

Sample AI Exposure Risk Report

Illustrative findings for Bright Harbor Creative, a fictional 18-person Michigan marketing agency. This sample demonstrates the structure and level of detail a client receives; it is not a real client result.

OVERALL RISK	TOOLS REVIEWED	RISKS LOGGED	TOP PRIORITY
HIGH	9	14	DATA EXPOSURE
Immediate action warranted	Approved and shadow	8 critical / 6 high	Consumer tools touching client data

Executive finding

The agency had useful AI activity but no common approval path. Personal accounts, embedded features, and inconsistent data handling created a visibility gap larger than leadership expected.

Top findings

1	Client material entered into consumer AI accounts	Confidentiality and contract risk	Move approved use cases to managed business accounts and publish data rules
2	No complete AI tool inventory or named owners	Leadership cannot explain who is using what	Create a signed inventory and assign one accountable owner per tool
3	AI output used externally without a review standard	Accuracy and reputational risk	Require documented human review for client-facing work
4	Embedded AI features enabled without vendor review	Unmapped processing and retention	Review contracts, DPAs, settings, retention, and sub-processors

Recommended 30-day response

0-7 DAYS	8-14 DAYS	15-30 DAYS
Stop Tier 3/4 data from entering unmanaged accounts. Name an executive AI owner. Preserve any incident evidence.	Confirm the tool inventory. Review highest-risk vendors and settings. Approve a short sanctioned-tool list.	Publish the acceptable-use policy. Train staff. Establish intake, incident reporting, and quarterly review.