NIST Cybersecurity Framework Implementation Overview

WHITE PAPER

ABSOLUTE®

TABLE OF CONTENTS

SUMMARY

In 2014, the National Institute of Standards and Technology (NIST) created a repeatable cybersecurity framework (CSF) to help organizations of all kinds adopt formal security disciplines. It was updated in 2018, based on feedback from industry and subject matter experts, and iterations will likely be ongoing due to the ever-changing nature of the cybersecurity landscape.

This paper outlines the five functions of the NIST CSF, focusing particularly on how NIST relates to the endpoint, and provides actionable guidelines for implementing it in your organization.

IMPLEMENTING A CYBERSECURITY FRAMEWORK

Organizations today are facing a perfect storm when it comes to cybersecurity: the threat landscape has increased in complexity, and people with the skillsets to navigate it are hard to find.

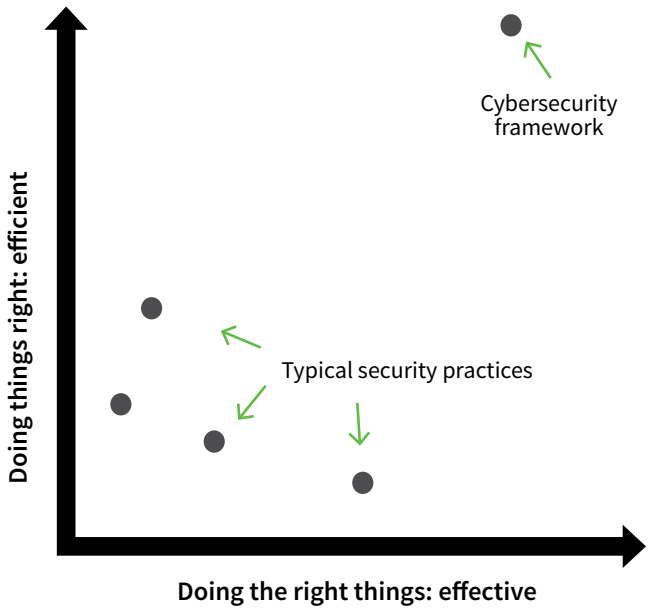
With data security regulations around the world tightening, organizations are facing more pressure to be accountable for the data in their care — and steeper penalties for non-compliance. So, with more work to do than there are people to do it, a cybersecurity framework (CSF) is no longer a nice-to-have — it's a necessity.

There are two main benefits to implementing a cybersecurity framework:

1.) **Security disciplines are formalized.** Teams can focus on repeatable methods so knowledge is shared and people focus on the right things.

2.) **Security operations can be scaled.** When all members buy into the process, teams can do more, even when faced with resource constraints.

The National Institute of Standards and Technology (NIST) in the U.S. built a model, the **NIST CSF**, to help organizations evaluate their security posture and implement five functions to ensure data security and business sustainability.

