CA.L2-3.12.4

Security Assessment

System Security Plan

"Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems."

Objectives

[a]
A system security plan is developed.

[b]
The system boundary is described and documented in the system security plan.

[c]
The system environment of operation is described and documented in the system security plan.

[d]
Security requirements identified and approved by the designated authority as non-applicable are identified.

[e]
The method of security requirement implementation is described and documented in the system security plan.

[f]
The relationship with or connection to other systems is described and documented in the system security plan.

[g]
The frequency to update the system security plan is defined.

[h]
The system security plan is updated with the defined frequency.

Key Discussion Points

8 Required Elements:
Boundary, environment of operation, non-applicable requirements, implementation methods, system connections, update frequency — all 8 must be present.

Boundary First:
Without a defined system boundary, an assessor cannot determine what is in scope — the boundary makes every other assessment activity possible.

No SSP = No Assessment:
The guide states explicitly: absence of an up-to-date SSP results in a finding that an assessment cannot be completed — violating DFARS 252.204-7012.

Annual Update Minimum:
At least annually — that is the floor. Major changes to the environment should trigger an interim SSP update before the next scheduled review.

Assessment Methods

EXAMINE

Security planning policy; organizational procedures addressing system security plan development; procedures addressing system security plan reviews and updates; enterprise architecture documentation; system security plan; records of system security plan reviews and updates.

INTERVIEW

Personnel with security planning and system security plan implementation responsibilities; personnel with information security responsibilities.

TEST

Organizational processes for system security plan development, review, update, and approval; mechanisms supporting the system security plan.

CA.L2-3.12.4

SECURITY ASSESSMENT — System Security Plan

Plain English

What this control is really saying:

The SSP is the foundational document of a CMMC compliance program. Without a current, complete SSP, an assessment cannot be completed — an outdated or missing SSP is not just a gap, it is a condition that ends the assessment. This control requires a real SSP that covers all eight specific content areas and is maintained on a defined schedule.

How it is used:

- The SSP defines the system boundary using network diagrams, asset inventories, and a written boundary description — all CUI-touching assets are within scope.
- Each NIST SP 800-171 control in the SSP has an implementation status (implemented, partially implemented, or not implemented) with a description of how it is met.
- System interconnections — VPN connections, cloud services, third-party access — are documented with the receiving/providing designation and data flow description.
- The SSP is reviewed and updated at least annually and whenever significant changes occur — update date and approver are recorded.

Real World Example

The Scenario

Acme Defense submitted an SSP with their CMMC Level 2 assessment request. The assessor opens the document. It is a four-page table listing all 110 controls as 'Implemented' with no descriptions, no system boundary, and no environment of operation.

What the assessor finds

The assessor cannot determine the system boundary, understand how any control is actually implemented, or verify any claim in the document. The assessment is halted pending a complete, compliant SSP. DFARS 252.204-7012 compliance cannot be confirmed.

SPRS Score Impact

3.12.4 carries a point value of 3. The SSP is the foundational artifact of any CMMC assessment — its absence or inadequacy stops the assessment and constitutes a material violation of DFARS 252.204-7012.

What Good Looks Like

SSP developed covering all 8 required elements, system boundary documented, environment of operation described, each control's implementation described, system interconnections listed, annual update frequency defined and met, SSP reviewed and approved by senior leadership.

Common Gaps

What assessors actually find in the field:

✗ No SSP exists

The organization has no SSP — without one, a CMMC assessment cannot be completed and DFARS 252.204-7012 is violated.

✗ SSP not updated

The SSP was written two years ago and has not been reviewed since — systems, personnel, and configurations have changed significantly.

✗ Boundary not documented

The SSP describes controls but does not include a system boundary definition — assessors cannot determine what is in scope.

✗ Interconnections missing

Cloud services and third-party access are not documented in the SSP — system connections are unknown to the assessor.

✗ Controls not described

The SSP lists controls as 'implemented' but provides no description of how they are implemented — assertions without evidence fail [e].