2025 NIST SP 800-171 Controls Checklist

Full list of 110 controls across 14 families

NIST Special Publication 800-171 defines the security requirements for protecting Controlled Unclassified Information (CUI) in non-federal systems. Revision 2 organizes 110 controls into 14 families covering policy, process and technical safeguards. This checklist summarises each family and helps you verify your implementation status.

Control Families Overview

Family	Focus
Access Control (AC)	Limit system access to authorized users and enforce least privilege
Awareness & Training (AT)	Ensure personnel are trained to carry out security responsibilities
Audit & Accountability (AU)	Create, protect and retain audit records; generate alerts and audit review
Configuration Management (CM)	Establish baselines and control changes to systems and software
Identification & Authentication (IA)	Verify identities before granting access using multifactor methods
Incident Response (IR)	Develop and test response plans; detect, report and respond to incidents
Maintenance (MA)	Perform periodic and timely maintenance on systems and employ remote maintenance protections
Media Protection (MP)	Protect CUI on digital and physical media during storage, transport and destruction
Personnel Security (PS)	Ensure personnel are trustworthy and coordinate security with HR processes
Physical Protection (PE)	Restrict physical access to systems, equipment and facilities
Risk Assessment (RA)	Assess organizational risks and vulnerabilities to determine appropriate safeguards
Security Assessment (CA)	Periodically assess and monitor security controls for effectiveness
System & Communications Protection (SC)	Protect communications and control network boundaries using encryption and segmentation
System & Information Integrity (SI)	Identify and manage flaws, malicious code and unauthorized changes

The 110 controls expand into 320 assessment objectives. Compliance requires documenting policies, implementing technical controls and preparing evidence for C3PAO audits.

[3] Agile IT explains that NIST 800-171 consists of 110 controls across 14 families and 320 assessment objectives.
[4] Diligent notes that the control families standardize how organizations handle CUI and summarises each family.

Preparing Your Checklist

To use this checklist effectively, evaluate each control for applicability to your environment and note implementation status. For each family:

- Review the specific control statements in NIST SP 800-171 and NIST SP 800-171A.
- Document existing policies, procedures and technical safeguards that address each requirement.
- Identify gaps and include them in your Plan of Action & Milestones (POA&M).
- Collect evidence for each control such as screenshots, logs, policies, training records and audit reports.
- Ensure controls remain effective through continuous monitoring and periodic assessments.

Note that NIST SP 800-171 Revision 3 introduces 17 security families and updates requirements. Align your program with the latest guidance while meeting current CMMC Level 2 obligations.