

AI Consultant Vetting Checklist

Ask these questions before engaging any consultant to build or deploy custom AI in your environment.

Before You Engage

- ☐ Ask for their full security documentation before you sign anything.
- ☐ If they won't share documentation, press pause. You can't secure what you can't see.
- ☐ Ask for their SOC 2 Type II certification. This tells you their security controls have been independently audited over time, not just at a single point.
- ☐ Verify they carry cyber liability insurance.
- ☐ Confirm they've worked in family office or comparable high-privacy environments.

Data and Access

- ☐ What data do they need, and for how long?
- ☐ Where does your data live during the engagement – their systems, yours, or a third-party cloud? Is it on-premise or cloud-based?
- ☐ Does the vendor have access to your full data, or only your metadata? If they claim to work only with metadata, ask how they generate meaningful outputs from it.
- ☐ What is their data retention policy once the work is done?
- ☐ Who on their team has access to your data, and under what conditions?

System and Security

- ☐ Can they clearly explain how their LLM or custom AI system handles sensitive data?
- ☐ Do they have documentation on how to use their tool in a compliant environment – covering HIPAA, FINRA, SEC, or equivalent regulations as they apply to you?
- ☐ Who trained their model, what data was used, and who is liable for inaccurate or harmful outputs?
- ☐ Has their system been independently penetration tested? Can they provide the results?
- ☐ How do they handle third-party vendors who may have access to your data or metadata?
- ☐ What happens to your data and any trained models when the engagement ends?
- ☐ Does their platform require internet access or is it designed to be air-gapped?

Red Flags

Refuses to share security documentation

Can't explain their data access requirements clearly

No SOC 2 Type II certification

No cyber liability insurance

No documentation on compliant use of their tool

Pushes to connect AI to your full environment immediately

Can't provide references from comparable clients