What is the NIST Cybersecurity Framework?

You may have heard "NIST CSF" thrown around by colleagues or leadership in relation to how security policies and procedures should be set up. The NIST CSF is one of several cybersecurity frameworks (along with CIS 20, ISA/IEC 62443, MITRE ATT&CK, and NIST 800-53) used in the cybersecurity field to set maturity standards for security.

According to Gartner, the ISO 27001 and the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) will remain the predominant enterprise security frameworks complemented by localized and industry-specific standards and regulations through 2024.

While they are not necessarily driven by regulatory compliance, these cybersecurity frameworks help you understand the inclusive set of security elements to include and how to establish the right target level for each. But what is it, what do you need to know, and what impact does it have for your business?

What does NIST CSF stand for?

NIST CSF is the Cybersecurity Framework (CSF) built by the National Institute of Standards and Technology (NIST), a division of the U.S. Department of Commerce. Previously called the National Bureau of Standards, NIST promotes and maintains measurement standards with active programs to advance innovation and secure industries such as advanced manufacturing, cybersecurity, health bioscience, and more.

Why was the NIST CSF created?

Critical infrastructure in the United States, such as transportation, energy, chemicals, and manufacturing, depend on security and reliability in order to keep the country safe and operating smoothly.

On February 12, 2013, President Barack Obama issued an Executive Order to improve cybersecurity in critical infrastructure due to the alarming number of cybersecurity breaches to U.S. critical infrastructure. The Executive Order was created "to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties."

The U.S. Government worked together with NIST to develop a framework (over the course of many iterations) that could be used by any organization whose processes, products, services, technology, or operations directly impacts the nation's critical infrastructure. As a third-party, unbiased agency, NIST was chosen to construct the framework based on its extensive experience in data protection, partnerships in various industries, education, and government entities, and overall cybersecurity intelligence.

In accordance with the Executive Order, the Cybersecurity Framework was established to:

- Identify security standards and guidelines applicable across sectors of critical infrastructure
- Provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach
- Help owners and operators of critical infrastructure identify, assess, and manage cyber risk
- Enable technical innovation and account for organizational differences
- Provide guidance that is technology-neutral and enables critical infrastructure sectors to benefit from a competitive market for products and services
- Include guidance for measuring the performance of implementing the CSF
- Identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations

The NIST Cybersecurity Framework is broken into three parts: framework core, profiles, and implementation tiers. The CSF framework core refers to the activities and outcomes of cyber security adoption. Profiles vary for each organization. They are chosen and optimized depending on the organization's unique challenges, needs, and opportunities to address different core objectives. Tiers specify to what level an organization addresses each of the CSF elements. It is not necessarily based on maturity levels but based on what level is necessary and acceptable for each element *for the specific organization*.

While the core functions of NIST CSF include categories, subcategories, and informative references, we're going to focus on outlining the five core functions from a 500-foot view:

Identify
Protect
Detect
Respond
Recover

Identify

The first core function is Identify. The purpose of this function is to establish what assets your organization relies on for business production to understand what you need to protect. These assets include the equipment, people, devices, systems, and data that make up the business environment.

Core elements of the Identify component are:

- Asset Management

This includes a robust inventory of all assets in the environment. Not only the hardware, but a deep view of the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes. They should be identified and their relative importance to business objectives and risky management clearly established.

- Business Environment

This defines the organization's mission, objectives, stakeholders, and activities are prioritized. This then informs the cybersecurity roles, responsibilities, and risk management decisions

- Governance

The policies, procedures and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risks.

- Risk Assessment

The organization defines and understands its risks to operational, organizational assets and individuals

- Risk Management Strategy

This defines the organization's priorities, constraints, tolerances, etc., and they are used to support risk decisions

- Supply Chain Risk Management

Same as the risk management strategy, but focused on supply chain risks.

Protect

The next core function of the NIST CSF is Protect. Now that you have identified and classified your assets, you'll want to proactively protect them against internal and external cyber threats. This includes a number of technical and procedural controls such as providing physical and electronic access restrictions on asset access, endpoint hardening, and the deployment of security-specific tools to protect and monitor health among many others.

