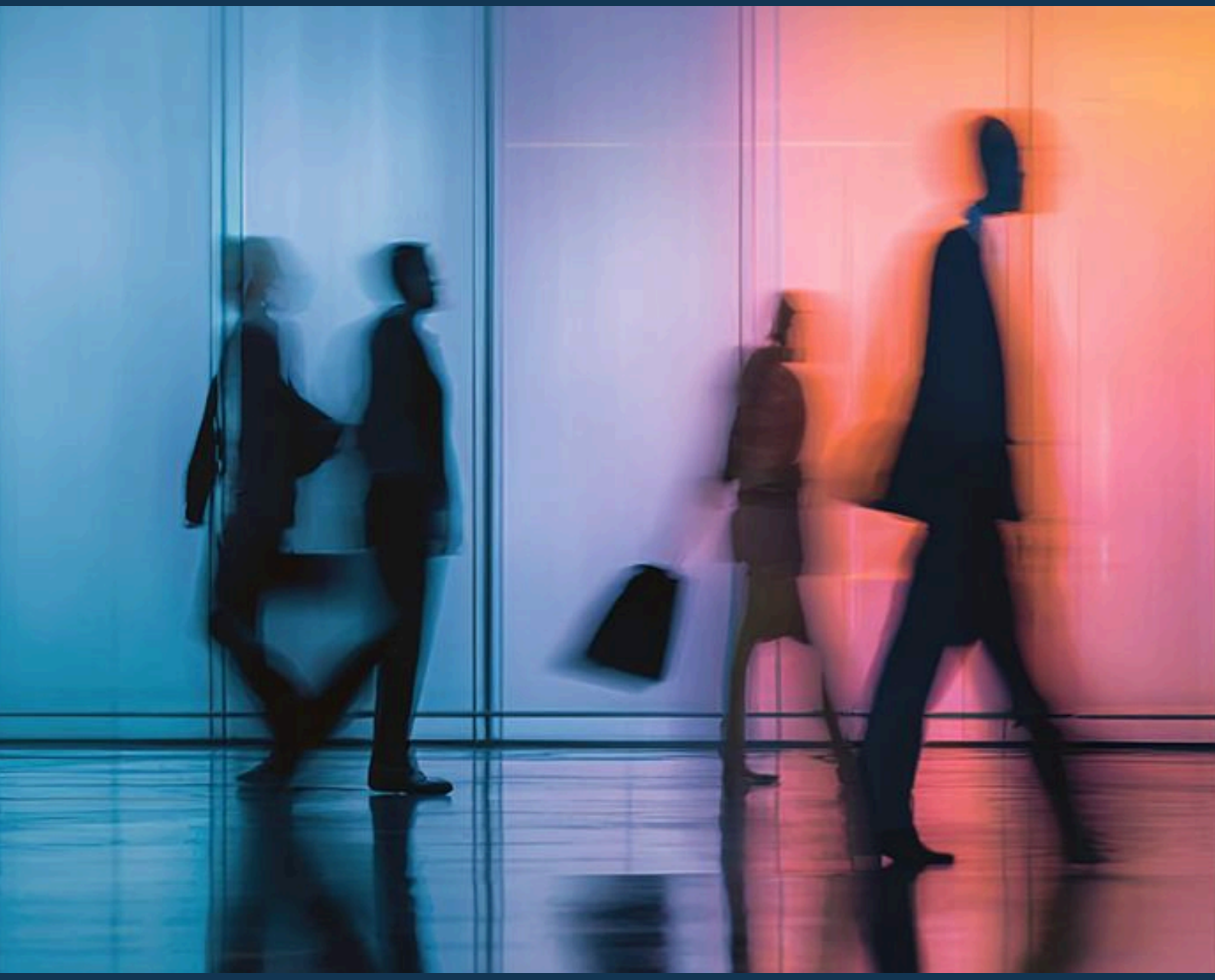
Halderstone



Training module

Privacy Risk & Impact Assessment (DPIA)

Assess privacy risks, reason about impacts, and document DPIAs within an ISO/IEC 27701-aligned PIMS

Are your DPIAs systematic and defensible?

Overview

ISO/IEC 27701 sets explicit requirements for privacy risk assessment and treatment within a PIMS and is no longer dependent on ISO/IEC 27001 certification. In practice, organisations struggle less with "doing a DPIA" than with making the assessment logic repeatable : consistent triggers, defensible impact reasoning, documented assumptions, and clear decision rights for residual risk.

This module focuses on DPIA logic as a management-system capability in a PIMS : structuring assessments, reasoning about impacts on individuals, linking outcomes to treatment decisions, and keeping assessments current as processing changes. It does not teach privacy fundamentals, scoping/role determination, operational privacy controls, or data subject rights execution; those are addressed in adjacent specialisation modules. It also does not re-teach generic risk methodology (scales, scoring models, risk appetite design), which is owned by Risk Management Foundations.

