CM.L2-3.4.5

Configuration Management

Access Restrictions for Change

"Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems."

Objectives

[a]
Physical access restrictions associated with changes to the system are defined.

[b]
Physical access restrictions associated with changes to the system are documented.

[c]
Physical access restrictions associated with changes to the system are approved.

[d]
Physical access restrictions associated with changes to the system are enforced.

[e]
Logical access restrictions associated with changes to the system are defined.

[f]
Logical access restrictions associated with changes to the system are documented.

[g]
Logical access restrictions associated with changes to the system are approved.

[h]
Logical access restrictions associated with changes to the system are enforced.

Key Discussion Points

Physical AND Logical: Both dimensions are required — who can physically touch the hardware AND who can log in and make changes must be defined and controlled.

All Four Steps: Define, document, approve, and enforce — for both physical and logical access. That's 8 objectives total, all required.

Temp Vendor Accounts: The guide example shows a temporary privileged account for a vendor that is disabled after the work is complete — least privilege in action.

Change Windows: Restricting when changes can be made (e.g., only between 8–10 AM) is a valid access restriction mechanism under this control.

Assessment Methods

EXAMINE

Configuration management policy; procedures addressing access restrictions for changes; system security plan; configuration management plan; logical access approvals; physical access approvals; access credentials; change control records; system audit logs.

INTERVIEW

Personnel with logical access control responsibilities; personnel with physical access control responsibilities; personnel with information security responsibilities; system or network administrators.

TEST

Organizational processes for managing access restrictions associated with changes; mechanisms supporting, implementing, and enforcing access restrictions associated with changes.

CM.L2-3.4.5

CONFIGURATION MANAGEMENT — Access Restrictions for Change

Plain English

What this control is really saying:

Not just anyone should be able to walk into the server room or log into a system to make changes. This control requires that you define who is authorized to make physical and logical changes, document and approve that list, and then technically enforce it. Unauthorized changes — even well-intentioned ones — are a security risk.

How it is used:

- Server room physical access is restricted by keycard — only three named individuals are authorized and documented in the access control records.
- Logical changes require a named privileged account; vendor access is via temporary accounts that expire 24 hours after the change window closes.
- All authorized change-makers are documented in the SSP with their role, access type, and approval date.
- Group Policy prevents software installation and configuration changes by non-privileged accounts — only named admins can make system changes.

Real World Example

The Scenario

Acme Defense has a server room accessible with a standard office key. The IT admin shares his admin credentials with two senior engineers for convenience. An MSP also has a permanent domain admin account from a project completed 18 months ago.

What the assessor finds

The MSP account is still active with full domain admin rights. Four people have the server room key with no access log. No documented list of authorized change-makers exists. The shared admin credentials mean actions cannot be attributed to a specific individual.

SPRS Score Impact

3.4.5 carries a point value of 3. Shared credentials and unrestricted physical access to systems undermine accountability — when anyone can make a change, it is impossible to know who made an unauthorized one.

What Good Looks Like

Named authorized change-makers documented and approved, physical access restricted and logged, logical access via individual accounts not shared credentials, vendor accounts time-limited and disabled post-work, restrictions documented in SSP.

Common Gaps

What assessors actually find in the field:

✗ **All admins can make changes**
Any domain admin can install software, change configs, and modify system settings — no restriction to a defined subset.

✗ **Vendor access never removed**
An MSP was given permanent admin access for a project — the account was never disabled when the work was done.

✗ **Physical access unrestricted**
The server room door uses a standard key shared with all staff — no named authorization list exists.

✗ **Access not documented**
The right people have access, but who is authorized to make changes has never been formally documented or approved.

✗ **No change window enforcement**
Changes are supposed to happen after hours but there is no technical control preventing daytime modifications.