Halderstone

Training module

Auditing Privacy Risk & Impact Assessment

Evaluate whether privacy risk assessments and DPIAs produce credible risk understanding and prioritisation in an ISO/IEC 27701 PIMS

Do DPIAs exist but privacy risks still surface unexpectedly?

Overview

Privacy risk and impact assessments form the analytical foundation of privacy information management systems. They identify how personal data processing can affect individuals, evaluate the likelihood and severity of harm, and establish priorities for risk treatment and governance decisions.

In practice, privacy risk and impact assessments often appear structured while their analytical value remains limited: processing activities are incompletely described, risk reasoning is inconsistent, impact analysis is superficial, and assessments become compliance artefacts rather than decision tools.

This module develops the capability to audit whether privacy risk and impact assessments credibly analyse processing activities and associated risks. Participants first review how privacy risk assessment and data protection impact assessments function within a privacy information management system, then learn how auditors test analytical completeness, risk reasoning, and impact evaluation evidence.

Target audience

- Aspiring auditors who want to audit privacy information management systems against ISO/IEC 27701 following best practices
- Practising ISO/IEC 27701 auditors who want to strengthen their audit knowledge, judgement, and effectiveness

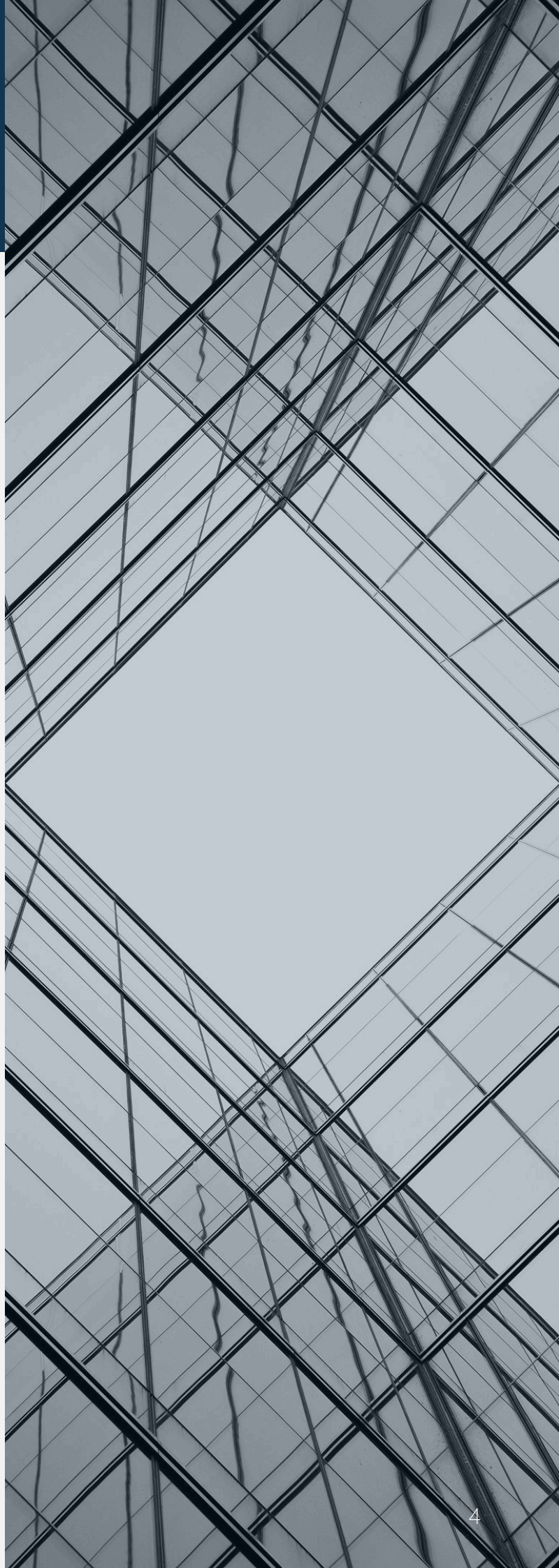
Is this module for you?

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

- audit privacy risk assessments or DPIAs within privacy information management systems.
- seek to judge whether privacy risks are identified and prioritised credibly.
- want to test analytical completeness and impact reasoning in DPIAs.
- need to evaluate how processing activities are analysed from a privacy risk perspective.
- expect to strengthen audit conclusions on privacy risk analysis effectiveness.

