This proven framework simplifies the process, helping you achieve compliance and protect your business from threats with less effort. Don't wait—secure your future today!

What is the NIST Cybersecurity Framework?

Overview

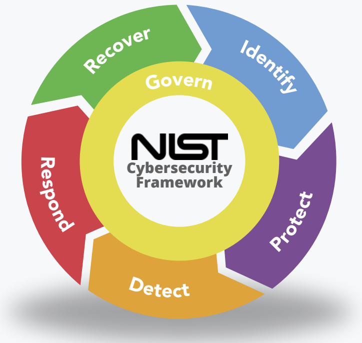
The NIST Cybersecurity Framework (CSF) 2.0 is a flexible tool designed to help organizations of all sizes manage cybersecurity risks. It's widely applicable across various sectors, including healthcare, finance, government, academia, and nonprofits, and adapts to organizations regardless of their cybersecurity program's maturity or technical expertise. The framework is not a one-size-fits-all approach; it recognizes that every organization faces unique risks, missions, and objectives, and allows for customization to address these differences.

At its core, the CSF provides guidance on managing cybersecurity risks alongside other enterprise risks, such as financial, privacy, and supply chain risks. It is designed to be understood by a wide audience, from executives to practitioners, regardless of their technical background. The CSF outcomes, which are sector-neutral, provide flexibility in addressing specific organizational risks and missions.

Key Components of CSF 2.0:

1. **CSF Core:** Organized around six functions—GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND, and RECOVER. These functions guide organizations in establishing a robust cybersecurity program by addressing everything from governance to recovery from cyber incidents.
2. **Profiles:** These help organizations describe and assess their current and target cybersecurity posture, enabling continuous improvement by comparing where they are versus where they need to be.
3. **Tiers:** Tiers characterize the maturity and rigor of an organization's cybersecurity practices, helping to evaluate and improve cybersecurity governance and risk management.

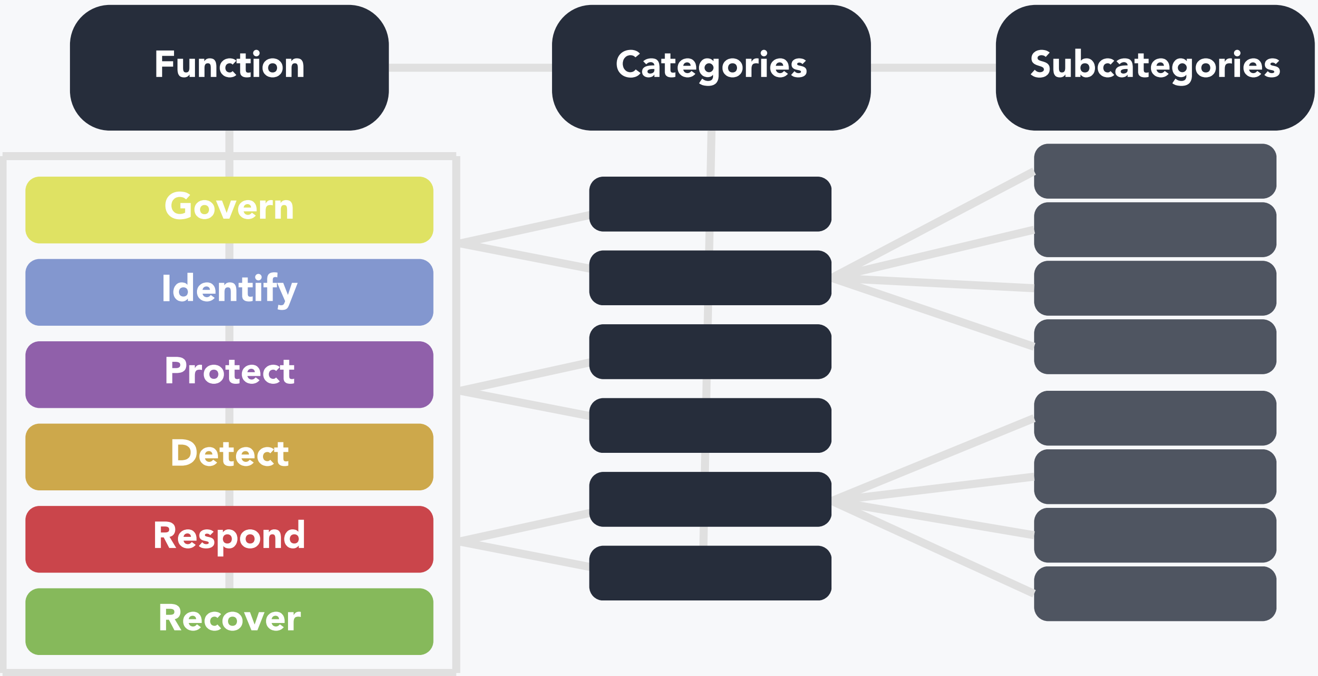
CSF 2.0 emphasizes governance, supply chain risks, and provides tools for smaller organizations to manage their cybersecurity more effectively. It is designed to evolve with technological advancements and is intended for long-term use by a wide range of organizations.



