ISO 27001:2022 vs NIST CSF 2.0

1.0, 28.0.2024

	ISO/IEC 27001:2022	NIST CSF 2.0
Type	International standard	Guide
Name	Information security, cybersecurity and privacy protection. Information security management systems. Requirements	NIST Cybersecurity Framework (CSF)
Website	www.iso.org/standard/27001	www.nist.gov/cyberframework
Description	ISO/IEC 27001 is the world's best-known standard for **information security management systems (ISMS)**. It defines requirements an ISMS must meet. The ISO/IEC 27001 standard provides companies of any size and from all sectors of activity with guidance for establishing, implementing, maintaining and continually improving an information security management system. Conformity with ISO/IEC 27001 means that an organization or business has put in place a system to manage risks related to the security of data owned or handled by the company, and that this system respects all the best practices and principles enshrined in this International Standard.	The NIST Cybersecurity Framework (CSF) 2.0 provides guidance to industry, government agencies, and other organizations **to manage cybersecurity risks**. It offers a taxonomy of high-level cybersecurity outcomes that can be used by any organization — regardless of its size, sector, or maturity — to better understand, assess, prioritize, and communicate its cybersecurity efforts. The CSF does not prescribe how outcomes should be achieved. Rather, it links to online resources that provide additional guidance on practices and controls that could be used to achieve those outcomes. This document describes CSF 2.0, its components, and some of the many ways that it can be used.
Current version	October 2022 + Amd 1:2024	2.0, February 2024
The first versions	BS 7799-1 (->27002): 1995 BS 7799-2 (->27001): 1999	1.0: February 2014 1.1: April 2018
Pages	19 (26)	27 (32)
Price	CHF 129 (150$)	Free
Framework	**Requirements** (clauses): 4. Context of the organization 5. Leadership 6. Planning 7. Support 8. Operation 9. Performance evaluation 10. Improvement **Annex A. IS Controls:** • 5. Organizational controls • 6. People controls • 7. Physical controls • 8. Technological	**CSF Core**: A taxonomy of high-level cybersecurity outcomes that can help any organization manage its cybersecurity risks. Its components are a hierarchy of Functions, Categories, and Subcategories that detail each outcome. There are six CSF Functions: Govern, Identify, Protect, Detect, Respond, and Recover. **CSF Organizational Profiles**: A mechanism for describing an organization's current and/or target cybersecurity posture in terms of the CSF Core's outcomes. **CSF Tiers**: A characterization of the rigor of an organization's cybersecurity risk governance and management practices.

Andrey Prozorov, CISM, CIPP/E, CDPSE, LA 27001
www.patreon.com/AndreyProzorov || www.linkedin.com/in/AndreyProzorov

ISO 27001:2022 vs NIST CSF 2.0

1.0, 28.0.2024

	ISO/IEC 27001:2022	NIST CSF 2.0
ISMS	Information security management systems	Cybersecurity program
IS Controls	4 Categories, 93 controls Detailed description and additional attributes are in ISO 27002	22 Categories, 106 Subcategories and 363 Implementation Examples (separate publication)
Profiles	Not used, but the Statement of Applicability (SoA) with specified statuses of controls can be used for this purpose	Yes • CSF 2.0 Organizational Profiles • CSF 2.0 Community Profiles
TIERs	Not mentioned, but the Maturity levels can be used (separate methodology)	There are four Tiers: • Partial (Tier 1) • Risk Informed (Tier 2) • Repeatable (Tier 3) • Adaptive (Tier 4)
Certification	Yes, formal audit and certification	No NIST does not offer certifications or endorsements of CSF-related products, implementations, or services, and there are no plans to develop a conformity assessment program.
Related standards and other publications	ISO 27k family, especially: • ISO 27000 (ISMS Overview and vocabulary) • ISO 27002 (IS Controls) • ISO 27003 (ISMS Guidance) Privacy: • ISO 27701 (PIMS): Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management. Requirements and guidelines Risk Management: • ISO 27005: Guidance on managing information security risks Supply chain security, ISO 27036 (set): • Part 1: Overview and concepts • Part 2: Requirements • Part 3: Guidelines for hardware, software, and services supply chain security • Part 4: Guidelines for security of cloud services	CSF Publications: • NIST's CSF 2.0 Quick Start Guides • NIST CSF 2.0 Informative References • FAQ Other NIST publications, especially: • NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations Privacy: • NIST Privacy Framework • NIST Privacy Risk Assessment Methodology (PRAM) Risk Management: • NIST SP 800-37 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy • NIST SP 800-30 Guide for Conducting Risk Assessments • NIST Risk Management Framework Supply chain security: • NIST SP 800-161 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

Andrey Prozorov, CISM, CIPP/E, CDPSE, LA 27001
www.patreon.com/AndreyProzorov || www.linkedin.com/in/AndreyProzorov