AU.L2-3.3.4

Audit & Accountability

Audit Failure Alerting

"Alert in the event of an audit logging process failure."

Objectives

[a]

Personnel or roles to be alerted in the event of an audit logging process failure are identified.

[b]

Types of audit logging process failures for which an alert will be generated are defined.

[c]

Identified personnel or roles are alerted in the event of an audit logging process failure.

Key Discussion Points

Failure Types Defined:
Hardware errors, software failures, audit mechanism failures, and log storage capacity exhaustion all count as audit logging failures.

Named Recipients:
Who gets the alert? System admin, security officer — specific people or roles must be identified in advance.

Automated Alerting:
The alert must be automated — email, SMS, SIEM alert. Manual checking for failures does not satisfy this control.

Adversary Consideration:
An attacker may deliberately cause audit logging to fail to hide their tracks. Alert response must account for this possibility.

Assessment Methods

EXAMINE

Audit and accountability policy; procedures addressing response to audit logging processing failures; system security plan; system configuration settings; list of personnel to be notified in case of an audit logging processing failure; system incident reports; system audit logs and records.

INTERVIEW

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

TEST

Mechanisms implementing system response to audit logging process failures.

AU.L2-3.3.4

AUDIT & ACCOUNTABILITY — Audit Failure Alerting

Plain English

What this control is really saying:

If your audit logging goes down and nobody knows it, you have a visibility gap that attackers can exploit. This control requires that someone gets alerted the moment logging fails — and that the failure types and recipients are defined before anything goes wrong, not after.

How it is used:

- The SIEM is configured to generate an automated alert to the IT admin and security officer if any log source goes silent for more than 15 minutes.
- Defined failure types include: log service stopped, disk full on log storage, log agent unreachable, and SIEM connection lost.
- Alert recipients are documented in the SSP — IT admin receives email and SMS, security officer receives email.
- A quarterly test of the alerting mechanism is conducted by temporarily stopping a non-critical log source and confirming alerts fire.

Real World Example

The Scenario

Acme Defense uses a Windows Event Collector to aggregate logs. The log storage drive on the collector is 500GB. There are no alerts configured for the logging infrastructure. The IT admin checks logs manually when investigating incidents.

What the assessor finds

The log storage drive is 94% full with no capacity alert. No audit failure alerts are configured. No recipient list exists. Three months of logs are missing from two workstations — the log agent crashed and nobody noticed.

SPRS Score Impact

3.3.4 carries a point value of 3. Silent audit failures are exactly the condition an attacker needs to operate undetected. Logs filling up quietly is one of the most common causes of audit coverage gaps in small DIB environments.

What Good Looks Like

Failure types defined in SSP, named recipients documented, automated alerts configured for log service failure and storage capacity thresholds, alerts tested periodically, response procedure defined for each failure type.

Common Gaps

What assessors actually find in the field:

✗ **No alerting configured**

Audit logging can fail silently for days — nobody would know until they tried to pull logs and found nothing.

✗ **No recipients defined**

The system has alerting capability but nobody has been designated to receive audit failure notifications.

✗ **Failure types not defined**

The organization has not defined what constitutes an audit logging failure requiring an alert.

✗ **Manual checking only**

The IT admin checks log availability once a week — not automated, not near-real-time.

✗ **Alert goes to generic inbox**

Audit failure alerts are sent to a shared 'helpdesk' email that nobody monitors outside business hours.