WIKIPEDIA

NIST Cybersecurity Framework

NIST Cybersecurity Framework is a guidance on how both internal and external stakeholders of organizations can manage and reduce cybersecurity risk. It lists organization specific and customizable activities associated with managing cybersecurity risk and it is based on existing standards, guidelines, and practices .[1] The framework has been translated to many languages and is used by the governments of Japan and Israel, among others.[2] It "provides a high level taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes."[3] It is being used by a wide range of businesses and organizations and helps shift organizations to be proactive about risk management.[4][5][6]

A security framework adoption study reported that 70% of the surveyed organizations see NIST's framework as a popular best practice for computer security, but many note that it requires significant investment.[7] It also includes guidance on relevant protections for privacy and civil liberties.[8]

Contents

Overview

The NIST Cybersecurity Framework is designed for individual businesses and other organizations to assess risks they face.

Version 1.0 was published by the US National Institute of Standards and Technology in 2014, originally aimed at operators of critical infrastructure. In 2017, a draft version of the framework, version 1.1, was circulated for public comment. Version 1.1 was announced and made publicly available on April 16, 2018. Version 1.1 is still compatible with version 1.0.

The changes include guidance on how to perform self-assessments, additional detail on supply chain risk management, guidance on how to interact with supply chain stakeholders, and encourages a vulnerability disclosure process.

The framework is divided into three parts, "Core", "Profile" and "Tiers". The "Framework Core" contains an array of activities, outcomes and references about aspects and approaches to cybersecurity. The "Framework Implementation Tiers" are used by an organization to clarify for itself and its partners how it views cybersecurity risk and the degree of sophistication of its management approach. A "Framework Profile" is a list of outcomes that an organization has chosen from the categories and subcategories, based on its needs and risk assessments.

An organization typically starts by using the framework to develop a "Current Profile" which describes its cybersecurity activities and what outcomes it is achieving. It can then develop a "Target Profile", or adopt a baseline profile tailored to its sector (e.g. infrastructure industry) or type of organization. It can then define steps for switching from its current profile to its target profile.

Functions and categories of cybersecurity activities

The NIST Cybersecurity Framework organizes its "core" material into five "functions" which are subdivided into a total of 23 "categories". For each category, it defines a number of subcategories of cybersecurity outcomes and security controls, with 108 subcategories in all.

For each subcategory, it also provides "Informative Resources" referencing specific sections of a variety of other information security standards, including ISO 27001, COBIT, NIST SP 800-53, ANSI/ISA-62443, and the Council on CyberSecurity Critical Security Controls (CCS CSC, now managed by the Center for Internet Security). Special Publications (SP) aside, most of the informative references requires a paid membership or purchase to access their respective guides. The cost and complexity of the framework has resulted in bills from both houses of Congress that direct NIST to create Cybersecurity Framework guides that are more accessible to small and medium businesses.[9][10]

Here are the functions and categories, along with their unique identifiers and definitions, as stated in the framework document.[11]

Identify

"Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities."

- 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 business objectives and the organization's risk strategy.
- Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
- Governance (ID.GV): 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 risk.
- Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
- Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
- Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated

with managing supply chain risk. The organization has in place the processes to identify, assess and manage supply chain risks.

Protect

"Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services."

- Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.
- Awareness and Training (PR.AT): 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.
- Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
- Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
- Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.
- Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

Detect

"Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event."

- Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.
- Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.
- Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

Respond

"Develop and implement the appropriate activities to take action regarding a detected cybersecurity incident."

- Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.
- Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.
- Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.
- Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.

- Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

Recover

"Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident."

- Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.
- Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.
- Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.

Online Informative References

In addition to informative references in the framework's core, NIST also maintains an online database of informative references.[12] Informative References show relationships between Framework Functions, Categories, and Subcategories and specific sections of standards, guidelines, and best practices common among Framework stakeholders. Informative References illustrate ways to achieve Framework outcomes.