Different types of access (i.e. physical, virtual/remote) require varying levels of cybersecurity protection. While physical security access is not always forefront in cyber, the NIST CSF is more heavily focused on electronic and procedural controls due to their criticality.

This core function also requires a host of security maintenance policies and procedures be developed and deployed such as software patch management and whitelisting. These are two of the most common practices that materialize within vulnerability management and protection.

Protect includes the following elements:

- Identity management, authentication and access control

Access to physical and logical assets and associated facilities us limited to authorized users, processes and devices and is managed consistent with the assessed risk of unauthorized activities.

- Awareness and Training

Organization's personnel and partners are provided cybersecurity awareness and education to perform their functions

- Data Security

Information is managed consistent with the organization's risk strategy to protect the confidentiality and integrity of the data

- Information protection

Security policies and procedures that are used to maintain the protection of information systems and assets

- Protective Technology

Technical solutions are managed to ensure the security and resilience of systems and assets

Detect

Detect is the third core function. Here, we're looking for red flags within and among/between our assets. During the Protect function, you likely created a baseline for what normal behavior looks like on the asset as well as on the networks they reside in. That way anything that doesn't match this baseline can be flagged as anomalous behavior and likely in need of additional investigation or correction. Monitoring assets for anomalous behavior on a regular basis allows you to detect suspicious activity in a timely matter so you can stop an attack (hopefully) before it happens.

Core elements of "detect" include:

- Anomalies and events

Anomalous activity is detected in a timely manner and the potential impacts of events is understood

- Security Continuous Monitoring

The information system and assets are monitored in discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures

Respond

Now that we've detected red flags and anomalous behavior within our assets (yikes!), let's do something about it. Organizations develop playbooks that determine what actions should take place in the event of a cybersecurity attack.

Response processes and procedures should be updated regularly to incorporate ongoing changes as organization systems evolve, improved from lessons learned from response activity results, be effectively communicated to appropriate participating stakeholders. Your policies are only as good as the education you provide the people who will be relied on to convert policies into action in pivotal moments.

The core elements of respond include:

- Response Planning

Response processes and procedures are executed and maintained to ensure timely response to detected cybersecurity incidents

- Communications

Response activities are coordinated with internal and external stakeholders to include external support from law enforcement

- Analysis

Conducted to ensure adequate response and support recovery activities

- Mitigation

Activities are performed to prevent expansion of an event, mitigate its effects, and resolve an incident

Recover

The final core function in the NIST CSF is Recover. We've detected threats in our assets and took action to remediate the problem. Now we want to get our systems back to where they were before the attack. It's crucial to continuously backup the current state of your systems so you can restore the affected assets back to a state of normalcy in a timely matter. You'll also want to assess how much damage was done from the cyberattack, and determine what actions are needed to future-proof the system. What lessons did you learn, and how can you establish stronger security methods to protect your identified assets against identified vulnerabilities and potential threats?

Recovery includes the ability to do recovery planning. This includes recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets.

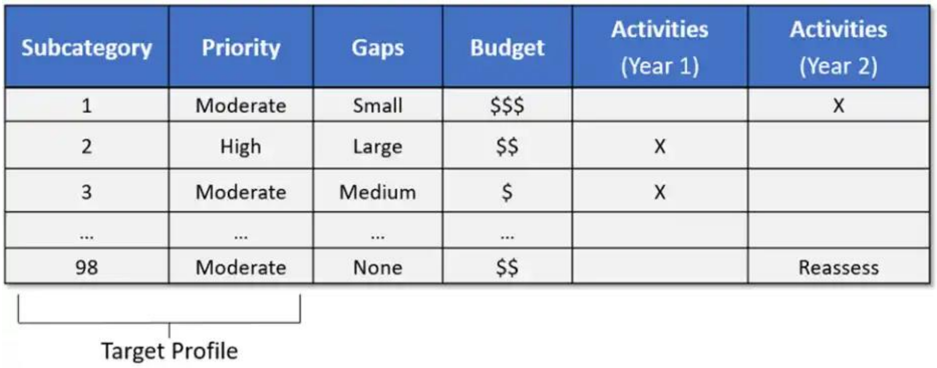
This brings us back to Identify, where you can re-configure a baseline for what "normal" looks like.

