netwrix

Kickstart Guide to Implementing the NIST Cybersecurity Framework

About the Author

Joe Skeen

Joe is a Principal Security Engineer at 7 Minute Security. Joe has over 20 years of experience in IT, leadership and cybersecurity. He has held a wide variety of positions - from Senior Security Architect to vCISO. At 7 Minute Security, Joe specializes in network and web application penetration testing and vCISO consulting. In his role Joe performs frequent NIST CSF assessments. Joe also holds the CISSP, OSCP, CRTP and CEH certifications.

Table of Contents

Introduction

I am going to say it right up front: I am biased. I think the NIST Cybersecurity Framework (NIST CSF) is quite simply the best framework for improving cybersecurity maturity. In my many years of cybersecurity, I have worked with nearly all of the frameworks and regulations. If you are interested in wholistically improving your cybersecurity program, the NIST CSF is the way to do it.

While initially targeted at critical infrastructure, the NIST CSF quickly found its place into all business sectors. The NIST CSF appears to be daunting at first glance. However, this white paper will demonstrate how business of all sizes can implement the NIST CSF with very little effort.

Before we can talk about implementing the NIST CSF, we need to understand what it is. Here is a brief description of its purpose from the NIST website:

"*Recognizing the national and economic security of the United States depends on the reliable function of critical infrastructure, the President issued Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, in February 2013. The Order directed NIST to work with stakeholders to develop a voluntary framework – based on existing standards, guidelines, vendor practices – for reducing cyber risks to critical infrastructure. The Cybersecurity Enhancement Act of 2014 reinforced NIST's EO 13636 role*."

NIST is ideally suited for the task of developing this framework since one of its primary objectives is developing standards and frameworks like this.

Benefits of the NIST CSF

People often ask me why they should use the NIST CSF. "*There are so many frameworks to choose from; why would I choose this one?*" And the answer is quite simple: Almost every other framework uses a binary measurement, and they are all about compliance. A binary measurement basically asks, "*Are we compliant with this activity or not?*" And that is simply not good enough in today's cybersecurity environment. Cybersecurity programs need to have a strategy and a maturity model that goes beyond checkbox programs. And I believe the NIST CSF does just that.

Moreover, NIST CSF offers the following unique benefits not found in other frameworks:

- ***Customizable*** *- The NIST CSF can be completely customized however you want; no other framework allows for such flexibility.*
- ***Easily understandable*** *- The language was written to be easily understood by everyone, not just auditors.*
- ***Risk-based*** *- As part of your customization, you get to decide where the priorities should be, and not all of the controls have equal weighting. We will go into more detail on this later.*

NIST CSF Components

The NIST CSF is made up of 3 major components: core, tiers and profiles, as shown in Figure 1.

