AI RISK CHECK REPORT

42

OUT OF 100

CRITICAL

AI RISK CHECK

Apex Advisory

AI Risk Check Report

Prepared for: Priya Nadar, Managing Director

Generated: 8/30/2026 | Ref: AP-2026-9877

Compliance Score: 42/100 CRITICAL

EXECUTIVE SUMMARY

KEY FINDINGS AT A GLANCE

- **No Human Oversight on AI-Assisted Portfolio Analysis Informing Client Recommendations**
- **No Data Lineage for Client Data Flowing Into AI Research Tools**
- **AI Inputs and Outputs Are Not Logged for Audit Purposes**

Executive Summary

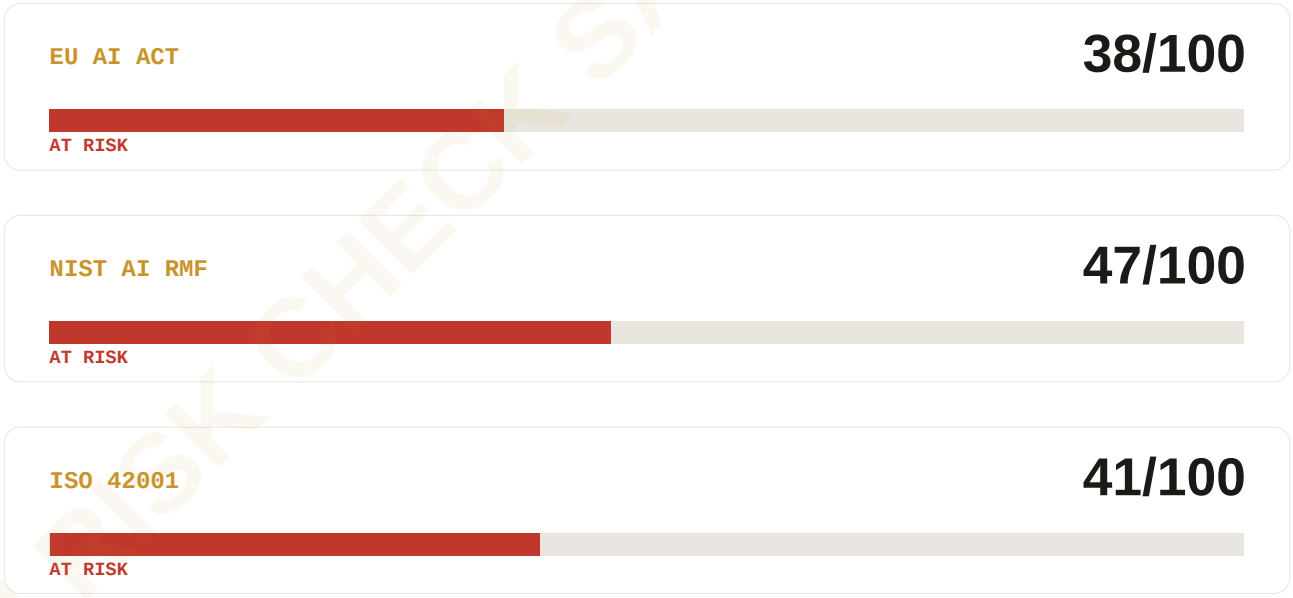
Apex Advisory is a boutique financial advisory firm based in Sydney with 12 employees, using AI tools across client research, document drafting, and portfolio analysis. This AI Risk Check identified a Critical compliance posture driven by four confirmed gaps.

The most material finding is the absence of human oversight on AI-assisted portfolio analysis that informs client-facing recommendations, which sits within the EU AI Act high-risk use case categories and creates direct advisory liability. Apex also lacks documented data lineage for the client data flowing into its research tools, and has no logging of AI inputs and outputs, leaving the firm unable to demonstrate how a given recommendation was reached if challenged.

Because Apex handles regulated financial data for clients with EU exposure, these obligations are phasing in and the preparation window is closing. Remediating the findings within the recommended timeframes is expected to raise the overall compliance score from 42 to above 85 out of 100, moving Apex into the STRONG band.

Framework Coverage

Your AI stack scored against the three core AI governance frameworks. SOC 2 Type II coverage is available in the Standard and Verified Audit tiers.



Key Findings

[CRITICAL] No Human Oversight on AI-Assisted Portfolio Analysis Informing Client Recommendations

Citation: EU AI Act Art. 14; NIST AI RMF GOVERN 3.2

Apex confirmed that AI tools generate portfolio analysis outputs that feed directly into client-facing advice without a mandatory human review checkpoint. The EU AI Act requires that high-risk AI systems be designed so that qualified individuals can effectively oversee, interpret, and override system outputs before they are actioned. AI systems supporting financial advisory decisions fall within the high-risk use case categories.

[CRITICAL] No Data Lineage for Client Data Flowing Into AI Research Tools

Citation: EU AI Act Art. 10; ISO 42001:2023 Annex A.7.5

Apex does not maintain a record of how client and market data is sourced, transformed, and fed into its AI research tools. Both the EU AI Act data governance requirement and the ISO 42001 data provenance control call for organisations to document the data underpinning AI system outputs. Without lineage, Apex cannot demonstrate to clients, auditors, or a regulator where the inputs behind a recommendation originated or whether they were handled lawfully.

[FLAGGED] AI Inputs and Outputs Are Not Logged for Audit Purposes

Citation: EU AI Act Art. 12; NIST AI RMF MANAGE 4.1

Apex does not log the prompts, inputs, and outputs of the AI tools used in client research and document drafting. The EU AI Act record-keeping obligation and the NIST AI RMF post-deployment monitoring expectation both require records that allow AI system behaviour to be monitored and reconstructed. Without logs, Apex cannot reconstruct how a specific piece of advice or drafted document was produced, which limits its ability to investigate errors, respond to complaints, or satisfy an auditor.

KEY FINDINGS

[FLAGGED] No Documented AI Usage Policy Covering Client-Confidential Information

Citation: NIST AI RMF GOVERN 1.1; NIST AI RMF GOVERN 1.2

Apex has no written policy governing how staff may use AI tools with client-confidential and market-sensitive information. The NIST AI RMF expects organisations to establish policies that define acceptable AI use, integrate trustworthy AI characteristics, and understand the legal requirements that apply. With 12 staff drafting documents and conducting research using AI, the absence of a policy creates uncontrolled risk of confidential client data being entered into third-party tools without appropriate safeguards or contractual coverage.

Remediation Direction

The immediate next step for each finding. A full prioritised remediation roadmap with effort and timeframe is included in the Standard and Verified Audit tiers.

No Human Oversight on AI-Assisted Portfolio Analysis Informing Client Recommendations

Introduce a mandatory sign-off step where a qualified adviser reviews and confirms every AI-assisted portfolio output before it reaches a client

No Data Lineage for Client Data Flowing Into AI Research Tools

Document the data sources and preprocessing steps behind each AI research tool to establish a baseline lineage record

AI Inputs and Outputs Are Not Logged for Audit Purposes

Enable logging of AI inputs and outputs for client-facing work, even a simple structured record per engagement

No Documented AI Usage Policy Covering Client-Confidential Information

Draft a short AI usage policy defining which tools are approved and what client information may and may not be entered

About AuditPulse

AuditPulse maps your AI stack against the frameworks investors, boards and regulators ask about, and delivers a dated, referenced report you can put in front of someone.

Need deeper analysis?

Upgrade to the Standard Audit ($500) for a full remediation roadmap and SOC 2 coverage, or the Verified Audit ($1,500) for a Legal Exposure Summary, Board Recommendations and an Attestation Letter built for investor data rooms.