- Informative References Home (https://www.nist.gov/cyberframework/informative-references)
- Derived Relationship Mapping (https://csrc.nist.gov/Projects/Cybersecurity-Framework/derived-relationship-mapping)
- Informative Reference Catalog (https://csrc.nist.gov/Projects/Cybersecurity-Framework/Informative-Reference-Catalog)

See also

- Cyber security standards
- NIST Privacy Framework
- Critical infrastructure protection
- ISO/IEC 27001:2013: an information security standard from the International Organization for Standardization
- COBIT: Control Objectives for Information and Related Technologies - a related framework from ISACA
- NIST Special Publication 800-53: “Security and Privacy Controls for Federal Information Systems and Organizations."

References

This article incorporates public domain material from the National Institute of Standards and Technology document: "NIST Cybersecurity Framework" (https://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf) (PDF).

1. Gordon, Lawrence A; Loeb, Martin P; Zhou, Lei (January 1, 2020). "Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model" (https://doi.org/1

0.1093/cybsec/tyaa005). *Journal of Cybersecurity*. **6** (tyaa005). doi:10.1093/cybsec/tyaa005 (https://doi.org/10.1093%2Fcybsec%2Ftyaa005). ISSN 2057-2085 (https://www.worldcat.org/issn/2057-2085).

2. "NIST Cybersecurity Framework" (https://www.nist.gov/document/sessioniii-barrettcsfpdf).
3. "Achieving Successful Outcomes With the NIST Cybersecurity Framework" (https://www.govloop.com/resources/achieving-successful-outcomes-with-the-nist-cybersecurity-framework/). *GovLoop*. Retrieved June 12, 2021.
4. "Workshop plots evolution of NIST Cybersecurity Framework" (http://fedscoop.com/nist-workshop-plots-evolution-of-cybersecurity-framework). *FedScoop*. Retrieved August 2, 2016.
5. HealthITSecurity. "NIST Cybersecurity Framework Updates, Clarification Underway" (http://healthitsecurity.com/news/nist-cybersecurity-framework-updates-clarification-underway). Retrieved August 2, 2016.
6. PricewaterhouseCoopers. "Why you should adopt the NIST Cybersecurity Framework" (http://www.pwc.com/us/en/increasing-it-effectiveness/publications/adopt-the-nist.html). Retrieved August 4, 2016.
7. "NIST Cybersecurity Framework Adoption Hampered By Costs, Survey Finds" (http://www.darkreading.com/attacks-breaches/nist-cybersecurity-framework-adoption-hampered-by-costs-survey-finds/d/d-id/1324901). Information Week Dark Reading. Retrieved August 2, 2016.
8. HealthITSecurity. "HIMSS: NIST Cybersecurity Framework Positive, Can Improve" (http://healthitsecurity.com/news/himss-nist-cybersecurity-framework-positive-can-improve). Retrieved August 2, 2016.
9. "MAIN STREET Cybersecurity Act of 2017" (https://www.congress.gov/bill/115th-congress/senate-bill/770). *congress.gov*. Retrieved October 5, 2017.
10. "NIST Small Business Cybersecurity Act of 2017" (https://www.congress.gov/bill/115th-congress/house-bill/2105). *congress.gov*. Retrieved October 5, 2017.
11. National Institute for Standards and Technology (NIST) (April 16, 2018). "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1" (https://doi.org/10.6028/NIST.CSWP.04162018). *NIST*. Gaithersburg, MD. doi:10.6028/nist.cswp.04162018 (https://doi.org/10.6028%2Fnist.cswp.04162018).
12. nicole.keller@nist.gov (November 27, 2017). "Informative References" (https://www.nist.gov/cyberframework/informative-references). *NIST*. Retrieved April 17, 2020.

External links

- Official website (https://www.nist.gov/cyberframework/)
- How To Use (And Not Use) The NIST Cybersecurity Framework | FRSecure LLC | Information Security Management (http://www.frsecure.com/how-to-use-and-not-use-the-nist-csf/)
- Harnessing the Power of the NIST Cybersecurity Framework (https://clearwatercompliance.com/nist-cybersecurity-framework/)
- A 10 Minute Guide to the NIST Cybersecurity Framework (https://threatsketch.com/free-nist-cybersecurity-framework-tools-and-resources/)

Retrieved from "https://en.wikipedia.org/w/index.php?title=NIST_Cybersecurity_Framework&oldid=1029615373"

This page was last edited on 21 June 2021, at 02:04 (UTC).