AU.L2-3.3.9

Audit & Accountability

Audit Management

"Limit management of audit logging functionality to a subset of privileged users."

Objectives

[a]

A subset of privileged users granted access to manage audit logging functionality is defined.

[b]

Management of audit logging functionality is limited to the defined subset of privileged users.

Key Discussion Points

Subset of Privileged:
Not all privileged users get audit management rights — it's a smaller, specifically designated group within the privileged tier.

Separation of Duties:
The person who administers systems should not also control the audit logs — they could suppress evidence of their own actions.

Define It in Writing:
The subset must be formally defined — a named list of roles or individuals documented in the SSP or access control records.

Extends 3.3.8:
3.3.8 protects logs from everyone. 3.3.9 specifically limits who among privileged users can manage the logging function itself.

Assessment Methods

EXAMINE

Audit and accountability policy; access control policy; procedures addressing protection of audit information; system security plan; system configuration settings; access authorizations; system-generated list of privileged users with access to audit logging management; access control list; system audit logs.

INTERVIEW

Personnel with audit and accountability responsibilities; personnel with information security responsibilities; system or network administrators; system developers.

TEST

Mechanisms managing access to audit logging functionality.

AU.L2-3.3.9

AUDIT & ACCOUNTABILITY — Audit Management

Plain English

What this control is really saying:

Just because someone is a privileged user doesn't mean they should control the audit logs. A sys admin who can disable logging can cover their own tracks. This control requires a separate, designated subset of privileged users who manage the audit function — distinct from those being audited.

How it is used:

- The SSP defines two roles: 'Audit Manager' (security officer only) and 'System Administrator' — neither role holds both designations.
- Only the security officer has permissions to modify audit log settings, change retention periods, or disable logging on any system.
- The IT admin has full system admin rights but cannot access SIEM configuration or modify audit policy via Group Policy.
- The list of personnel with audit management rights is reviewed and reaffirmed annually as part of the access review process.

Real World Example

The Scenario

Acme Defense has one IT admin who manages all systems and also controls all audit logging — configuring what is logged, setting retention periods, and reviewing logs. There are no other privileged users and no separation of the audit management function.

What the assessor finds

No subset of privileged users is defined for audit management — there is only one IT admin who controls everything. The same person who is subject to audit can disable, modify, or clear logs. No documentation exists of who has audit management rights.

SPRS Score Impact

3.3.9 carries a point value of 3. When the person being audited also controls the audit log, the entire AU domain is undermined — separation of the audit management function is what makes the program credible.

What Good Looks Like

Audit manager role formally defined and documented in SSP, assigned to a named individual separate from general sys admins, access control list reflects the designation, reviewed annually, sys admins cannot modify audit settings.

Common Gaps

What assessors actually find in the field:

✗ **All admins control logging**

Any domain admin can modify audit policy, change log settings, or clear logs — no subset is defined.

✗ **No subset defined in writing**

The organization assumes the IT admin handles auditing but has never formally designated who manages the audit function.

✗ **Roles conflated**

The same person who administers systems also manages audit logging — a single individual can suppress their own audit trail.

✗ **No access control list**

No ACL or role assignment restricts audit management functions to a specific subset of privileged users.

✗ **Vendor has audit access**

An MSP with admin rights also has unrestricted access to audit log settings — not a designated subset.