



Uno is a leading AI native platform for GRC, TPRM, ERM, and BCM. This is an assessment generated for a publicly available SOC 2 report at <https://www-assets.kolide.com/assets/marketing/documents/soc2-f9823fc1.pdf>. The assessment is based on the SOC 2 quality and reliability available at <https://s2guild.org>. This material is provided by Uno.ai, Inc. for educational and informational purposes only. No claims are made regarding the accuracy or completeness of the rubric or the assessment conducted against it, and no liability is assumed for any decisions or actions taken in reliance on this content.

SOC 2 RELIABILITY ASSESSMENT

Kolide, Inc.

Type 2 Report | January 1 – June 30, 2024

Auditor: Prescient Assurance LLC | Report Date: September 10, 2024

Assessment Date: February 17, 2026

STRUCTURE	SUBSTANCE	SOURCE
MOSTLY PASS	MODERATE CONCERNS	MODERATE CONCERNS

OVERALL VERDICT

CONDITIONALLY ACCEPTABLE — WITH NOTED LIMITATIONS

This report meets basic structural requirements and carries a clean opinion with no exceptions. However, several substantive and source-related concerns warrant practitioner attention before placing full reliance on the report. The use of Vanta as both a GRC and MDM tool, Prescient Assurance's positioning as a high-volume startup auditor, and notable vagueness in certain test procedures collectively reduce the evidentiary weight of this report. For low-to-medium risk vendor relationships, this report is acceptable. For high-risk or data-intensive engagements, supplemental evidence is recommended.



1. Executive Summary

This assessment evaluates the Kolide, Inc. SOC 2 Type 2 report (audit period January 1 to June 30, 2024) against the SOC 2 Reliability Rubric across three pillars: Structure, Substance, and Source. The report was issued by Prescient Assurance LLC, signed by John D. Wallace, CPA, from Chattanooga, TN, and dated September 10, 2024.



Key strengths of this report include a complete and properly structured auditor's report, a signed Management's Assertion from named company leadership, a clean unqualified opinion with no exceptions, and a reasonably specific system description naming actual infrastructure components. The report does not identify any material control deficiencies.

Key concerns include: Prescient Assurance's business model as a high-volume, flat-fee startup auditor with close GRC platform integrations; the vendor's use of Vanta as both a continuous monitoring tool and a key evidence source throughout the testing matrices; vague test procedure descriptions that frequently rely on policy inspection alone without evidence of re-performance; a very short 6-month audit window; and an internal inconsistency regarding the CEO's name between the Management's Assertion and the System Description.

2. Pillar 1: Structure

Structure evaluates whether the report includes all required components and maintains professional consistency across sections.

2.1 Required Auditor's Report Section Structure

Required Auditor's Report Paragraphs	✓ PASS
<p> Observation: The Auditor's Report contains all required labeled paragraphs: Scope, Service Organization's Responsibilities, Service Auditor's Responsibilities, Inherent Limitations, Opinion, and Restricted Use. The Opinion paragraph clearly addresses (a) the fairness of the system description, (b) suitable design of controls, and (c) operating effectiveness of controls — all three elements required for a Type 2 report. The report also correctly references Section 4 testing for the Type 2 opinion, and the opinion language is unqualified with no "except for" language.</p> <p> Recommendation: <i>No action required. Structure is in order and meets AICPA requirements.</i></p>	

2.2 Management's Assertion Completeness

Management's Assertion

✓ PASS

Observation: Management's Assertion is present as a standalone section (Section 1) and contains all three required elements: (a) the system description is accurate for the period, (b) controls were suitably designed, and (c) controls operated effectively throughout the period. The assertion is signed by Antigoni Sinanis, CEO. The assertion appropriately references the DC 200 description criteria and TSP 100 trust services criteria.

Recommendation: No action required. The assertion is complete and signed by an executive.

2.3 Inconsistent Language Across Sections

Cross-Section Consistency

⚠ CONCERN

Observation: A notable inconsistency exists in the executive names referenced across sections. Section 3.3 (People) names the CEO as "Jason Meller," while Management's Assertion (Section 1) is signed by "Antigoni Sinanis, CEO." The report notes that Kolide was acquired by 1Password in February 2024 (mid-audit-period), and that Antigoni Sinanis is also listed in Section 3.3 as "VP Operations" — not CEO. This creates genuine ambiguity about corporate structure and signatory authority during the observation period. Additionally, the MFA test under CC6.6 references "AWS" accounts, yet AWS does not appear in the Section 3 infrastructure or software inventory (Heroku is the stated IaaS/PaaS provider), which suggests either boilerplate testing language or undisclosed infrastructure.

