SOC 2 Type II Readiness Assessment

FinSight AI

Date: May 25, 2026

Prepared for: FinSight AI Management

Prepared by: Nexus Audit & Advisory Partners

Scope: Security, Availability, and Confidentiality Trust Services Criteria

1. Executive Summary

Nexus Audit & Advisory Partners was engaged by FinSight AI to perform a SOC 2 Type II Readiness Assessment. The objective of this assessment is to evaluate the design and operational effectiveness of FinSight AI's internal controls against the AICPA Trust Services Criteria (TSC) for Security, Availability, and Confidentiality.

As of May 25, 2026, FinSight AI demonstrates a maturing control environment. Management has established foundational policies and technical safeguards. However, several critical gaps remain in formalized evidence collection, access review cadence, and vendor risk management that must be addressed prior to commencing the formal Type II observation period.

2. Introduction and Scope

2.1 Purpose

This report outlines the findings of the readiness assessment, identifies specific control deficiencies, and provides a prioritized remediation roadmap. It is intended solely for the internal use of FinSight AI management to prepare for an upcoming SOC 2 Type II examination.

2.2 Scope and Methodology

The assessment covered the FinSight AI core analytics platform and supporting infrastructure hosted on Amazon Web Services (AWS). The methodology included management interviews, technical configuration reviews, and sampling of existing control evidence spanning the period of January 1, 2026, to May 15, 2026.

3. Control Environment Overview

FinSight AI has established a strong "tone at the top" regarding information security, led by the Chief Information Security Officer (CISO). The organization utilizes a modern technology stack with inherent security capabilities. Key strengths observed include:

- Comprehensive deployment of Multi-Factor Authentication (MFA) across all critical systems.
- Automated continuous integration and continuous deployment (CI/CD) pipelines with integrated static code analysis.
- Robust endpoint management using centralized MDM solutions.

4. Trust Service Criteria Mapping & Findings

The following table details the specific gaps identified during the assessment, categorized by the relevant Trust Services Criteria and assigned a severity level based on audit risk.

TSC Ref.	Control Objective	Observation / Gap	Severity
CC2.1	Communication of internal control matters	Annual security awareness training was not completed by 14% of active contractors.	Medium
CC6.1	Logical access provisioning	Quarterly logical access reviews for production databases are not formally documented or retained.	High
CC6.8	Unauthorized or malicious software protection	Vulnerability scanning is performed, but remediation SLAs for critical findings are not consistently met or tracked.	High
CC9.2	Vendor risk management	No formal vendor risk assessment matrix is maintained for tier-2 service providers.	Medium
A1.2	System capacity and performance	Capacity planning metrics are monitored but not formally reviewed in documented monthly engineering meetings.	Low

5. Remediation Roadmap (30-60-90 Day Plan)

To ensure readiness for the formal observation period, management should execute the following prioritized remediation plan.

Phase	Timeline	Key Deliverables & Actions	Owner
Phase 1	30 Days	- Implement formal quarterly access review process and document Q2 review. - Enforce 100% completion of security awareness training for all staff and contractors. - Define and publish vulnerability remediation SLAs.	CISO / HR

Phase	Timeline	Key Deliverables & Actions	Owner
Phase 2	60 Days	- Develop and populate the Vendor Risk Management register. - Implement automated ticketing for capacity planning alerts. - Conduct table-top incident response exercise and document results.	Compliance / DevOps
Phase 3	90 Days	- Perform internal dry-run audit of all Phase 1 and Phase 2 evidence. - Finalize system description narrative (Section 3). - Officially commence SOC 2 Type II observation period.	CISO

6. Evidence Checklist

The following table outlines the status of critical artifact collection required for the final audit.

Artifact Description	System / Source	Status
Information Security Policy (Approved)	Compliance Portal	Complete
AWS Configuration & Architecture Diagrams	Confluence	Complete
New Hire Background Check Records	HRIS	Complete
Quarterly Access Review Sign-offs	Jira / IAM	Missing
Penetration Test Report (Annual)	Third-Party Vendor	Complete
Vendor Risk Assessments	Compliance Portal	In Progress

7. Conclusions

FinSight AI possesses a fundamentally sound technical architecture and security posture. The deficiencies identified are primarily related to process formalization and documentation retention rather than technical vulnerabilities. By executing the 30-60-90 day remediation plan, FinSight AI will be well-positioned to successfully undergo a SOC 2 Type II examination without material exceptions.

8. Management Attestation

I acknowledge receipt of this readiness assessment report and agree to the remediation roadmap outlined herein. Management commits to addressing the identified gaps prior to the commencement of the formal SOC 2 Type II observation period.

_____

Name: _____

Title: _____

Date: _____