Halderstone

Training module

AI Systems & Architectures

Core AI concepts, AI system types, AI agents, and the technical building blocks behind modern AI-enabled products and services

Do you understand how AI systems and AI agents work?

Overview

Organisations often adopt "AI" as an umbrella label that hides critical differences: rules vs. machine learning, predictive vs. generative behaviour, single-model services vs. agentic patterns, and model-in-a-box vs. AI as part of a wider socio-technical system. Without a clear mental model, governance discussions drift, requirements get misapplied, and assurance work focuses on surface artefacts rather than how the system actually operates.

This training module establishes practical AI literacy: key terms, AI system types, AI agents, and the technical building blocks that recur across most implementations (data pipelines, models, prompts, orchestration, interfaces, and supporting IT controls such as access management, encryption, and logging). It intentionally does not cover AI risk and harm assessment, lifecycle scoping and inventory methods, operational control design, or detailed failure-mode analysis; those are handled in the dedicated follow-up modules.

Target audience

- AI management system managers and implementers working with technical teams
- Governance, risk, and compliance professionals who need AI domain fluency
- Product owners and process owners responsible for AI-enabled services
- Auditors who need a shared baseline understanding of AI systems (not audit craft)
- Anyone who wants to get a basic understanding of AI fundamentals

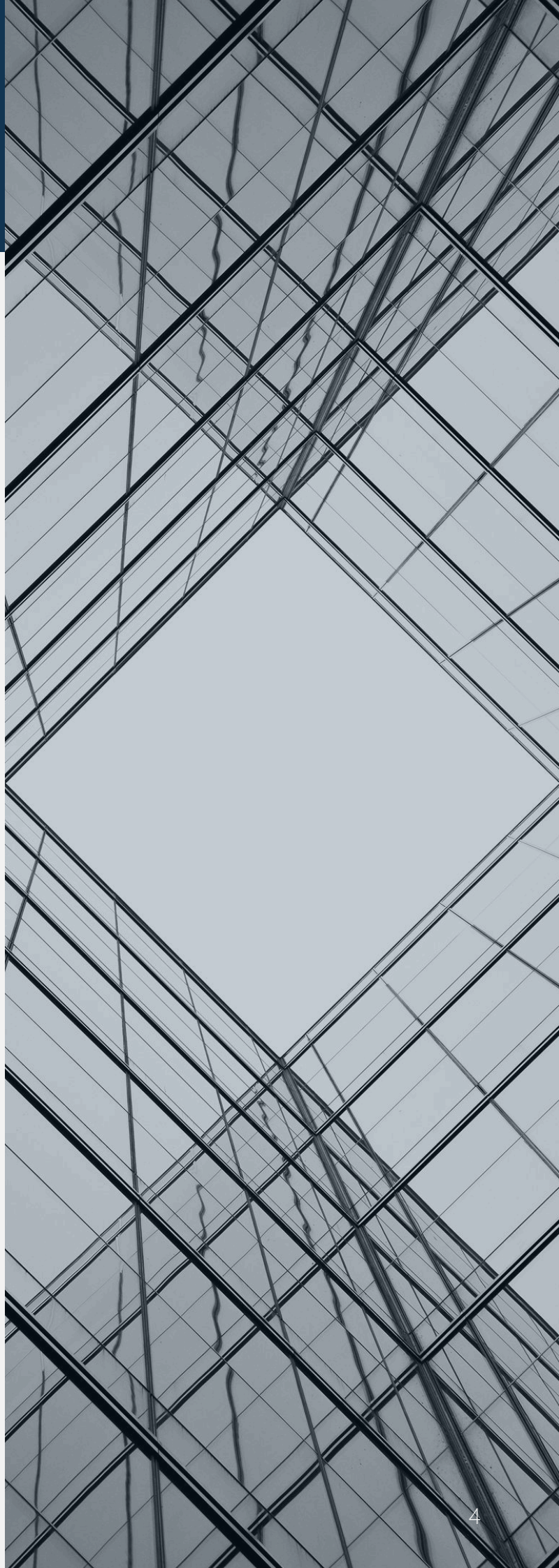
Is this module for you?

It is a good fit for you if you...

- want a clear, shared mental model of how AI systems actually work.
- need to distinguish rules, ML, and generative AI beyond buzzwords.
- work with AI systems and must ask better questions of technical teams.
- need concept-level literacy to interpret AI risks, controls, or evidence.
- want to reason about AI systems without relying on specific tools or vendors.

It may be less suitable for you if you...

