S|3 SPECIALIZED SECURITY SERVICES

NIST GUIDE

NIST: WHICH FRAMEWORK BEST SUPPORTS YOUR BUSINESS?

The National Institute of Standards and Technology (NIST) provides cybersecurity standards that help organizations strengthen security, manage risk, and comply with federal regulations. NIST assessments identify vulnerabilities, improve data integrity, and enhance your overall security posture.

These evaluations can lead to better threat detection, stronger data protection, reduced regulatory risk, and greater consumer trust. However, not all NIST frameworks are the same. Each one serves different cybersecurity needs and is designed for specific industries or use cases.

That's why S3 Security created this summary guide: to help you take the first step in choosing the right NIST framework. We outline seven of the most common options and highlight which ones may offer the greatest long-term value for your business.

Contents:

NIST CyberSecurity Framework (NIST CSF) 3
NIST SP 800-171 4
NIST SP 800-53 5
NIST RMF 6
NIST Cloud (SP 800-144 and Others) 7
NIST Privacy Framework 8
NIST AI Risk Management Framework (AI RMF) 9
Summary 10

NIST CyberSecurity Framework (NIST CSF)

Purpose

A strategic, voluntary framework that helps organizations identify, assess, and improve cybersecurity risk management.

Audience

Executives, CISOs, risk leaders, and cross-functional stakeholders across all industries.

Structure

CSF 2.0 includes six core functions (Govern, Identify, Protect, Detect, Respond, Recover), 23 categories, and over 100 subcategories. It integrates cybersecurity into enterprise risk and governance.

Use Case

Enables organizations to build, benchmark, and mature cybersecurity programs aligned with business priorities.

Primary Business Drivers

- Align security programs with business strategy and risk appetite.
- Improve board-level visibility and reporting on cyber risk.
- Strengthen stakeholder trust and differentiate in competitive markets.
- Demonstrate credible security posture to clients, investors, and regulators.
- Maintain a consistent cybersecurity strategy across business units, geographies, and brand portfolios.

Assessment Use Case

Maturity assessments and gap analyses against CSF categories to support strategic planning and performance measurement.

NIST SP 800-171

Purpose

Provides a structured set of 110 controls to safeguard Controlled Unclassified Information (CUI) in nonfederal environments.

Audience

Organizations across industries that handle CUI, intellectual property (IP), or sensitive customer/partner data.

Structure

14 control families including Access Control, Incident Response, and System Integrity.

Use Case

Enables organizations to meet customer and contractual data protection requirements and prepare for CMMC.

Primary Business Drivers

- Qualify for and retain contracts that involve sensitive information.
- Meet partner and supply chain security expectations.
- Reduce risk of data leakage and loss of competitive advantage.
- Prepare for CMMC or other third-party validation processes.
- Maintain consistency in data protection practices across business units, subcontractors, or brand portfolios.

Assessment Use Case

Readiness and gap assessments to evaluate control implementation and prepare for third-party review or internal validation.

NIST SP 800-53

Purpose

A comprehensive catalog of customizable security and privacy controls used to protect enterprise systems and sensitive data.

Audience

Large or regulated organizations seeking an adaptable control set to manage system and program-level risk.

Structure

20+ control families with baselines (Low, Moderate, High) that scale to system sensitivity and business needs.

Use Case

Provides a robust foundation for internal security programs or for organizations aligning with multiple frameworks (e.g., ISO 27001, HIPAA, PCI DSS).

Primary Business Drivers

- Strengthen system-level controls and risk accountability.
- Support unified policy and control mapping across regulatory standards.
- Reduce duplication of effort across compliance requirements.
- Improve audit readiness and internal governance.
- Maintain a consistent cybersecurity strategy across business units, geographies, and brand portfolios.

Assessment Use Case

Program-level control assessments, internal audits, and crosswalk exercises for control alignment.

NIST RMF

Purpose

A 7-step lifecycle approach for managing system-level risk from planning through monitoring.

Audience

Organizations designing, operating, or securing complex systems, especially those supporting critical business functions.

Structure

Prepare, Categorize, Select, Implement, Assess, Authorize, and Monitor. Each step is tied to organizational risk and aligned with NIST SP 800-53 controls.