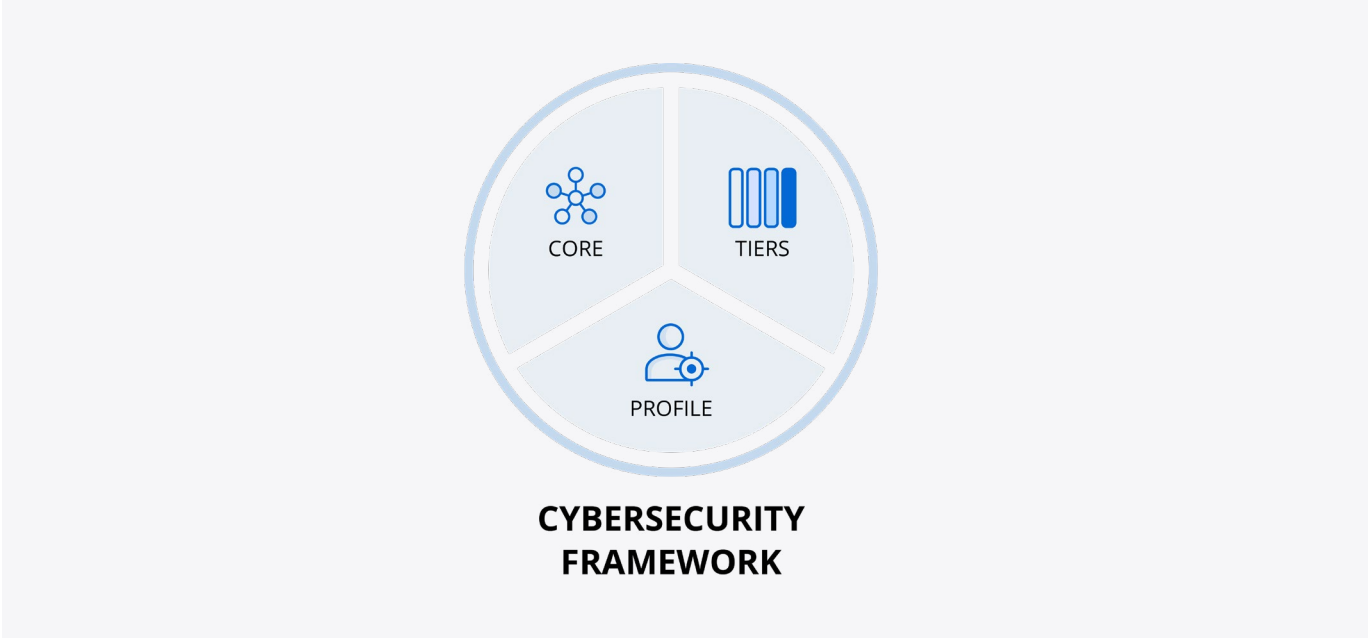


Figure 1

Core

The bulk of the NIST CSF is known as the core. The core is also probably the most recognizable portion. As noted earlier, the core is meant to be written in common and accessible language. The core of the framework is most often recognized by its five functions as shown in Figure 2. These functions are groupings of activities or outcomes.

Each function is divided into 23 categories. For example, under the identify function, there are categories like asset management, business environment, governance, risk assessment, risk management strategy and supply chain risk management. These 23 categories are further subdivided into 108 sub-categories.

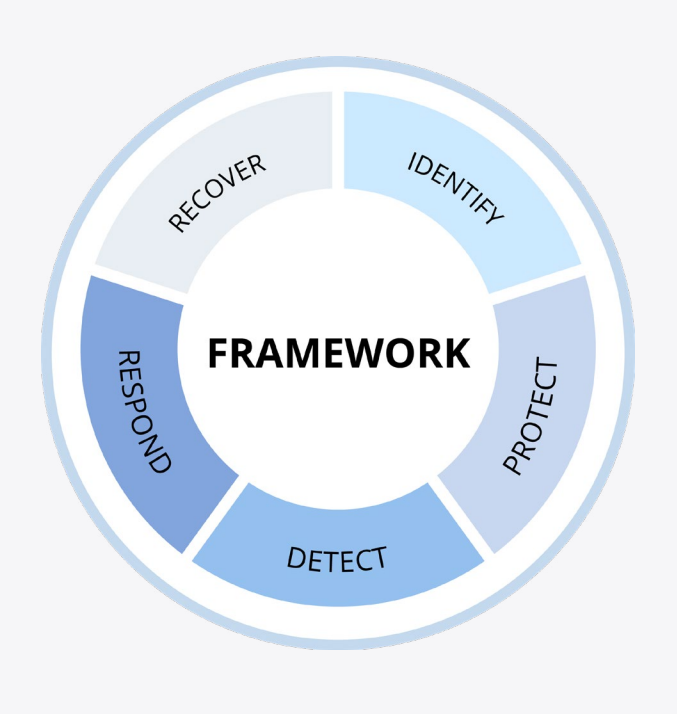


Figure 2

This sounds daunting at first, but it is not as bad as it sounds. If we look at the graphic in Figure 3, we can see that the functions and categories fit together into easy-to-understand areas:

