SERVICE OVERVIEW / CK-SVC-003

AI Security & Governance

Adopt AI with clear accountability, proportionate safeguards and evidence behind important decisions.

What this service achieves

Organisations piloting or scaling AI models, assistants, Copilot implementations and autonomous agents.

CyberKarl helps organisations understand the situation, choose proportionate safeguards and maintain evidence that those safeguards work.

How we can help

- AI discovery, inventory and use-case assessment
- AI governance roles, policies and decision-making
- AI risk assessments and control design
- ISO/IEC 42001 AI management system support
- AI agent permissions, data access and human oversight
- AI incident readiness, monitoring and lifecycle assurance

What you receive

- An actionable view of AI opportunities, risks and obligations
- Clear approval and oversight checkpoints for AI use cases
- Practical evidence to support responsible deployment and review

A practical engagement

Stage	What happens
1 Understand	Agree business objectives, scope, stakeholders, important risks and current evidence.
2 Prioritise	Identify material gaps and set achievable, risk-based improvements.
3 Implement	Support the responsible teams with controls, governance, documentation and practical changes.
4 Assure	Review evidence, report progress and adjust the programme as needs evolve.

Relevant standards and guidance

ISO/IEC 42001, NIST AI RMF, relevant provisions of the EU AI Act, NCSC secure AI guidance and MITRE ATLAS, as applicable.

Would you like a hand?

Thinking about adopting AI, or wondering whether current AI use is properly governed? We would be happy to help you work through it.

Free, no-obligation 30-minute chat: cyberkarl.com | hello@cyberkarl.com | **0330 043 7633**