Target audience

- People involved in implementing, operating, or improving a PIMS aligned with ISO/IEC 27701
- Executives and department heads accountable for the effectiveness and performance of a PIMS
- Those responsible for processes, policies, IT systems, risks, and controls related to data protection
- Auditors of ISO/IEC 27701 who want to deepen their understanding of management-side best practices (not audit technique)

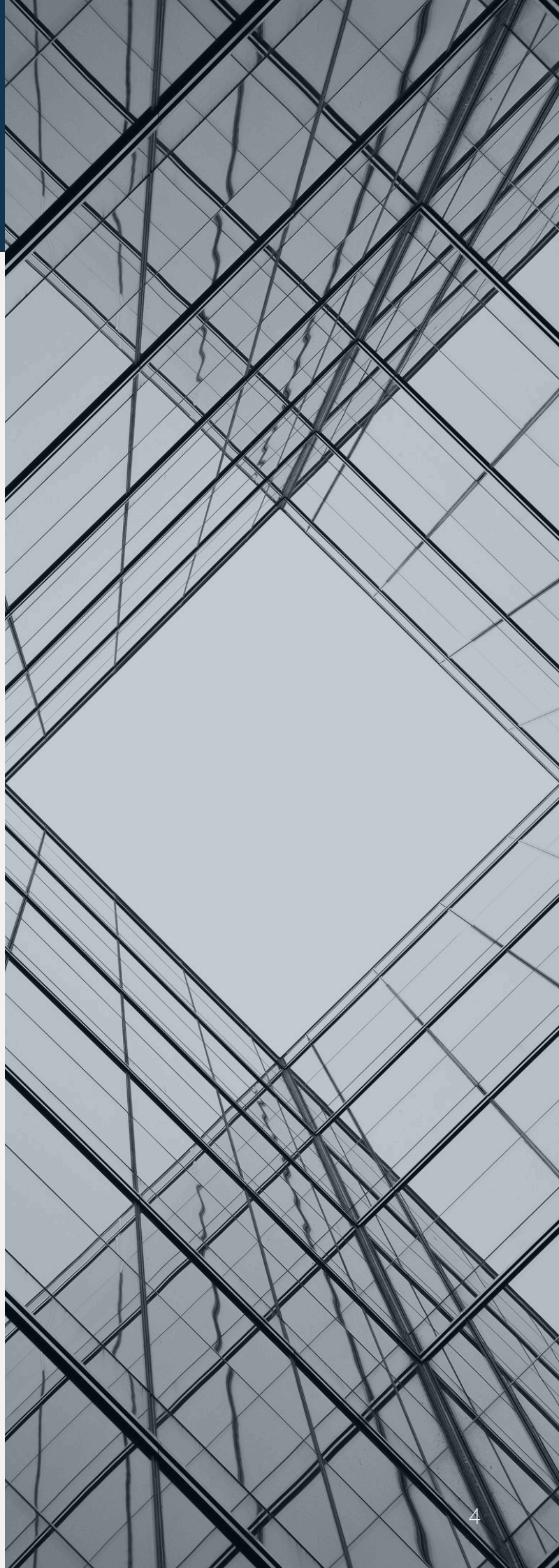
Is this module for you?

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

- need a repeatable DPIA logic rather than ad-hoc assessments.
- want clear triggers, roles, and decision ownership for DPIAs.
- need defensible impact reasoning for approval and acceptance decisions.
- want DPIAs to stay current as processing and systems change.
- support audit-ready, consistent DPIA governance in a PIMS.

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

- are looking for privacy fundamentals or legal theory.
- want a generic risk methodology or scoring model.
- expect detailed guidance on technical privacy controls.
- already run stable, well-embedded DPIA processes at scale.



Learning outcomes

Key outcomes

- Explain how ISO/IEC 27701 expects privacy risk assessment and treatment to function within a PIMS
- Define DPIA trigger logic and proportionality rules that apply consistently across the organisation
- Structure DPIA-style assessments around real processing activities with shared services and suppliers

Additional capabilities

- Apply a disciplined approach to impact reasoning on individuals and document assumptions transparently
- Translate assessment outcomes into clear treatment decisions and residual risk acceptance criteria
- Produce a maintainable DPIA documentation pack with traceability and review triggers so DPIAs stay current

Agenda

Where privacy risk assessment sits in a PIMS

How privacy risk assessment provides decision-ready inputs for treatment, control selection, and justification, rather than acting as a parallel compliance exercise

Assessment boundaries and inputs

How to define clear assessment boundaries based on maintained processing context, roles, and scope artefacts, and avoid generic checklists or opinion-based inputs