- ***Identify*** *is all about assets, strategy and risk management.*
- ***Protect*** *is focused on identity management, awareness, and protective technology.*
- ***Detect*** *is all about how you will detect when something bad is happening in your environment.*
- ***Respond*** *covers the "how" of responding to events, incidents and breaches.*
- ***Recover*** *deals with cleaning up after an incident and improvement and communication processes.*

Function	Category	ID
IDENTIFY	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
PROTECT	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes and Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
DETECT	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
RESPOND	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
RECOVER	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Figure 3

To see how the NIST CSF can be easily understood and customized, let's take a deeper dive into one specific category of the NIST CSF, the asset management category under the Identify function. According to NIST, the Identify function "*assists in developing an organization understanding of managing risks to systems, people, data and capabilities*." Now is a good time to mention that the framework focuses on outcomes. The outcome measurements in the Identify area are as follows:

- *Identify physical and software assets (asset management program)*
- *Identify policies for governance*
- *Create a risk management strategy.*

The first category in the *Identify* function is asset management (ID.AM) as shown in Figure 4, which is taken from the downloadable spreadsheet on the NIST CSF website. As you can see, the desired outcome of asset management is: "*The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with the relative importance to organizational objectives and the organization's risk strategy.*" That is a mouthful, but it explains what NIST thinks is important about that category. You might think of this as, "*Do we have an asset management program that assigns relative risks to assets?*"

Please keep in mind that a core principle of NIST CSF is you can **fully customize it to your organization's needs**. If you want to change the outcome, feel free. I may repeat myself several times on this, but you can — and should — make the NIST CSF your own.

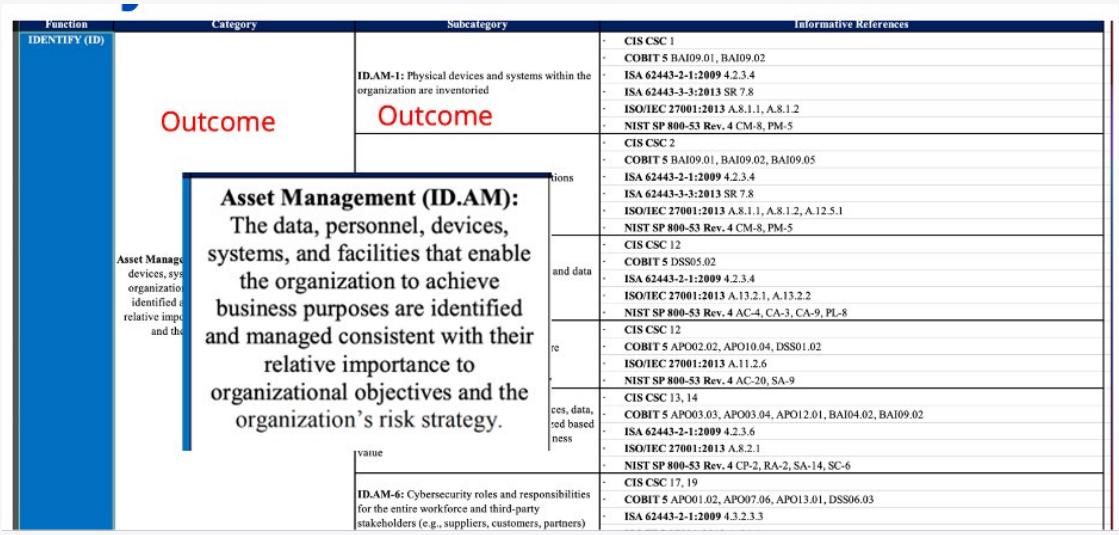


Figure 4

The first subcategory, ID-AM-1, gives you the desired outcome: *Physical devices and systems within the organization are inventoried*. Notice that this description holds true to the principle of common and accessible language. Physical device inventory is easy to understand, and later we will talk about measuring how well you do inventory. Remember, this is not a binary measurement system. We want to know how mature we are in this area.

