Compliance Evidence

Compliance Evidence

Compliance evidence is the audit-ready record that governance activity produces. Qortara does not only enforce policy; it records each decision, scan, and verification in a structured, tamper-evident form that maps to compliance framework controls, so the work of demonstrating governance is largely a byproduct of doing it.

> **Availability.** Compliance evidence generation and reporting are Qortara Cloud Governance capabilities and are in pre-launch. The endpoints, report shapes, and framework mappings below describe the hosted design. They are designed to support the named frameworks; they are not a certification, and using Qortara does not by itself make you compliant.

How evidence is generated

Evidence is produced two ways.

1. **Continuously.** Every policy evaluation produces a governance record that maps to specific framework controls. This is designed to happen automatically, with no per-event configuration.
2. **On demand.** A compliance scan evaluates your tenant's overall posture against a chosen framework and produces a scored report with findings and recommendations.

Both feed the same underlying record. The continuous stream is the detailed history; the scan is a periodic, framework-shaped summary built on top of it.

Supported frameworks

Framework	What Qortara is designed to map
SOC 2	Logical access (CC6.1), system authentication (CC6.2), monitoring (CC7.2), change management (CC8.1), external access (CC6.6), termination (CC6.3)
GDPR	Processing principles (Art. 5), lawful basis (Art. 6), data protection by design (Art. 25), records of processing (Art. 30), security of processing (Art. 32)
EU AI Act	Risk management (Art. 9), record-keeping (Art. 12), transparency (Art. 13), human oversight (Art. 14), accuracy and robustness (Art. 15)
NIST AI RMF	Govern, Map, Measure, and Manage functions

These mappings describe what Qortara is designed to support, not a guarantee that a

given control is satisfied in your environment. EU AI Act Article 12 record-keeping in particular is supported by Qortara's tamper-evident governance records, but that is a design intent ("designed for" record-keeping), not a certification. Whether your overall system meets Article 12, or any other control, is determined by your auditor and your full implementation, not by Qortara alone.

Running a compliance scan

```bash
curl -X POST https://api.qortara.com/v1/compliance/scan \
  -H "$AUTH_HEADER" \
  -H "Content-Type: application/json" \
  -d '{
    "framework": "soc2",
    "context": {
      "tenant_id": "qor:your-tenant-id",
      "agent_count": 5,
      "policies_active": 3
    }
  }'
```

A scan returns a scored report with the controls that passed, the findings that did not, and concrete remediation guidance.

```json
{
  "id": "rpt_soc2_20260410",
  "framework": "soc2",
  "status": "partial",
  "score": 0.83,
  "total_checks": 6,
  "passed_checks": 5,
  "scanned_at": "2026-04-10T12:00:00Z",
  "findings": [
    {
      "check_id": "CC7.2",
      "control": "System Monitoring",
      "status": "fail",
      "detail": "No webhook endpoints configured for real-time event delivery",
      "remediation": "Configure at least one webhook endpoint for event delivery"
    }
  ],
  "passed": [
    {"check_id": "CC6.1", "control": "Logical Access Controls", "detail": "Active policies enforce access restrictions"},
    {"check_id": "CC6.2", "control": "System Authentication", "detail": "Signed
```

authentication enforced on write routes"},
    {"check_id": "CC8.1", "control": "Change Management", "detail": "Policy versioning active with an audit trail"},
    {"check_id": "CC6.6", "control": "External Access", "detail": "Trust attestations configured for cross-org interactions"},
    {"check_id": "CC6.3", "control": "Termination Procedures", "detail": "Agent deactivation procedures in place"}
  ]
}
```

The score and findings are diagnostic, not a pass or fail verdict on your program. A finding tells you where evidence is thin and what to do about it; the remediation field points at a concrete next step.

## What triggers evidence generation

| Trigger | Evidence produced | Frequency |
| --- | --- | --- |
| Each policy evaluation | A governance record with the decision, policy, agent, and framework tags | Per evaluation (100 to 10,000 per day is typical) |
| A compliance scan | A scored report with findings and recommendations | On demand (daily is a reasonable cadence, monthly a minimum) |
| A cross-org trust lookup | A signed trust attestation with a Merkle proof | Per lookup |
| A saga verification | A verified or mismatch result linked to the original action | Per saga step |
| A budget threshold crossing | A budget alert event | Event-driven |

## Presenting evidence to an auditor

For a SOC 2 review, an auditor typically wants to see five things, and Qortara is designed to produce each as an export.

1. **That policies exist.** Export your active policies.
2. **That policies are enforced.** Export governance records over the audit period showing allow and deny decisions.
3. **That the record is tamper-evident.** Run a chain integrity verification to show the records have not been altered.
4. **That scans pass over time.** Export scan history for the framework to show your score trend.
5. **That monitoring is in place.** Show your webhook configuration and SIEM integration.

The combination of a continuous governance record, periodic scans, and a tamper-evident chain is designed to give an auditor a complete and verifiable picture of governance posture over the period under review.
```

Export formats

Format	How you get it
JSON	All API responses are JSON by default.
Structured report	Retrieve a full scan report by its report id.
Governance records	Export records with pagination over a date range.
Chain verification	Request an integrity proof over a range of records.

JSON is the native format. If you need a document for a reviewer, your compliance team's reporting tools can render the JSON into their preferred format.

Limits and caveats

- Compliance evidence and reporting are hosted Cloud Governance and are pre-launch.
- Evidence can support a compliance program, but it does not guarantee compliance. Your auditor decides whether the control and the evidence satisfy your requirements.
- Framework mappings describe what Qortara is designed to support. They are not certifications, and they cover only the controls Qortara is positioned to observe, not your entire system.
- Evidence reflects the activity that actually flowed through Qortara. An action taken outside the governed path leaves no record, so route the activity you need to evidence through Qortara deliberately.

Related concepts

- [Policy enforcement](/docs/concepts/policy-enforcement) produces the governance records that become evidence.
- [Saga verification](/docs/concepts/saga-verification) contributes verification outcomes to the record.
- [Webhooks and events](/docs/concepts/webhooks-events) stream the same activity to your SIEM in real time.

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