PRESCIENT SECURITY

Exploring NIST CSF, 800-171, and 800-53

What are NIST Frameworks?

The National Institute of Standards and Technology (NIST) frameworks are guidelines to help organizations manage and reduce cybersecurity risks.

NIST CSF, 800-171, and 800-53 are three frameworks crucial to risk management, information security and privacy, safeguarding sensitive information on federal contractors IT systems and networks, and enabling federal information systems and organizations to help meet the Federal Information Security Management Act (FISMA) requirements.

Key Components of NIST CSF, 800-171, and 800-53

Feature	NIST CSF	NIST 800-171	NIST 800-53
Purpose	To provide a voluntary framework for improving cybersecurity risk management across organizations.	To protect controlled unclassified information (CUI) in non-federal systems in organizations.	To provide a catalog of security and privacy controls for federal information systems and organizations.
Scope	Broad, covers all types of organizations and sectors.	Focused in non-federal organizations handling CUI.	Primarily for federal information systems, but adaptable for non-federal systems.
Assessment Type	Risk-based, ongoing assessments and continuous improvement.	Compliance-focused, typically assessed via self-assessment or third-party audit.	Comprehensive, detailed assessments, often by federal auditors or third parties.
Complexity of Controls	Moderate- flexible controls, adaptable to the organization's risk appetite and resources.	Moderate - specific to protecting CUI, but less complex than NIST 800-53.	High - extensive and detailed controls, requiring significant resources to implement and manage.
Control Families	5 Functions (Identity, Protect, Detect, Respond, Recover).	14 Families (e.g., Access Control, Incident Response, System and Communications Protection).	20 Families (e.g., Access Control, Audit and Accountability, System and Information Integrity).
Intended Audience	Any organization, particularly those looking for a flexible framework to manage cybersecurity risks.	Non-federal organizations handling CUI, including contractors and subcontractors.	Federal agencies, contractors, and any organization seeking to implement stringent cybersecurity controls.
Mapping to Other	Can be mapped to ISO 27001, COBIT, and other frameworks.	Maps to NIST 800-53 integrated with NIST CSF.	Directly maps to NIST 800-171 CUI protection, also maps to other federal and international standards.
Flexibility	High - highly adaptable to any sector and scalable according to organizational needs.	Moderate - specific to CUI protection, but with flexibility in implementation.	Low- highly prescription, designed for stringent federal compliance.