The last column in the spreadsheet, as shown in Figure 4, is Informative References. This can be confusing to first-time users of the NIST CSF: Why does the NIST CSF reference other frameworks like COBIT? The answer is simple: The NIST CSF is focused on outcomes, and the Informative Reference column lists standards, guidelines and practices that provide methods for achieving those outcomes.

Tiers

As noted earlier, a key difference between the NIST CSF and other frameworks is that instead of offering binary measurements (e.g., Do we have an inventory, yes or no?), the NIST CSF wants to help us have a more mature program by assessing the maturity of each control. Tiers describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the framework.

As shown in Figure 5, the tiers range from Partial (Tier 1) to Adaptive (Tier 4). They describe an increasing degree of rigor — specifically, how well cybersecurity risk decisions are integrated into broader risk decisions, and the degree to which the organization shares and receives cybersecurity info from external parties. Frankly, the tiers are more complex than they need to be, which leaves room for you to make them less complicated.

Figure 5

NIST is clear that the tiers are not meant to necessarily represent maturity levels, but most originations treat them as a maturity scale. According to the NIST CSF website: "*Organizations should determine the desired Tier, ensuring that the selected level meets organizational goals, reduces cybersecurity risk to levels acceptable to the organization, and is feasible to implement, fiscally and otherwise*."

Let's review the descriptions of each of the tiers based on the NIST CSF publication. We will highlight the key details for each.

Tier 1 - Partial

- ***Risk Management Processes:*** *Cybersecurity risk management is typically* ***performed in an ad hoc or reactive manner****. Furthermore, cybersecurity activities are typically* ***performed with little to no prioritization*** *based on the degree of risk that those activities address.*
- ***Integrated Risk Management Program:*** *The* ***lack of processes*** *associated with cyber risk management makes the communication and management of that risk difficult for these organizations. As a result, the organization works with cybersecurity risk management on a case-by-case basis because of the lack of consistent information.*
- ***External Participation:*** *These organizations lack a greater understanding of their role in the greater business ecosystem — its position in the supply chain, dependents, and dependencies. Without an understanding of where it sits in the ecosystem, a* ***Tier 1 organization does not share information with third parties*** *effectively (if at all) and is generally unaware of the supply chain risks that it accepts and passes on to other members of the ecosystem.*

Tier 2 - Risk Informed

- ***Risk Management Processes:*** *Risk management practices, while approved by management, are typically* ***not established as organizational-wide*** *policies at Tier 2 organizations. While risk management practices are not standard, they do directly inform the prioritization of cybersecurity activities alongside organizational risk objectives, the threat environment, and business requirements.*
- ***Integrated Risk Management Program:*** *The awareness of cybersecurity risk exists at the organizational level, but it is* ***not standardized organization-wide****, and the information around cybersecurity is only shared informally. While some consideration for cybersecurity exists in organizational objectives, it is not standard. A cyber risk assessment may occur, but it is not standard and periodically repeated.*

- ***External Participation:*** *Tier 2 organizations understand either their role in the ecosystem in terms of dependencies or dependents, but not both.* ***Organizations like this typically receive information but do not share it out****, and while they're aware of the risk associated with their supply chain, they do not typically act on it.*

Tier 3 - Repeatable

- ***Risk Management Processes:*** *Tier 3 organizations have* ***formally approved risk management practices and are expressed as policy****. These practices are regularly updated based on changes in business requirements and changing threat landscape.*

- ***Integrated Risk Management Program:*** *In this tier, there is an* ***organization-wide approach to managing cybersecurity risk****. Risk-informed policies, processes, and procedures are defined and implemented and reviewed. There are methods in place to consistently respond effectively to changes in risk, and personnel possess the knowledge and skills to perform their roles. Senior cybersecurity and business-side executives communicate regularly regarding cybersecurity risk.*

