AC.L2-3.1.2

Access Control

Transaction & Function Control

"Limit system access to the types of transactions and functions that authorized users are permitted to execute."

Objectives

[a]

The types of transactions and functions that authorized users are permitted to execute are defined.

[b]

System access is limited to the defined types of transactions and functions for authorized users.

Key Discussion Points

Role-Based Access:
Access is tied to job function — what someone does determines what they can see and do, not who they know or how long they have been there.

CRUD Permissions:
Create, Read, Update, Delete — define which of these four operations each role is permitted to perform on CUI and enforce it technically.

Technical Enforcement:
Role definitions in policy are not enough — permissions must be configured in the system and enforced by the file server, application, or database.

Review on Role Change:
When a user changes roles, access must be recalibrated immediately — inherited permissions from old roles accumulate into over-privilege.

Assessment Methods

EXAMINE

Access control policy; procedures addressing access enforcement; system security plan; system design documentation; list of approved authorizations including remote access authorizations; system audit logs and records; system configuration settings and associated documentation.

INTERVIEW

Personnel with access enforcement responsibilities; system or network administrators; personnel with information security responsibilities; system developers.

TEST

Mechanisms implementing access control policy.

AC.L2-3.1.2

ACCESS CONTROL — Transaction & Function Control

Plain English

What this control is really saying:

Being authorized to access the system is not the same as being authorized to do anything inside it. 3.1.2 defines what each user can actually do — read, create, update, delete — and limits their system access to exactly those functions. A machinists does not need to delete CUI files. An accountant does not need to access engineering drawings.

How it is used:

- Active Directory security groups are defined by role — Engineers have read/write to engineering shares, accounting has no access, administrators manage configurations only.
- File share permissions enforce least-privilege by role — a manufacturing engineer can read CUI drawings but cannot delete or export them.
- When an employee changes roles, IT reviews and revises their access group memberships before the transition takes effect.
- Role definitions and associated permissions are documented in the SSP and reviewed annually.

Real World Example

The Scenario

Acme Defense has 45 employees across engineering, manufacturing, and administration. They have a Windows file server with shared folders for each department. Active Directory exists but group policies for folder access have never been configured.

What the assessor finds

All 45 employees have full read/write access to every folder on the file server including CUI engineering drawings. The accounting clerk and shop floor supervisor have the same access to export-controlled design files as the lead engineer. No role-based access controls have ever been configured.

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

Role-based access groups defined in AD, least-privilege permissions enforced per role, access reviewed quarterly, role changes trigger immediate access review, permissions documented in SSP.

Common Gaps

What assessors actually find in the field:

✗ **Blanket permissions**

All 45 employees have full read/write to all shared folders including CUI engineering files — no role-based differentiation.

✗ **No role definitions**

Access rights have never been formally defined — users get whatever access they ask for or inherit from previous employees.

✗ **Inherited access**

Employees who changed roles still have all access from their previous position on top of their new one.

✗ **Excessive admin rights**

Too many users have administrator-level access that far exceeds what their job function requires.

✗ **No periodic review**

Access rights are assigned at hire and never reviewed — accumulated permissions grow unchecked over time.