HYRELOG

SECURE. IMMUTABLE. AUDITABLE.

SOC 2 Audit Trail Checklist

A practical framework used by SaaS teams preparing for enterprise security reviews and SOC 2 assessments.

This checklist reflects common questions raised during enterprise procurement and independent audit processes. It is designed to help technical leaders evaluate whether their audit logging architecture is defensible, complete, and review ready.

hyrelog.com

SOC 2 Audit Trail Readiness Framework

Use this structured checklist to assess whether your audit logging architecture meets enterprise expectations.

---

1. Audit Log Coverage

- Are all security sensitive actions logged including authentication, role changes, exports, billing, and administrative actions?
- Are both user and system initiated actions captured?
- Do logs include actor, action, target, timestamp, IP address, and contextual metadata?
- Are failed login attempts and permission denials recorded?

2. Integrity and Tamper Protection

- Can logs be altered or deleted by application level roles?
- Is there tamper evident or immutable protection implemented?
- Is log integrity verifiable using cryptographic methods such as hash chains?
- Is access restricted using role based controls?

3. Retention and Storage Controls

- Is a documented retention policy enforced technically and procedurally?
- Are logs retained for at least one year or longer where required?
- Is long term archival secure and access controlled?
- Is there a documented legal hold process?

4. Data Residency and Regional Controls

- Can audit logs be restricted to specific geographic regions if required?
- Are residency policies enforced at the storage layer rather than application logic?
- Is access to audit logs itself fully logged and monitored?

5. Search and Investigative Capability

- Can logs be filtered by user, entity, action, and date range?
- Can teams reconstruct a defensible sequence of events?
- Are investigation workflows clearly documented?

6. Export and Evidence Preparation

- Can logs be exported in structured formats such as CSV or JSON?
- Is export activity itself logged?
- Can evidence bundles be generated specifically for SOC 2 reviews?

7. Monitoring and Alerting

- Are critical audit events monitored continuously?
- Are alerts generated for privilege escalation or sensitive configuration changes?
- Are integrity failures detectable?

8. Documentation and Governance Alignment

- Is the audit logging architecture formally documented?
- Are responsibilities clearly assigned?
- Does logging align with written security and compliance policies?

HYRELOG

SECURE. IMMUTABLE. AUDITABLE.

Enterprise Security Reviews Expect Defensible Audit Trails

HyreLog provides immutable, compliance grade audit logging built specifically for SaaS companies moving upmarket.

If you are preparing for SOC 2, ISO 27001, GDPR requirements, or enterprise procurement questionnaires, we would welcome a conversation.

Join the waitlist at hyrelog.com

HyreLog. Secure. Immutable. Auditable.