RA.L2-3.11.1

Risk Assessment

Risk Assessments

"Periodically assess the risk to organizational operations, organizational assets, and individuals resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI."

Objectives

[a]

The frequency to assess risk to organizational operations, organizational assets, and individuals is defined.

[b]

Risk to organizational operations, organizational assets, and individuals resulting from the operation of an organizational system that processes, stores, or transmits CUI is assessed with the defined frequency.

Key Discussion Points

Defined Frequency:
The interval must be specified — 'periodically' is not sufficient. Annual is the most common DIB practice; the frequency must be in the SSP.

Four Risk Elements:
A complete risk assessment addresses threats, vulnerabilities, likelihood, and impact — partial assessments leave the risk picture incomplete.

External Parties Too:
Service providers, contractors, and outsourced functions with CUI access must be included — risk does not stop at the organizational boundary.

Enables the SPRS Score:
The SPRS score submitted to DoD must reflect the results of a current risk assessment — an outdated or missing assessment undermines the entire score.

Assessment Methods

EXAMINE

Risk assessment policy; security planning policy and procedures; procedures addressing organizational risk assessments; system security plan; risk assessment; risk assessment results; risk assessment reviews; risk assessment updates.

INTERVIEW

Personnel with risk assessment responsibilities; personnel with information security responsibilities.

TEST

Organizational processes for risk assessment; mechanisms for conducting, documenting, reviewing, disseminating, and updating the risk assessment.

RA.L2-3.11.1

RISK ASSESSMENT — Risk Assessments

Plain English

What this control is really saying:

A risk assessment is a structured look at what could go wrong, how likely it is, and what the impact would be. This control requires that you do this periodically — on a defined schedule — for your CUI systems. Not once at contract award and never again, but regularly, so the assessment reflects the actual current state of your environment.

How it is used:

- An annual risk assessment is conducted following the NIST SP 800-30 process — threats, vulnerabilities, likelihood, and impact are all evaluated for each CUI system.
- The risk assessment covers internal threats, external threats, supply chain risks, and service providers with access to CUI — not just technical vulnerabilities.
- Risk assessment results are documented in a formal report, reviewed by management, and used to prioritize remediation in the Plan of Action and Milestones.
- The SSP documents the risk assessment frequency and process — the last assessment date and the next scheduled assessment are recorded.

Real World Example

The Scenario

Acme Defense completed a risk assessment when they first received a CUI contract three years ago. The assessment has never been updated. Since then, they have added cloud storage for CUI, onboarded two new subcontractors, and expanded the remote workforce.

What the assessor finds

The three-year-old assessment does not include the cloud storage system, two subcontractors with CUI access, or any remote work risks. New threat actors relevant to DIB contractors are not addressed. The SPRS score submitted to DoD is based on the outdated assessment.

SPRS Score Impact

3.11.1 carries a point value of 5. A risk assessment is the foundation of the entire security program — without it, there is no defensible basis for the SPRS score submitted to DoD or for any prioritization of security investment.

What Good Looks Like

Risk assessment frequency defined in SSP, formal assessment conducted on schedule using NIST SP 800-30, all CUI systems and external parties in scope, results documented, reviewed by management, used to update POAM and SPRS score.

Common Gaps

What assessors actually find in the field:

✗ **No risk assessment conducted**

The organization has never formally assessed risk — security decisions are made reactively with no structured threat or vulnerability analysis.

✗ **Frequency not defined**

The SSP says risk assessments will be conducted 'periodically' but no specific interval is defined — the schedule is vague and unenforceable.

✗ **Assessment not updated**

A risk assessment was completed four years ago at contract award and has never been revised — it does not reflect current systems or threats.

✗ **Results not documented**

Risk discussions happen informally in staff meetings but no formal assessment document exists — there is no evidence for assessors.

✗ **Scope is incomplete**

The risk assessment covers internal IT but does not address external parties, cloud services, or supply chain risks involving CUI.