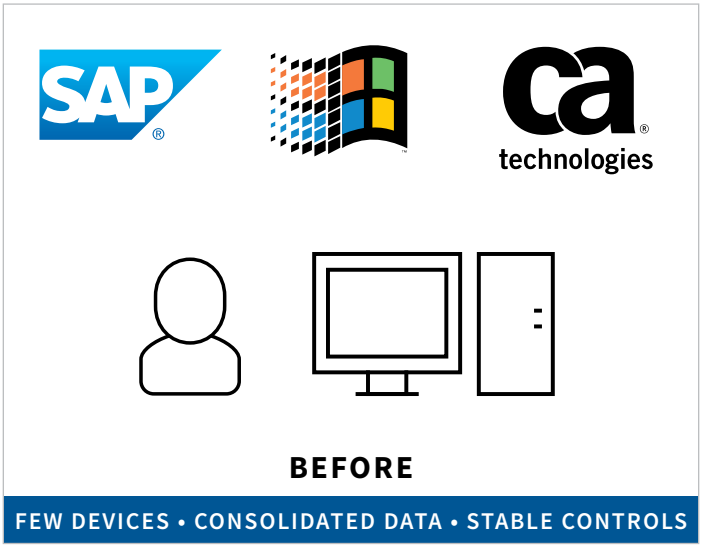


FIVE FUNCTIONS OF THE NIST CYBERSECURITY FRAMEWORK

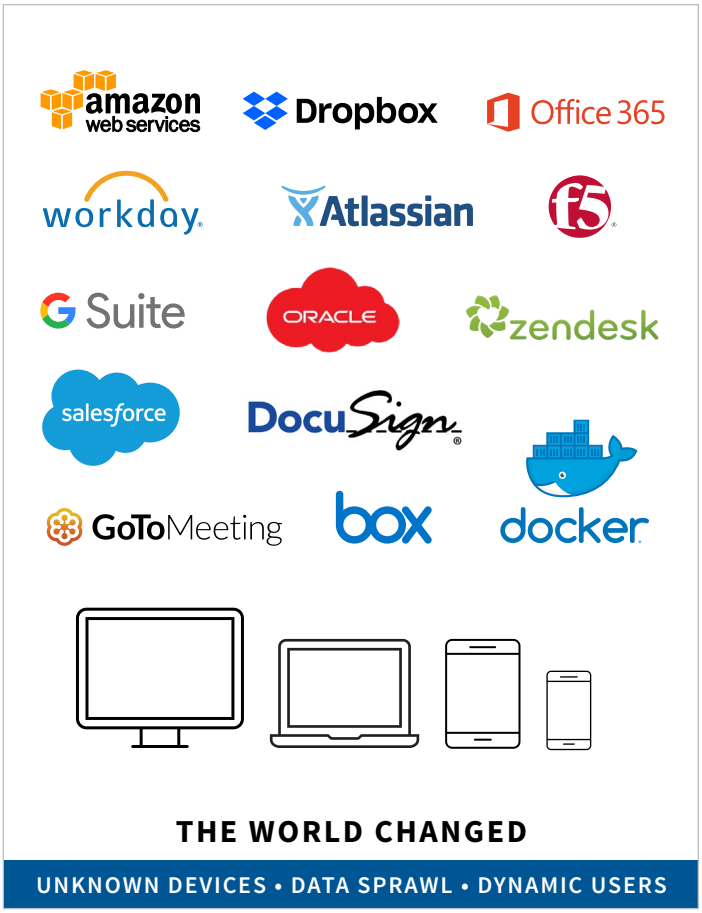
1. **Identify** devices that store, transmit, and process information.
2. **Protect** data and manage sensitive assets throughout their lifecycle — particularly removing, transferring, disposing, and sanitization of assets and data.
3. **Detect** issues and be aware of changing circumstances and negligent users.
4. **Respond** to vulnerabilities and threats in a consistent, rational way to ensure fast remediation.
5. **Recover** and iterate — question assumptions, change security controls, and use new knowledge to influence future decisions.

1 IDENTIFY

In the early days of digital, cybersecurity was straightforward. IT teams managed a few static assets that accessed data through firewalls, preventing unauthorized access to the network. Apps were large, on-premise, and relatively homogenous. To protect data, they simply fortified the network perimeter with access controls.



As digital work increasingly became web-based, IT lost control and risk shifted toward the end user. The NIST CSF "Identify" function includes a series of sub-categories to help organizations deal with this new world: asset management, business environment, governance, risk assessment, and risk management strategy.



ASSET MANAGEMENT

"The data, personnel, devices, and systems that enable organizations to achieve business purposes are identified and managed consistent with their relative importance to objectives and risk." – NIST CSF

Asset management has grown to encompass more than simple device inventory. NIST recommends a more intelligent, holistic view that considers the business function associated with the IT resource. When you consider other assets in your organization — a desk, for example — you don't think about it as brackets, wood, and so on. Instead, you synthesize a situation in which that resource is used, *i.e.* 'Jane's work space'. NIST recommends this holistic view because it lets organizations weigh the value of particular resources against their cost and risk.

