



SAMPLE — METHODOLOGY DEMONSTRATION

AI Risk Landscape Assessment

Prepared for: a hypothetical 65-person integrated agency, London and Manchester (“the Agency”)

Assessment date: September 2026 | Fee reference: £2,350 + VAT engagement format

A note on this document

This is an illustrative sample. The Agency, its clients and every finding below are fictional, built to show what a Meriol assessment of a UK agency looks like: the format, the depth, and the way findings are tied to specific contracts and rules. It describes no real organisation and uses no non-public information about one. Regulatory references are accurate as of the assessment date and would be re-verified against the facts of any live engagement.

12

AI tools found in use

3

formally approved

8

holding client information

1.3 / 5

governance maturity

1. Agency Snapshot

Drawn from the Agency's questionnaire responses and a 45-minute discovery call.

- 65 staff: 48 in London, 17 in Manchester. Services: brand, creative, content, social and paid media.
- Four clients make up 58% of fee income. All four operate in regulated sectors (below).
- No written AI policy. Staff guidance to date: “use common sense, don't paste anything sensitive.”
- Microsoft 365 Copilot licensed for 15 seats in 2025. Every other AI tool arrived bottom-up, paid on personal or team cards.
- The Operations Director owns IT; the Managing Director owns client contracts. Nobody owns AI.

Clients in scope (anonymised)

Client	Sector and regulator	Share of fees	Work
Client A	UK motor and home insurer (FCA)	22%	Retained: brand, social, paid media
Client B	Regional building society (FCA / PRA)	14%	Project: mortgage and savings campaigns
Client C	Pharmaceutical company, prescription respiratory brand (ABPI Code / MHRA)	13%	HCP and patient-awareness campaigns, localised for Ireland and Germany
Client D	City law firm (SRA)	9%	Brand, thought leadership, events

2. AI Footprint Mapping

12 AI tools in use. 3 formally approved. Client information entered into 8. In 5, it sits on accounts the Agency does not control — personal subscriptions governed by an individual employee's contract with the vendor, not the Agency's.

Tool	Who uses it	Approved	Client data in it?	Note
Otter.ai / Fireflies meeting bots	Account teams; auto-join from calendars	No	Yes — full call transcripts	Joined client calls, including Client D. Transcripts held on the vendor's cloud under personal accounts.
ChatGPT (free and Plus, personal)	~30 staff: copy, strategy, social	No	Yes — briefs, drafts, research	Consumer accounts can use conversations for model training unless each user opts out. No Agency visibility.
ChatGPT Team (Manchester)	6 seats on a team credit card	Informal	Yes	Business terms exclude training, but no central admin, no retention settings reviewed.
Midjourney	Studio: 4 designers, personal plans	No	Brand assets as references	On plans without Stealth Mode, outputs appear in Midjourney's public gallery — including unreleased campaign concepts.
Adobe Firefly (in Creative Cloud)	Studio	Yes	Brand assets	Adobe's IP indemnity for Firefly applies to certain enterprise licences only. The Agency is on Creative Cloud for Teams: check.
ElevenLabs	Social team	No	Scripts	Synthetic voiceover used in rough cuts of a Client C patient-awareness video.
Microsoft 365 Copilot	15 seats: leadership, account management	Yes	Yes — email, SharePoint	Copilot surfaces anything the user can open. SharePoint permissions are flat across clients.

Tool	Who uses it	Approved	Client data in it?	Note
Google PMax / Meta Advantage+	Paid media team	Via briefs	Yes — hashed customer lists (A, B)	Customer Match uploads run under client data agreements; AI audience expansion not mentioned in them.
Grammarly (free extension)	~20 staff	No	Yes — reads text typed in the browser	Includes client portals and webmail.
Notion AI	Strategy team	No	Yes — research notes	Workspace owned by a former employee.
Claude / Gemini (personal)	A handful of staff	No	Some	Usage unknown in detail.
Descript	Content team	Yes	Interview footage	Approved for internal editing only.

3. Risk Identification

Ranked by what each could cost the Agency — a client, an indemnity claim, or a regulator’s attention on a client — not by how novel the technology is.

