A WRITING GUIDE, NOT A COMPLETED SSP

Make the security plan match the environment.

An annotated outline and practical review checklist for small and midsize defense contractors.

> Use this as a starting structure.
> This Continuum guide suggests a working format. It is not a government template, a complete requirement set, a compliance determination, or an official assessment. No client information or outcomes appear in these examples.

Before drafting

01 Confirm the requirements and assessment baseline that apply to the relevant contract and environment. Record the source and any unresolved applicability questions.

02 Bring the system owner, information owners, IT providers, and compliance owner into the same scope discussion. Identify who can confirm the facts.

03 Describe what is actually implemented. Distinguish planned work, uncertain claims, inherited services, and evidence that has not yet been validated.

04 Keep the SSP and supporting artifacts in an appropriately controlled workspace. Do not submit CUI, account exports, credentials, or sensitive diagrams through a public website.

> Choose the correct revision.
> NIST has published SP 800-171 Revision 3 and SP 800-171A Revision 3. Earlier publications are identified by NIST as superseded. Your contract and applicable assessment rules determine the required baseline; publication status alone does not make that decision. Do not mix identifiers from different revisions.

ANNOTATED OUTLINE | ENVIRONMENT

Describe the system before the controls.

These sections help a reader understand what the plan covers and who is responsible for keeping it accurate.

01 Document control and ownership

Identify the system and organization, plan owner, approval authority, version, review date, and change history. Describe how changes to the environment trigger a plan review.

Review prompt: Can a reader identify the current version and the people responsible for its accuracy?

02 Applicable requirements and assumptions

Record the relevant contractual and assessment baseline, with the revision and source. Identify scope assumptions and questions that require customer or contracting-authority clarification.

Review prompt: Can each selected baseline be traced to a relevant obligation rather than a generic checklist?

03 Boundary, information, and environment

Explain the business purpose, information types, relevant users, locations, components, and information flows. Describe the boundary and the relationships or connections to other systems. Use controlled supporting diagrams as appropriate.

Review prompt: Does the narrative describe the actual environment, including remote access, cloud services, and external connections where relevant?

04 Responsibilities and service relationships

Assign system, security, information, and process ownership. Describe what service providers do, what the contractor retains responsibility for, and the evidence needed to support shared or inherited claims.

Review prompt: Is responsibility explicit at each handoff, and can the relevant provider evidence be obtained?

Keep scope decisions visible.
A provider contract, a security product, or a boundary diagram alone does not demonstrate that every applicable requirement is implemented. Record what has been confirmed and what remains open.

ANNOTATED OUTLINE | IMPLEMENTATION

Explain the practice. Connect the evidence.

Write requirement-level narratives that a system owner, implementer, and independent reviewer can trace.

05 Requirement implementation narratives

For the applicable baseline, explain who performs the activity, how it operates, which systems it covers, and where supporting procedures are maintained. State incomplete or uncertain implementation plainly.

Review prompt: Does the description explain actual operation, including the division of responsibilities, rather than repeat requirement text?

06 Evidence and validation references

Connect each relevant claim to controlled evidence references. Record evidence owner, collection date, scope, and known limitations. Plan examination, interviews, and testing as appropriate to the applicable assessment procedures.

Review prompt: Would another reviewer be able to locate the evidence and understand what it can and cannot establish?

07 Open gaps and planned action

Separate current implementation from planned remediation. Link findings to responsible roles, dependencies, target dates agreed with the owners, and validation criteria. Check any program-specific plan-of-action restrictions separately.

Review prompt: Can management distinguish a completed task from a validated finding and from an overall assessment result?

08 Maintenance and review

Describe how system, service, personnel, and requirement changes are reflected in the plan and evidence. Identify review ownership and how unresolved decisions are escalated.

Review prompt: Does a system change reach the plan owner and the people who maintain related evidence?

Illustrative wording improvement.
Weak: "Access is controlled." More useful: "The system owner approves access; IT provisions accounts through the documented workflow. Supporting records are in the evidence index. Account reconciliation remains open under finding F-001." Fictional wording is not proof of implementation.

PRACTICAL REVIEW CHECKLIST

Check the claim, the evidence, and the limits.

Use this review aid before treating a draft as ready for an internal readiness discussion. It is not a complete assessment checklist.

- [ ] The baseline and revision are identified, with applicability questions recorded.
- [ ] The boundary, information flows, connections, and provider relationships match the current environment.
- [ ] Responsible people have reviewed the parts of the narrative they operate.
- [ ] Implemented, planned, and unvalidated activities are clearly distinguished.
- [ ] Evidence can be located, is relevant to the claim, and has a known owner, date, and scope.
- [ ] Missing evidence and implementation gaps have accountable actions and validation criteria.
- [ ] Completed actions are supported by a documented review or test appropriate to the finding.
- [ ] The current version is controlled and future environment changes have a review path.

Official publications and templates

NIST SP 800-171 Rev. 2 - requirements and official SSP / plan-of-action templates
https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final

NIST SP 800-171A (2018) - earlier assessment procedures
https://csrc.nist.gov/pubs/sp/800/171/a/final

NIST SP 800-171 Rev. 3 - revised security requirements
https://csrc.nist.gov/pubs/sp/800/171/r3/final

NIST SP 800-171A Rev. 3 - companion assessment procedures
https://csrc.nist.gov/pubs/sp/800/171/a/r3/final

Need help applying this to your environment?
Schedule a compliance readiness consultation at continuumreadiness.com/consultation

Continuum provides readiness consulting and preparation. Official CMMC certification assessments must be performed by appropriately authorized or accredited assessment organizations. No outcome is guaranteed.