Pivotalogic

NIST CSF 2.0

Cybersecurity Framework Core Explained



The Cybersecurity Framework (CSF) Core is a set of cybersecurity outcomes arranged by Functions, Categories, and Subcategories. It provides flexibility in operationalizing risk management, rather than being a checklist of actions. The six CSF Core Functions are:

- **GOVERN (GV)** — Establishes and communicates the organization's cybersecurity risk management strategy, policy, and governance activities. Ensures cybersecurity is integrated into enterprise risk management (ERM).
- **IDENTIFY (ID)** — Helps understand the organization’s current cybersecurity risks by identifying assets, suppliers, and threats. Enables prioritization of efforts aligned with the risk management strategy.
- **PROTECT (PR)** — Implements safeguards to secure identified assets and reduce the likelihood of cybersecurity incidents. Covers areas like access control, data security, and technology resilience.
- **DETECT (DE)** — Facilitates timely discovery of potential cybersecurity attacks and incidents through anomaly detection and event analysis to support response efforts.
- **RESPOND (RS)** — Manages detected cybersecurity incidents by containing their effects through incident management, mitigation, and communication.
- **RECOVER (RC)** — Supports the restoration of affected assets and normal operations after an incident, ensuring timely recovery and communication.

Cybersecurity Framework Core Explained

This table presents the core Functions and Categories of the Cybersecurity Framework (CSF) core mentioned above.

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PT.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

Govern

Step-by-Step Implementation Guide

Establish Organizational Context (GV.OC)

- **Understand the Mission:** Define how the organizational mission informs cybersecurity risk management.
- **Identify Stakeholders:** List internal and external stakeholders and assess their needs and expectations regarding cybersecurity.
- **Assess Legal and Regulatory Requirements:** Document and manage all relevant legal, regulatory, and contractual obligations related to cybersecurity.
- **Communicate Critical Objectives:** Identify and communicate key objectives, capabilities, and services that stakeholders depend on.

Develop Risk Management Strategy (GV.RM)

- **Set Risk Management Objectives:** Collaborate with stakeholders to establish clear risk management objectives.
- **Define Risk Appetite and Tolerance:** Create and communicate statements on risk appetite and tolerance.
- **Integrate with Enterprise Risk Management:** Ensure cybersecurity activities align with broader enterprise risk management processes.
- **Establish Strategic Direction:** Communicate risk response options and maintain clear lines of communication regarding cybersecurity risks.
- **Standardize Risk Assessment Methodology:** Develop and communicate a standardized approach to categorize and prioritize cybersecurity risks.
- **Incorporate Positive Risks:** Include discussions of strategic opportunities (positive risks) in cybersecurity risk conversations.

Define Roles, Responsibilities, and Authorities (GV.RR)

- **Assign Accountability:** Ensure organizational leadership is accountable for cybersecurity risk and fosters a risk-aware culture.
- **Clarify Roles and Responsibilities:** Clearly establish and communicate roles and responsibilities related to cybersecurity risk management.
- **Allocate Resources:** Ensure resources are adequate for the cybersecurity risk strategy.
- **Integrate with HR Practices:** Include cybersecurity considerations in human resources processes.

Govern

Step-by-Step Implementation Guide

Establish Cybersecurity Policy (GV.PO)

- **Develop Cybersecurity Policy:** Create a comprehensive policy for managing cybersecurity risks based on the organizational context and priorities.
- **Review and Update Policy:** Regularly review and update the policy to reflect changes in requirements, threats, and technology.

