DRATA

# NIST SP 800-171 Compliance Automation

NIST 800-171 establishes security requirements for protecting Controlled Unclassified Information in nonfederal organizations. Drata helps centralize evidence, map controls, and streamline monitoring to support readiness.




## DISCOVER THE DRATA DIFFERENCE

### ▶ Clarify CUI Risk Across Systems and Suppliers

Drata links NIST 800-171 requirements to risks across systems and processes that handle Controlled Unclassified Information (CUI). As environments, users, or third parties change, teams maintain a current view of where CUI-related risk exists and which controls mitigate it—supporting clear accountability and defensible assessment discussions.

### ▶ Analyze Control Test Issues With AI

Drata AI explains control test issues tied to NIST 800-171 requirements, including when controls behave unexpectedly. Teams quickly see what's happening, why it affects CUI protection, and what to review next for self-assessments, SPRS submissions, and government evaluations.

### ▶ Sustain Continuous Readiness for Assessments

Drata supports NIST 800-171 with continuously monitored controls and always-current evidence aligned to defined security requirements. Teams maintain visibility into control status throughout the year, reducing reliance on point-in-time self-assessments and staying prepared for government-driven reviews and evaluations.

### ▶ Simplify Preparation for Government Reviews

Drata centralizes evidence, control context, and assessment artifacts related to NIST 800-171 in a single workspace. Teams reduce back-and-forth during self-assessments, SPRS-related reviews, and third-party evaluations by presenting consistent, well-organized documentation without disrupting operational teams.

## ADDITIONAL CAPABILITIES

**Define CUI Controls**
Track NIST 800-171 controls with clear ownership across systems handling controlled requirements.

**Centralize Evidence**
Unify NIST 800-171 evidence to support audits, surveillance reviews, and ongoing oversight.

**Automate Workflows**
Route NIST 800-171 control tasks, reviews, and remediation through custom governance workflows.

**Validate Configurations**
Verify system and application configuration changes against NIST 800-171 controls using automated tests.

**Assess Supplier Risk**
Review supplier security posture against NIST 800-171 requirements using scalable TPRM workflows.

**Share Compliance Materials**
Publish approved NIST 800-171 documentation securely through Trust Center for partners.

## TRUSTED BY 8,000+ GLOBAL CUSTOMERS

WIZ asana GitLab Brex OpenAI Vercel

Navigate NIST 800-171 with Confidence [DRATA.COM]