- ***External Participation:*** *Tier 3 organizations understand their role in the ecosystems and contribute to the broader understanding of risks.* ***They collaborate with other entities regularly****. These organizations are aware of the risks associated with their supply chains and* ***act formally on those risks****, including implementing written agreements to communicate baseline requirements, governance structures, and policy implementation and monitoring.*

Tier 4 - Adaptive

- ***Risk Management Processes:*** *These organizations adapt their cybersecurity practices based on* ***previous and current cybersecurity activities, including lessons learned and predictive factors. They implement a process of continuous improvement*** *– including incorporating advanced cybersecurity technologies and practices, actively adapting to a changing threat and technology landscape.*

- ***Integrated Risk Management Program:*** *Building on Tier 3, Tier 4 organizations clearly understand the link between organizational objectives and cybersecurity risk.* ***Senior executives monitor cybersecurity risk in the same context as financial risk and other organizational risks****. These organizations base budgeting decisions on an understanding of the current and potential risk environment. Cybersecurity risk is integrated into the organizational culture and evolves from an awareness of previous activities and continuous awareness.*

- ***External Participation:*** *Integrating itself further into the ecosystem beyond Tier 3, Tier 4 organizations receive, generate, and contribute to the understanding of the ecosystem around risk. Further integration of* ***sharing information to internal and external stakeholders, the organization uses real-time information*** *to understand and regularly act on supply chain risks. They also have a formalized process integrated into their documentation with their dependencies and dependents.*

Tier Summary

As you can see, we can take the complexity out of the tiers by simply taking the key sections as shown below:

	Risk Management Processes	Integrated Risk Management Program	External Participation
Tier 1	Ad Hoc	Informal or nonexistent policies, processes and procedures	Does not share with third parties
Tier 2	Risk Informed	Partial implementation of policies, processes and procedures (not organi-zation-wide)	Consumes data from third parties
Tier 3	Repeatable	Formal company-wide policies, processes and procedures	Shares with third parties
Tier 4	Adaptive	Activities inform and improve policies, process and procedures; culture of continuous improvement	Actively involved with sharing data with third parties

Profiles

Organizations should not strive to be at Tier 4 in all areas. Instead, each one determines the risk it is willing to tolerate. And that is where profiles come into play. Profiles will help you determine which areas of the CSF to focus on.

Specifically, profiles help organizations prioritize functions, categories and subcategories. Figure 6 shows an example provided on the NIST website of one way to create a profile. The subcategory is 1 – ID-AM-1: *Physical devices and systems within the organization are inventoried*. The example shows this as a moderate priority to the organization. They have very few gaps, so physical asset management would be easy to implement. The budget, however, would be large, as indicated by the multiple dollar signs — perhaps asset management software is expensive. They anticipate that they will not undertake this activity until Year 2 of the assessment period.