Use Case

Enables consistent, risk-informed decision-making across system and program lifecycles.

Primary Business Drivers

- Establish governance and accountability for high-risk systems.
- Enable secure-by-design approaches in digital transformation.
- Demonstrate executive-level oversight of security and compliance.
- Improve risk acceptance and mitigation transparency across stakeholders.

Assessment Use Case

Assessment support for each RMF phase, from system categorization to continuous monitoring.

NIST Cloud (SP 800-144 and Others)

Key Publications

- **SP 800-144**: *Guidelines on Security and Privacy in Public Cloud Computing*
- **SP 800-145**: *Definition of Cloud Computing*
- **SP 800-146**: *Cloud Computing Synopsis and Recommendations*

Purpose

Offers guidance on cloud-specific risks, deployment models, and best practices for cloud security and privacy.

Audience

Organizations adopting or assessing cloud services.

Structure

Does not have control families. Instead, it provides a general guide to cloud computing with recommendations and considerations for security.

Use Case

Not a framework per se, but a collection of guidance documents to evaluate and implement cloud computing securely.

Primary Business Drivers

- Evaluate cloud providers and ensure safe cloud adoption.
- Build or review shared responsibility models for cloud security.
- Mitigate risks related to data residency, multi-tenancy, and vendor lock-in.
- Ensure consistent security expectations across hybrid or multi-cloud environments.
- Maintain consistent risk management practices across systems owned by different business units or operational teams.

Assessment Use Case

Cloud readiness assessments, architecture reviews, or provider risk evaluations.

NIST Privacy Framework

Purpose

A risk-based framework for improving how organizations manage privacy risks and protect personal data.

Audience

Legal, compliance, governance, and executive teams focused on privacy accountability and consumer trust.

Structure

Based on CSF structure, with core functions: Identify, Govern, Control, Communicate, and Protect.

Use Case

Aligns privacy practices with business objectives, evolving regulations, and stakeholder expectations.

Primary Business Drivers

- Strengthen data governance and privacy accountability.
- Demonstrate alignment with privacy laws (e.g., GDPR, CCPA).
- Protect brand trust and avoid reputational damage.
- Enable privacy-by-design in digital product and service development.
- Ensure privacy accountability and consistent data handling practices across global operations or brand portfolios.

Assessment Use Case

Privacy program maturity assessments, governance structure reviews, policy and practice gap analysis.

NIST AI Risk Management Framework (AI RMF)

Purpose

A voluntary framework to help organizations manage risks associated with the development, deployment, and use of artificial intelligence (AI) systems in a trustworthy, transparent, and accountable way.

Audience

Organizations building, procuring, or integrating AI technologies — including technology leaders, risk managers, legal

Structure

The AI RMF is built around two main parts:

1. **Core Functions**: Govern, Map, Measure, and Manage — designed to guide organizations through identifying, assessing, and mitigating AI risks across the AI lifecycle.
2. **Profile**s: Tailored implementations for specific use cases, industries, or risk levels.

Use Case

Used to identify and mitigate unintended consequences of AI, improve transparency and accountability, and align AI development with organizational values and societal expectations.

Primary Business Drivers

- Build and deploy AI systems responsibly, with ethical and legal considerations.
- Improve transparency, fairness, and reliability in automated decision-making.
- Reduce reputational, legal, and operational risks associated with AI.
- Align AI innovation with governance, compliance, and stakeholder trust.
- Demonstrate proactive risk management in emerging technologies.

Assessment Use Case

AI risk assessments, governance reviews, impact mapping, and program design to support responsible AI use and compliance with internal or regulatory standards.

SUMMARY

When planned and executed properly, all of these NIST assessments not only provide the benefits above, but also support continuous improvement to help your organization adapt to evolving cybersecurity challenges and maintain resilient, secure systems.

But choosing the right NIST framework starts with understanding your company's unique goals, data environment and current risk profile. As a trusted advisor to regulated industries, S3 Security helps you turn these frameworks into actionable strategies that build programs demonstrating compliance, strengthening board and stakeholder confidence, and positioning you to win contracts and drive long-term success.

Still wondering which NIST framework best supports your business?

Let's talk about the path that's right for you.

INFO@S3SECURITY.COM