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

- prefer to conduct privacy risk assessments or DPIAs yourself.
- are looking for methods to design privacy controls or safeguards.
- focus primarily on privacy engineering or compliance implementation.
- do not intend to audit privacy risk and impact assessments.



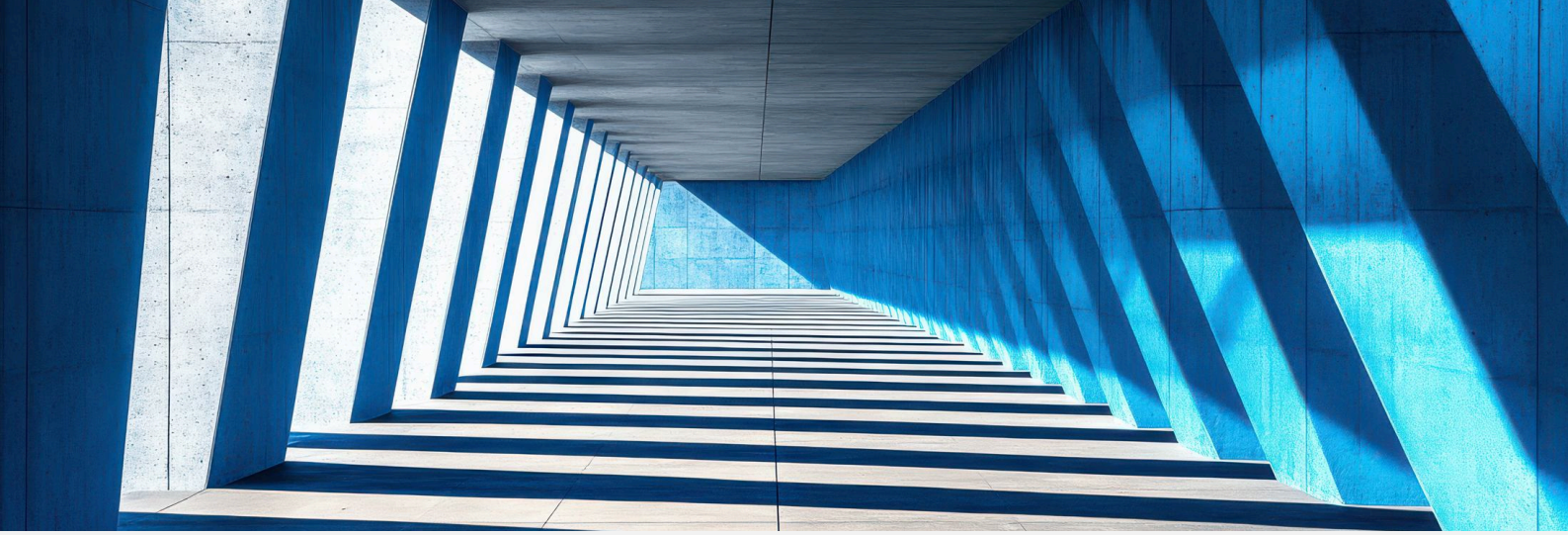
Learning outcomes

Key outcomes

- Assess whether privacy risk assessments and DPIAs identify relevant processing activities and risks
- Test impact reasoning and likelihood assessments for consistency and plausibility
- Trace privacy risk conclusions to underlying processing activities using defensible audit evidence

Additional capabilities

- Evaluate whether impact analysis credibly considers risks to individuals rather than organisational risk only
- Detect common privacy risk assessment failure patterns such as template-driven assessments or incomplete processing descriptions
- Select meaningful sampling targets when auditing privacy risk and impact assessments
- Formulate defensible audit conclusions on the credibility and usefulness of privacy risk analysis



Agenda

Privacy risk and impact assessment in a PIMS

How privacy risk assessments and DPIAs analyse personal data processing activities and establish risk understanding within a privacy information management system

Effective auditing of privacy risk and impact assessment

How auditors judge whether privacy risk analysis produces credible understanding rather than relying on documentation completeness

Processing activity identification and scope

How to evaluate whether privacy risk assessments correctly describe processing activities, purposes, data categories, actors, and data flows

Privacy impact reasoning

How to test whether impact analysis considers risks to individuals across confidentiality, misuse, discrimination, or other harms

Likelihood and risk evaluation logic

How to evaluate whether risk likelihood and severity assessments are consistent and supported by credible reasoning

Completeness of privacy risk analysis

How to detect omitted processing scenarios, overlooked stakeholders, or missing lifecycle stages in privacy risk assessments

