AC.L2-3.1.15

Access Control

Privileged Remote Access

"Authorize remote execution of privileged commands and remote access to security-relevant information."

Objectives

[a]
Privileged commands authorized for remote execution are identified.

[b]
Security-relevant information authorized to be accessed remotely is identified.

[c]
The execution of the identified privileged commands via remote access is authorized.

[d]
Access to the identified security-relevant information via remote access is authorized.

Key Discussion Points

Avoid If Possible:
v2.13 states remote execution of privileged commands should be avoided if possible — the default posture is prohibition, not permission. Authorization is the exception, not the rule.

Document the Need:
Each authorized capability must be tied to a documented operational need — 'the admin needs it' is not a documented need. The specific function and justification must be written down.

Four-Part Structure:
[a] identifies commands, [b] identifies security data, [c] authorizes the commands, [d] authorizes the data access — all four objectives are independently evaluated.

Review and Revoke:
Remote privileged access authorizations must be revisited — needs change, projects end, and stale authorizations from past operational needs are a persistent finding.

Assessment Methods

EXAMINE

Access control policy; procedures addressing remote access to the system; system configuration settings and associated documentation; system security plan; system audit logs and records.

INTERVIEW

System or network administrators; personnel with information security responsibilities.

TEST

Mechanisms implementing remote access management.

AC.L2-3.1.15

ACCESS CONTROL — Privileged Remote Access

Plain English

What this control is really saying:

Being able to connect remotely does not mean being able to run privileged commands or access security-relevant data remotely. v2.13 says remote execution of privileged commands should be avoided if possible — and if it is absolutely necessary, it must be explicitly authorized, documented, and technically limited to only the identified commands and data.

How it is used:

- The SSP documents which privileged commands are authorized for remote execution — PowerShell remoting is authorized for server maintenance; firewall rule changes are not permitted remotely.
- Security-relevant information authorized for remote access is listed in the SSP — audit log configuration is accessible to the security manager with documented justification.
- Remote privileged command execution is restricted to specific accounts via GPO and firewall rules — the authorization is scoped to the minimum necessary for the documented operational need.
- All remote privileged command execution is logged separately and reviewed — the logs identify who executed which command, from where, and at what time.

Real World Example

The Scenario

Acme Defense contracted an MSP to handle IT support. The MSP was given remote administrator access to all systems two years ago. The MSP also has unrestricted remote access to all system logs and security configuration settings.

What the assessor finds

The MSP's remote admin access has never been scoped, justified, or reviewed. There is no documentation of which privileged commands are necessary or which security-relevant information the MSP needs to access. The MSP can remotely run PowerShell, access audit logs, and modify security configurations on all systems with no limits.

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 commands authorized for remote execution identified in SSP, security-relevant information authorized for remote access documented, remote privileged access restricted to specific accounts and commands, all remote privileged execution logged and reviewed, authorizations reviewed regularly and revoked when no longer needed.

Common Gaps

What assessors actually find in the field:

✗ **Blanket remote admin access**

All IT staff have unrestricted remote admin access to all systems — no specific privileged commands are identified and [a] and [b] are not met.

✗ **No documented operational need**

Remote privileged access was set up for convenience — no operational need was ever documented and [c] and [d] cannot be demonstrated.

✗ **Security data accessible without justification**

Audit logs and security configurations are accessible remotely by multiple accounts with no documented authorization — [d] is not met.

✗ **Former operational needs remain active**

Remote privileged access granted for a past project remains active long after the project ended — no review process exists to revoke stale authorizations.

✗ **MSP unrestricted access**

A managed services provider has ongoing unrestricted remote admin access — no operational need documentation, no scope limits, no review.