THE NATIONAL CYBERSECURITY SOCIETY

NIST Cybersecurity Framework

What is the NIST Cybersecurity Framework?

The National Institute of Standards and Technology (NIST), a non-regulatory U.S. government agency, developed the framework in 2014 to promote innovation and industrial competitiveness. NIST's "Framework for Improving Critical Infrastructure Cybersecurity" ("Cybersecurity Framework") offers guidance for how U.S. private sector organizations can assess and improve their ability to prevent, detect, and respond to cyber-attacks.

Recognizing the dependence of U.S. national and economic security on the reliable function of critical infrastructure, the President directed NIST to work with stakeholders to develop a voluntary Cybersecurity Framework (Framework) for reducing cyber risks. Created through collaboration between industry and government, the Framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk.

The NCSS Cares Assessment is modeled on the Framework; as well as the educational aids the NCSS develops for our community.

FACT 1: Framework Components

The Cybersecurity Framework consists of three main components: the Core, Implementation Tiers, and Profiles.

- The Framework **Core** provides a set of cybersecurity activities and outcomes using common language that is easy to understand. The Core guides organizations in managing and reducing their cybersecurity risks in a way that complements an organization's existing cybersecurity and risk management processes.
- The Framework **Implementation Tiers** assist organizations by providing context on how an organization views cybersecurity risk management. The Tiers guide

Did you know?

√ NCSS CARES assessment is based on the NIST Cybersecurity Framework

√ The Framework can be applied to organizations of all sizes

√ This resource was developed from the NIST website. For more information about the Framework, see

https://www.nist.gov/cyberframework/online-learning/components-framework

√ The Framework was recently updated to include supply chain risks

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.

JOIN THE NCSS

Become a member of **The National Cybersecurity Society** today and learn more about how to protect your business from a cyber attack.

NIST Cybersecurity Framework continued....

organizations to consider the appropriate level of rigor for their cybersecurity program and are often used as a communication tool to discuss risk appetite, mission priority, and budget.

- Framework **Profiles** are an organization's unique alignment of their organizational requirements and objectives, risk appetite, and resources against the desired outcomes of the Framework Core. Profiles are primarily used to identify and prioritize opportunities for improving cybersecurity at an organization.

FACT 2: Core Parts

The Core consists of three parts: Functions, Categories, and Subcategories. The Core includes five high level functions: Identify, Protect, Detect, Respond, and Recover. These 5 functions are not only applicable to cybersecurity risk management, but also to risk management at large. The next level down is the 23 Categories that are split across the five Functions. The graphic below is from the NIST website:

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 & 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

The set of educational aids and tools developed by the NCSS are consistent with the categories and sub-categories of the Framework.

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.