3.1 Meeting bots on client calls — critical

Transcription bots joined at least six Client D calls, including one about an unannounced restructuring. The law firm’s engagement terms prohibit disclosure to third parties, including service providers, without consent. The transcripts now sit with a US vendor under individual staff accounts. A law firm that discovers this is likely to treat it as a confidentiality breach and may treat it as a reportable data incident. The other call participants were recorded without being told.

3.2 Client material in personal AI accounts — high

Briefs, draft copy and research for all four clients have gone into personal ChatGPT, Claude, Gemini and Notion accounts. Where that material includes personal data, the Agency, as the clients’ processor, has used sub-processors none of them authorised. That breaches UK GDPR Article 28 and the data-processing terms in each contract. When a staff member leaves, the chat history leaves with them.

3.3 AI imagery and voice in deliverables — high

Client C’s contract carries an uncapped IP indemnity and a warranty that deliverables are original and non-infringing. Midjourney concepts have moved into final artwork, and synthetic voice into video. UK law does not settle who owns AI-generated output, so the Agency may not hold the copyright it promises to assign. Separately, unreleased concepts sit in Midjourney’s public gallery.

3.4 AI-drafted regulated copy — high

Copy for Clients A and B is first-drafted in ChatGPT. The clients approve financial promotions, but Client A’s contract has the Agency warrant that its work is accurate and compliant. For Client C, social cut-downs are generated *after* the ABPI signatory has certified the master asset. Under Clause 8 of the ABPI Code, certification covers material in its final form; altered versions are uncertified, which puts the client in breach and the Agency in the spotlight.

3.5 Copilot oversharing — medium

Copilot answers from whatever the user can access. With flat SharePoint permissions, a junior on Client A can surface Client C’s launch plan with one prompt. No breach has been reported; the exposure is structural.

3.6 Ad-platform AI and customer data — medium

Customer Match uploads for Clients A and B fall under existing data agreements, which predate AI audience expansion. The ASA holds advertisers responsible for automated placement and creative, so the clients carry the regulatory risk, and the Agency carries the relationship risk.

4. Regulatory Exposure Review

Organised around what actually bites for this Agency and these four clients, what carries a firm date, and what a generic checklist would get wrong.

4.1 What already applies, now

- **UK GDPR and the Data Protection Act 2018.** For client personal data the Agency is a processor. Article 28 requires the client's written authorisation before any sub-processor is used. Personal AI accounts and meeting bots are sub-processors nobody authorised.
- **The CAP Code, enforced by the ASA.** The Code is media-neutral and does not require ads to disclose AI use. But AI imagery that exaggerates what a product does can mislead, and the ASA's June 2026 statement made clear that automation does not move responsibility away from the advertiser.
- **FCA financial promotion rules and the Consumer Duty** (Clients A and B). The obligation sits with the authorised client, which approves each promotion; it reaches the Agency through contract warranties and approval workflows.
- **ABPI Code of Practice 2024, Clause 8** (Client C). Promotional material must be certified in its final form by a qualified signatory. Any AI-generated variant made after certification needs certifying again.
- **EU AI Act, Article 50(4)** (Client C's Irish and German campaigns). Since 2 August 2026, deployers publishing AI-generated or manipulated image, audio or video that could be mistaken for real must disclose it. The Digital Omnibus left this date unchanged.

4.2 Known dates and live developments

- **2 December 2026.** End of the EU grace period for AI providers' machine-readable marking of generated content (Article 50(2)). This duty sits with the tool vendors, not the Agency, but export and compression steps that strip that marking from client assets should be checked before then.
- **UK copyright and AI.** The government's report of 23 March 2026 dropped the proposed opt-out exception and committed to monitoring rather than legislating. Ownership and infringement questions for AI output stay unsettled into 2027.
- **Getty Images v Stability AI** [2025] EWHC 2863 (Ch), 6 November 2025. The court found the model was not an infringing copy, but upheld limited trade mark claims over watermarks appearing in outputs. It did not give agencies a clean bill of health for using AI imagery.

