AU.L2-3.3.1

Audit & Accountability

System Auditing

"Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity."

Objectives

[a]
Audit logs needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity are specified.

[b]
The content of audit records needed to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity is defined.

[c]
Audit records are created (generated).

[d]
Audit records, once created, contain the defined content.

[e]
Retention requirements for audit records are defined.

[f]
Audit records are retained as defined.

Key Discussion Points

Define First, Then Log:
Before logging, organizations must define which event types to capture and what content each record must contain.

Record Content:
Timestamps, source/destination addresses, user identifiers, event descriptions, and success/failure indicators are all expected.

Retention Period:
Logs must be retained long enough to support incident investigation — attackers may lurk weeks or months before discovery.

All CUI Systems:
Every system that processes, stores, or transmits CUI must generate audit records — not just servers.

Assessment Methods

EXAMINE

Audit and accountability policy; procedures addressing auditable events; system security plan; system configuration settings; procedures addressing control and generation of audit records; system audit logs and records; system incident reports.

INTERVIEW

Personnel with audit and accountability responsibilities; personnel with information security responsibilities; personnel with audit review, analysis and reporting responsibilities; system or network administrators.

TEST

Mechanisms implementing system audit logging.

AU.L2-3.3.1

AUDIT & ACCOUNTABILITY — System Auditing

Plain English

What this control is really saying:

If you don't log it, you can't prove what happened — or that anything happened at all. Audit logs are the forensic record of your CUI environment. You need to know what to log, make sure it's actually being logged, verify the records contain what they're supposed to, and keep them long enough to be useful.

How it is used:

- Auditable event types are defined in the SSP — logon success/failure, privilege use, account changes, file access, and system restarts.
- Windows Event Logging and Syslog are configured on all CUI systems to capture timestamps, user ID, source IP, event type, and success/failure.
- Audit log retention is set to 12 months on all systems — 90 days online, 9 months archived — consistent with the SSP.
- Log completeness is verified quarterly by reviewing a sample of systems to confirm required events are being captured.

Real World Example

The Scenario

Acme Defense runs Windows workstations, a file server, and a CNC machine controller in their CUI environment. The IT admin enabled Windows Event Logging on the workstations last year. The file server and CNC controller have never been configured.

What the assessor finds

No auditable event types are defined in the SSP. The file server has no logging. Workstation logs overwrite after 7 days. The CNC controller has no logging capability documented. No retention policy exists.

SPRS Score Impact

3.3.1 carries a point value of 5. Without audit logs you cannot detect, investigate, or prove any security incident — it's the foundation for the entire AU domain.

What Good Looks Like

Event types defined in SSP, logging enabled on all CUI systems, records contain timestamps/user IDs/event type/success-failure, retention policy documented and enforced, log completeness verified periodically.

Common Gaps

What assessors actually find in the field:

✗ No audit logging configured

CUI systems have default logging only — no defined event types, no centralized collection, no retention policy.

✗ Logs missing required content

Logs exist but lack timestamps, user IDs, or success/failure indicators needed for investigation.

✗ No retention policy

Logs are overwritten after 30 days — far too short to detect a compromise that occurred months earlier.

✗ Some systems not logging

The file server and CNC workstation have logging disabled — CUI access on these systems is completely unrecorded.

✗ Event types not defined

Logging is on but the organization has never defined which events to capture — the log is cluttered and incomplete.