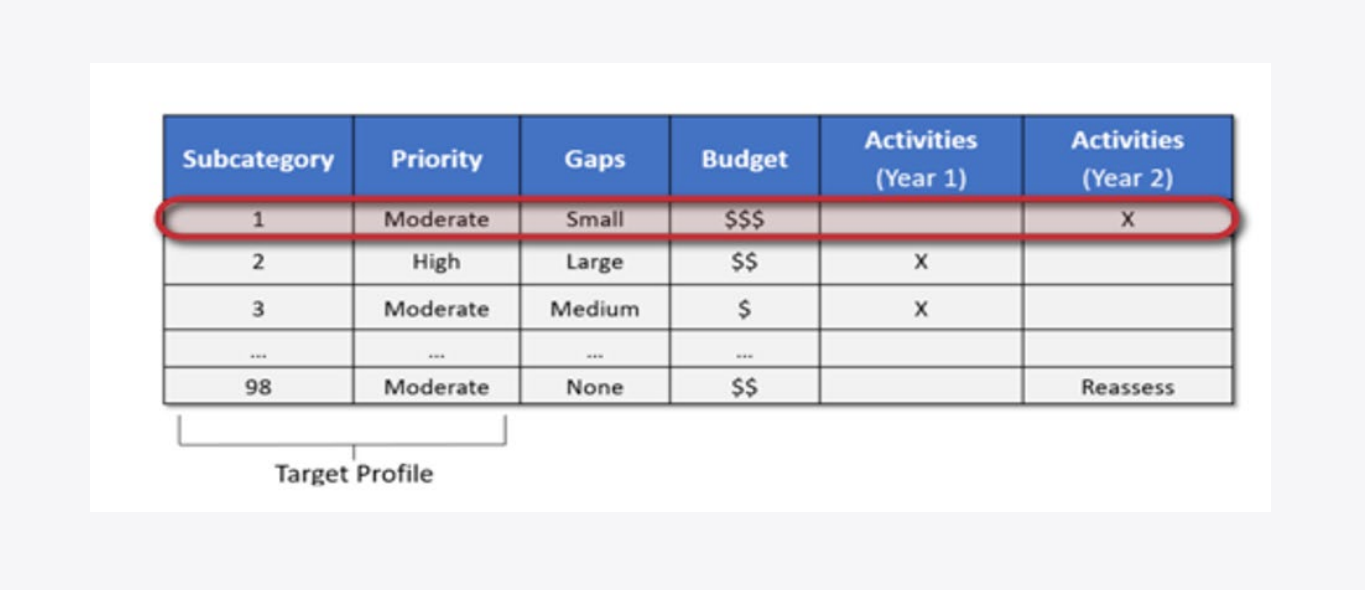


Figure 6

I like to add two columns to profiles: the current tier and the target tier. This information can be used to help shape what areas to focus on. For instance, if the gap is just too large and the financial lift is too much, maybe it will not be a priority for the organization. Do not spend too much time on profiles and get stuck in analysis paralysis. They are just meant to help you prioritize and plan.

