

AI Risk Review: Findings

Example only. The firm and its findings are made up, so no client's information is shared.

Sample Firm, LLP · Tax and advisory · 14 staff, 2 locations

Reviewed by **Brian Butterfield, CISSP** · More than 30 years in IT and cybersecurity
Microtech IT & Cybersecurity Services, Fort Lauderdale, since 1996

What we found

AREA	FINDING	PRIORITY
AI tools in use	Nine AI tools in use across 14 staff. Leadership knew about four.	HIGH
Free vs. paid accounts	Four staff used free versions whose terms let the vendor keep what's typed.	HIGH
AI built into software	The document assistant could open any file a user could, including the partner share.	MEDIUM
Written security plan	Last updated in 2021, with no AI section.	MEDIUM

Next three steps

STEP		OWNER	TARGET
1	Name one person to own AI and publish a list of approved tools	Managing partner	30 days
2	Limit the built-in document assistant to what each role needs	IT provider	30 days
3	Add AI to the written security plan and train staff on it	Owner + IT	60 days



Want to know where your firm stands?

Book a free 15-minute call with Brian Butterfield, CISSP, by video or phone.
micro-tech.com/txcpa · 954-327-1001



A review is not a penetration test, an audit, or a compliance certification. General information from Microtech's IT and cybersecurity team. Not legal, tax, accounting, or insurance advice, and not a compliance certification. Talk with your attorney or compliance adviser about your firm's obligations.