Profiles:

According to NIST, Profiles are an organization's specific design of their organizational requirements and risk appetites against the desired outcomes of the Framework core elements. Profiles help to identify areas of improvement for the organization. Often they are defined as "current state" profile and "target" profile. This allows an organization to understand where it is currently against the framework's core elements and then evaluate as it matures its cybersecurity.

Organizations can map their framework to their overall cybersecurity objectives and methodologies along with current practices. Then aligning those against the subcategories of the Framework elements.

The creation of these target profiles allows the organization to determine a prioritized implementation plan and the cost of corrective actions.



Subcategory	Priority	Gaps	Budget	Activities (Year 1)	Activities (Year 2)
1	Moderate	Small	$$$		X
2	High	Large	$$	X	
3	Moderate	Medium	$	X	
...	...	...	...		
98	Moderate	None	$$		Reassess

Target Profile

Implementation Tiers

The third component of the NIST CSF is implementation tiers. Tiers describe the degree to which an organization’s risk management practices exhibit the elements of the framework’s core four components. The tiers range from partial up to adaptive. They do not necessarily represent different maturities Any organization can determine its desired level. There are four tiers within NIST CSF:

- Tier 1: Partial. This tier also covers organizations with no security practices at all

Typically organizations at this level perform cybersecurity as an ad hoc manner. There is little to no prioritization. Because there are few processes, there is no real risk management program other than a case-by-case basis. They also do not have much participation with external parties (government, industry, or otherwise)

- Tier 2: Risk Informed

Policies and procedures in Tier 2 organizations are usually approved by management but not as part of an enterprise-wide program and not standardized. Cybersecurity is often not a core strategic element of the organization. Information around cybersecurity is not shared consistently and they often understand their broader role in the ecosystem only as dependent on other parts of the ecosystem rather than as a contributor.

- Tier 3: Repeatable

These organizations likely have formally approved risk management practices that enable a regular operationalization of cybersecurity controls. These processes and procedures are documented and regularly reviewed. There is also usually a greater, higher-level focus of leadership on cybersecurity across the enterprise.

- Tier 4: Adaptive

In adaptive organizations, the processes and procedures are regularly revised to adapt to new threats and risks. The organization treats cybersecurity as an enterprise risk management process as part of a continuous improvement program. They understand the link between organizational objectives and the cyber risks that may pose issues with that objective. They integrate deeply into the ecosystem participating actively in receiving, generating and sharing data with the community.

What does the NIST CSF mean for OT security?

Ultimately, the NIST Cybersecurity Framework is not a one-size-fits-all solution for managing cyber security risk as every company faces different threats, levels of severity, and points of intrusion. This is where the NIST CSF profiles and tiers come into play for organizations to determine which strategies are essential to protecting their critical infrastructure.

In the world of OT cybersecurity, industrial companies are coming to the realization that their manufacturing or processing facilities are at risk from both targeted and untargeted cybersecurity threats. While awareness of the issue is growing, many struggle to grasp exactly how to make an impact in protecting these critical assets.

Verve Industrial Protection has a successful track record in assisting industrial companies to increase their maturity relative to the NIST CSF standards through our professional design, and support services as well as by deploying the Verve Security Center on customers' OT or Industrial Control Systems.

No matter where you are in the cybersecurity journey from a basic understanding to more mature adoption, we can help you significantly increase your level of defense and reliability with our end-to-end solution to assist with all five core functions of the NIST CSF.

Retrieved from https://verveindustrial.com/resources/blog/what-is-the-nist-cybersecurity-framework/ on 3 Oct 2022