Implement Oversight Mechanisms (GV.OV)

- **Review Strategy Outcomes:** Regularly review outcomes of cybersecurity risk management to inform strategy adjustments.
- **Evaluate Performance:** Assess organizational performance in cybersecurity risk management to identify necessary adjustments.

Manage Cybersecurity Supply Chain Risks (GV.SC)

- **Establish a Supply Chain Risk Management Program:** Create a comprehensive program for managing cybersecurity risks in the supply chain.
- **Define Roles for Suppliers:** Communicate and coordinate cybersecurity responsibilities with suppliers and partners.
- **Integrate into Risk Management:** Ensure supply chain risk management processes are integrated into overall cybersecurity and enterprise risk management.
- **Prioritize Suppliers:** Identify and prioritize suppliers based on their criticality to the organization.
- **Set Requirements in Contracts:** Establish cybersecurity requirements for suppliers and include them in contracts.
- **Conduct Due Diligence:** Perform risk assessments before entering relationships with suppliers.
- **Monitor Supplier Risks:** Continuously assess and respond to risks posed by suppliers throughout the relationship.
- **Include Suppliers in Incident Planning:** Integrate suppliers into incident response and recovery planning activities.
- **Monitor Supply Chain Practices:** Regularly review and monitor supply chain security practices throughout the product/service lifecycle.

Identify

Step-by-Step Implementation Guide

Establish Asset Management (ID.AM)

- **Maintain Hardware Inventories:** Create and regularly update inventories of all hardware assets managed by the organization.
- **Maintain Software and Services Inventories:** Develop and maintain inventories of software, services, and systems used within the organization.
- **Document Network Configurations:** Keep representations of authorized network communications and data flows, both internal and external.
- **Inventory Supplier Services:** Track and maintain inventories of services provided by external suppliers.
- **Prioritize Assets:** Classify and prioritize assets based on their criticality, resources, and impact on organizational objectives.
- **Maintain Data Inventories:** Keep inventories of data and corresponding metadata for designated data types.
- **Manage Assets Throughout Their Lifecycle:** Ensure that systems, hardware, software, services, and data are managed effectively throughout their lifecycle.

Conduct Risk Assessment (ID.RA)

- **Identify Vulnerabilities:** Regularly identify, validate, and record vulnerabilities associated with assets.
- **Gather Threat Intelligence:** Collect cyber threat intelligence from information-sharing forums and other reliable sources.
- **Assess Internal and External Threats:** Identify and record potential internal and external threats to the organization.
- **Analyze Impact and Likelihood:** Evaluate and document the potential impacts and likelihood of threats exploiting identified vulnerabilities.
- **Understand Inherent Risk:** Use the gathered data on threats, vulnerabilities, likelihoods, and impacts to inform an understanding of inherent risk and prioritize risk responses.
- **Choose Risk Responses:** Select, prioritize, and plan risk responses, ensuring they are tracked and communicated effectively.
- **Manage Changes and Exceptions:** Establish processes for managing changes and exceptions, assessing their risk impact, and tracking them.
- **Establish Vulnerability Disclosure Processes:** Create processes for receiving, analyzing, and responding to vulnerability disclosures.
- **Assess Authenticity of Assets:** Evaluate the authenticity and integrity of hardware and software before acquisition and use.
- **Assess Critical Suppliers:** Conduct risk assessments for critical suppliers prior to acquisition.

Identify

Step-by-Step Implementation Guide

Implement Improvement Processes (ID.IM)

- **Identify Improvements from Evaluations:** Regularly evaluate cybersecurity processes and identify areas for improvement.
- **Identify Improvements from Testing:** Gather insights from security tests and exercises to identify potential improvements, including those involving suppliers.
- **Identify Improvements from Operations:** Review execution of operational processes to identify areas for improvement.
- **Establish Incident Response Plans:** Develop, communicate, maintain, and improve incident response plans and other relevant cybersecurity plans.

Protect

Step-by-Step Implementation Guide

Establish Identity Management, Authentication, and Access Control (PR.AA)

- **Manage User Identities and Credentials:** Implement processes to manage identities and credentials for all authorized users, services, and hardware.
- **Proof and Bind Identities:** Ensure that identities are validated and securely linked to credentials based on the context of their interactions.
- **Authenticate Users and Services:** Require authentication for all users, services, and hardware accessing the organization's resources.
- **Protect Identity Assertions:** Safeguard identity assertions during transmission and verification processes.
- **Define Access Permissions:** Develop policies defining access permissions and authorizations, enforcing principles of least privilege and separation of duties.
- **Manage Physical Access:** Monitor and control physical access to assets according to the assessed risk level.

