NIST 800-171 Rev. 2 → Rev. 3

Redspin

Preparing for What's Next Without Breaking What Works Today

REV.2: Where we are today

- CMMC Level 2 = NIST SP 800-171 Rev. 2 (110 controls)
- Required today for DoD contracts
- Assessments follow 800-171A Rev. 2
- Rev. 3 is NOT required yet (pending rulemaking)

REV.3: Whats Coming

- Aligns more closely with NIST SP 800-53 Rev. 5
- New control families (ex. Supply Chain Risk)
- More assessment objectives 320 → 420
- Organization Defined Parameters (ODPs) standardized by DoD
- NFO controls now required (previously assumed)

CAUTION:FEWER CONTROLS ≠ LESS WORK

- Controls were merged, not removed
- Evidence expectations increase
- More specificity = more to prove

KEY CHANGES AT A GLANCE

Supply Chain Risk	• Formal third-party risk requirements • Stronger flow-down to subcontractors
Access & Identity	• MFA required for ALL system accounts • Tighter identity & authentication controls
Configuration & Software	• Shift to deny-by-default / allow-by-exception • Stronger baseline & exception documentation
Policy & Evidence	• Formalized policy lifecycle requirements • Increased expectation for proof—not intent

NIST 800-171 Rev. 2 → Rev. 3

Level 2 certification is based on a defined system, boundary, & scope. Preparing for Rev. 3 is necessary, but doing it incorrectly could invalidate your current certification.

DO

(what you should be doing now)

- Improve documentation, policies, and procedures
- Define and standardize ODPs (passwords, timeouts, etc.)
- Strengthen existing controls (more evidence, better implementation)
- Clarify CUI boundaries and data flows
- Implement controls within your current scope

These actions strengthen compliance without changing your certified state

DON'T

(What Can Break Compliance)

- Changing system architecture or network design
- Expanding or redefining CUI scope/boundary
- Adding new in-scope systems, users, or providers
- Shifting where or how CUI is stored/processed
- Making changes that invalidate your assessed environment

These may trigger a reassessment requirement

Ned Says:

"Before making a change, ask:

- *Does this change what's in scope?*
- *Does it change where CUI lives?*
- *Does it change how systems connect or operate?*

*If **YES** → Proceed carefully (reassessment risk)*
*If **NO** → Likely safe to move forward"*

Bottom Line:

- Stay aligned to your current certified environment
- Focus on incremental, defensible improvements
- Avoid changes to scope, boundary, or architecture
- Build toward Rev. 3—without triggering reassessment

info@redspin.com