STANDARD SUMMARY · CERT.GT

NIST CSF 2.0 overview

Version 1.0 · Reviewed Oct 11, 2026 · TLP:CLEAR · For: Management and security officers in organizations of any size.

The NIST Cybersecurity Framework organizes everything an organization does to manage its cybersecurity risk into six functions that are easy to explain to management. It is free, voluntary and cannot be certified. Version 2.0 was published in February 2024 and is no longer aimed only at critical infrastructure.

The six functions

Govern (GV)	Establish the risk management strategy, expectations and policy. It is the new function and underpins the others.
Identify (ID)	Know what you have: assets, data, suppliers and the risks they face.
Protect (PR)	Apply safeguards: access, training, data security and platform security.
Detect (DE)	Find and analyze possible attacks and compromises.
Respond (RS)	Take action on a detected incident: manage it, analyze it, communicate it and mitigate it.
Recover (RC)	Restore the affected assets and operations.

How it is organized

- Six functions, 22 categories and 106 subcategories. Each subcategory is an expected outcome, not an instruction.
- Govern: organizational context, risk management strategy, roles and responsibilities, policy, oversight and supply chain risk.
- Identify: asset management, risk assessment and improvement.
- Protect: identity and access control, awareness, data security, platform security and infrastructure resilience.
- Detect: continuous monitoring and adverse event analysis.
- Respond: incident management, analysis, communication and mitigation.
- Recover: recovery plan execution and communication.

Profiles and tiers

- Current Profile: which outcomes you achieve today. Target Profile: which ones you want to achieve. The difference is your work plan.
- Tiers 1 to 4 (Partial, Risk Informed, Repeatable and Adaptive) describe how rigorous your risk management is.
- The tiers are not a mandatory maturity rating: choose the one that matches your risk and your budget.

What changed from version 1.1

- The Govern function was added, which takes cybersecurity to the top management level.
- The scope went from critical infrastructure to every type of organization.
- Greater emphasis on the supply chain.
- NIST publishes implementation examples, quick-start guides and cross-references to other frameworks.

How to get started

- Use the small business quick-start guide that NIST publishes.
- Define the scope: the whole organization or one service.
- Build the Current Profile by answering, for each category, whether the outcome is met, partly met or not met.
- Choose the Target Profile based on your main risks, not on what others are doing.
- Prioritize a few gaps, assign owners and dates, and repeat the exercise every year.

How it relates to other standards

- It does not compete with ISO 27001: the CSF provides the language and the priorities; ISO provides the certifiable management system.
- The CIS Controls work as a concrete list of actions for fulfilling the Protect and Detect functions.
- NIST maintains mapping tables to ISO 27001, the CIS Controls and other frameworks.

Official text

NIST Cybersecurity Framework 2.0 (NIST CSWP 29), free at nist.gov/cyberframework.

cert.gt is a private, community-driven initiative of Devel Group.

cert.gt · devel.group · Report an incident at cert.gt/en/reportar or email incidentes@cert.gt

Summary prepared by cert.gt for educational purposes; it is not the official text of the standard and does not replace legal or compliance advice. This is not a document from a government entity. You may copy and adapt it with attribution (CC BY 4.0).