

AI Decisions That Matter

Understanding AI, protecting corporate data and asking the right questions

FA-0823 · 0.5 day

AI for Leaders & Business · DevOps, Cloud & Infrastructure · Cybersecurity

A half-day executive briefing on evaluating AI proposals, on-premises infrastructure, corporate data protection and adoption priorities.

Introduction

Introducing AI across a company involves decisions about business value, information access, infrastructure, spending and accountability. Leaders need enough understanding to assess proposals, recognise risks and identify where specialist advice is required.

This executive briefing explains how AI works, where its limitations matter and what an on-premises AI platform needs to serve the wider organisation. Keeping private data private requires attention to the entire system, including document access, external connections, conversation histories and operational controls.

Participants will develop the confidence to recognise gaps in their understanding and ask useful questions of technical teams, vendors and advisers.

Learning outcomes

By the end of this briefing, participants will be able to:

- Explain the essential workings, capabilities and limitations of modern AI.
- Recognise significant business, security and privacy risks.
- Identify the main infrastructure and controls required for corporate on-premises AI.
- Recognise knowledge gaps and ask informed questions before approving proposals.
- Assess adoption priorities, ownership costs and readiness for wider deployment.

Prerequisites

- Working knowledge of the organisation's operations and business priorities.

Training outline

1. Understanding How AI Works

1. AI, generative AI, language models and agents
2. Training, inference, prompts and context limits
3. Using internal knowledge: retrieval and fine-tuning
4. Capabilities, limitations and suitable business applications

2. AI Risks and Leadership Responsibilities

1. Hallucinations, bias and excessive reliance on AI
2. Data leakage, malicious instructions and unsafe agent actions
3. Intellectual property, compliance and accountability
4. Human oversight, output verification and acceptable use

3. Designing an On-Premises Corporate AI Platform

1. Shared employee access, model serving and business-system integration
2. Model selection, commercial licensing and internal knowledge architecture
3. Compute, memory, storage, networking, power and cooling
4. Capacity planning for workloads, concurrent users and response times
5. Availability, monitoring, maintenance and operational ownership

4. Keeping Corporate Data Private

1. Data classification and approved information sources
2. Corporate identity, departmental permissions and encryption
3. Local processing and control of external connections
4. Protection and retention of conversations, search indexes, logs and backups

5. Asking the Right Questions and Planning Adoption

1. Recognising knowledge gaps and engaging appropriate specialists
2. Challenging vendor claims and requesting evidence
3. Business value, total ownership costs and procurement decisions
4. Pilot success criteria, workforce upskilling and phased deployment

Disclaimer

This outline serves as a guideline. The trainer reserves the right to amend the content, sequence or emphasis, without prior notice, to reflect participants' needs, available time, technological developments and relevant industry requirements.