

NIST MATRIX

Is your organization considering an NIST assessment? This simple summary of the seven common frameworks can help you identity which one might best suit your needs and provide the greatest benefits.

FRAMEWORK	BUSINESS FOCUS	KEY USERS	CORE BENEFITS	STRATEGIC VALUE
NIST CSF	Cyber Risk Visibility & Prioritization	Executives, CISOs, Risk Leaders	Provides a structured, business-aligned view of cybersecurity risk to guide investment and oversight.	Aligns cybersecurity with business priorities, improves board-level communication and drives program maturity.
SP 800-171	Data Protection & Supplier Assurance	CISOs, Compliance Officers, COOs, CTOs, Contract Managers, Executives overseeing supplier/partner	Establishes consistent controls to protect intellectual property, CUI and other sensitive data shared across clients, suppliers and/or contracts.	Strengthens contract readiness, CMMC preparation and partner confidence.
SP 800-53	Enterprise Security Program Design	CISOs, Security Architects, GRC Leaders, Compliance Teams, Privacy Officers, CIOs	Offers a defensible, scalable foundation of controls for managing organizational security and privacy risks.	Supports cross-framework harmonization (e.g., ISO, HIPAA, PCI) reducing duplication and cost.
NIST RMF	Operational Risk Governance	CISOs, CTOs, System Owners, Governance Leaders, Program Managers	Provides a full lifecycle risk process that ensures systems are built, operated and maintained securely.	Increases consistency in risk decision-making, supports secure transformation and strengthens audit readiness.
NIST CLOUD	Cloud & SaaS Risk Assessment	CISOs, Cloud Architects, Procurement Teams, CTOs, Legal Counsel	Helps evaluate cloud providers, define shared responsibility and reduce vendor risk in digital transformation.	Accelerates secure cloud adoption and improves vendor accountability.
PRIVACY FRAMEWORK	Privacy by Design & Trust Management	General Counsel, Privacy officers, CISOs, CMOs, Data Governance Leaders	Helps integrate privacy into operations, mitigate regulatory risk and support customer trust initiatives.	Demonstrates accountability, supports compliance (GDPR, CCPA) and builds brand equity.
NIST AI RMF	Responsible and Risk-Aware AI Adoption	Executives, CISOs, CTOs, AI Dvelopers, Legal, Compliance and Risk Leaders	Helps identify, manage and mitigate risks related to AI systems, from design to deployment and use.	Supports trustworthy AI innovation, aligns with ethical and regulatory expectations and strengthens stakeholder trust.