QORTARA CLOUD GOVERNANCE

SOC 2 Evidence

SOC 2 Evidence

Qortara is designed to map your AI agent governance to the SOC 2 Trust Services Criteria and to generate the evidence your auditor examines. Instead of compiling evidence by hand, you produce it from the actual runtime behavior of your agents: the allow and deny decisions, the policy versions behind them, and a tamper-evident record of the whole sequence.

> **Read this first.** Qortara does not hold SOC 2 certification or any third-party certification. Qortara does not issue a SOC 2 report and using Qortara does not make your organization compliant with SOC 2 or any other framework. What Qortara is designed to do is generate evidence that you can hand to your own auditor for the agent-governance portion of their examination. Your auditor (a CPA firm) determines whether your controls and evidence satisfy the criteria.

Availability

The export commands, compliance scans, and evidence endpoints on this page are part of Qortara Cloud Governance, the hosted control plane. That product is in pre-launch and has not been deployed, so the endpoints below describe the pre-launch design rather than a running service. The underlying governance decisions and their tamper-evident records are produced by the open-source Qortara Governance sidecar today.

Control Mapping

This table shows how Qortara governance evidence is designed to support specific SOC 2 controls. It is a mapping of evidence to criteria, not a certification.

SOC 2 Control	Criteria	What Qortara is designed to generate
CC6.1	Logical and Physical Access Controls	Evidence that agents are restricted to authorized resources: a policy evaluation log showing allow and deny decisions per agent per resource pattern.
CC6.2	System Access Authentication	Evidence that agents are authenticated before accessing resources: auth enforcement records and agent identity verification.
CC6.3	Termination Procedures	Evidence that deactivated agents can no longer act: agent lifecycle events showing deactivation followed by denial of subsequent access attempts.

CC6.6	External Access Management	Evidence that cross-organization interactions are governed: trust federation attestations and cross-org trust-score requirements in policies.
CC7.2	System Monitoring	Evidence that governance events are monitored in real time: webhook configuration showing the SIEM integration plus event delivery history.
CC8.1	Change Management	Evidence that policy changes are tracked and auditable: policy version history and a tamper-evident chain of every modification.

What Your Auditor Wants to See

A SOC 2 Type II audit covering an AI agent fleet typically asks for the evidence categories below. Each one shows what the auditor is checking and the pre-launch export command that is designed to produce it.

1. Policy Documentation (CC6.1, CC8.1)

What: your active policies and their version history.

```bash
# List all active policies
curl https://api.qortara.com/v1/policy/policies \
  -H "$AUTH_HEADER"

# Get version history for a specific policy
curl https://api.qortara.com/v1/policy/policies/pol_789ghi/versions \
  -H "$AUTH_HEADER"
```

What the auditor verifies: policies exist, are documented with descriptions, have version history showing when they were created and modified, and cover the access patterns in your agent fleet.

2. Access Decision Log (CC6.1, CC6.2)

What: a complete log of every policy evaluation over the audit period (typically 3 to 12 months).

```bash
curl "https://api.qortara.com/v1/portal/audit?start=2025-10-01&end=2026-04-01&limit=10000" \
  -H "$AUTH_HEADER"
```

What the auditor verifies: every agent action went through policy evaluation (no bypasses), deny decisions were enforced (the agent did not subsequently reach the resource), and the log is complete and tamper-evident.

3. Chain Integrity Proof (CC8.1)

What: verification that the audit trail has not been tampered with.

```bash
curl "https://api.qortara.com/v1/portal/audit/verify?offset=0&limit=50000" \
  -H "$AUTH_HEADER"
```

```json
{
  "verified": 48723,
  "total": 48723,
  "valid": true,
  "first_break": null
}
```

What the auditor verifies: `valid` is `true` and `verified` equals `total`, meaning every event in the chain is intact. If `first_break` is not null, there is a tampered or missing event at that position, which is an audit finding.

4. Monitoring Configuration (CC7.2)

What: proof that governance events are being monitored, not just logged.

```bash
# Show webhook endpoints (SIEM integrations)
curl https://api.qortara.com/v1/portal/webhooks \
  -H "$AUTH_HEADER"

# Show delivery history (proof events are reaching the SIEM)
curl "https://api.qortara.com/v1/portal/webhooks/wh_abc123/deliveries?limit=100" \
  -H "$AUTH_HEADER"
```

What the auditor verifies: at least one webhook endpoint is configured and active, the delivery success rate is high, and the SIEM is actually processing the events (your auditor may ask for SIEM dashboard screenshots).

5. Compliance Scan History

What: the trend of your governance scan results over time.

```bash
curl "https://api.qortara.com/v1/compliance/reports?framework=soc2" \
```

```
  -H "$AUTH_HEADER"
```

What the auditor verifies: scans run regularly (at least monthly), results are stable or improving, and findings are remediated promptly (compare findings across consecutive scans).

Tips for a Clean SOC 2 Audit

1. **Run governance scans at least monthly.** Weekly is better. A consistent trend is something auditors look for.

2. **Remediate findings within 30 days.** If a scan flags a CC7.2 gap (no SIEM), configure a webhook endpoint. Auditors check that findings are addressed, not just recorded.

3. **Keep at least three active policies.** This gives CC6.1 (logical access) real coverage and gives CC8.1 (change management) something to track. The built-in templates in the policy authoring guide are good starting points.

4. **Configure at least one webhook endpoint.** Even pointing a webhook at a simple HTTP logger satisfies the monitoring intent of CC7.2.

5. **Deactivate policies, do not delete them.** Auditors want the full history, including retired policies. Deactivation preserves the version chain.

6. **Export everything about 30 days before the audit.** That gives your compliance team time to review the data and close any gaps before the auditor arrives.

What Qortara Does NOT Provide

Be honest with your auditor and with yourself about the boundary.

- **Qortara does not provide a SOC 2 report.** It generates the evidence your auditor examines. The actual report is issued by your auditor, a CPA firm.
- **Qortara does not cover all SOC 2 criteria.** It is designed to support the agent-governance-relevant criteria (CC6.1, CC6.2, CC6.3, CC6.6, CC7.2, CC8.1). Your overall SOC 2 posture also includes infrastructure, HR, physical security, and other areas that Qortara does not address.
- **Qortara does not hold SOC 2 certification.** Qortara is designed to generate evidence for your audit. Qortara itself is pre-launch and has not completed its own SOC 2 examination, and nothing here should be read as a claim that it has.

Related

- [Compliance Evidence](/docs/concepts/compliance-evidence): what an evidence record contains.

- [Policy Authoring](/docs/guides/policy-authoring): write the policies whose decisions become evidence.
- [Webhooks and Events](/docs/concepts/webhooks-events): stream governance decisions into a SIEM for CC7.2.

Product: Qortara Cloud Governance
Source owner: Qortara
Last reviewed: 2026-06-10
Verified against: Qortara pre-launch docs