- are looking for hands-on model building or coding exercises.
- expect vendor- or platform-specific AI tooling training.
- want ISO/IEC 42001 requirements, roles, or processes explained in detail.
- already have deep technical AI expertise and seek advanced methods.



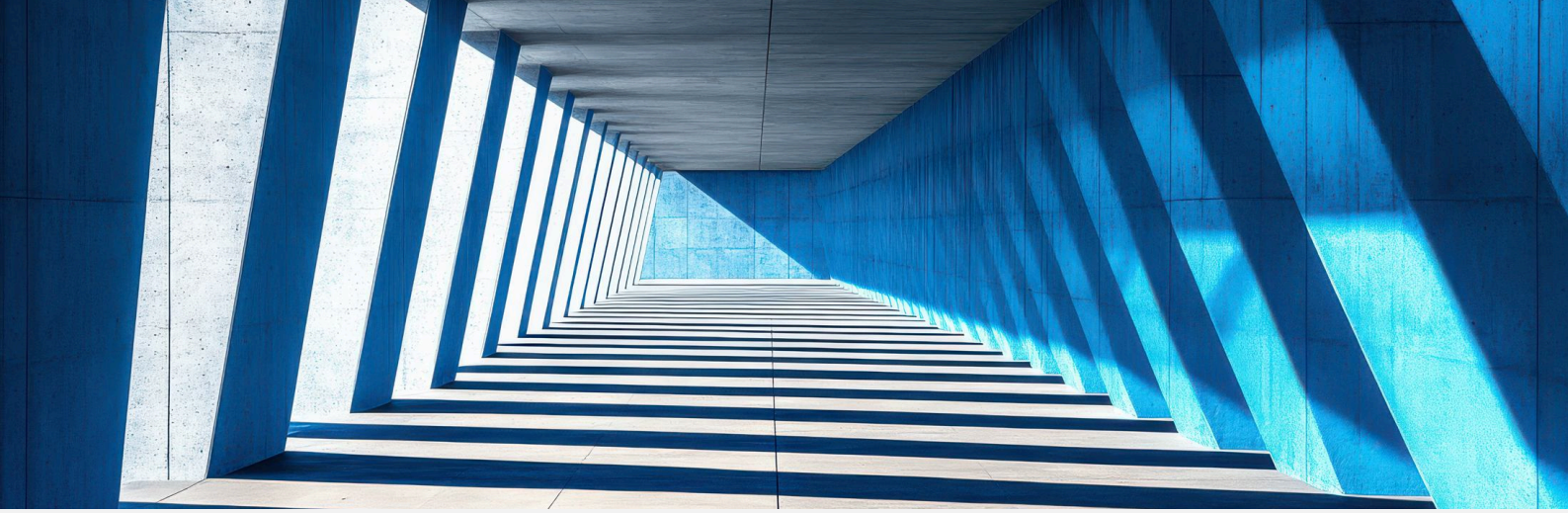
Learning outcomes

Key outcomes

- Distinguish automation, analytics, machine learning, generative AI, and AI agents in organisational contexts
- Explain how AI systems are built from data, models, inference, prompts, and orchestration
- Identify core components, interfaces, and supporting technical controls in AI-enabled services and agentic workflows

Additional capabilities

- Recognise common AI system types, agent patterns, and architectural structures
- Explain how datasets, labels, splits, provenance, and prompts shape behaviour
- Identify typical deployment, integration, and orchestration patterns
- Formulate structured technical questions about AI components, tools, and agent flows



Agenda

AI in organisations: what “AI” does and does not mean

How AI is positioned in organisations by clearly distinguishing automation, analytics, machine learning, generative AI, and agentic patterns, and by clarifying where AI actually sits in products and decision processes

Core concepts: data, models, inference, and prompts

How AI systems are built from data, models, inference, and prompts, including the practical distinction between training and inference and the role of features, embeddings, and prompts in different system designs

AI system types, AI agents, and typical architectures

How different AI system types (rule-based, ML-based, generative, hybrid, and agentic) are structured and how pipelines, services, orchestration layers, tools, and human touchpoints typically interact

Data building blocks that matter for AI systems

How datasets, labels, provenance, splits, and transformations shape AI behaviour and create dependencies across the AI stack

Deployment patterns, orchestration, and operational context

How AI systems are deployed in practice via APIs, embedded or edge use, workflow integration, agent orchestration, and human-in-the-loop patterns, including their operational dependencies

