AC.L2-3.1.7

Access Control

Privileged Functions

"Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs."

Objectives

[a]
Privileged functions are defined.

[b]
Non-privileged users are defined.

[c]
Non-privileged users are prevented from executing privileged functions.

[d]
The execution of privileged functions is captured in audit logs.

Key Discussion Points

Define Both Sides:
[a] defines privileged functions; [b] defines non-privileged users — both must be documented before [c] can be technically enforced and [d] can be audited.

Block + Log = Both:
Technical blocking without audit logging fails [d]. Logging without blocking fails [c]. Both requirements are independently evaluated by assessors.

UAC Is Critical:
User Account Control is the primary Windows mechanism for [c] — disabling it for user convenience eliminates the technical barrier this control requires.

Insider Threat Link:
v2.13 explicitly calls out insider threat — logging privileged function execution is the primary mechanism for detecting authorized users abusing their access.

Assessment Methods

EXAMINE

Privacy and security policies; procedures addressing system use notification; system audit logs and records; system design documentation; system security plan; system use notification messages; system configuration settings and associated documentation.

INTERVIEW

Personnel with responsibilities for defining least privileges necessary to accomplish specified tasks; personnel with information security responsibilities; system developers.

TEST

Mechanisms implementing least privilege functions for non-privileged users; mechanisms auditing the execution of privileged functions.

AC.L2-3.1.7

ACCESS CONTROL — Privileged Functions

Plain English

What this control is really saying:

Standard users must not be able to execute administrative functions — and when admins do execute them, those actions must be logged. Both halves are required. Technical blocking without audit logging fails [d]. Audit logging without technical blocking fails [c]. Privileged function execution that leaves no trail is undetectable insider threat activity.

How it is used:

- Privileged functions are defined and documented — account management, system configuration changes, cryptographic key management, and audit log configuration are listed in the SSP.
- Windows Group Policy and RBAC configurations technically prevent standard users from accessing administrative consoles, modifying security settings, or installing software.
- User Account Control is enabled and enforced by GPO — elevation prompts are required and logged for all privileged function execution.
- Windows Event Log captures all privilege use events — logs are forwarded to a SIEM and reviewed regularly for anomalous privileged function execution.

Real World Example

The Scenario

Acme Defense runs Windows 10 workstations. The IT admin disabled UAC two years ago because employees complained about prompts. All employees also have local administrator rights on their own machines 'for troubleshooting purposes.'

What the assessor finds

Any employee can install software, modify system settings, and access local security functions without restriction. UAC is disabled. No audit logs capture these events. The local admin account uses a shared password known to the office manager. No privileged function list has ever been documented.

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

Privileged functions defined in SSP, standard users technically blocked from executing them, UAC enabled and enforced by GPO, no local admin rights for standard users, all privileged function execution captured in audit logs and reviewed.

Common Gaps

What assessors actually find in the field:

✗ **UAC disabled**

User Account Control has been disabled 'because it was annoying' — standard users can execute admin functions without an elevation prompt.

✗ **All users have local admin**

All workstation users have local administrator rights — every standard user can install software, modify security settings, and circumvent endpoint controls.

✗ **Privileged functions not defined**

The organization has never documented which functions are considered privileged — [a] is not met and [c] cannot be systematically enforced.

✗ **Shared admin credentials**

The admin password is known to non-admin staff and used occasionally for convenience — [c] is not met when non-privileged users know privileged credentials.

✗ **Privilege use not logged**

Privileged function execution is not captured in audit logs — insider threat activity and accidental privilege abuse are invisible.