Trigger logic: when a DPIA-style assessment is needed

How to recognise practical change triggers that require deeper assessment and apply proportional triage between lightweight reviews and full DPIA-style assessments with defensible rationale

Defining the assessment unit

How to structure assessments around concrete processing activities, so responsibility and outcomes remain clear

Impact reasoning focused on individuals

How to reason about impacts on rights and freedoms using severity, scale, reversibility, and vulnerability, while keeping assumptions explicit and evidence-based

Likelihood reasoning in privacy terms

How to trace causal chains from processing design choices to exposure and harm pathways, using credible indicators and uncertainty notes instead of false numerical precision

Treatment logic and residual risk decisions

How to link assessment outcomes to treatment options, document decision rationale, and handle residual risk acceptance through clear decision rights, escalation paths, and consultation triggers

DPIA documentation pack and traceability

How to maintain a minimal, coherent DPIA record set that supports traceability from assessment through decisions to implementation evidence

Technology as an enabler

How to use registers, workflows, versioning, and AI-assisted summaries to keep assessments current and connected to change signals while preserving human judgement

Case-based workshop

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

Included materials

Learning materials

- Slide deck
- Participant workbook

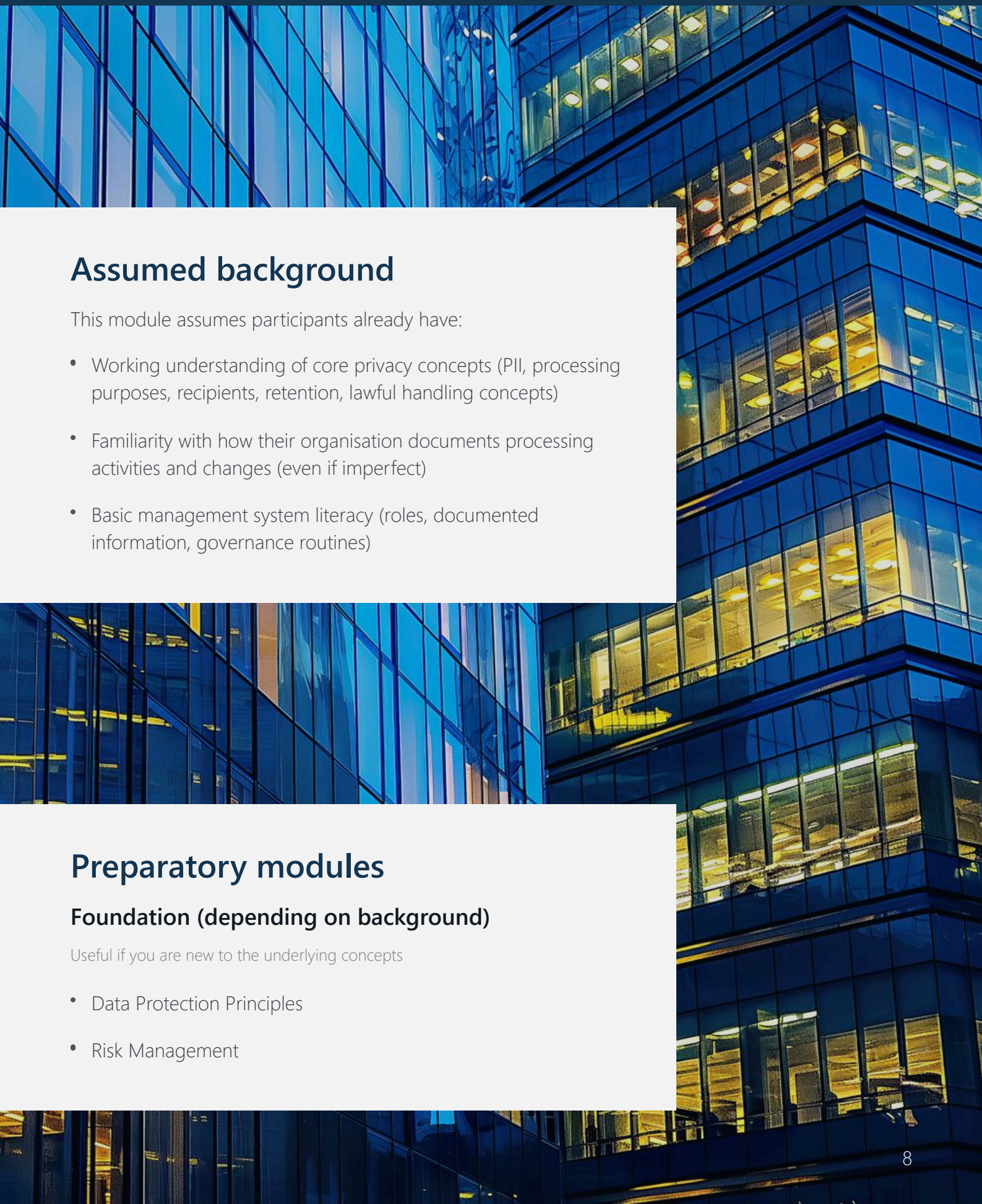
Templates & tools

- DPIA trigger & triage decision tree
- DPIA / privacy risk assessment template
- Impact reasoning worksheet
- Risk-to-treatment traceability matrix
- DPIA review & change trigger checklist
- Supporting AI prompt set