BUSINESS ENVIRONMENT

"The organization's mission, objectives, stakeholders and activities are understood and prioritized and used to inform cybersecurity roles, responsibilities and risk management." – NIST CSF

To identify resources with confidence, it's important to understand the wider business environment. Perhaps you just went through a merger or acquisition. Maybe you provide resources for contractors, or your employees work remotely. These contextual variants help you to better analyze the current state of your cybersecurity posture.

GOVERNANCE

"The policies, procedures and processes to manage and monitor regulatory, legal, risk and operational requirements are understood and inform the management of cybersecurity risk." – NIST CSF

Policy, i.e. what is allowed, is what remains when the controls, metrics, reporting variables, and regulatory requirements are stripped away. With a full understanding of your organization's procedures, processes, and regulatory requirements, you can grade your current security controls relative to your standards. Some policies may need a revision; some may need to be scrapped. Either way, the evidence to complete your governance audit is out there on your endpoints.

RISK ASSESSMENT

"The organization understands the cybersecurity risk to operations, organizational assets and individuals." – NIST CSF

It's impossible to accurately assess risk without intimate knowledge of your devices. What are their vulnerabilities? How are the used on a daily basis? What's the potential cost if a risk comes to fruition? Vulnerable resource risks must be calculated carefully, but also with a wide lens on the potential threats that could harm the resource.

RISK MANAGEMENT STRATEGY

"The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions." – NIST CSF

A risk management strategy is more than a simple SWOT analysis or roadmap. It comes down to your goals and how you use technology to achieve them. Without a thorough understanding of your inherent risks and associated costs, you would be at a loss to implement technical controls that align with those goals and the risks associated.

2 PROTECT

Once the Identify function is established, focus can move to protecting devices, data, apps, and users. The NIST CSF provides four sub-categories to help you establish the "Protect" function: access control, awareness and training, data security, and protective technology.

ACCESS CONTROL

"Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions." – NIST CSF

To secure data, we must control to how, when, to whom, and in which circumstances we grant access. This begins with managing the identities and credentials of those accessing the data. Authentication techniques are built on trust, and that trust is achieved when you provide one or more of the following:

- Something you know (a password)
- Something you have (a smart card or token)
- Something you are (fingerprint or retinal scan)

Managing identities and credentials is important — but so is context. The NIST CSF references two contexts for access control:

1. ***Physical context*** puts the user in the same geospatial location as the resource which needs to be managed by the 'trust but verify' principle. Physical access controls put matter in place to guard devices, data, and apps from unauthorized access.
2. ***Remote context*** is similar but, instead of matter, you use bits and bytes to 'build a moat' around your resources.

AWARENESS AND TRAINING

"The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements." – NIST CSF

Simulated phishing scams help identify vulnerable employees, but do little to educate them on the principles of cybersecurity. A deeper user awareness, cultivated through thoughtful training, is a critical part of the "Protect" function.

Awareness initiatives can include video tutorials, signage, policy reviews, and gamification to ensure each user understands security best practices *and* the unique security needs of their organization. Training initiatives can be collaborative between IT and HR and should occur regularly — not just during employee onboarding.

DATA SECURITY

"Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information." – NIST CSF

There are two different kinds of data that need protection: data at-rest and data in-transit. Asset monitoring is an important practice to protect both. Assets should be managed throughout their entire lifecycle: from initial installation and activation of security controls, to continuous monitoring throughout its life, to appropriate decommissioning at end-of-life.

NIST challenges our assumptions about data security; specifically, the assumption that encryption is enough.

NIST SP 800-88 and "Media Sanitization"

In recent years, organizations have placed a renewed focus on their ability to ensure that data is fully erased from electronic storage media. This attention has been boosted by NIST Special Publication 800-88, which lays out 3 categories of media sanitization:

1. Clear: using logical techniques to remove data, often through the standard read/write commands on a device. This includes rewriting to a new value or resetting the device to a factory state.