Implement Awareness and Training (PR.AT)

- **Provide General Awareness Training:** Ensure all personnel receive training on cybersecurity risks relevant to their roles.
- **Specialized Role Training:** Offer tailored training for individuals in specialized roles to equip them with necessary cybersecurity knowledge and skills.

Enhance Data Security (PR.DS)

- **Protect Data-at-Rest:** Implement measures to safeguard the confidentiality, integrity, and availability of stored data.
- **Protect Data-in-Transit:** Ensure that data being transmitted is secured against unauthorized access or alteration.
- **Protect Data-in-Use:** Manage the confidentiality, integrity, and availability of data actively being used.
- **Create and Maintain Backups:** Establish processes for regular data backups, ensuring they are protected, maintained, and tested for reliability.

Protect

Step-by-Step Implementation Guide

Ensure Platform Security (PR.PS)

- **Establish Configuration Management:** Develop and apply configuration management practices to maintain security across hardware and software.
- **Maintain Software and Hardware:** Regularly assess and update software and hardware to manage associated risks effectively.
- **Generate Log Records:** Implement logging practices to facilitate continuous monitoring of system activities.
- **Prevent Unauthorized Software:** Ensure that unauthorized software installations and executions are blocked.
- **Integrate Secure Development Practices:** Incorporate secure software development practices throughout the software lifecycle and monitor their effectiveness.

Enhance Technology Infrastructure Resilience (PR.IR)

- **Protect Networks from Unauthorized Access:** Implement measures to safeguard networks and environments from unauthorized logical access.
- **Protect Against Environmental Threats:** Ensure technology assets are secured against potential environmental threats.
- **Achieve Resilience Requirements:** Implement mechanisms to maintain resilience during both normal operations and adverse conditions.
- **Maintain Resource Capacity:** Ensure adequate resource capacity is available to uphold system availability under various conditions.

Detect

Step-by-Step Implementation Guide

Establish Continuous Monitoring Framework

- **Identify Assets:** Catalog all networks, network services, physical environments, personnel activities, and external services that require monitoring.
- **Define Monitoring Requirements:** Determine the types of anomalies and indicators of compromise relevant to each asset.

Implement Monitoring Mechanisms

- **Network Monitoring:** Set up systems to continuously monitor networks for unusual activities.
- **Physical Environment Monitoring:** Use surveillance and environmental sensors to detect unauthorized access or anomalies.
- **Personnel Activity Monitoring:** Track user activity and technology usage to identify suspicious behavior.
- **External Service Monitoring:** Monitor third-party service providers to detect any potential risks.
- **Hardware and Software Monitoring:** Ensure that computing environments and data are continuously observed for irregularities.

Conduct Adverse Event Analysis

- **Analyze Anomalies:** Regularly evaluate detected anomalies to understand their context and associated activities.
- **Correlate Information:** Integrate data from various sources to gain a comprehensive view of potential threats.
- **Assess Impact and Scope:** Estimate the potential impact of identified events on the organization’s operations.
- **Communicate Findings:** Share information about adverse events with authorized personnel and necessary tools.

Detect

Step-by-Step Implementation Guide

Integrate Cyber Threat Intelligence

- **Incorporate Threat Intelligence:** Use threat intelligence feeds to enhance the analysis of adverse events and improve detection capabilities.
- **Develop Incident Criteria:** Define clear criteria for declaring an incident based on the analysis of adverse events.

Continuous Improvement

- **Review and Update:** Regularly evaluate and update monitoring practices and incident criteria based on emerging threats and organizational changes.
- **Training and Awareness:** Provide ongoing training for staff on recognizing and responding to potential cybersecurity incidents.

Respond

Step-by-Step Implementation Guide

Develop and Execute an Incident Response Plan

- **Create the Plan:** Establish a comprehensive incident response plan that outlines roles, responsibilities, and procedures.
- **Coordinate with Third Parties:** Ensure the plan includes collaboration with relevant external partners and stakeholders.
- **Execute Upon Declaration:** Activate the incident response plan immediately once an incident is detected.