Recommendation: Request clarification from the vendor on the correct CEO at the time of report signing, and on whether AWS is used in any capacity. This inconsistency, while not fatal, reduces confidence in the accuracy of the system description.

3. Pillar 2: Substance

Substance evaluates whether the controls, testing, and conclusions logically align and provide meaningful evidence of control effectiveness.

3.1 System Description Specificity

System Description (Section 3) — Specificity

✓ **MOSTLY PASS**

Observation: Section 3 provides meaningful specificity for a company of Kolide's size. It names specific infrastructure (Heroku Platform, Heroku Postgres, Heroku Redis, Heroku Pipelines), specific SaaS tools (Okta, GitHub, Stripe, Vanta, Slack, Google Workspace, Checkr, Notion), and the primary development language (TypeScript/PostgreSQL/Redis). Data classification categories are named and described. The 32-employee headcount and organizational structure (Management, Operations, IT, Product Development) add useful context. The description appropriately discloses that Kolide was acquired by 1Password during the observation period — a significant operational change. The subservice organization (Heroku) is identified and a carve-out approach is applied.

Recommendation: *The description is generally solid and company-specific. One concern is that the staff list in Section 3.3 states 'approximately 3' organized in functional areas, while DC 1 states '32 full-time employees' — this inconsistency should be clarified with the vendor. Additionally, there is no architecture diagram included in the report, which would strengthen the description.*

3.2 Control-to-Criteria Mapping Logic

Control-to-Criteria Mapping (Section 4)

⚠ **CONCERN**


Observation: Spot-checking reveals several mapping concerns. A significant volume of controls are mapped to CC6.1 (logical access software/infrastructure) that describe policy documents rather than implemented technical controls — for example, inspecting the Access Control Policy is used repeatedly as evidence for distinct technical sub-criteria (MFA enforcement, SSH key requirements, firewall restriction, OS-level access, encryption key access). This pattern may indicate that policy inspection is being used as a proxy for actual technical control verification. Additionally, the control mapped to CC6.4 (physical access restriction) is tested only via a quarterly access review, which is a logical access control — not a physical access control — suggesting the mapping for a fully remote/cloud organization is being applied somewhat formulaically.


Recommendation: *For critical access controls (MFA, production access, encryption key management), request direct technical evidence such as configuration screenshots or system-generated access reports rather than relying on policy inspection alone.*

3.3 Control Description Quality

Vague or Conflicting Control Descriptions

 **CONCERN**


 **Observation:** Several controls lack specificity in terms of how, who, and when. For example, the backup monitoring control states 'Customer data is backed up and monitored by the CEO for completion and exceptions' — this is unusual for a 32-person company and raises questions about whether this is a formally defined and documented control or an informal practice. Section 3.5.2 states 'User access and roles are reviewed on an annual basis,' while Section 4 (CC6.2/CC6.3) lists a quarterly access review cadence. This frequency inconsistency between the System Description and the testing matrix is a rubric red flag. The people section also creates an apparent contradiction: 'approximately 3 organized in functional areas' versus '32 full-time employees' stated in DC 1.


 **Recommendation:** Ask the vendor to clarify the actual access review frequency (annual per Section 3 or quarterly per Section 4). Request backup monitoring documentation to confirm the control is formalized and not dependent on a single individual.

3.4 Test Procedure Detail and Specificity

Test Procedure Detail (Section 4)

 **CONCERN**

 **Observation:** Testing procedures rely heavily on 'Inspected [Policy Name] to determine that...' language, particularly for technical controls. For example, MFA enforcement (CC6.1) is tested by inspecting a sample of accounts on Google Workspace, Okta, GitHub, and Netlify — however, the test result notes AWS accounts were sampled, which is inconsistent with the stated infrastructure. The vulnerability scanning control is tested by 'Observing a list of open vulnerabilities identified by the GitHub vulnerability scanner' — this is evidence of a live list, not evidence that critical vulnerabilities were remediated within SLA. For the quarterly access review control, testing inspection notes 'no changes were observed' in the access review document, but does not indicate whether the completeness of the review was validated or how many users were in scope. Sample sizes are not disclosed in the test results for most controls, making it impossible to evaluate whether sampling was sufficient. Multiple controls were noted as 'Not tested' due to non-occurrence (no contractors, no incidents, no performance evaluations completed during the period) — while non-occurrence is acceptable to disclose, three separate controls being not tested due to non-occurrence in a 6-month window is notable.

