SOC 2 Readiness & Gap Analysis

Representative Engagement

Executive Summary

This SOC 2 readiness assessment evaluates the organization's preparedness for a SOC 2 Type I audit, with a focus on material readiness, evidence quality, and operational realism.

The objective is not to simulate an audit, but to determine whether the organization can successfully support one without disruption, rework, or last-minute remediation.

Overall Readiness Level

Partial

Primary Gaps

Documentation consistency, incident response formalization, vendor oversight

Key Constraint

Limited internal compliance ownership

Assessment Scope

The assessment was conducted against the Trust Services Criteria (Security focus) and included:

In Scope

- Governance and policy framework
- Logical access controls
- Change management practices
- Incident response readiness
- Vendor and third-party oversight
- Evidence generation and retention

Out of Scope

- Auditor selection and coordination
- Penetration testing
- Type II operational effectiveness testing

These areas were intentionally excluded to preserve readiness focus.

Readiness Assumptions

This assessment assumes:

Timeline

A Type I audit target within 3–6 months

Maturity Stage

Early-stage to mid-stage operational maturity

Ownership Model

Engineering-led security ownership

Documentation State

Documentation exists informally but lacks consistency

Control Evidence

Controls may exist without structured evidence

Recommendations reflect these conditions.

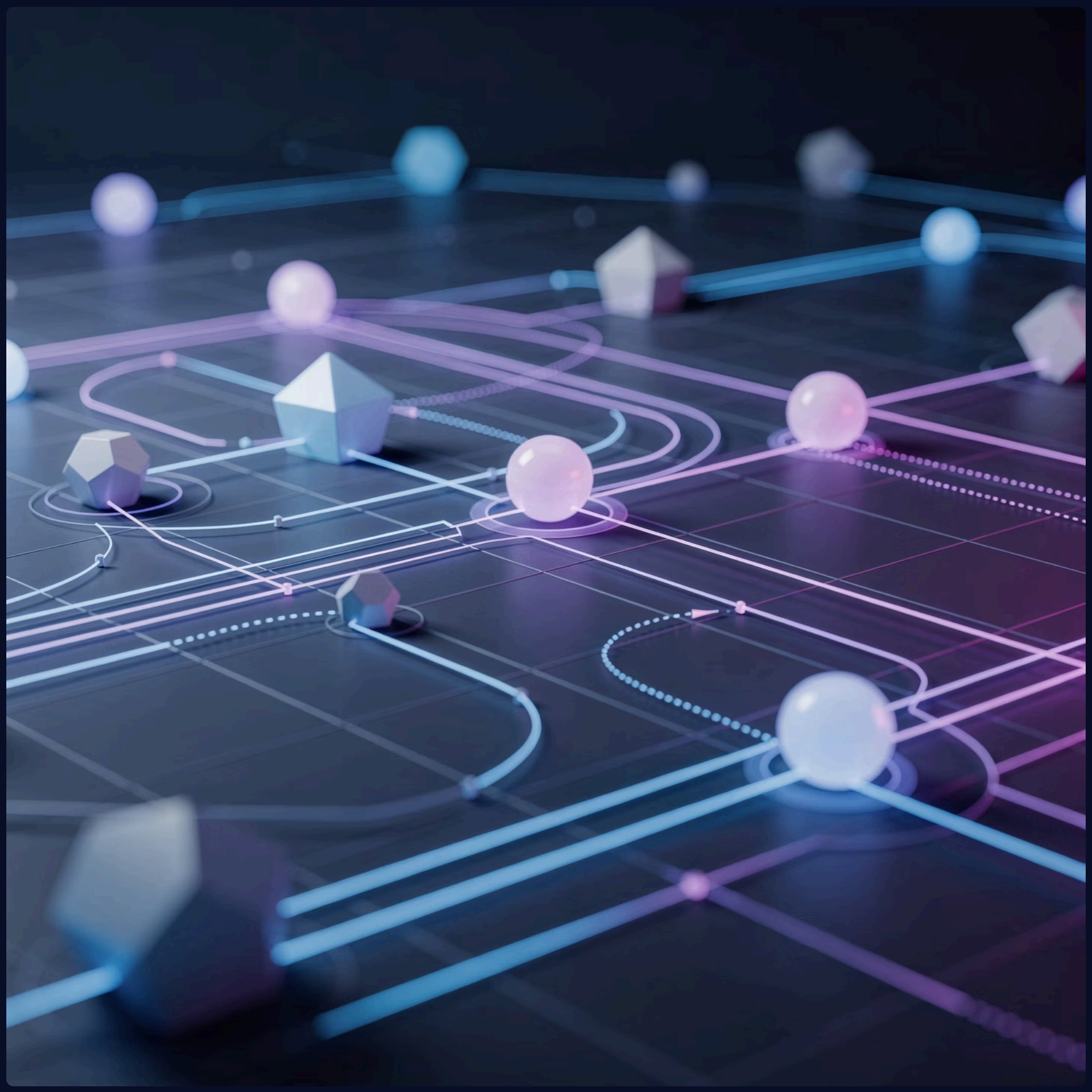
Control Maturity Framework

Controls were evaluated using a four-level maturity scale:

1	Ad hoc or informal
2	Defined but inconsistently applied
3	Implemented and repeatable
4	Measurable and monitored

Most organizations overestimate Level 3 readiness.

Trust Services Criteria Snapshot



Governance & Policies	Level 2
Access Controls	Level 3
Logging & Monitoring	Level 2
Incident Response	Level 2
Vendor Management	Level 1
Change Management	Level 2

The largest readiness risks stem from documentation and evidence, not missing controls.

Material Gaps Identified

Gap 1: Incident Response Formalization

Impact: High

Incident handling practices exist but are undocumented and lack defined escalation thresholds.

Gap 2: Vendor Risk Management

Impact: Medium

Third-party access and data handling are not consistently reviewed or documented.

Gap 3: Evidence Consistency

Impact: High

Controls are implemented but evidence collection is informal, increasing audit friction.

Evidence Risk Analysis

SOC 2 delays are more commonly caused by evidence gaps than control gaps.

Access Reviews	Medium
Change Management	High
Incident Response	High
Vendor Oversight	Medium

Evidence generation must be operationalized, not treated as a one-time task.

