

SELF ASSESSMENT

NIST SP 800-171 Controls Checklist

A simplified, technical-control-level review of your NIST SP 800-171 implementation status, useful for SPRS score estimation. This does not replace a formal control-by-control assessment. Scoring: Yes = 2 pts | Partial = 1 pt | No = 0 pts.

Access Control

Control	Yes – 2	Partial – 1	No – 0
Account creation, modification, and removal follows a documented process	☐	☐	☐
Session lock enforced after a period of inactivity	☐	☐	☐
Wireless access authorized and encrypted prior to use	☐	☐	☐
Mobile devices encrypted before connecting to CUI systems	☐	☐	☐

Audit & Accountability

Control	Yes – 2	Partial – 1	No – 0
System audit records enable tracing of actions to individual users	☐	☐	☐
Audit log storage capacity sized to prevent capacity failures	☐	☐	☐
Time stamps used for audit records and synchronized with authoritative source	☐	☐	☐

Configuration Management

Control	Yes – 2	Partial – 1	No – 0
System component inventory maintained and kept current	☐	☐	☐
Nonessential programs, functions, and services disabled or removed	☐	☐	☐
User-installed software restricted via policy or technical control	☐	☐	☐

Identification & Authentication

Control	Yes – 2	Partial – 1	No – 0
Authenticators (passwords, tokens, certificates) managed per policy	☐	☐	☐
Replay-resistant authentication mechanisms used for network access	☐	☐	☐

Identifiers reused only after a defined disable period	☐	☐	☐
--	--------------------------	--------------------------	--------------------------

Incident Response

Control	Yes – 2	Partial – 1	No – 0
Incident-handling capability includes preparation, detection, and recovery	☐	☐	☐
Incident response tested via tabletop or simulation at least annually	☐	☐	☐

Media Protection

Control	Yes – 2	Partial – 1	No – 0
Access to media containing CUI restricted to authorized individuals	☐	☐	☐
Portable storage devices prohibited absent an identified owner	☐	☐	☐

Personnel Security

Control	Yes – 2	Partial – 1	No – 0
Systems containing CUI protected during and after personnel actions	☐	☐	☐

Physical Protection

Control	Yes – 2	Partial – 1	No – 0
Physical access devices (badges, keys) managed and inventoried	☐	☐	☐
Alternate work sites assessed for adequate security controls	☐	☐	☐

Risk Assessment

Control	Yes – 2	Partial – 1	No – 0
Vulnerability scans performed periodically and after significant changes	☐	☐	☐
Identified vulnerabilities remediated per defined risk-based timelines	☐	☐	☐

Security Assessment

Control	Yes – 2	Partial – 1	No – 0
System Security Plan (SSP) documents how each control is implemented	☐	☐	☐

Plan of Action & Milestones (POA&M;) tracks unimplemented controls	☐	☐	☐
--	--------------------------	--------------------------	--------------------------

System & Communications Protection

Control	Yes – 2	Partial – 1	No – 0
Communications denied by default, allowed by exception at boundaries	☐	☐	☐
Cryptographic mechanisms used to protect CUI confidentiality during transmission	☐	☐	☐
Collaborative computing devices (cameras/mics) prohibit remote activation	☐	☐	☐

System & Information Integrity

Control	Yes – 2	Partial – 1	No – 0
Flaws identified, reported, and corrected within defined timelines	☐	☐	☐
System monitoring detects unauthorized use of organizational systems	☐	☐	☐
Spam protection mechanisms deployed at system entry/exit points	☐	☐	☐

Add the total of each column

TOTAL

*A total below **85% of the maximum possible score** typically corresponds to a low or negative SPRS score — a strong signal that a formal gap analysis is needed before attesting to a customer or contracting officer. This checklist covers representative controls, not all 110 in the full catalog.*

Want a Professional Review?

Contact Cenova Cyber at cenovacyber.com for a free NIST 800-171 gap analysis and SPRS scoring support.

www.cenovacyber.com