 **Recommendation:** For your highest-priority controls (MFA, production access, vulnerability remediation), request direct evidence: configuration screenshots, user access listings with timestamps, vulnerability reports with remediation tickets. The test procedures as documented are not sufficient to independently verify these controls were operating effectively.


4. Pillar 3: Source


Source evaluates the credentials, independence profile, and track record of the audit firm.

4.1 CPA Firm Registration and Peer Review

CPA Firm Registration — Prescient Assurance LLC

 **VERIFY REQUIRED**


 **Observation:** The report is signed by John D. Wallace, CPA, from Chattanooga, TN. The signing firm is listed as Prescient Assurance LLC. NASBA CPAVerify should be used to confirm the firm is registered as a licensed CPA firm in Tennessee (or the relevant state). Public information confirms Prescient Assurance LLC is PCAOB-registered (PCAOB ID 7044), which is a positive signal. Their website references being AICPA Peer Review enrolled. However, verification of peer review pass status at aicpa.org and confirmation the peer review acceptance date is within the last 3 years should be performed before accepting this report.


 **Recommendation:** Verify: (1) CPA firm registration at NASBA CPAVerify for Tennessee. (2) AICPA Peer Review status at peerreview.aicpa.org — confirm 'Pass' rating and that acceptance date is within 3 years of the report date. This verification step is important as the report cannot be relied upon from an unlicensed or lapsed firm.

4.2 CPA-to-SOC Reports Ratio

CPA Firm Volume and Capacity

 **CONCERN**


 **Observation:** Prescient Assurance/Prescient Security markets itself as serving 'over 5,000 customers worldwide' and is listed as a preferred auditor on Drata's auditor directory and described as working closely with 'every major GRC platform.' Their website promotes SOC 2 audits at flat fees for startups and emphasizes speed and cost-effectiveness. Client reviews reference turnaround timelines of weeks. While Prescient is PCAOB-registered and has genuine credentials, the volume-oriented, startup-focused business model raises questions about whether audit depth for each engagement matches the time and resource investment required to issue a rigorous Type 2 report. The LinkedIn footprint of the firm would need to be assessed to calculate the CPA-to-report ratio, but the marketing signals are consistent with a firm operating at higher volume relative to licensed CPA staffing.


 **Recommendation:** Research Prescient Assurance's current licensed CPA headcount on LinkedIn and estimate annual SOC report volume. If the ratio exceeds 50 reports per licensed CPA, consider this a contributing risk factor and request supplemental evidence for your critical controls.

4.3 Auditor Experience and Independence

Auditor Experience

 **CONCERN**


 **Observation:** Prescient Assurance is positioned as a cybersecurity-first audit firm with genuine attestation credentials and PCAOB registration. The signer, John D. Wallace, CPA, is identified from Chattanooga, TN. The firm has a track record with large enterprises and startup clients alike. However, the firm's close integration with GRC platforms (they market themselves as working seamlessly with Vanta and Drata) creates a potential independence consideration — particularly given that Vanta is also the vendor's primary compliance tool and is used as a key evidence source throughout the testing matrices (Vanta is used as MDM, continuous compliance monitoring, and audit evidence platform simultaneously). While not disqualifying, this relationship warrants consideration.


 **Recommendation:** Research John D. Wallace on LinkedIn to assess SOC 2 audit experience. Note that Vanta is simultaneously the vendor's compliance tool and a key evidence source in the audit — in multiple tests, 'Observing the Vanta compliance platform' is listed as direct audit evidence. This requires an assessment of whether the auditor independently verified the accuracy of Vanta's outputs or accepted them at face value.

