AU.L2-3.3.2

Audit & Accountability

User Accountability

"Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions."

Objectives

[a]

The content of the audit records needed to support the ability to uniquely trace users to their actions is defined.

[b]

Audit records, once created, contain the defined content.

Key Discussion Points

Individual Traceability:
Every logged action must tie back to a specific named user — shared accounts make this impossible.

Key Fields Required:
User ID, source/destination address, machine name, and timestamp are the minimum for individual traceability.

Non-Repudiation:
The purpose is to prevent users from denying their actions — logs must make denial implausible.

Extends 3.3.1:
3.3.1 defines what to log. 3.3.2 ensures the logs actually tie actions to individuals — both must be met.

Assessment Methods

EXAMINE

Audit and accountability policy; procedures addressing audit records and event types; system security plan; system configuration settings; procedures addressing audit record generation; reports of audit findings; system audit logs and records; system incident reports.

INTERVIEW

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

TEST

Mechanisms implementing system audit logging.

AU.L2-3.3.2

AUDIT & ACCOUNTABILITY — User Accountability

Plain English

What this control is really saying:

Logging is only useful if you can answer 'who did that?' A log that shows an action occurred but can't tell you which specific person did it is not enough. This control requires that your audit records actually tie actions to individual users — not just to a workstation, a shared account, or a service.

How it is used:

- Every user has a unique Active Directory account — no shared accounts permitted on CUI systems.
- VPN logs capture user ID, source IP, machine name, and timestamp for every remote access session.
- File server audit logs record the username, file accessed, action taken, and timestamp for all CUI file activity.
- Audit record content requirements are documented in the SSP and verified against actual log output quarterly.

Real World Example

The Scenario

Acme Defense configures VPN logging and file server access logging. Three engineers share an 'engineer' login on the CNC workstation for convenience. The VPN logs IP addresses but not user IDs — the RADIUS server is not integrated.

What the assessor finds

CNC workstation actions cannot be traced to an individual — three people share one account. VPN logs show which IP connected but not which user authenticated. Individual traceability is broken on two of three CUI access paths.

SPRS Score Impact

3.3.2 carries a point value of 5. Shared accounts and missing user IDs in logs make forensic investigation impossible — you can prove something happened but not who did it.

What Good Looks Like

All users have unique individual accounts, no shared accounts on CUI systems, logs capture user ID on every event, VPN integrated with RADIUS for user-level attribution, audit record content verified against SSP definition.

Common Gaps

What assessors actually find in the field:

✗ **Shared accounts in use**

Multiple employees share a single 'admin' or 'operator' login — actions cannot be traced to any individual.

✗ **No user ID in logs**

Logs capture the event but not the user — 'someone' deleted a CUI file but the log has no username.

✗ **Machine-level logging only**

Logs track which workstation performed an action but not which user was logged in at the time.

✗ **VPN not logging user IDs**

Remote access logs show IP addresses but are not correlated to authenticated user identities.

✗ **Generic service accounts**

Applications run under a shared service account — all activity is attributed to that account, not individual users.