Faysal Aziz

AI Awareness Unlocked

Concepts, tools and responsible use

FA-0559

Agentic & Generative AI · AI for Leaders & Business

An accessible workshop on AI fundamentals, model and tool choices, agentic workflows, limitations and responsible organisational use.

Introduction

This awareness workshop helps non-technical participants understand how AI systems work at a high level and where they may be useful. It separates practical capabilities from speculation and examines machine learning, neural networks, language models, AI-assisted tools and agents.

Illustrative industry scenarios connect the concepts to deployment choices, interpretability, privacy, fairness and human oversight. The course is a survey, not model-development training or legal advice. Examples and product availability should be checked for the delivery context; AGI predictions and promised business outcomes are not part of the course.

Learning outcomes

The workshop teaches participants to:

- Distinguish common AI concepts, practical capabilities and speculative claims.
- Explain machine learning, deep learning and transformers using accessible examples.
- Recognise data-quality, evaluation, interpretability and unexpected-behaviour challenges.
- Compare hosted and downloadable model options, including licence and deployment trade-offs.
- Describe common AI tools, retrieval-augmented generation and low-code approaches.
- Explain tool-using agents, bounded autonomy and oversight needs.
- Identify business opportunities and responsible-use questions involving privacy, fairness, security and accountability.

Prerequisites

- No technical background required.
- Basic digital literacy.

Training outline

1. 1 – Demystifying AI

- Separating fact from fiction: Common AI myths and why they persist
- Reality check: capabilities, limitations and evidence in the selected examples.
- Hype cycle analysis: Understanding where we are in AI adoption
- Historical context: How we got from chess computers to conversational AI
- Setting realistic expectations: Avoiding both over-optimism and unnecessary fear

2. 2 – Types of AI and capability claims

- Narrow/task-focused AI: recommendations, voice assistance and navigation.
- General intelligence as a contested concept: definitions and uncertainty, not a consensus timeline.
- Agentic systems: planning and tool use within configured constraints; agentic behaviour does not by itself establish general intelligence.

3. 3 – How AI works

Machine Learning fundamentals: Teaching computers to learn from patterns

- The three pillars: supervised, unsupervised, and reinforcement learning
- Data quality, coverage and quantity: why all matter for reliable modelling.

Deep Learning architectures: The brain-inspired approach

- Neural networks explained through everyday analogies
- What multiple layers enable, and what depth alone does not guarantee.

Transformer models revolution: The technology behind ChatGPT and beyond

- Attention mechanisms and their role in transformer models.
- From language to vision to multimodal applications

The training process: From raw data to intelligent systems

- Data pipelines and preprocessing essentials
- Training cycles, validation, and continuous improvement

4. 4 — Interpretability and unexpected behaviour

Why AI decisions can be mysterious: Understanding opacity in complex systems

- The trade-off between performance and interpretability
- When black boxes become problematic in business contexts

Explainable AI (XAI) approaches: Opening the black box

- Techniques for understanding AI decision-making
- Transparency and risk-management frameworks, including voluntary NIST guidance; distinguish standards from legal requirements.

Emergent properties phenomenon: When AI surprises its creators

- Unexpected capabilities that weren't explicitly programmed
- Illustrative unexpected behaviours and implications for evaluation and deployment.

5. 5 — Industry uses and emerging directions

- Illustrative uses in healthcare and drug discovery, finance and fraud detection, manufacturing and maintenance, creative work, and transport/logistics.
- Distinguish a research example, pilot, deployed system and evidence of success; examine cautionary scenarios.
- Agentic workflows and integration challenges.
- AI-assisted cybersecurity and response automation: useful capabilities and failure modes.

- Local/edge AI for mobile and IoT: resource, privacy and performance trade-offs.
- Responsible adoption and changing regulation; investment claims require current evidence.

6. 6 — Model options and deployment choices

- Commercial hosted model ecosystems: OpenAI, Anthropic, Google and xAI as examples, not a version ranking.
- Downloadable models and families such as Llama, DeepSeek, Mistral, Falcon, Gemma and Phi: inspect the specific model card, licence and supported use.
- Distinguish open source, open weights, hosted access and custom licence restrictions.
- Compare total cost, customisation, control, infrastructure, data handling and sector requirements.

7. 7 — AI tools and application building blocks

- Hugging Face model/dataset discovery, LangChain workflows and model-serving tools such as OpenLLM where suitable.
- Cloud versus on-premises hosting, inference costs and resource trade-offs.
- Retrieval-augmented generation, vector search and integration patterns; retrieval does not guarantee correctness.
- Low-code/no-code builders versus custom development: capabilities, limits and access requirements.

8. 8 — Agentic AI in workflows

Agentic behaviour: goals, tools and bounded autonomy.

- Goal-oriented vs. reactive systems
- Decision-making independence and constraints

Illustrative agent workflows and deployment conditions.

- Customer-service assistance, escalation and reliability considerations.
- Supply chain management and optimization
- Personal productivity assistants and their capabilities

Integration strategies: Bringing agentic AI into existing workflows

- Phased implementation approaches
- Change management and user adoption

Risk assessment and mitigation: The responsible path forward

- Identifying potential failure modes
- Monitoring and control mechanisms
- Building human oversight into autonomous systems

Future directions and uncertainty

- Potential capabilities and limits: separate evidence from speculation.
- Industry-specific applications in development

9. 9 — Ethics, governance and organisational practice

Core principles

- Fairness: historical bias examples, evaluation across groups, mitigation and limits.
- Transparency and explainability: communicate decisions and trade-offs appropriately.
- Privacy: data minimisation, consent, anonymisation limitations and cross-border questions.
- Human agency: meaningful oversight, approval boundaries and augmentation of judgement.

Governance and legal awareness

- Compare binding laws, voluntary risk frameworks, sector requirements and organisational policies.
- EU AI Act: risk-based obligations and prohibited uses at an awareness level; applicability and requirements depend on the system and legal context.
- United States and Asia-Pacific approaches: federal/state/sector obligations and differing national or voluntary frameworks; no universal compliance recipe.
- Understand the role and limitations of industry initiatives, internal review boards and independent assessments.

From principles to practice

- Assign responsibilities and review processes; assess risks and engage stakeholders.
- Document decisions and evaluation evidence; test fairness, safety and robustness.
- Monitor systems and plan incident response, remediation and vendor due diligence.
- Review data handling and relevant contractual requirements with appropriate specialists.

Emerging ethical issues and culture

- Synthetic media, provenance/detection limits, attribution and creative rights.
- Hiring, surveillance, autonomous decisions and military-use contexts: discuss discrimination, civil liberties, accountability and relevant specialist review.
- Awareness training, concerns/escalation channels and cross-functional collaboration.
- Engage affected communities and choose meaningful measures for responsible use.

© 2026 Faysal Aziz · Kuala Lumpur