4.4 GRC Tool Assessment

Vendor GRC Tool — Vanta

 **CONCERN**

 **Observation:** Kolide uses Vanta as its primary GRC and compliance platform. Vanta is explicitly referenced throughout Section 4 as a primary evidence source: it is used for continuous control self-assessment, as an MDM tool, and as a log aggregation platform (GitHub, Slack, G Suite, Jira are linked to Vanta). The auditor observed the 'Vanta compliance platform' directly as audit evidence in multiple test procedures. Prescient Assurance is listed as a preferred/integrated auditor in Drata's auditor directory and markets close relationships with 'every major GRC platform' including Vanta. Vanta does market rapid SOC 2 compliance timelines. The audit window itself is only 6 months (minimum for a Type 2), which is a shorter period than the 12-month window typically preferred by enterprise practitioners.

 **Recommendation:** Be aware that this report reflects 6 months of observation, not a full year. Where Vanta is used as both the control monitoring tool and the primary audit evidence source, consider requesting independent corroborating evidence for the most critical controls (access management, MFA, vulnerability tracking) rather than accepting Vanta-generated outputs as sole evidence of control effectiveness.

5. Findings Summary

Signal	Rating	Priority Action
Auditor's Report Structure	✓ PASS	None required
Management's Assertion	✓ PASS	None required
Cross-Section Consistency	⚠ CONCERN	Clarify CEO name discrepancy & AWS reference
System Description Specificity	✓ MOSTLY PASS	Clarify "~3 staff" vs "32 employees" discrepancy
Control-to-Criteria Mapping	⚠ CONCERN	Spot-check access & physical control mappings
Control Description Quality	⚠ CONCERN	Resolve annual vs quarterly access review frequency
Test Procedure Depth	⚠ CONCERN	Request direct evidence for MFA, access, vuln mgmt
CPA Firm Registration	⚠ VERIFY	Confirm TN CPA registration & AICPA peer review pass
CPA-to-Report Ratio	⚠ CONCERN	Research firm headcount vs volume on LinkedIn
Auditor Independence	⚠ CONCERN	Assess Vanta dual-role as tool & evidence source
GRC Tool (Vanta)	⚠ CONCERN	6-month window; request supplemental evidence



6. Recommended Next Steps

Immediate Verification Steps (All Engagements)

- Verify Prescient Assurance LLC CPA registration at NASBA CPAVerify (Tennessee or firm home state)
- Search AICPA Peer Review Public File at peerreview.aicpa.org — confirm "Pass" rating with acceptance date within 3 years of September 2024
- Resolve the CEO name discrepancy (Jason Meller in Section 3.3 vs. Antigoni Sinanis signing the assertion) — request vendor confirmation of corporate structure at time of report
- Resolve the "approximately 3 staff" vs "32 full-time employees" discrepancy in Section 3

For Medium-to-High Risk Engagements — Request Supplemental Evidence

- MFA enforcement: Request a system-generated screenshot of enforced MFA across all named systems (Okta, GitHub, Google Workspace). The current testing references AWS accounts not mentioned in the system description.
- Production access: Request a current user access listing for Heroku production with role assignments
- Vulnerability management: Request a sample of critical/high vulnerability tickets with open-to-close timestamps to verify SLA compliance
- Access review: Confirm frequency — the system description states annual reviews; the testing matrix states quarterly. Request a completed quarterly access review from the audit period.
- Backup monitoring: Request backup logs for at least 1 quarter during the observation period, given that this control is attributed to the CEO personally

Risk-Based Acceptance Guidance

Risk Level	Guidance
Low Risk	Accept report as-is. Document Vanta dual-role and 6-month window in your risk notes.
Medium Risk	Accept with documented caveats. Request supplemental evidence for access management and MFA controls. Require a full 12-month period report in the next cycle.
High Risk / Data-Intensive	Do not rely on this report as sole assurance. Conduct a supplemental evidence review for all critical control areas. Consider contractual requirement for a 12-month audit with a different auditor in the next cycle. Note that Kolide was mid-acquisition during this period, which may have introduced operational risk.



This assessment was prepared using the SOC 2 Reliability Rubric v1.0 (published February 15, 2026) by the SOC 2 Quality Guild, licensed under CC BY-SA 4.0. This assessment reflects the evaluator's professional judgment based on the report contents and publicly available information about the audit firm. It is not a substitute for an independent audit, legal advice, or a formal third-party risk assessment.