AC.L2-3.1.4

Access Control

Separation of Duties

"Separate the duties of individuals to reduce the risk of malevolent activity without collusion."

Objectives

[a]
The duties of individuals requiring separation are defined.

[b]
Responsibilities for duties that require separation are assigned to separate individuals.

[c]
Access privileges that enable individuals to exercise the duties that require separation are granted to separate individuals.

Key Discussion Points

Define First:
[a] requires formally documenting which duties must be separated — without a separation of duties matrix in the SSP, [b] and [c] cannot be evaluated.

Audit Independence:
The person who administers access controls cannot also be the sole reviewer of audit logs — this is explicitly called out in the v2.13 discussion.

People and Permissions:
Both [b] and [c] must be satisfied — separate people AND separate access privileges. Assigning different people who share the same credentials satisfies neither.

Compensating Controls:
Small organizations may not be able to fully separate all duties — but they must document compensating controls. Citing size alone is not sufficient.

Assessment Methods

EXAMINE

Access control policy; procedures addressing divisions of responsibility and separation of duties; system security plan; system configuration settings; list of divisions of responsibility and separation of duties; system access authorizations; system audit logs and records.

INTERVIEW

Personnel with responsibilities for defining divisions of responsibility and separation of duties; personnel with information security responsibilities; system or network administrators.

TEST

Mechanisms implementing separation of duties policy.

AC.L2-3.1.4

ACCESS CONTROL — Separation of Duties

Plain English

What this control is really saying:

No single person should be able to control a critical function from start to finish — especially functions that involve CUI access, system administration, or audit review. Separation of duties requires defining which functions need to be split, assigning them to different people, and configuring system access so that no one person has the permissions to perform both sides alone.

How it is used:

- Account creation requires a ticket submitted by a manager — the IT admin creates the account but cannot grant CUI system access without approval from a separate system administrator.
- Audit log review is assigned to the security manager, not the IT admin who configures the systems being audited — the person who sets up logging cannot also be the only one reviewing it.
- The SSP documents the separation of duties matrix — which functions are separated, who holds each role, and the access privileges that enforce the separation technically.
- Security personnel who administer access controls do not also administer audit functions — system access authorizations enforce this separation.

Real World Example

The Scenario

Acme Defense has one IT administrator who manages all user accounts, system configurations, and access controls. The same person also reviews system audit logs, approves his own change requests, and is the only one with access to the CUI system admin console.

What the assessor finds

The IT admin created his own account with domain administrator rights and approved the change himself. He is the only person who reviews audit logs — he could modify logs or grant himself access to CUI systems without any oversight. The SSP has no separation of duties matrix.

SPRS Score Impact

3.1.1 carries a point value of 1. An acceptable use policy without monitoring is unenforceable — and monitoring without a defined authorized use baseline cannot reliably distinguish authorized from unauthorized activity.

What Good Looks Like

Duties requiring separation defined in SSP matrix, separate individuals assigned to each role, system access authorizations enforce the separation technically, audit log review independent of IT operations, compensating controls documented where full separation is impractical.

Common Gaps

What assessors actually find in the field:

✗ IT admin does everything

A single IT administrator creates accounts, grants CUI access, and reviews audit logs with no oversight — no separation exists for any critical function.

✗ Self-approval

The IT admin can grant himself elevated access without anyone else's involvement — [b] and [c] are not met.

✗ No defined separation

The organization has never formally documented which duties require separation — [a] is not met and the rest of the control cannot be evaluated.

✗ Small team cited as exception

'We're too small for separation of duties' is not an accepted finding — compensating controls must be documented when full separation is impractical.

✗ Policy without technical enforcement

Separation is described in policy but system access authorizations are not configured to prevent one person from exercising both separated functions.