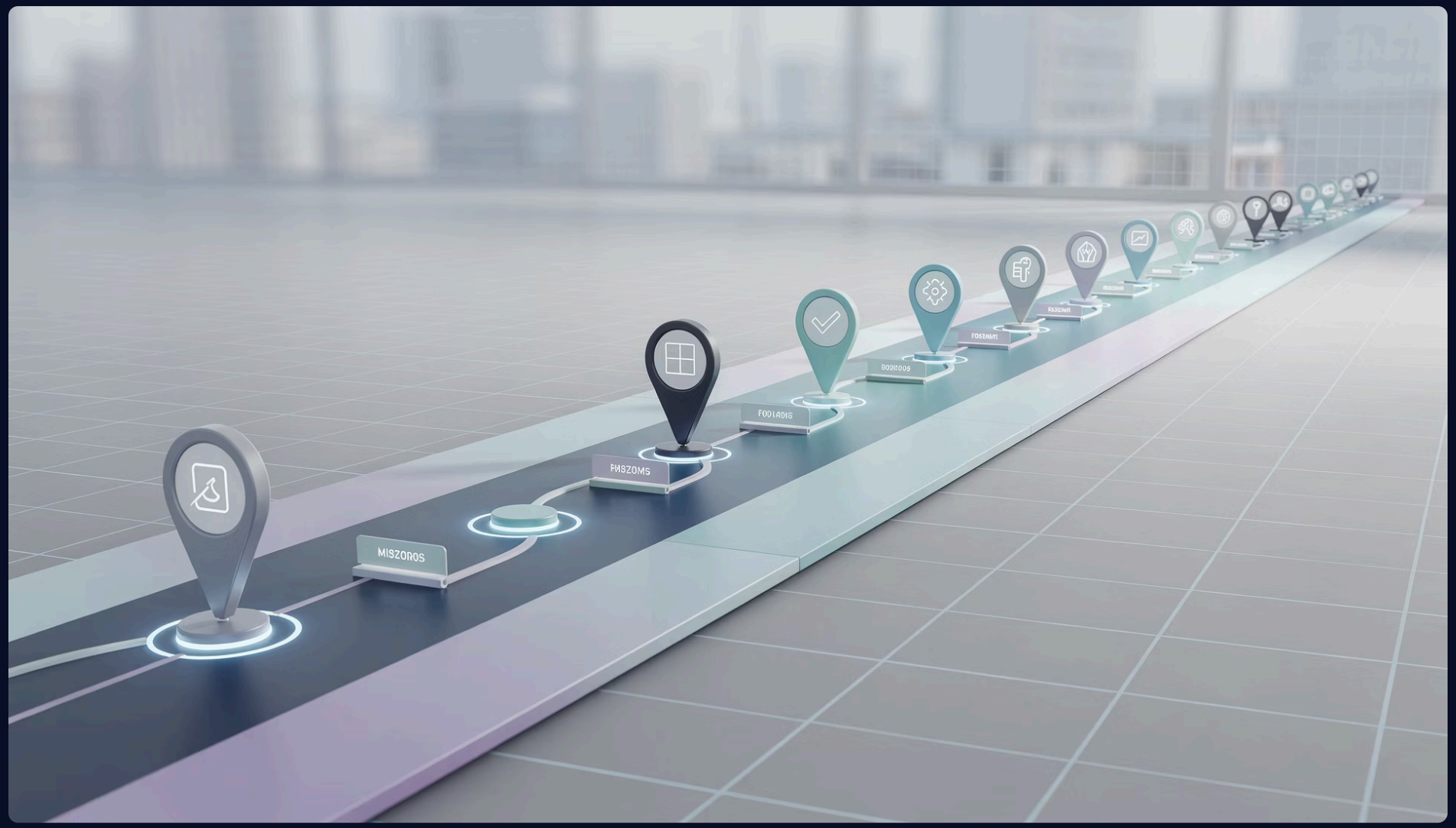
What Was Intentionally Deprioritized

The following were identified but deferred:

- **Advanced policy tooling**
- **Automated GRC platforms**
- **Continuous compliance monitoring**

These add complexity without improving near-term audit success.

Readiness Remediation Roadmap



01

Phase 1: Foundation (0–30 Days)

- Finalize core security policies
- Define incident response roles and escalation
- Identify required audit evidence

02

Phase 2: Evidence Alignment (30–60 Days)

- Establish access review cadence
- Formalize vendor review process
- Create repeatable evidence artifacts

03

Phase 3: Audit Preparation (60–90 Days)

- Conduct internal readiness walkthrough
- Validate documentation accuracy
- Align teams on audit expectations

Expected Outcome

Executing this roadmap materially reduces:

- **Audit delays**
- **Cost overruns**
- **Scope creep**
- **Internal disruption**

The organization enters the audit with predictable readiness rather than reactive remediation.

Strategic Guidance for Leadership

