The NIST SP 800-171 and SPRS Self-Assessment Checklist

The pause on formal CMMC third-party assessments shifts the immediate burden of proof back to your internal control operations and SPRS entries. Contractors must maintain a continuous, auditable operational rhythm that map directly to existing regulatory obligations.

This checklist provides an operational architecture to organize your compliance artifacts, verify system boundaries, and document a defensible compliance posture that satisfies the data flow-down demands of prime contractors.

PHASE 1 Boundary Definition and Data Scoping

- [ ] **Map CUI data flows**
  Document exactly where CUI enters, travels through, and exits your organization.
- [ ] **Isolate the enclave**
  Establish strict network segmentation to minimize the systems subject to C3PAO scrutiny.
- [ ] **Audit the cloud supply chain**
  Verify that every cloud platform within the boundary holds an active FedRAMP Certified Class C (rev5) authorization.

PHASE 2 Control Implementation and GRC Automation

- [ ] **Align with NIST SP 800-171**
  Implement the 110 security controls required for Level 2 compliance.
- [ ] **Establish centralized evidence collection**
  Shift away from siloed spreadsheets toward automated mechanisms to maintain continuous compliance.
- [ ] **Formalize policy governance**
  Create a repeatable policy lifecycle that maps corporate governance documentation directly to operational controls.
- [ ] **Cross-map framework requirements**
  Link your active controls across multiple programs to satisfy overlapping audit criteria with a single piece of evidence.

PHASE 3 Risk Integration and Continuous Evaluation

- [ ] **Deploy an enclave risk register**
  Establish a dedicated risk register to document, prioritize, and track vulnerabilities unique to the assets inside the CUI boundary.
- [ ] **Link controls to active threats**
  Connect automated control test statuses directly to your risk registers so that a control failure automatically elevates your risk exposure metric.
- [ ] **Automate vulnerability intake**
  Ingest telemetry from external security scanners and threat intelligence feeds directly into your risk workflow to bypass manual data entry.
- [ ] **Generate board-ready reporting**
  Produce filterable analytics summaries to provide corporate leadership and prime partners with clear visibility into your true security posture.

PHASE 4 Assessment Preparation and Continuous Monitoring

- [ ] **Generate the system security plan**
  Compile a comprehensive, living SSP that automatically reflects current control ownership, boundary limits, and active system components.
- [ ] **Link risks to controls**
  Utilize an integrated risk register to ensure that control degradation immediately alerts risk owners before an assessor arrives.
- [ ] **Verify SPRS score defensibility**
  Conduct final internal evaluations of all 110 controls to ensure your entered database score is backed by a verified, unalterable audit trail.
- [ ] **Isolate collaborator portal access**
  Establish a restricted workspace portal within your platform to share specific evidence packages securely with upstream prime contractors or internal auditors
- [ ] **Maintain rollout agility**
  Keep control environments aligned with both Revision 2 and Revision 3 changes so your team can adapt as federal guidance evolves out of the program review window.

PHASE 5 C3PAO Assessment Readiness *(If the C3PAO requirement is reinstated)*

- [ ] **Formulate plan of action and milestones templates**
  Document any temporary deficiencies within a structured POA&M framework to track remediation paths, noting that Phase 2 certification requires zero open items at the final evaluation.
- [ ] **Isolate auditor workspace access**
  Create a secure, restricted portal within your GRC environment to share pre-mapped evidence packages with the C3PAO assessor without exposing non-audit telemetry.
- [ ] **Secure your C3PAO assessment slot**
  Formalize your engagement contract early to navigate the 18-month market backlog and prevent contract award delays.