SmartSuite

Framework / Cybersecurity / NIST Frameworks

NIST Cybersecurity Framework (CSF) v1.1

NIST Cybersecurity Framework Version 1.1 (April 16, 2018) is the superseded edition: five Functions, 23 Categories, 108 Subcategories, Tiers and Profiles. CSF 2.0 is current.



What it is

NIST Cybersecurity Framework (CSF) Version 1.1, published on April 16, 2018 as “Framework for Improving Critical Infrastructure Cybersecurity,” is a superseded edition: NIST published CSF 2.0 on February 26, 2024, and keeps version 1.1 on an archive page. The current edition is covered on the NIST CSF 2.0 page . Version 1.1 is voluntary guidance for owners and operators of critical infrastructure and organizations in any sector, and this page describes its structure for teams that still hold Profiles or assessments built on it.

The Framework grew out of Executive Order 13636, “Improving Critical Infrastructure Cybersecurity,” of February 2013, which led to Version 1.0 in February 2014. The Cybersecurity Enhancement Act of 2014 (Public Law 113-274, December 18, 2014) then directed NIST to identify a prioritized, flexible, repeatable, performance-based and cost-effective approach that owners and operators may adopt voluntarily. Version 1.1 refines and clarifies Version 1.0, and NIST made compatibility with 1.0 an explicit objective.

At a glance

PUBLISHER National Institute of Standards and Technology (NIST)	TYPE Framework	VERSION Version 1.1 (superseded by CSF 2.0)
EFFECTIVE April 16, 2018	DOMAIN Cybersecurity	FAMILY NIST Frameworks
REGION United States	ADOPTION MODEL Voluntary	IMPLEMENTATION COMPLEXITY Medium

Source: nist.gov/cyberframework/csf-11-archive

Why it matters

- **One outcome vocabulary** The Core states outcomes, not tasks. ID.AM-1, for example, reads 'Physical devices and systems within the organization are inventoried', so executives and practitioners share a plain target.
- **Profiles expose the gap** Section 2.3 compares a Current Profile with a Target Profile; the difference becomes a prioritized action plan sized to business needs and available resources.
- **Tiers describe rigor, not maturity** Section 2.2 rates risk management process, integrated risk management program and external participation from Tier 1 to Tier 4, and states that Tiers do not represent maturity levels.
- **Supply chain outcomes** Version 1.1 added the Supply Chain Risk Management Category (ID.SC) with five Subcategories covering supplier assessment, contracts, audits and joint response planning.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports NIST CSF v1.1

Subcategory Library

Load the 108 Subcategories under their five Functions and 23 Categories, each with an owner, status and linked evidence.

Current and Target Profiles

Record the outcome achieved and the outcome targeted for each Subcategory in each scope, then track the gap and action plan from steps 3 to 7 of section 3.2.

Implementation Tier Record

Document the Tier chosen for risk management process, integrated risk management program and external participation, with the reasons and the approver.

Supplier Risk Register

Track the ID.SC-1 to ID.SC-5 outcomes in Third Party Risk Management: supplier prioritization, contract measures, audits and test results, and joint response and recovery testing.

Vulnerability Handling

Log vulnerabilities received from internal and external sources (RS.AN-5) and the vulnerability management plan (PR.IP-12) in Cyber & IT Risk with owners and actions.

Transition to CSF 2.0

Keep the 1.1 Profile as a record and map each Subcategory to its CSF 2.0 outcome, using NIST's Core transition overview as the reference.

Common framework mappings

CIS Controls v8.1 · COBIT 2019 · FedRAMP Rev. 5 · GDPR · HIPAA (NIST SP 800-66 Rev. 2) · ISO 27001:2022 · NIST 800-53 Rev.5 · PCI DSS 4.0.1 · SOC 2

Official resources

NIST Cybersecurity Framework Version 1.1 (NIST CSWP 04162018)

The April 16, 2018 publication "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1": structure, core functions, tiers and profiles.

nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NIST CSF FAQs

Outlines frequently asked questions about the implementation and scope of the framework.

nist.gov/cyberframework/faqs

NIST CSF 1.1 online learning

NIST's archived online learning modules for Cybersecurity Framework version 1.1.

nist.gov/cyberframework/csf-11-online-learning

Frequently asked questions

Is NIST CSF 1.1 still the current version of the Cybersecurity Framework?

No. NIST published CSF 2.0 (CSWP 29) on February 26, 2024, and keeps version 1.1 (April 16, 2018) on a CSF 1.1 archive page. Version 1.1 is still useful for reading Profiles and assessments written against it. NIST publishes a CSF 1.1 to 2.0 Core transition overview spreadsheet for moving them to the current edition.

How is the CSF 1.1 Core organized?

Appendix A lists five Functions (Identify, Protect, Detect, Respond, Recover), 23 Categories identified in Table 1 from ID.AM to RC.CO, and 108 Subcategories, each with Informative References. NIST states in section 2.1 that the Core is not a checklist of actions to perform and that the Functions run concurrently and continuously.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What changed between CSF 1.0 and CSF 1.1?

The Note to Readers lists the updates: a clarification of what “compliance” with the Framework means, a new section 4.0 on self-assessment, an expanded treatment of cyber supply chain risk management (sections 3.3 and 3.4 and the new ID.SC Category), refinements to authentication, authorization and identity proofing (PR.AC renamed Identity Management and Access Control), a clearer link between Tiers and Profiles, and a Subcategory on coordinated vulnerability disclosure.

What are the CSF 1.1 Implementation Tiers?

Section 2.2 defines Tier 1 Partial, Tier 2 Risk Informed, Tier 3 Repeatable and Tier 4 Adaptive. Each is described across three dimensions: risk management process, integrated risk management program and external participation. NIST states that Tiers do not represent maturity levels and that success is judged against the outcomes in the Target Profile, not the Tier.

Is CSF 1.1 mandatory or certifiable?

No. The Cybersecurity Enhancement Act of 2014 directed NIST to develop an approach that owners and operators of critical infrastructure may adopt voluntarily, and the Framework places no regulatory requirements on businesses. NIST also warns that “compliance with the Framework” is an ambiguous phrase. There is no certification of the Framework itself.

License included / downloadable: Yes NIST publications are works of the U.S. government; CSF 1.1 is available free of charge from NIST, which links the PDF, the Core spreadsheet and the Quick Start Guide on its CSF 1.1 archive page.

Full framework page and mappings: smartsuite.com/frameworks/nist-cybersecurity-framework-csf-v1-1