AU.L2-3.3.3

Audit & Accountability

Event Review

"Review and update logged events."

Objectives

[a]

A process for determining when to review logged events is defined.

[b]

Event types being logged are reviewed in accordance with the defined review process.

[c]

Event types being logged are updated based on the review.

Key Discussion Points

Config, Not Log Review:
This control is about reviewing what you are logging — not reviewing the logs themselves. That's AU.L2-3.3.5 and 3.3.6.

Defined Review Process:
When do you review? Annually? After incidents? After system changes? The trigger must be defined in policy.

Evolving Threats:
New attack techniques require new event types — VPN sessions, cloud access, or remote tools may need to be added over time.

Update, Not Just Review:
The review must result in an update if gaps are found — reviewing and doing nothing does not satisfy [c].

Assessment Methods

EXAMINE

Audit and accountability policy; procedures addressing audit records and event types; system security plan; list of event types to be logged; reviewed and updated records of logged event types; system audit logs and records; system incident reports.

INTERVIEW

Personnel with audit and accountability responsibilities; personnel with information security responsibilities.

TEST

Mechanisms supporting review and update of logged event types.

AU.L2-3.3.3

AUDIT & ACCOUNTABILITY — Event Review

Plain English

What this control is really saying:

The threat landscape changes. New systems get added. Old assumptions become wrong. This control requires you to periodically look at your event type list and ask: is this still the right set of things to be logging? And if the answer is no, you have to update it.

How it is used:

- The SSP defines an annual event type review process and a triggered review after any security incident or major system change.
- The event type list is maintained as a controlled document — version history shows when it was last reviewed and what changed.
- After a phishing incident last year, the review added email gateway logging to the event type list.
- The most recent review added cloud storage access events after Microsoft 365 was deployed as a CUI storage platform.

Real World Example

The Scenario

Acme Defense configured audit logging when they built their current environment two years ago. Since then they added a Microsoft 365 tenant and a new CNC machine. The original event type list has not been touched.

What the assessor finds

No review process is defined. The event type list has never been updated. Microsoft 365 access events are not captured. The new CNC machine is not in scope for logging. No records of any review activity exist.

SPRS Score Impact

3.3.3 carries a point value of 3. A static logging configuration that was never revisited after new systems were added leaves visibility gaps that attackers can exploit.

What Good Looks Like

Review process defined in SSP with triggers (annual, post-incident, post-system-change), event type list maintained as controlled document, reviews documented with dates and changes recorded, new systems evaluated for logging scope on deployment.

Common Gaps

What assessors actually find in the field:

✗ **No review process defined**

The organization has never documented when or how event types should be reviewed — no process exists.

✗ **Set-and-forget logging**

Logging was configured three years ago at system build and has never been reviewed or updated since.

✗ **Review without update**

An annual review occurs but no changes are ever made — the list is treated as permanent rather than living.

✗ **New systems not evaluated**

A new cloud storage platform was added but nobody assessed what new event types should be captured from it.

✗ **No documentation of reviews**

Staff say they review logging periodically but cannot produce any records of when reviews occurred or what changed.