Supporting technical controls around AI components

How basic technical controls such as access management, encryption, logging, traceability, and change points support AI components across pipelines, services, and agentic workflows

Case-based workshop

Applying the learned concepts, methods, and approaches in a realistic case setting

Included materials

Learning materials

- Slide deck
- Participant workbook

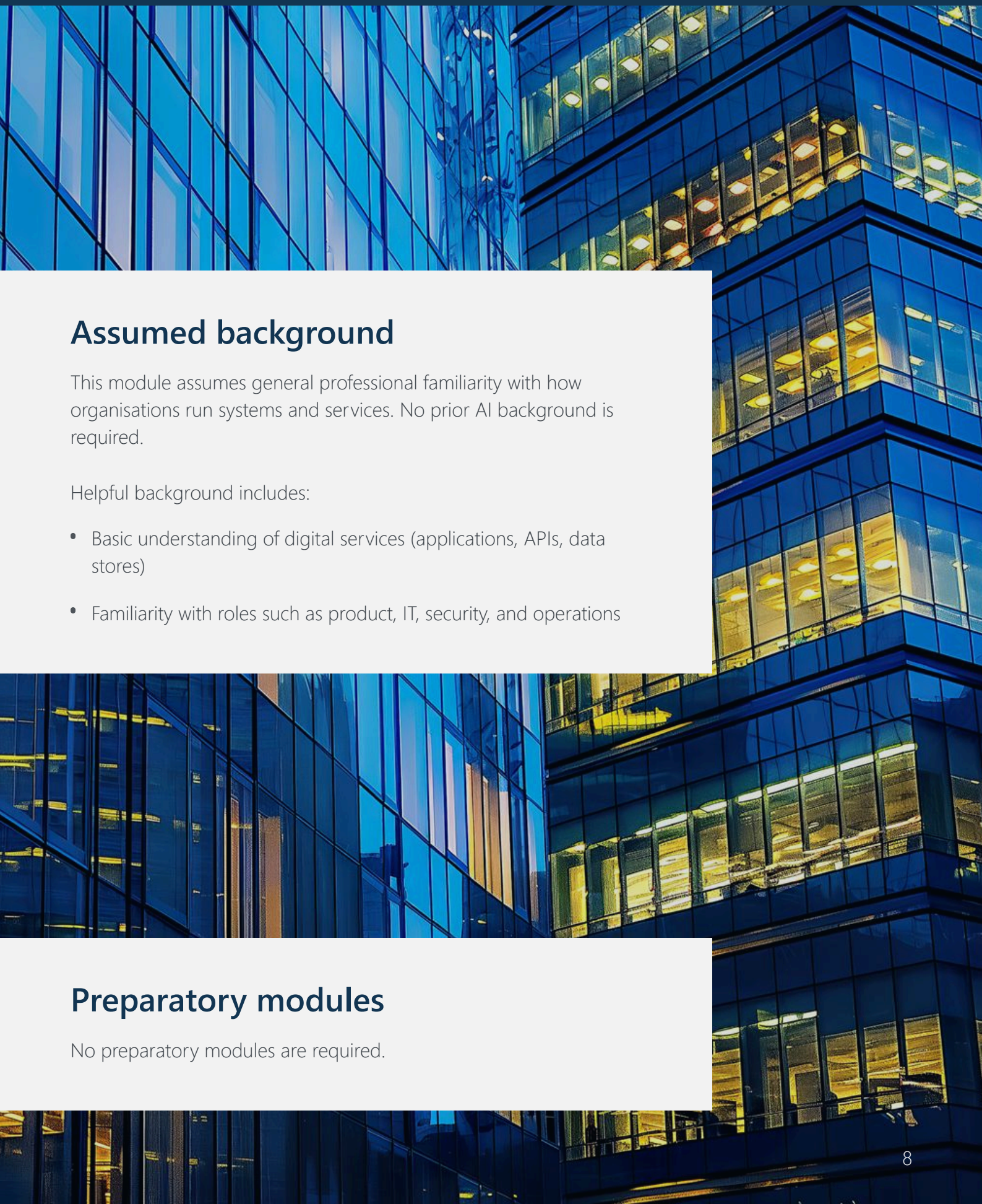
Templates & tools

- AI terminology and concept glossary
- AI system types and agent patterns quick-reference sheet
- AI system and agent component map
- Data / model artefact primer
- Question prompts for technical walkthroughs

Confirmation

- Confirmation of participation

Preparation guidance



Assumed background

This module assumes general professional familiarity with how organisations run systems and services. No prior AI background is required.