Common DPIA failure patterns

How to detect template-driven assessments, superficial analysis, or organisational bias in privacy risk evaluation

Case-based audit simulation

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

Included materials

Learning materials

- Slide deck
- Participant workbook

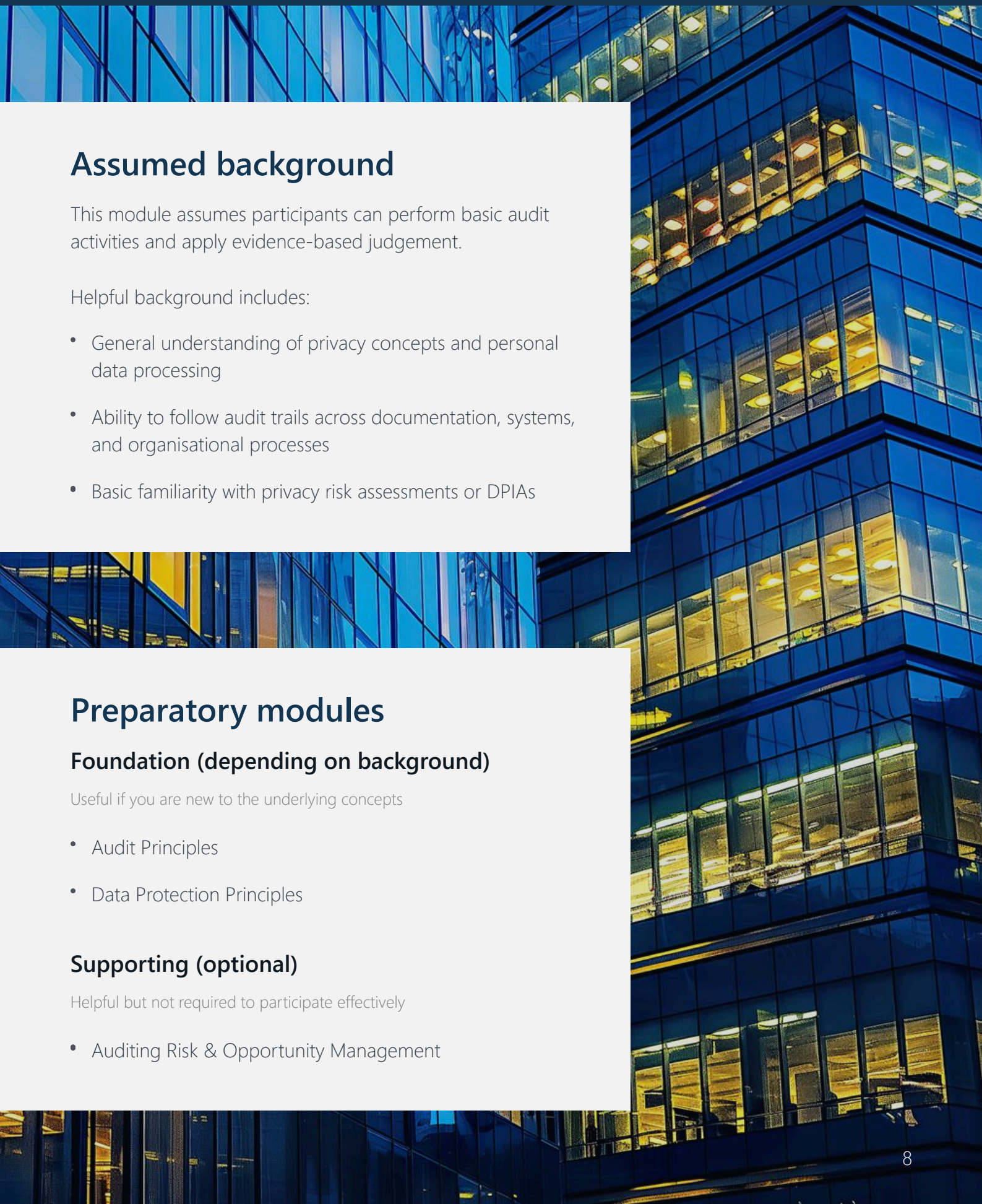
Templates & tools

- Audit interview planning tool
- Documented information checklist
- Sampling tool
- Audit analysis worksheets
- Failure pattern library
- Supporting AI prompt set

Confirmation

- Confirmation of participation

Preparation guidance



Assumed background

This module assumes participants can perform basic audit activities and apply evidence-based judgement.

