

# NIST SP 800-171A Rev.1

NIST SP 800-171A provides assessment procedures to evaluate implementation of security controls protecting Controlled Unclassified Information.



## What it is

NIST SP 800-171A is an assessment guideline that helps organizations evaluate the implementation and effectiveness of security requirements for protecting Controlled Unclassified Information (CUI) in non-federal systems and environments. Its primary purpose is to guide organizations and assessors in determining whether the necessary cybersecurity safeguards for CUI are in place and functioning as intended.

Published by the National Institute of Standards and Technology (NIST), NIST SP 800-171A is used by federal contractors, suppliers, assessors, and compliance professionals in connection with government contracts and regulatory mandates. The framework provides assessment procedures focused on technical, administrative, and physical security controls outlined in NIST SP 800-171, supporting risk management and compliance oversight across defense and civilian supply chains.

## At a glance

|                                                                                       |                                                               |                                                            |
|---------------------------------------------------------------------------------------|---------------------------------------------------------------|------------------------------------------------------------|
| <div>PUBLISHER</div> <div>National Institute of Standards and Technology (NIST)</div> | <div>TYPE</div> <div>Assessment / Maturity Model</div>        | <div>VERSION</div> <div>Rev. 1</div>                       |
| <div>EFFECTIVE</div> <div>June 13, 2018</div>                                         | <div>DOMAIN</div> <div>Cybersecurity</div>                    | <div>FAMILY</div> <div>NIST Special Publications</div>     |
| <div>REGION</div> <div>United States</div>                                            | <div>INDUSTRY</div> <div>Government &amp; Public Sector</div> | <div>ADOPTION MODEL</div> <div>Regulatory Compliance</div> |
| <div>IMPLEMENTATION COMPLEXITY</div> <div>High</div>                                  |                                                               |                                                            |

Source: <https://csrc.nist.gov/pubs/sp/800/171/a/r3/final>

## Why it matters

- **Strengthen compliance assurance** Enable organizations to systematically demonstrate compliance with federal CUI requirements and reduce risks of noncompliance.
- **Improve security oversight** Support continuous monitoring and evaluation of implemented security controls to ensure they remain effective over time.
- **Enhance incident response readiness** Facilitate early detection of security weaknesses, improving organizational ability to respond to and contain incidents effectively.
- **Promote consistent data protection** Standardize assessment practices to ensure CUI is uniformly safeguarded across different systems and operational environments.

## How SmartSuite supports NIST 800-171A Rev.1

### Assessment Procedure Library

Organize NIST SP 800-171A assessment procedures mapped to the corresponding 800-171 security controls.

### Assessment Planning and Scheduling

Plan and schedule assessment activities, assign assessors, and define scope for control evaluations.

### Evidence and Testing Documentation

Capture assessment artifacts, system evidence, and control test results supporting evaluation outcomes.

### Assessment Findings and Remediation Tracking

Track assessment findings, assign corrective actions, and monitor remediation progress across systems.

### CUI Security Implementation Monitoring

Monitor implementation of security requirements protecting Controlled Unclassified Information.

### Assessment Reporting and Readiness

Provide dashboards summarizing assessment results, open findings, and readiness for compliance reviews.

## Common framework mappings

CIS Controls v8.1

CMMC 2.0

COBIT 2019

FedRAMP Rev. 5

HIPAA

ISO 27001:2022

NIST CSF 2.0

NIST 800-53 Rev.5

PCI DSS 4.0.1

SOC 2

## Official resources

### NIST SP 800-171A Document

Provides assessment procedures for security requirements of Controlled Unclassified Information.

[csrc.nist.gov/publications/detail/sp/800-171a/final](https://csrc.nist.gov/publications/detail/sp/800-171a/final)

### NIST SP 800-171 Revision 2

Outlines the requirements for protecting Controlled Unclassified Information in non-federal systems.

[csrc.nist.gov/publications/detail/sp/800-171/rev-2/final](https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final)

## Frequently asked questions

### What is NIST SP 800-171A used for?

NIST SP 800-171A is designed to provide assessment procedures for evaluating the implementation and effectiveness of security requirements in NIST SP 800-171. It is primarily used by organizations handling Controlled Unclassified Information (CUI) in non-federal systems to ensure compliance with federal cybersecurity requirements.

### Is NIST SP 800-171A required for compliance?

While NIST SP 800-171A itself is not a mandatory standard, it is often required as part of contractual obligations with federal agencies and is referenced in enforcement of NIST SP 800-171 requirements. Organizations are expected to follow its guidance to demonstrate compliance with the underlying NIST SP 800-171 controls.

### Who must comply with NIST SP 800-171A?

Any non-federal organization that processes, stores, or transmits Controlled Unclassified Information (CUI) under a federal contract or agreement is subject to the requirements of NIST SP 800-171 and, by extension, should use NIST SP 800-171A for assessment. This includes defense contractors, subcontractors, and vendors in the federal supply chain.

### What are the key concepts or artifacts required by NIST SP 800-171A?

Key artifacts include documented assessment procedures, evidence of control implementation, policy documents, configuration records, and assessment results. NIST SP 800-171A guides assessors in evaluating technical, physical, and administrative safeguards protecting CUI.

### **How do organizations implement NIST SP 800-171A?**

Organizations implement NIST SP 800-171A by conducting self-assessments or third-party assessments using the procedures outlined in the publication. This involves reviewing evidence, interviewing personnel, and testing controls to verify compliance with each NIST SP 800-171 requirement.

### **How does NIST SP 800-171A relate to other cybersecurity frameworks?**

NIST SP 800-171A aligns closely with NIST SP 800-171 and supports federal requirements such as DFARS and CMMC. It integrates into a broader compliance ecosystem that may also include NIST SP 800-53, ISO 27001, and other federal or industry standards for information security.

### **How would SmartSuite support NIST SP 800-171A?**

SmartSuite can help organizations manage NIST SP 800-171A by providing centralized tools for risk tracking, control management, and evidence collection. It streamlines audit readiness through automated workflows and facilitates reporting for internal reviews and external audits, ensuring ongoing compliance with NIST SP 800-171A assessment requirements.

License included / downloadable: Yes NIST SP 800-171A is publicly available for free from NIST's website. License included with platform

Full framework page and mappings: [smartsuite.com/frameworks/nist-sp-800-171a-assessing-security-requirements-for-controlled-unclassified-information](https://smartsuite.com/frameworks/nist-sp-800-171a-assessing-security-requirements-for-controlled-unclassified-information)