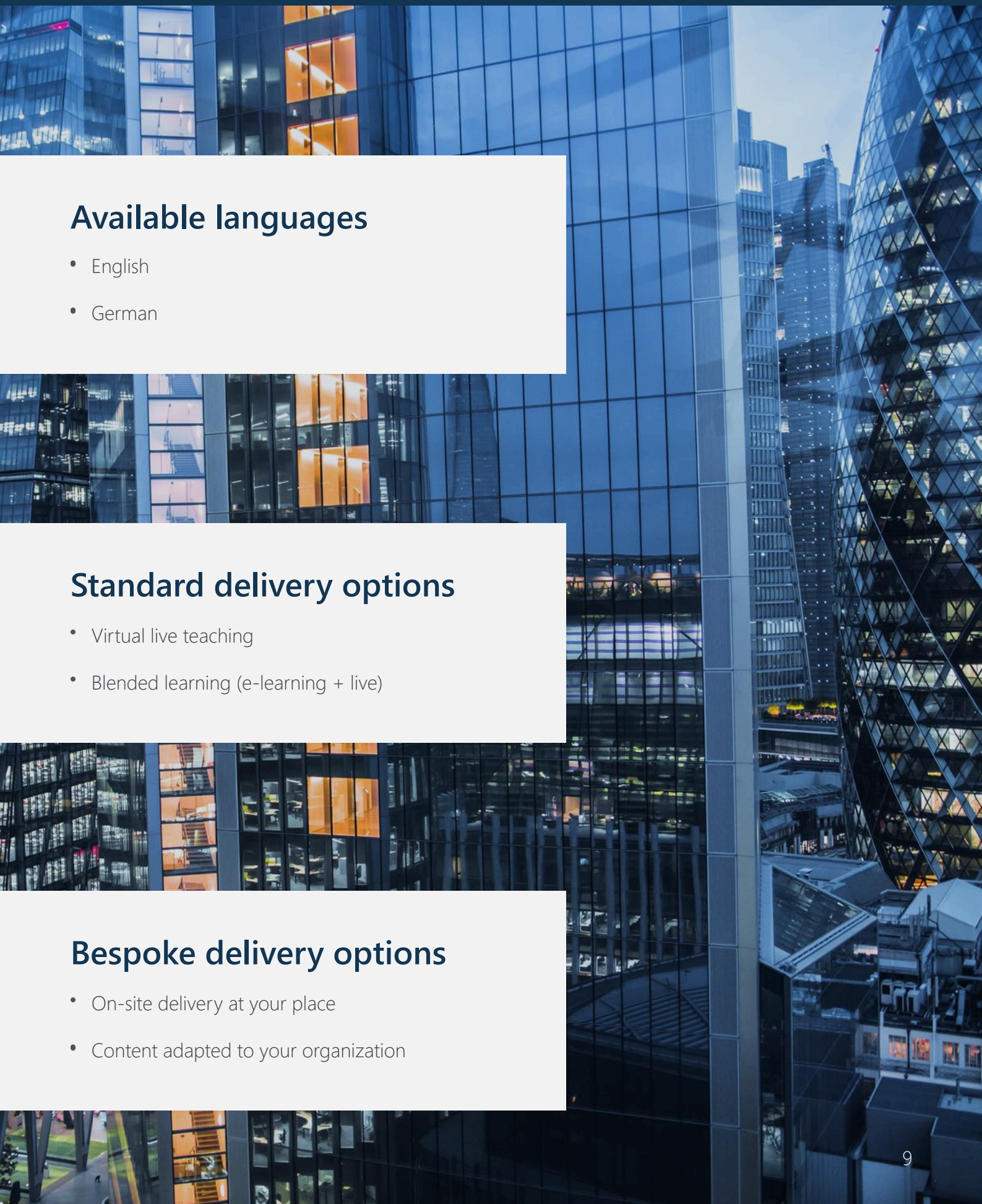
Helpful background includes:

- Basic understanding of digital services (applications, APIs, data stores)
- Familiarity with roles such as product, IT, security, and operations

Preparatory modules

No preparatory modules are required.

Logistics



Available languages

- English
- German

Standard delivery options

- Virtual live teaching
- Blended learning (e-learning + live)

Bespoke delivery options

- On-site delivery at your place
- Content adapted to your organization

Halderstone

Halderstone by Langer & Co
Zürcherstrasse 2
CH-8852 Altendorf
Switzerland
info@halderstone.com
www.halderstone.com