Why use NIST's Cybersecurity Framework

Which Framework is right for you?

NIST CSF

NIST offers a helpful guide to help an organization prioritize activities based on importance to business continuity and security. It provides a common language to address cybersecurity risk management, which is understood by those within and outside the organization.

ISO – 27000 FAMILY

The International Standards Organization developed this ISO 27000 series. Because it is broad in scope, any type or size of organization can benefit from being familiar with it and adopting its recommendations, as appropriate to your industry and business type.

SOC 2 and SOC 3

AICPA Trust Services Principles and Criteria (SOC) is a set of controls that is utilized in SOC 2 and SOC 3 engagements. It is a set of five trust principles with focus on Security, Availability, Confidentiality, Processing Integrity and Privacy. SOC 2 focuses on a business's non-financial reporting controls as they relate to security, availability, processing integrity, confidentiality, and privacy of a system, as opposed to SOC 1/SSAE 18 which is focused on the financial reporting controls.

Selecting a framework is not always easy

An information security framework, when implemented properly, will allow any security leader to more intelligently manage their organizations cyber risk.

The framework consists of a number of documents that clearly define the adopted policies, procedures, and processes by which your organisation abides. It effectively explains to all parties (internal, tangential and external) how information, systems and services are managed within your organisation.

The main point of having an information security framework in place is to reduce risk levels and the organizations exposure to vulnerabilities. The framework is not your go-to document in an emergency (you should have an Incident Response Plan for that), but it outlines daily procedures designed to reduce your exposure to risk.

Implementing a solid information security framework provides a host of advantages if you are trying to instill confidence in an industry or establish a strong reputation with potential business partners and customers. The framework allows these business partners and customers to understand how you will protect their data or services from harm.

See it perhaps like this: if anyone asks you at any time what would you do if X-cyber-disaster happened, any authorized person in your organization would be able to look up the procedure in the framework and present the exact same response to a third party.

There are hundreds information security frameworks in existence today. Finding the right one for your organization is not always an easy task for the uninitiated. They are not all compartmentalized across one matrix. There are geographical frameworks, industry-wide frameworks, and technology frameworks.

The first step is to get familiar with the more well known frameworks available. Of course, there is a ton of overlap between frameworks, and that is actually an advantage. Once you align with your preferred framework, you can more easily align with additional ones, such as those that provide certification, for example.

Most frameworks out there are tailored for specific environments, industries or technologies, but the key benefits often include:

- ensure you have robust security policies, procedures, and standards in place,
- address operational framework maturity, maintenance and strategy,
- improve overall security posture against the evolving cyber threat,
- reduce overall operational risk,
- facilitate business and service partnerships by giving third parties detailed, and information on your cybersecurity posture.

TBG SECURITY

Is NIST the right choice for your organization?

"Let's be honest here: navigating the sea of NIST resources and guidelines can be pretty daunting. But we know this stuff better than the back of our hands. Since its inception in 2014, we've helped many, many organizations - from retail to finance - create a solid cyber framework with NIST. "

- Kevin Gorsline VP Compliance Services

"The Cybersecurity Framework from NIST consists of standards, guidelines, and best practices to manage cybersecurity-related risk. The Cybersecurity Framework is prioritized, flexible, and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security."

nist.gov/cyberframework

Why NIST Cybersecurity Framework makes sense for your organization.

NIST is one of the most mature security frameworks currently available. It is widely used by federal and state organizations. It is also used as a baseline for other security frameworks - once implemented, it can radically simplify adherence to other compliance regulations, such as GDPR, PCI-DSS, HIPAA, or Federal and state regulations, among others.

The NIST Cybersecurity Framework is not just for large corporations. Organizations of all sizes, sectors, and maturities can benefit from NIST guidelines. This framework, designed to reduce risk to critical infrastructure, is versatile and customizable, perfect for any organizations regardless of sector or size because it has been designed to be financially and resource efficient.

In short, broad use of the NIST Cybersecurity Framework serves as a great model to strengthen critical infrastructure, increase interoperability and innovation. It also encourages efficient and effective use of resources. TBG Security recommends that it be implemented as a sustainable information security baseline.

The framework itself is divided into three components: core, implementation tiers, and profiles.

RISK MANAGEMENT AND THE NIST CSF

Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, organizations should understand the likelihood that an event will occur and the resulting impact. With this information, organizations can determine the acceptable level of risk for delivery of services and can express this as their risk tolerance.

NIST was created with scalability and gradual implementation so any business can benefit.

With an understanding of risk tolerance, organizations can prioritize cybersecurity activities, enabling organizations to make informed decisions about cybersecurity expenditures. Implementation of risk management programs offers organizations the ability to quantify and communicate adjustments to their cybersecurity programs. Organizations may choose to handle risk in different ways, including mitigating the risk, transferring the risk, avoiding the risk, or accepting the risk.

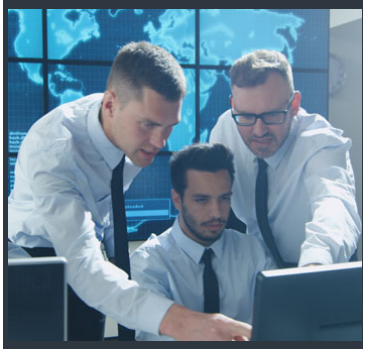
GET YOUR CYBERSECURITY FRAMEWORK IMPLEMENTED

When people ask us how long it will take to implement, it can be a complex answer, and for a very simple reason: Everybody is different.

Every organization's cybersecurity resources, capabilities, and needs are different. How long it will take to implement the framework will vary depending on the size, focus and requirements of your organization, ranging from as short as a few weeks to several years. It can be vastly more efficient if someone leading the team is very experienced with NIST.

HOW LONG WILL IT TAKE TO IMPLEMENT?

Each organization's cybersecurity resources, capabilities, and needs are different. So the time to implement the Framework will vary among organizations, ranging from as short as a few weeks to several years. The Framework Core's hierarchical design enables organizations to apportion steps between current state and desired state in a way that is appropriate to their resources, capabilities, and needs. This allows organizations to develop a realistic action plan to achieve Framework outcomes in a reasonable time frame, and then build upon that success in subsequent activities.



About TBG Security

Where possible, TBG designs and delivers solutions to work in harmony with your existing operations. Fortune® 2000 companies depend on TBG services in areas including:

- Risk Management
- Penetration Testing
- Red Team Services
- Data Breach Protection
- Splunk Managed Services
- CISO On Demand

How TBG Security can help

- We can assess the effectiveness and efficiency of your use of existing cybersecurity standards, guidelines, and practices, if any are in place.
- We can work with you to quickly identify which cybersecurity-related activities critical to your critical business operations.
- We can help you allocate your cybersecurity investments based on your operational priorities.
- We can provide guidance in mapping and prioritising key technologies, making sure they are properly defended from unauthorized access or tampering.
- We can guide you in educating staff and stakeholders, so they fulfill their information security requirements through best practice.

Whatever route you choose, the most important first step to graduating your operations to the next level is ensuring the implementation of a robust cybersecurity framework, like NIST.

TBG SECURITY

31 Hayward St
Franklin, MA 02038
877.233.6651 ph
508.355.5782 fax
https://tbgsecurity.com
info@tbgsecurity.com

Resources:

https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf
https://www.nist.gov/cyberframework
https://www.qmulos.com/wp-content/uploads/2017/05/cybersecurity-framework-021214_version_1.0.pdf