Roc

AI assurance service

SOLUTION SHEET

Empower your business, your people and protect your data

Artificial Intelligence is transforming the way businesses operate, drive efficiency, productivity and innovation. Adopting AI without the right data structures and security controls can expose organisations to significant risks - data leaks, compliance issues and governance challenges to name a few. To leverage AI's potential while safeguarding critical information, businesses need a structured approach to AI assurance and security.

Our AI Assurance Service equips organisations to implement AI securely and strategically. By assessing data access, security policies and governance frameworks in the context of AI, we help IT teams and business leaders optimise AI adoption. Employees can harness AI tools with confidence, unlocking new ways of working whilst reducing risk.

Ideal for you if...

- You are exploring AI adoption but concerned about security risks
- You are concerned employees are already adopting AI tools in the workplace
- Your organisation requires better governance over AI-driven data access
- You want to optimise your data strategy for AI innovation
- Your IT team needs support in structuring and protecting enterprise data
- You are developing your own GenAI tools to support your customers

Why Roc?

24/7/365 In house MSOC	100% UK coverage	70+ highly trained engineers	100% engineers SC or DV cleared
CYBER ESSENTIALS PLUS accredited	ISO9001 accredited	14001 accredited	27001 accredited

Service benefits

- Protect your critical and sensitive data
- Optimise governance and compliance for enterprise AI tools
- Reduce risk of data leaks and regulatory breaches
- Increase efficiency and productivity through AI-driven automation
- Enhance IT team oversight and control over AI implementation

Find out more about how Roc can help secure your business.
Contact us today or visit our website at **roctechnologies.com**

Service overview

Optimising AI adoption

AI can revolutionise the workplace, but without the right controls, sensitive data could be exposed through AI-driven queries. Our service ensures that AI tools are deployed securely, allowing businesses to take advantage of new capabilities without compromising data integrity. We assess the risks of open-source and enterprise AI tools, ensuring governance structures are in place to protect information while optimising AI's full potential.

Enhancing security and data protection

Unrestricted AI adoption can create unintended data exposure. We help IT teams establish security controls that safeguard against unauthorised access, reducing the risk of data leaks. We enable organisations to embrace AI with confidence by implementing best practices for privileged identity management, data tagging, and access control.

Providing actionable insights for AI success

We provide a roadmap for secure AI deployment through stakeholder workshops, security audits, and AI impact assessments. Our insights help IT teams and business leaders identify where AI can add the most value while addressing potential risks before implementation. We empower businesses to drive innovation while maintaining control over their digital assets by aligning AI adoption with organisational goals.

Providing AI guardrails

We ensure that your AI tools respond to prompts in a logical manner, and that your data and learning models are protected from malicious interference, bias manipulation or poisoning that could produce undesired responses.

AI Assurance Service

Before AI adoption, Roc will conduct a thorough assessment of your IT estate, ensuring you are leveraging existing licenses and technology sufficiently to protect your data. This assessment includes:

- Privileged Identity Management
- Data Tagging
- Data Storage (locations and user access)
- Use and access of Outlook, SharePoint and Exchange Online

A fully documented approach is developed, with clear steps, to ensure your organisation is ready, and protected at the point of deploying AI technology.