4.3 What a generic list would include — and why it's left out here

- **"The UK AI Act."** There isn't one in force. The UK still regulates AI through existing law and regulators. Listing it would invent an obligation.
- **EU AI Act high-risk obligations.** Now due on 2 December 2027, and they cover uses such as recruitment and credit scoring, not copywriting, imagery or media buying. Relevant only if the Agency uses AI to screen job applicants (open question 4).
- **Automated decision-making reforms** under the Data (Use and Access) Act 2025. These govern decisions about individuals, which this Agency does not make.

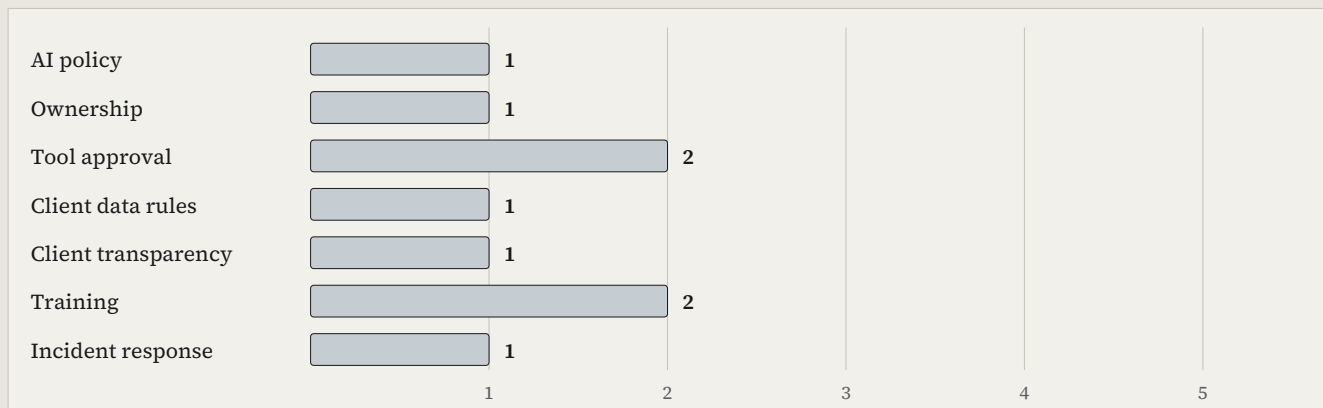
5. Contract Exposure

The four largest client agreements, read against current practice. This is where the money is.

Client	What the contract says	What actually happens	Exposure
A — insurer (MSA renewed March 2026)	No client materials in generative AI tools without prior written consent. Annual supplier assurance questionnaire with an AI section, next due January 2027.	ChatGPT used on Client A briefs and copy. No consent requested.	Material breach and a termination right, on 22% of fee income. The January questionnaire will ask.
B — building society (2022 framework)	Standard confidentiality and data-processing terms. No AI clause.	Customer Match uploads; ChatGPT on campaign copy.	Unauthorised sub-processing under the data terms. Lower contractual risk today.
C — pharma (MSA)	Originality and non-infringement warranty; uncapped IP indemnity. Approved material may not be altered without re-approval.	Midjourney concepts in final artwork; synthetic voice in video; post-certification cut-downs.	Uncapped indemnity exposure, plus ABPI certification breaches attributed to the client.
D — law firm (engagement terms)	Strict confidentiality; no disclosure to service providers without consent.	Meeting bots on at least six calls.	Confidentiality breach on a client that talks to other law firms.

6. Governance Maturity

Scored 1 (absent) to 5 (embedded), from questionnaire answers and the discovery call.



Dimension	Evidence behind the score
AI policy	None written.
Ownership	No named owner; the Operations Director by default.
Tool approval	Copilot and Firefly went through IT procurement. Nothing else did.
Client data rules	No rule on what may go into which tool.
Client transparency	No disclosure language; no consents obtained where contracts require them.
Training	One lunch-and-learn in 2025.
Incident response	No process for an AI-related data or IP incident.

