SmartSuite

Framework / Cybersecurity / NIST Special Publications

NIST SP 800-171A Rev. 3

NIST SP 800-171A Rev. 3 provides assessment procedures to evaluate implementation of security requirements for protecting Controlled Unclassified Information.

What it is

NIST SP 800-171A Revision 3 is an assessment guideline that helps organizations evaluate the implementation and effectiveness of security requirements for protecting Controlled Unclassified Information (CUI) in non-federal information systems. Its primary purpose is to support consistent and objective assessments of compliance with the requirements specified in NIST SP 800-171.

Developed and published by the National Institute of Standards and Technology (NIST), this framework is used by federal agencies, contractors, and third-party assessors to verify that appropriate cybersecurity controls are in place for safeguarding CUI. NIST SP 800-171A outlines assessment procedures covering risk management, security control effectiveness, and compliance oversight in line with federal mandates.

At a glance

PUBLISHER
National Institute of Standards and Technology (NIST)

TYPE
Assessment / Maturity Model

VERSION
Rev. 3

EFFECTIVE
May 14, 2024

DOMAIN
Cybersecurity

FAMILY
NIST Special Publications

REGION
United States

INDUSTRY
Government & Public Sector

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
High

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

Why it matters

- **Improve security oversight** Provide structured mechanisms for evaluating the effectiveness of information security safeguards on a regular basis.
- **Increase audit readiness** Document assessment procedures and outcomes to support independent audits and reviews of security compliance.
- **Enhance regulatory alignment** Help demonstrate compliance with federal requirements and contracts involving the handling of sensitive government information.
- **Support risk management efforts** Enable organizations to identify gaps and prioritize remediation actions based on formal assessment results.

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports NIST 800-171A Rev.3

Rev. 3 Assessment Procedure Library

Organize NIST SP 800-171A Rev. 3 assessment procedures mapped to corresponding security control requirements.

Assessment Planning and Scheduling

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

Evidence Collection and Control Testing

Capture artifacts, configuration evidence, and system documentation supporting assessment procedures.

Findings and Remediation Workflows

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

CUI Security Oversight

Monitor implementation and effectiveness of security controls protecting Controlled Unclassified Information.

Compliance and Assessment Reporting

Provide dashboards summarizing control assessments, open findings, and readiness for external reviews.

Common framework mappings

CIS Controls v8.1 | FedRAMP Rev. 5 | HIPAA (NIST SP 800-66 Rev. 2) | 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 Rev. 3

Provides assessment procedures for NIST SP 800-171, detailing security requirements for protecting CUI.

csrc.nist.gov/pubs/sp/800/171/a/r3/final

NIST SP 800-171

Defines the security requirements for protecting Controlled Unclassified Information (CUI) in non-federal systems.

csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

NIST SP 800 Series Overview

Outlines the series of publications addressing computer security from NIST including SP 800-171.

csrc.nist.gov/publications/sp800

CUI Program Overview

Describes policies and procedures for CUI protection across federal and non-federal entities.

archives.gov/cui/about

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 compliance with NIST SP 800-171A mandatory?

Compliance with NIST SP 800-171A is generally required for contractors and organizations that handle CUI on behalf of U.S. federal agencies, as dictated by contractual or regulatory obligations. While the assessment guidelines themselves are not certifiable, demonstrating proper implementation of NIST SP 800-171 controls is mandatory within the scope of government contracts.

Who does NIST SP 800-171A apply to?

NIST SP 800-171A applies to non-federal organizations, including contractors, subcontractors, and other third parties that process, store, or transmit CUI on behalf of federal agencies. It is relevant for both prime and subcontractors across federal supply chains who must meet NIST SP 800-171 requirements.

 © 2026 SmartSuite Inc. All rights reserved.

What are the key assessment concepts and artifacts in NIST SP 800-171A?

Key assessment concepts in NIST SP 800-171A include security controls, assessment objectives, evidence collection, and assessment methods such as examination, interview, and testing. Artifacts generated during assessments may include assessment plans, documented results, and supporting documentation demonstrating evidence of control implementation.

How do organizations implement NIST SP 800-171A assessments?

Organizations implement NIST SP 800-171A by developing an assessment plan, selecting relevant controls, and applying specified assessment methods to gather evidence. The process involves evaluating whether each security requirement is implemented as intended and effectively protecting CUI, followed by documenting assessment findings.

How does NIST SP 800-171A relate to NIST SP 800-171 and other frameworks?

NIST SP 800-171A is designed to assess the requirements detailed in NIST SP 800-171, focusing specifically on the verification of CUI security controls. While NIST SP 800-171 defines the security requirements, 800-171A outlines assessment procedures, and both align with broader federal frameworks such as the NIST Risk Management Framework and CMMC.

What are ongoing compliance requirements for NIST SP 800-171A?

Ongoing compliance requires organizations to conduct regular assessments, update documentation, remediate identified gaps, and maintain evidence of CUI protection measures. Continuous monitoring, control testing, and periodic self-assessments are recommended to ensure sustained compliance and readiness for external audits.

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 Rev. 3 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-rev-3

 © 2026 SmartSuite Inc. All rights reserved.