

AI Tool Evaluation Framework

A practical guide for MSPs reviewing AI solutions

Before deploying any AI tool, work through this framework. Start with the problem, not the product. If the tool doesn't solve a real issue you're facing today, doesn't protect your customer experience, or doesn't have a future you can trust, don't deploy it.

The Three Questions

Does this solve a current business problem?

- 1
- Not a hypothetical or future problem, a problem you have today. Ticket backlog, after-hours coverage, alert fatigue, response times. If it isn't solving something real, it's a toy.

Does this improve or retain the same customer experience?

- 2
- If it degrades the experience your end users receive, it doesn't matter how efficient it makes your team. Your reputation is the product. AI that saves money but costs trust is a slow-motion churn event.

Does this have longevity and a roadmap we agree with?

- 3
- Flash-in-the-pan tools die. Is the vendor funded, stable, and going somewhere you want to follow? If the roadmap is vague or conflicts with your values, walk away now, not after you've integrated it.

Decision Flow

All Yes

Bet | Proceed. Deploy with an owner, a metric, and a review date.

Any No

Stop | Do not deploy. Go back to the problem and find the right solution.

If any answer is No, loop back. Re-define the problem, re-evaluate the solution. Don't force-fit.

The 98% Rule

AI triage must only take automated action if the system is at least 98% certain. Below that, it flags for human review. This framework isn't theoretical. It's how Uptime already operates. ISO 27001 and ISO 9001 certified.

Security & Data Questions

Data Location | Where is data stored and processed? Which countries/regions host the data centres?

Backend AI Model | What AI model powers the tool? Is it proprietary or built on a third-party LLM (OpenAI, Anthropic, Google)?

Training Data | Is your data used to train the vendor's models? Can you opt out of data training permanently?

Data Retention | How long is data retained after processing? Can you set custom retention policies?

Access Controls | Who at the vendor can access your data? Is access logged, audited, and restricted by role?

Encryption | Is data encrypted in transit and at rest? What encryption standards are used?

Compliance | Does the vendor hold relevant certifications (SOC 2, ISO 27001)? Is a DPA or BAA available?

Data Portability | Can you export and permanently delete your data if you leave? What's the offboarding process?

See how Uptime's AI-Optimised Helpdesk already meets this framework | uptimeglobal.tech

