IA.L2-3.5.5

Identification & Authentication

Identifier Reuse

"Prevent reuse of identifiers for a defined period."

Objectives

[a]

A period within which identifiers cannot be reused is defined.

[b]

Reuse of identifiers is prevented within the defined period.

Key Discussion Points

Define the Period:
The reuse prohibition period must be explicitly defined in policy — common practice is 12–24 months after an identifier is retired.

New Person, New ID:
When an employee departs and a new hire takes a similar role, the old username cannot be reassigned — even if names are identical.

Devices Too:
Device identifiers (hostnames, asset tags) are covered — a decommissioned machine's ID should not be reused on a new device.

Supports Accountability:
If an old identifier is reused, audit logs become ambiguous — actions before and after the reuse are attributed to the same ID.

Assessment Methods

EXAMINE

Identification and authentication policy; system security plan; procedures addressing authenticator management; procedures addressing user identification and authentication; system design documentation; list of system authenticator types; system configuration settings; system audit logs.

INTERVIEW

Personnel with authenticator management responsibilities; personnel with information security responsibilities; system or network administrators.

TEST

Mechanisms supporting or implementing authenticator management capability.

IA.L2-3.5.5

IDENTIFICATION & AUTHENTICATION — Identifier Reuse

Plain English

What this control is really saying:

When an employee leaves and a new person takes their role, giving the new employee the old username seems harmless — but it muddies your audit trail. If something malicious happened under that username, you can no longer be sure which person did it. This control requires that retired identifiers stay retired for a defined period.

How it is used:

- Policy defines a 24-month identifier reuse prohibition — no username or device ID retired in the past 24 months may be reassigned.
- When an employee departs, the account is disabled immediately and flagged in Active Directory with the termination date.
- New hires whose names match departed employees receive a sequentially numbered variant (e.g., jsmith02) rather than the previous ID.
- Device hostnames are documented in the asset inventory with a decommission date — retired identifiers are not reused for 24 months.

Real World Example

The Scenario

Acme Defense had an employee named Mike Smith who left the company. Six months later a new employee also named Mike Smith joined. The IT admin reactivated and renamed the original msmith account for the new employee without creating a new identifier.

What the assessor finds

The new Mike Smith now has an account with activity records stretching back to the previous employee's tenure. No identifier reuse policy exists. Audit logs from 18 months ago and audit logs from last week are attributed to the same msmith identifier.

SPRS Score Impact

3.5.5 carries a point value of 3. Identifier reuse corrupts the audit trail — when an old username is recycled, all historical log data for that identifier becomes ambiguous and potentially unreliable in an investigation.

What Good Looks Like

Reuse prohibition period defined in policy (minimum 12 months recommended), departed accounts disabled and retained, new hires assigned new identifiers, device IDs tracked with decommission dates, Active Directory configured to prevent account name reuse.

Common Gaps

What assessors actually find in the field:

✗ **No reuse period defined**

The organization has no policy defining how long a retired identifier must remain inactive before reuse.

✗ **Old accounts reassigned**

When employees depart, their username is renamed and handed to the new hire — the old audit trail is now shared.

✗ **Device IDs recycled**

When a workstation is replaced, the new machine gets the same hostname — no reuse prohibition period is observed.

✗ **Policy exists but not enforced**

A reuse period is defined in policy but Active Directory has no technical control preventing reuse of a disabled account name.

✗ **No tracking of retired IDs**

Departed accounts are deleted rather than retained — there is no record of what usernames were previously in use.