Overall: 1.3 out of 5 — ad hoc. Typical for an agency that adopted AI fast and bottom-up. Fixable inside 30 days.

7. Procurement-Ready Answers

Draft answers to the AI questions now appearing in client supplier questionnaires. They become true once the 30-day plan in §9 is complete — not before. Answering them today would be a misrepresentation.

Client question	Draft answer
Do you use generative AI to deliver our work?	Yes, within a written AI policy. We use [approved tools], each reviewed for security, data retention and training terms. Our full tool register is available on request.
Is our data used to train AI models?	No. Approved tools run on business terms that exclude training. Personal AI accounts are prohibited for client work.
Do you have our consent where our contract requires it?	Yes. We obtained written consent on [date] for the uses set out in the attached schedule.
How do you manage IP risk in AI-generated content?	AI imagery and voice are only used from tools with commercial-use terms and, where available, vendor indemnities, and every use is logged against the deliverable. Final assets are cleared by a named reviewer.
Who is accountable for AI use at your agency?	[Name], Operations Director, owns our AI policy, tool register and incident process, and reports to the board quarterly.

8. Assumptions & Open Questions

A live engagement resolves these on the call. Guessing them is where a generic report goes wrong fastest.

- 1 Were Client D's calls recorded by the bots, or only transcribed? Who has accessed the transcripts, and can the vendor confirm deletion?
- 2 Is Client A's AI-consent clause new at the March 2026 renewal, or did it exist in the previous agreement? That changes how long the breach has run.
- 3 Which Creative Cloud licence tier does the Agency hold, and does Adobe's Firefly indemnity apply to it?
- 4 Does the Agency use any AI to screen job applicants? If so, recruitment rules (and, for EU candidates, the 2027 high-risk regime) come into play.
- 5 Do Client C's Irish and German campaign assets include any synthetic people or voices? That decides whether Article 50(4) labelling applies today.

9. Recommendations and 30-Day Plan

If you do nothing else, do this

1. Today: remove meeting bots from all client calls and ask both vendors to delete Client D transcripts, with written confirmation.
2. This week: stop using AI on Client A material until written consent is in place, and request it. The January questionnaire will ask, and the honest answer must be ready before then.

Week	Actions	Owner
1	Remove meeting bots; vendor deletion requests. Pause AI on Client A work; request consent. Move studio Midjourney use to plans with Stealth Mode or stop. Freeze new AI tools pending the register.	MD / Ops Director
2	Publish a two-page AI policy: approved tools, banned uses, what client data may go where. Replace personal ChatGPT with a centrally administered business workspace. Fix SharePoint permissions by client before widening Copilot.	Ops Director
3	Add AI disclosure and consent language to the contract templates. Build an AI step into the Client C workflow: no post-certification variants without re-certification. Check the Firefly licence tier.	MD / Client C lead
4	Train all staff (60 minutes, recorded). Name an AI owner. Finalise the procurement answers in §7 and the tool register. Set a quarterly review.	Ops Director

Sources

- UK GDPR, Article 28 (processors); Data Protection Act 2018.
- ASA, “Generative AI & Advertising: Decoding AI Regulation”, 31 August 2023; ASA statement on AI-generated content and deepfakes, June 2026.
- FCA Handbook COBS 4 (financial promotions); FCA Consumer Duty (PRIN 2A), in force since 31 July 2023.
- ABPI Code of Practice 2024, Clause 8 (certification and examination), PMCPA.
- EU AI Act (Regulation (EU) 2024/1689), Article 50; Digital Omnibus on AI (Regulation (EU) 2026/1744), in force 27 July 2026.
- UK Government, Report on Copyright and Artificial Intelligence, 23 March 2026 (under ss.135–136, Data (Use and Access) Act 2025).
- Getty Images v Stability AI [2025] EWHC 2863 (Ch), 6 November 2025.
- IPA and ISBA, principles for the use of generative AI in advertising, November 2023.

Prepared by Meriol Intelligence. This illustrative sample demonstrates methodology and format. It is not legal advice, and no part of it describes a real organisation or client.