2. Purge: using physical or logical techniques that make it infeasible to recover data using modern laboratory techniques. This can include the removal of hidden drives and firmware-based commands.

3. Destroy: using physical techniques to not only make data recovery infeasible, but to make the media completely incapable of storing data. These physical techniques include shredding, incinerating, pulverizing, melting, and similar techniques, but notably does not include de-Gaussing.

Your organization can determine the appropriate data sanitization method by comparing and contrasting these variables:

- Confidentiality levels of specific data and devices
- The nature and location of the storage medium
- The risk involved should your data be retrieved post-hoc
- Your intentions to either reuse, donate, or destroy the device

PROTECTIVE TECHNOLOGY

"Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements." – NIST CSF

People and processes are important, but they must be complemented by technology. NIST CSF suggests areas where protective technology can help:

1. ***Audits*** serve as a forcing mechanism to push toward greater compliance.
2. ***Logs*** give a clear picture of the current security posture.
3. ***Removable Media Security*** can be detected with **asset management** and examined for compliance.
4. ***Least Privilege*** policies can be exercised with access controls — role provisions, permissions, exfil restrictions, two-factor authentication, geofencing, and sensitive data discovery.
5. ***Gestalt Security*** — fortifying the network and communications channels — is achieved with WireShark, DPI, UCC, NGFW.

3 DETECT

The NIST CSF Detect function is split into three sub-categories: anomalies and events, information security continuous monitoring, and detection processes.

ANOMALIES AND EVENTS

"Anomalous activity is detected in a timely manner and the potential impact of events is understood." – NIST CSF

Once a security incident has been identified, asset intelligence plays a central role. Where is the device located? Is there additional behavior (machine or human) happening simultaneously? Is the current anomaly outside the bounds of the security policy? What was happening on the device immediately before the event? What data is at risk? Asset intelligence — intimate knowledge of the device, data, users, apps, and behaviors — allows you to satisfy this function.

Conditional Cyber Risks:

- Corporate Network
- Physical Environment
- Mobile Assets
- Endpoints
- User Activity
- Business Apps
- Corporate Data
- Consumer/Customer Data

Unconditional Cyber Risks:

- Malicious Code
- External Service Provider
- Out-of-Network Connections
- Mobile/Access Point Code
- Unauthorized Hardware & Software
- Unauthorized Users
- Unauthorized Connections

INFORMATION SECURITY CONTINUOUS MONITORING

"The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures." – NIST CSF

Within the sub-goals of the "Detect" function, there are two types of variables:

- *Conditional variables,* under normal circumstances, won't generate cybersecurity events. These can include networks, physical environments, and personnel – they're part of the organization's fabric and provide measurable benefits when each has authorized access to data.
- *Unconditional variables,* irrespective of circumstance, are menaces to digital security, such as malicious code, unauthorized software, personnel, connections, and devices, external service providers, and vulnerabilities.

Conditional variables should be subjected to a principled cost-benefit analysis, while unconditional variables should be rooted out consistently.

DETECTION PROCESSES

"Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events." – NIST CSF

To maintain and test the effectiveness of any detection process, look at each component and evaluate the gaps. This approach challenges assumptions of what it means to detect threats. First, you must acknowledge that anomalies depend on a rational and secure baseline for any device. Once these endpoints are brought to a state of pristine hygiene, you can detect deviations from what is standard, normal, or expected.

4 RESPOND

Despite how rigorously you establish the Identify, Protect, and Detect functions, security breaches are always a risk. NIST CSF's "Respond" function outlines five sub-categories to help you respond in the event of an IT crisis: response planning, communications, analysis, mitigation, and improvements.