Confirmation

- Confirmation of participation

Preparation guidance



Assumed background

This module assumes participants already have:

- Working understanding of core privacy concepts (PII, processing purposes, recipients, retention, lawful handling concepts)
- Familiarity with how their organisation documents processing activities and changes (even if imperfect)
- Basic management system literacy (roles, documented information, governance routines)

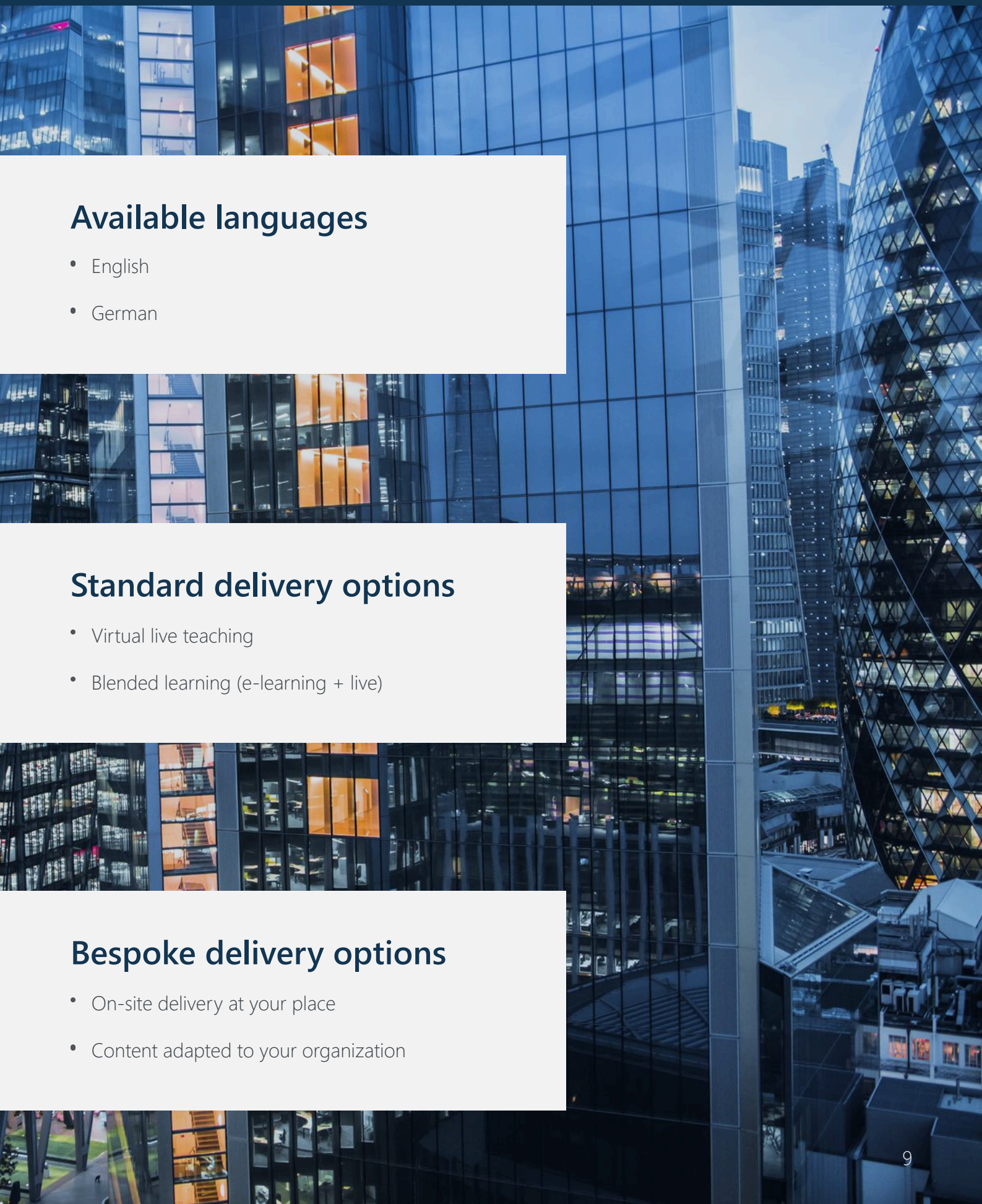
Preparatory modules

Foundation (depending on background)

Useful if you are new to the underlying concepts

- Data Protection Principles
- Risk 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