Helpful background includes:

- General understanding of privacy concepts and personal data processing
- Ability to follow audit trails across documentation, systems, and organisational processes
- Basic familiarity with privacy risk assessments or DPIAs

Preparatory modules

Foundation (depending on background)

Useful if you are new to the underlying concepts

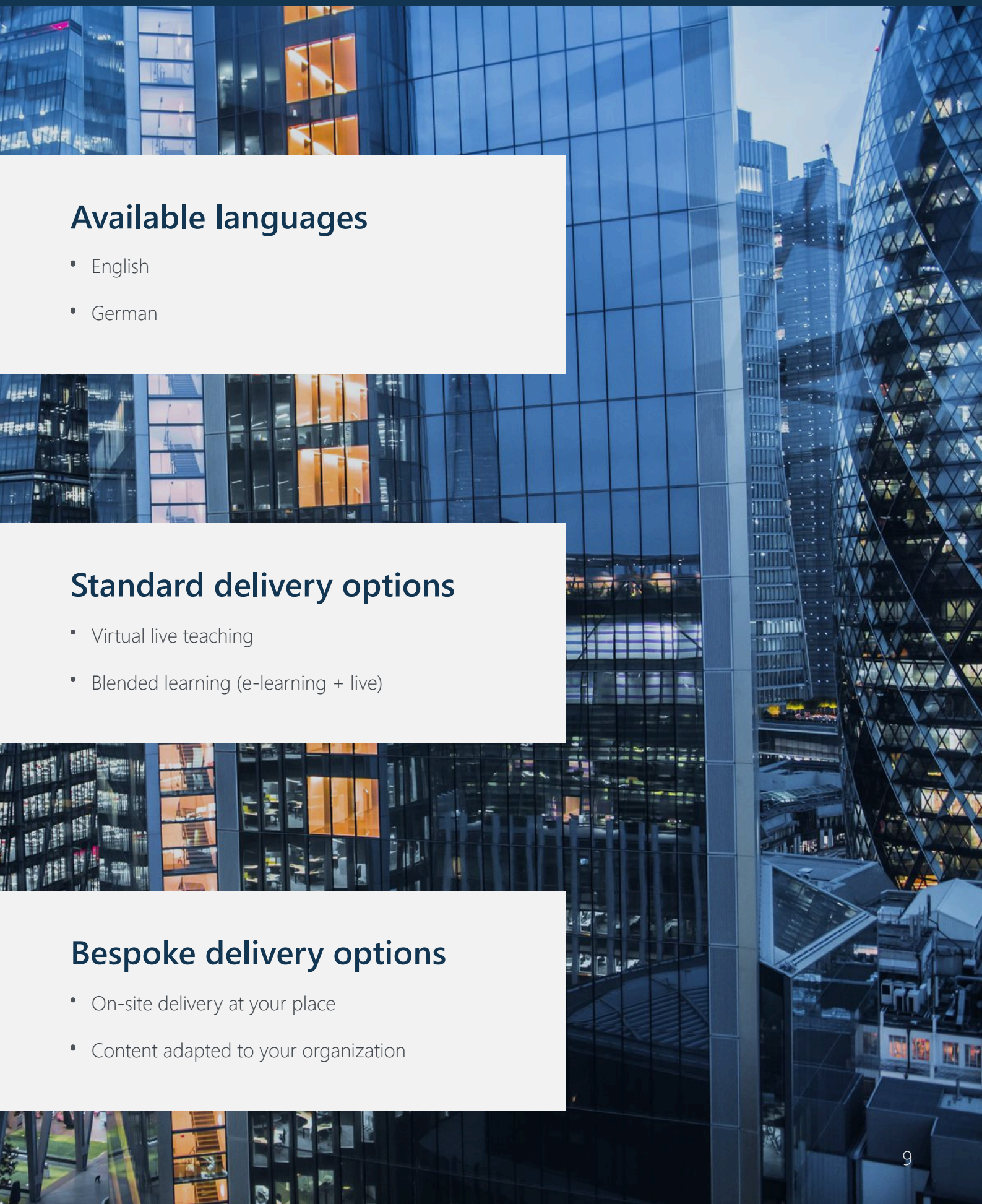
- Audit Principles
- Data Protection Principles

Supporting (optional)

Helpful but not required to participate effectively

- Auditing Risk & Opportunity Management

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