RESPONSE PLANNING

"Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events." – NIST CSF

NIST presumes response planning procedures are already in place in your organization and recommends measuring them against five simple questions:

- ***What could happen?***
  An honest view of your current ***security posture*** shows you where your weaknesses are and helps you identify what could happen and the steps you can take to mitigate the damage.
- ***What should happen?***
  Security policy is the bedrock of all security — defining what is allowed and what is not.
- ***What would happen?***
  Security modeling gives you a picture of what would happen under a set of circumstances. It does not have to take place inside clever apps with enhanced visualizations. It can be as simple as brainstorming the effect of proposed policy changes to demonstrate counterfactual situations and isolate influential factors.
- ***What is happening?***
  Security monitoring allows you to examine current happenings in the network, within devices, across IoT, and the endpoint to discover anomalous activities.
- ***What did happen?***
  Security investigations provide a repository of previous events that serve as vital inputs to assess the likelihood of a repeat occurrence.

COMMUNICATIONS

"Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies." – NIST CSF

In a security crisis, there are three important questions to ask before sending a communication:

- ***Is it true?*** Be truthful and state the facts.
- ***Is it helpful?*** Only provide information that is helpful to your stakeholders.
- ***Is it necessary?*** A security event can be damaging enough that it's necessary to communicate it to law enforcement.

ANALYSIS

"Analysis is conducted to ensure adequate response and support recovery activities." – NIST CSF

When analyzing what happened, stay goal-oriented. Leave the investigation to those who have time to comb through the incident. Instead, consider your security modeling and use a response scenario with actions that lead to an expedited recovery.

MITIGATION

"Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident." – NIST CSF

Halt the spread of vulnerable resources. Return to the first two functions of the NIST CSF: Identify and Protect. Once the potential expansion is understood, **isolate infected systems**, remove communication, block port access, and lock an endpoint with remote command. These actions mitigate damaging effects because the attack surface is narrowed to include only the points of compromise. Once isolated, examine the current state of the compromise and take action.

IMPROVEMENTS

"Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities." – NIST CSF

Introspection allows you to challenge assumptions and follow learning that is empirical and verifiable. This takes us right back to the top of the response planning phase. You now have a new input to signal if your security posture, policy, modeling, monitoring, or forensics are vulnerable. By repeating the process, operations become more agile.

5 RECOVER

The final function, "Recover," calls for reflection on what happened and the opportunity to incorporate new knowledge to improve your people, process, and technology for greater resilience. Approach the Recover function with three sub-goals: planning, improve identify, protect, detect, respond, and communication.

PLANNING

"Recovery processes are executed and maintained to ensure restoration." – NIST CSF

When preparing for compromise, processes must focus on restoring systems, data, access, applications, and users. It can be tempting to go with your gut during a security event. The Recover function gives you the opportunity to develop plans in advance so you're not reacting in panic.

Ask yourself these questions:

- Does this part of the plan ensure restoration?
- Does it raise the probability of adequate (and speedy) recovery?

In doing so, you move away from bias toward the goal of timely restoration.

IMPROVE IDENTIFY, PROTECT, DETECT, RESPOND

"Recovery planning is improved by incorporating lessons learned into future activities." – NIST CSF

