AC.L2-3.1.12

Access Control

Control Remote Access

"Monitor and control remote access sessions."

Objectives

[a]
Remote access sessions are permitted.

[b]
The types of permitted remote access are identified.

[c]
Remote access sessions are controlled.

[d]
Remote access sessions are monitored.

Key Discussion Points

Define Permitted Types:
[b] requires explicitly identifying which remote access methods are authorized — VPN, RDP, SSH, web portal. Methods not on the list are prohibited by default.

Monitor = Active:
[d] requires active monitoring — generating VPN logs that nobody reviews is not monitoring. Someone must review connection activity on a defined schedule.

Control = Technical:
[c] requires technical controls — only authorized devices, authenticated users, and approved methods can connect. Policy without enforcement does not satisfy [c].

Cloud Access Included:
v2.13 explicitly includes access to cloud-based email and infrastructure containing CUI — remote access controls apply to Microsoft 365 and cloud storage, not just VPN connections to HQ.

Assessment Methods

EXAMINE

Access control policy; procedures addressing remote access implementation and usage including restrictions; configuration management plan; system security plan; system design documentation; system configuration settings; remote access authorizations; system audit logs and records.

INTERVIEW

Personnel with responsibilities for managing remote access connections; system or network administrators; personnel with information security responsibilities.

TEST

Remote access management capability for the system.

AC.L2-3.1.12

ACCESS CONTROL — Control Remote Access

Plain English

What this control is really saying:

Remote access lets employees work from anywhere — and it lets attackers in too. This control requires defining what remote access methods are permitted, technically controlling who can connect and how, and actively monitoring remote sessions for suspicious activity. An unmonitored VPN connection is an invisible attack surface.

How it is used:

- VPN is the only authorized remote access method — RDP, SSH, and direct connections from the internet to internal systems are blocked at the firewall.
- SIEM aggregates VPN connection logs and alerts on unusual connection times, source locations, or session durations — all remote sessions are visible in near real time.
- Only managed, domain-joined devices are permitted to initiate VPN connections — personal devices are blocked at authentication.
- Administrators can terminate any active VPN session from the management console — the procedure is documented and tested quarterly.

Real World Example

The Scenario

Acme Defense engineers work from home several days per week, accessing CUI files on the corporate server. The company deployed Cisco AnyConnect VPN last year. Several engineers also use personal LogMeIn accounts to connect directly to their office workstations.

What the assessor finds

LogMeIn connections bypass the VPN entirely and are not monitored or logged in any corporate system. VPN connection logs exist but are never reviewed. The network admin has never terminated an active VPN session and does not know how. RDP port 3389 is open on the firewall alongside the VPN.

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

Permitted remote access types defined in SSP, VPN as sole authorized method with all other paths blocked, SIEM monitoring VPN sessions with alerting, only managed devices permitted, admin capability to terminate sessions documented and tested, logs reviewed regularly.

Common Gaps

What assessors actually find in the field:

✗ **Uncontrolled RDP exposure**

RDP port 3389 is open on the perimeter firewall — any user can attempt remote desktop connections directly without VPN, bypassing all session controls.

✗ **No monitoring of remote sessions**

VPN connections are made and activity is invisible — connections are only reviewed after an incident, not in real time.

✗ **Unauthorized remote tools in use**

Employees use personal LogMeIn, TeamViewer, or AnyDesk accounts to connect to work systems — these bypass the VPN and generate no corporate logs.

✗ **No disconnect capability**

Nobody knows how to terminate an active VPN session — there is no documented procedure and the capability has never been tested.

✗ **Remote access types not defined**

No policy identifies which remote access methods are permitted — [b] is not met and the organization cannot distinguish authorized from unauthorized connections.