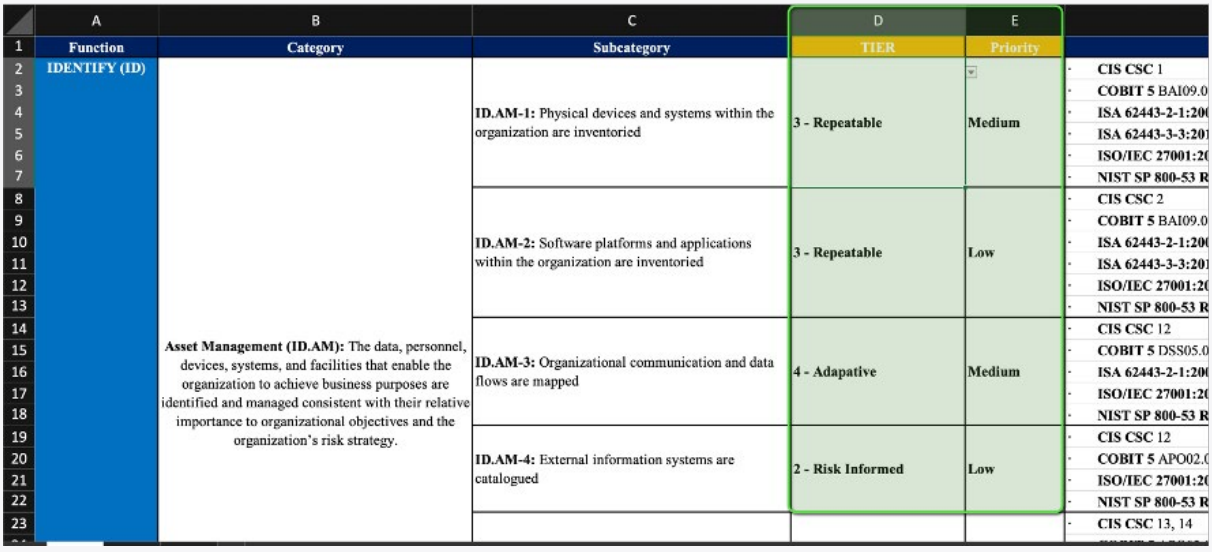
Resource Requirements

You may be wondering at this point how you are ever going to get this done, and how many resources are going to be required to reach your tier targets. And I wish there were a simple answer for that. Profiles can help you estimate how far away you are, but a task like capturing the device inventory will naturally be more resource-intensive for an organization with a 100k devices than for one with 200 devices. I can tell you that conducting a NIST CSF assessment does not have to be complicated or even that time-consuming. However, moving from Tier 2 to Tier 3 will require some support and may not be easy. The only way to mature your program is to invest the time in the areas that are a priority in your target profile.

Simple Steps to Success

Let's put all of what we have learned into action. Download the NIST CSF spreadsheet. It is set up as a "pick list," which is really easy to use. If you need help, just do a web search on "how to make drop-down list in Excel" to find four simple steps that will make the data entry go much faster.

Insert two columns called *tier* and *priority*, as shown in Figure 7. For each of the 108 subcategories, fill in a value for each of those new columns. Just make your best guess for a first pass. The real work is not conducting a CSF assessment; it's maturing the areas that are not at your target levels.



	A	B	C	D	E	
1	Function	Category	Subcategory	TIER	Priority	
2	IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	3 - Repeatable	Medium	CIS CSC 1
3						COBIT 5 BAI09.0
4						ISA 62443-2-1:20(
5						ISA 62443-3-3:201
6						ISO/IEC 27001:2(
7						NIST SP 800-53 R
8			ID.AM-2: Software platforms and applications within the organization are inventoried	3 - Repeatable	Low	CIS CSC 2
9						COBIT 5 BAI09.0
10						ISA 62443-2-1:20(
11						ISA 62443-3-3:201
12						ISO/IEC 27001:2(
13						NIST SP 800-53 R
14			ID.AM-3: Organizational communication and data flows are mapped	4 - Adapative	Medium	CIS CSC 12
15						COBIT 5 DSS05.0
16						ISA 62443-2-1:20(
17						ISO/IEC 27001:2(
18						NIST SP 800-53 R
19			ID.AM-4: External information systems are catalogued	2 - Risk Informed	Low	CIS CSC 12
20						COBIT 5 APO02.0
21						ISO/IEC 27001:2(
22						NIST SP 800-53 R
23						CIS CSC 13, 14

Figure 7

Summary

The NIST CSF is made up of core, tiers and profiles. The *core* is the bulk of the NIST CSF and is made up of five categories and 108 sub-categories. *Tiers* help you measure maturity, and *profiles* help you set priorities. You do not have to make it any more complicated than that. And remember, you can and should make it your own.

Keep this last graphic in mind when you undertake your NIST CSF journey.

1. **Start simple:** Just download the spread sheet and give it a shot.
2. **Don't make it overly complicated:** If it feels like it's getting hard, you are making it too complex.
3. **Make the CSF your own:** If you don't like something, change it. They tell you to!
4. **It's a journey:** It may take some time but that does not mean it has to be hard!