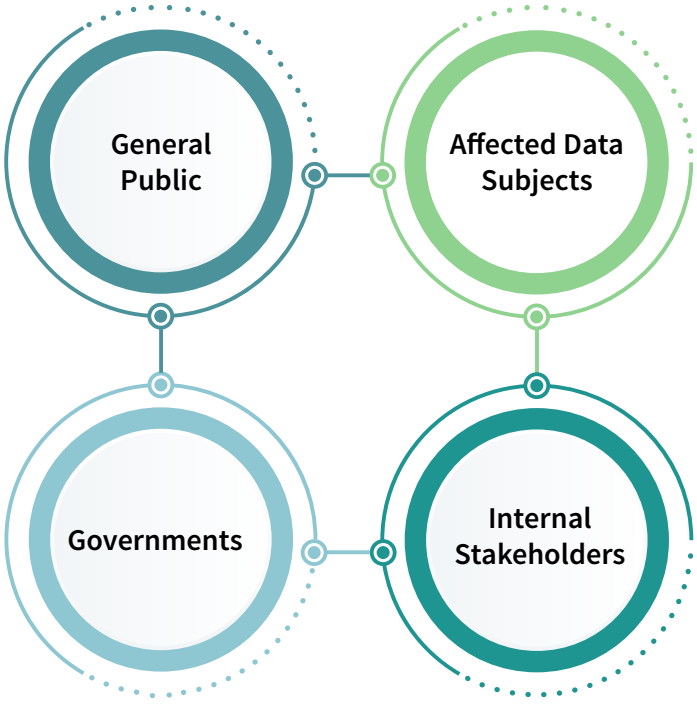
The second portion of the Recover function is a call to improve the other four disciplines — Identify, Protect, Detect, and Respond — by weaving your new knowledge into your cyber defenses, along with your recovery plans for future incidents. It's at this point that you must once again ask yourself the 5 essential questions:

- ***What could happen?*** ▸ *Security posture*
- ***What should happen?*** ▸ *Security policy*
- ***What would happen?*** ▸ *Security modeling*
- ***What is happening?*** ▸ *Security monitoring*
- ***What did happen?*** ▸ *Security investigations*

COMMUNICATION

"Restoration activities are coordinated with internal and external parties." – NIST CSF

Finally, probe your communications for weaknesses so you can more effectively transfer information in the future. The goal of communication is information transfer. There are four groups of stakeholders you need to think about during your recovery: the general public, affected data subjects, governments, and internal stakeholders. Adopt consecutive, logically-flowing statements. There is nothing to gain from finger-pointing, shifting blame, or vying for sympathy. Be honest and outline the steps you're taking to lower the probability of a repeat occurrence.



CONCLUSION

Don't view the NIST CSF as a huge mountain to climb. You are already performing many of the functions — and you have been for many years. The framework simply documents your functions and processes so your security disciplines are formalized, sustainable, and scaleable. It also helps your resource-constrained teams to work more effectively and efficiently with a simple, repeatable model based on the principle of doing the right things right.

By wrapping a structure around your team's abilities, the processes you've developed, and the technologies you've invested in, you will deliver world-class data protection for your organization.

ARE YOU READY TO START IMPLEMENTING THE NIST CYBERSECURITY FRAMEWORK IN YOUR ORGANIZATION?

Find out by using our checklist.

GET IT NOW

The information in this white paper is provided for informational purposes only. The materials are general in nature; they are not offered as advice on a particular matter and should not be relied on as such. Use of this white paper does not constitute a legal contract or consulting relationship between Absolute and any person or entity. Although every reasonable effort is made to present current and accurate information, Absolute makes no guarantees of any kind. Absolute reserves the right to change the content of this white paper at any time without prior notice. Absolute is not responsible for any third party material that can be accessed through this white paper. The materials contained in this white paper are the copyrighted property of Absolute unless a separate copyright notice is placed on the material.

/ABSOLUTE®

ABOUT ABSOLUTE

Absolute enables a world where security and IT professionals always retain control over their devices and data. We're the first and only company to offer uncompromised visibility and near real-time remediation of security breaches at the source.

Absolute Persistence® returns devices to their desired state of safety and efficacy after malicious attacks or user error, thanks to our unique location in the firmware of more than 500 million devices built by most of the world's top device manufacturers.

EMAIL:
sales@absolute.com

SALES:
absolute.com/request-a-demo

PHONE:
North America: 1-877-660-2289
EMEA: +44-118-902-2000

WEBSITE:
absolute.com

© 2020 Absolute. All rights reserved. Absolute and Persistence are registered trademarks of Absolute. Self-healing Endpoint Security is a trademark of Absolute. All other trademarks are property of their respective owners. ABT-NIST-Cybersecurity-Framework-WP-E-052020.