> SOC 2 success depends less on tooling and more on discipline, consistency, and clarity.

The most effective readiness strategy is to align controls with how the business already operates, rather than forcing artificial processes to satisfy audit optics.

Key Success Factors

Operational Realism

Controls must reflect actual business operations, not theoretical compliance frameworks that create friction and resistance.

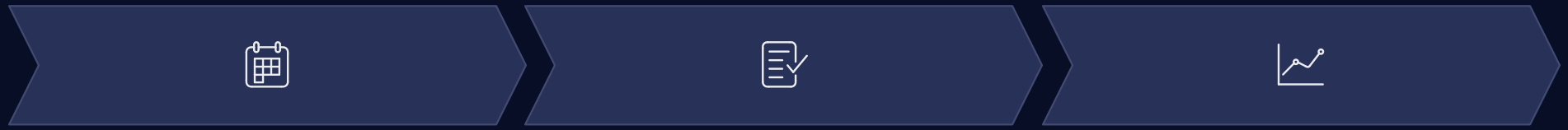
Evidence Discipline

Consistent documentation practices prevent last-minute scrambling and ensure audit readiness is maintained continuously.

Cross-Functional Alignment

Security, engineering, and operations teams must coordinate on control implementation and evidence generation.

Next Steps



Schedule Kickoff

Align stakeholders on timeline and responsibilities

Prioritize Gaps

Address high-impact evidence and documentation needs first

Track Progress

Establish weekly checkpoints to monitor remediation efforts

Footer

This document represents a sample engagement created to demonstrate methodology and deliverables. It does not reference a specific organization.