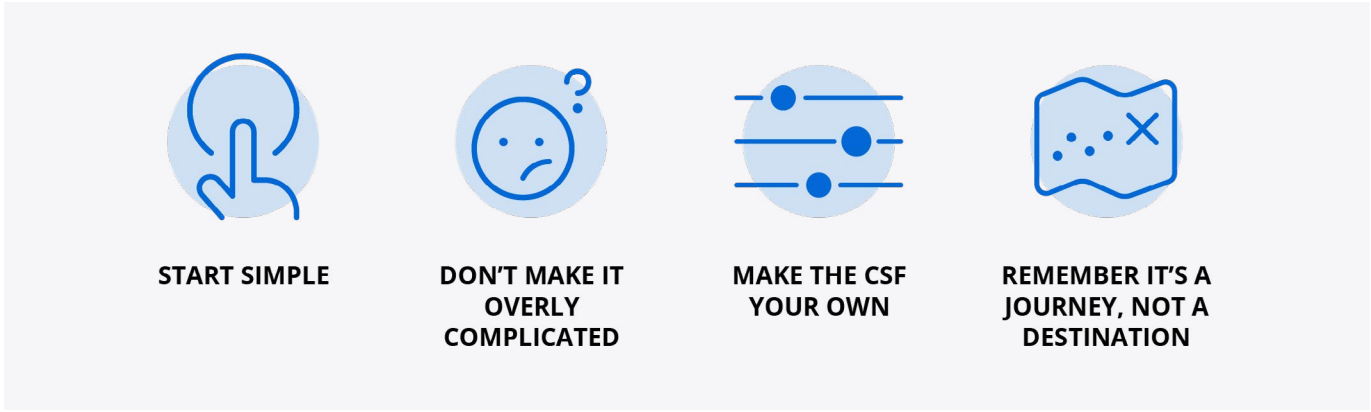


Figure 8

How the Netwrix Data Security Platform can help you implement the NIST CSF

Netwrix functionality helps organizations adopt many NIST CSF recommendations with less effort. In particular, you can:

- **Identify** both data and infrastructure security gaps, and prioritize mitigating the ones that put you at greatest risk.
- **Protect** your sensitive data by reducing your attack surface and minimizing the risk of a breach.
- **Detect** data threats faster by staying on top of improper changes and anomalous activity.
- **Respond** to incidents faster by getting valuable context during the investigation and by automating response to anticipated threats.
- **Recover** from security incidents more efficiently and learn from past incidents.

Download free 20-day trial

Discover more useful information on this topic:

Webinar - Practical Tips for Implementing the NIST Cybersecurity Framework

Feature Mapping - NIST CSF Controls and Netwrix Functionality Mapping

Blogpost - What Is the NIST Cybersecurity Framework?

About Netwrix

Netwrix is a software company that enables information security and governance professionals to reclaim control over sensitive, regulated and business-critical data, regardless of where it resides. Over 10,000 organizations worldwide rely on Netwrix solutions to secure sensitive data, realize the full business value of enterprise content, pass compliance audits with less effort and expense, and increase the productivity of IT teams and knowledge workers.

Founded in 2006, Netwrix has earned more than 150 industry awards and been named to both the Inc. 5000 and Deloitte Technology Fast 500 lists of the fastest growing companies in the U.S.
For more infroamtion, visit www.netwrix.com.

Next Steps

Free trial — Set up Netwrix in your own test environment: netwrix.com/freetrial

In-Browser Demo — See the unified platform in action, no deployment required: netwrix.com/browser_demo

Live Demo — Take a product tour with a Netwrix expert: netwrix.com/livedemo

Request Quote — Receive pricing information: netwrix.com/buy

CORPORATE HEADQUARTER:

300 Spectrum Center Drive
Suite 200 Irvine, CA 92618

565 Metro Place S, Suite 400
Dublin, OH 43017

5 New Street Square
London EC4A 3TW

PHONES:

1-949-407-5125
Toll-free (USA): 888-638-9749

1-201-490-8840

+44 (0) 203 588 3023

OTHER LOCATIONS:

Spain:	+34 911 982608
Netherlands:	+31 858 887 804
Sweden:	+46 8 525 03487
Switzerland:	+41 43 508 3472
France:	+33 9 75 18 11 19
Germany:	+49 711 899 89 187
Hong Kong:	+852 5808 1306
Italy:	+39 02 947 53539

SOCIAL:

netwrix.com/social