Manage Incident Reporting

- **Triage and Validate Reports:** Assess incident reports to determine their legitimacy and urgency.
- **Categorize and Prioritize Incidents:** Classify incidents based on their severity and impact to allocate appropriate resources.
- **Escalate as Needed:** Ensure that incidents are escalated to higher management or specialized teams when necessary.

Conduct Incident Analysis

- **Investigate the Incident:** Analyze the incident to understand its nature and determine the root cause.
- **Preserve Integrity of Records:** Document all actions taken during the investigation and ensure the integrity of records and data.
- **Estimate Incident Magnitude:** Assess the scale and impact of the incident to inform response strategies.

Communicate Effectively

- **Notify Stakeholders:** Inform both internal and external stakeholders about the incident as required by policies and regulations.
- **Share Relevant Information:** Disseminate pertinent information to stakeholders to ensure transparency and coordinated responses.

Respond

Step-by-Step Implementation Guide

Implement Incident Mitigation Strategies

- **Contain the Incident:** Take immediate action to limit the spread of the incident and its effects on systems and data.
- **Eradicate the Threat:** Remove the cause of the incident and restore affected systems to normal operation.

Review and Improve Response Processes

- **Post-Incident Review:** Conduct a thorough review of the incident response process to identify areas for improvement.
- **Update the Response Plan:** Revise the incident response plan based on lessons learned from the incident to enhance future responses.

TIP: Regularly test your incident response plan with tabletop exercises to identify gaps and areas for improvement. This ensures your organization is better prepared when a real event occurs.

Recover

Step-by-Step Implementation Guide

Initiate the Recovery Process

- **Execute Recovery Plan:** Activate the recovery portion of the incident response plan once the incident response process concludes.

Select and Prioritize Recovery Actions

- **Scope Recovery Actions:** Identify specific recovery actions needed to restore affected systems and services.
- **Prioritize Activities:** Determine the order of recovery tasks based on criticality to business operations.

Verify Integrity of Restoration Assets

- **Check Backups:** Ensure that backups and other restoration assets are intact and free from compromise before initiating restoration efforts.

Restore Systems and Services

- **Consider Critical Functions:** Evaluate which critical mission functions and cybersecurity risk management aspects must be addressed during recovery.
- **Verify Restoration Integrity:** Confirm the integrity of restored assets to ensure systems and services are functioning correctly.
- **Confirm Normal Operations:** Ensure that all systems are back to normal operating status before declaring recovery complete.

Declare End of Recovery

- **Complete Documentation:** Finalize incident-related documentation and declare the end of the recovery process based on established criteria.

Coordinate Communication

- **Communicate Progress:** Regularly update internal and external stakeholders on the progress of recovery activities.
- **Public Updates:** Share approved public communications regarding the incident recovery process using designated messaging channels.

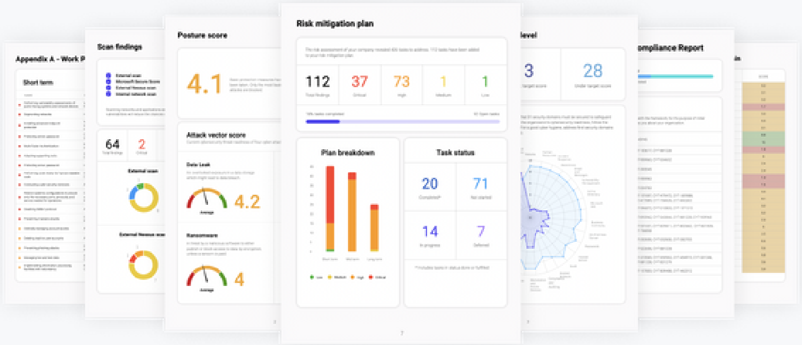
Pivotalogic

Complimentary Cybersecurity Review - Take the first step toward securing your business with confidence.

We understand that the first step can be the hardest to take. To make it easier for you, we're offering a limited number of complimentary security reviews. Let us help you assess your risks and enhance your security posture—take advantage of this opportunity today!

Your guided review will cover the following:

✓ Customized Cybersecurity Risk Profile
✓ Comprehensive Review of your 3 most critical domains
✓ External Vulnerability Scan to identify weaknesses
✓ Detailed Report highlighting Cybersecurity gaps
✓ Insightful Analysis performed by Cybersecurity Experts
✓ Actionable Recommendations to fortify your security



Give Me My Security Review!

☎ 612-230-7440 ✉ info@pivotalogic.com 🌐 www.pivotalogic.com