AU.L2-3.3.7

Audit & Accountability

Authoritative Time Source

"Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records."

Objectives

[a]
Internal system clocks are used to generate time stamps for audit records.

[b]
An authoritative source with which to compare and synchronize internal system clocks is specified.

[c]
Internal system clocks used to generate time stamps for audit records are compared to and synchronized with the specified authoritative time source.

Key Discussion Points

NTP Required:
Network Time Protocol (NTP) is the standard mechanism — all systems must sync to the same authoritative NTP source.

Why It Matters:
If clocks differ between systems, log entries cannot be reliably correlated — incident timelines fall apart.

UTC or Local + Offset:
Time must be expressed in UTC or local time with a UTC offset — this enables cross-system and cross-timezone correlation.

Specify the Source:
The authoritative time source must be explicitly specified — pointing to 'time.windows.com' or a domain controller counts.

Assessment Methods

EXAMINE

Audit and accountability policy; procedures addressing time stamp generation; system design documentation; system security plan; system configuration settings; system audit logs and records.

INTERVIEW

Personnel with information security responsibilities; system or network administrators; system developers.

TEST

Mechanisms implementing time stamp generation; mechanisms implementing internal system clock synchronization.

AU.L2-3.3.7

AUDIT & ACCOUNTABILITY — Authoritative Time Source

Plain English

What this control is really saying:

Audit logs from five systems that all show slightly different times are nearly useless for incident investigation. Time synchronization sounds trivial but it's the invisible foundation that makes every other AU control work. If the timestamps don't agree, the timeline doesn't hold together.

How it is used:

- All Windows workstations and servers are joined to Active Directory — Group Policy configures NTP to sync to the domain controller.
- The domain controller is configured to sync to time.windows.com (pool.ntp.org) as the authoritative external time source.
- The NTP server and time source are documented in the SSP — confirmed via Group Policy review and w32tm /query /status.
- Network devices (firewall, switches) are independently configured with the same NTP server to ensure log timestamp consistency.

Real World Example

The Scenario

Acme Defense has five Windows workstations and a Linux file server. The workstations are joined to a domain but NTP is not configured via Group Policy. The Linux server's time settings have never been touched since deployment two years ago.

What the assessor finds

The Linux server clock is 23 minutes behind the workstations. No NTP server is specified in the SSP. The assessor cross-references a file access event across workstation and server logs and finds the timestamps are irreconcilably different.

SPRS Score Impact

3.3.7 carries a point value of 3. Unsynchronized clocks undermine the reliability of every other AU control — a log timeline that doesn't hold together is useless for incident investigation or legal proceedings.

What Good Looks Like

All systems synced to same authoritative NTP source, time source documented in SSP, domain-joined systems configured via GPO, non-domain devices configured independently, NTP status verified periodically.

Common Gaps

What assessors actually find in the field:

✗ **No NTP configured**

Systems use local hardware clocks with no synchronization — timestamps drift and diverge over time.

✗ **No authoritative source named**

NTP is enabled but the organization has never documented which time source is authoritative for the environment.

✗ **Network devices excluded**

Workstations sync via NTP but the firewall and switches use their own unconfigured clocks — log timestamps don't align.

✗ **Significant clock drift**

Systems were configured with NTP but the service stopped — clocks are now off by 15+ minutes.

✗ **No verification**

NTP is configured but nobody has ever verified it is functioning and keeping clocks synchronized.