Halderstone

Training module

Information Security Risk Management

Systematically assess, treat & document information security risks with traceable decisions in line with ISO/IEC 27001

Does your risk management practice produce artefacts that fail to influence control decisions?

Overview

Risk registers and scoring exercises often sit in isolation, disconnected from control selection and acceptance decisions.

This training module explains how ISO/IEC 27001 frames risk assessment and treatment, how to define risk criteria and statements, and how to document assessment results in a way that supports treatment planning and residual risk acceptance. Participants learn to produce coherent risk treatment artefacts that link risks, treatment options, selected controls and the Statement of Applicability. The module emphasises traceability and maintenance rather than the mechanics of scoring models.

Target audience

- People involved in designing, building, operating, or improving an ISMS aligned with ISO/IEC 27001
- Executives and department heads accountable for the effectiveness and performance of an ISMS
- Those responsible for processes, policies, assets, risks, and controls related to information security
- Auditors of ISO/IEC 27001 who want to deepen their understanding of management-side best practices (not audit technique)

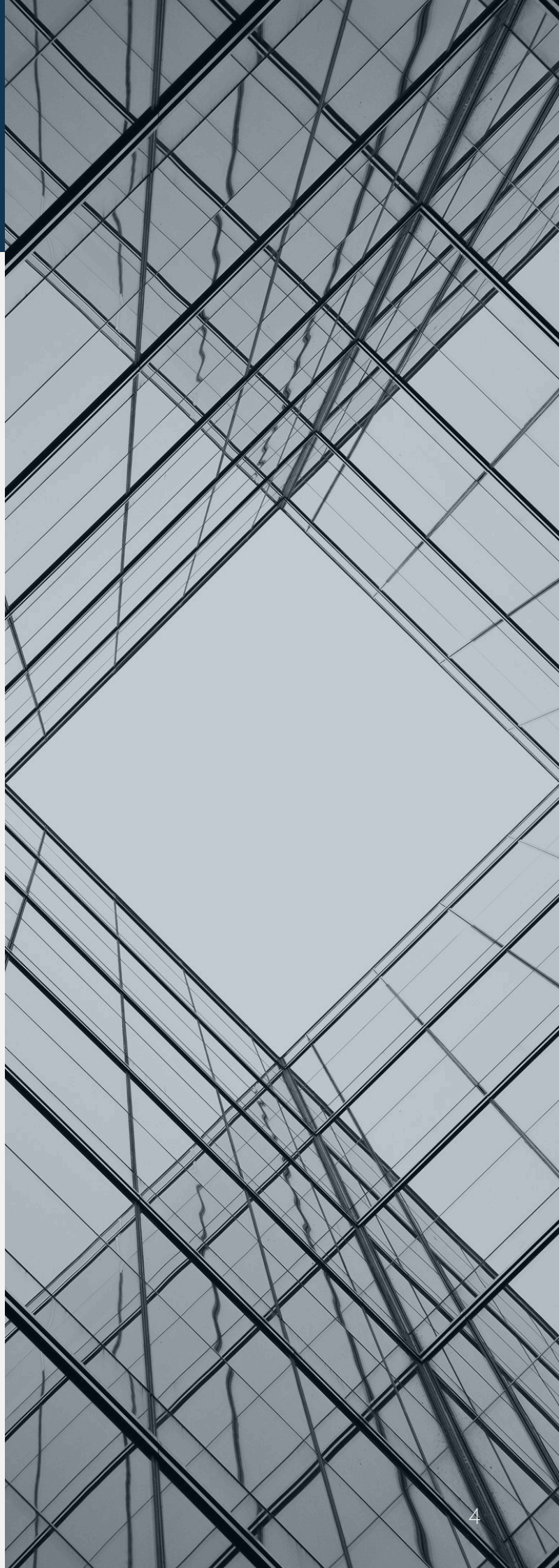
Is this module for you?

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

- are responsible for ISMS risk assessment, treatment, or acceptance decisions.
- struggle with inconsistent risk criteria, weak risk statements, or unclear ownership.
- need risk outputs that clearly justify control selection and SoA decisions.
- must produce risk artefacts that hold up in audits and management review.
- want risk management to function as a repeatable decision process, not a one-off exercise.

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

- are looking for a general introduction to information security risk concepts.
- expect quantitative risk modelling or advanced risk analytics.
- want a tool-specific or template-driven risk assessment walkthrough.
- already operate a consistent, well-understood, and reviewable ISMS risk process.



Learning outcomes

Key outcomes

- Interpret ISO/IEC 27001 risk assessment and treatment requirements in practical terms
- Define documented elements (criteria, statements, decision records) needed for consistent risk methods
- Produce risk treatment artefacts that evidence decisions and residual risk acceptance

Additional capabilities

- Maintain traceability from risks through treatment decisions to controls and the Statement of Applicability
- Identify common pitfalls in risk assessment and treatment that lead to paper exercises
- Set maintenance routines and review triggers to keep risk records current and useful

Agenda

Role of risk management inside an ISMS

How ISO/IEC 27001 uses risk management to enable traceable decisions rather than paperwork, and how risk work connects to scope, objectives, controls, and management review

ISO/IEC 27001 risk terminology and required definitions

How information security risk concepts are used in the standard, including risk owners, acceptance, and residual risk, and what must be defined and maintained as the risk method without re-teaching it

Risk criteria and consistency requirements

How governance intent is translated into usable impact, likelihood, and acceptance criteria, and why poorly designed criteria fail consistency and defensibility tests

Risk assessment outputs that support treatment decisions

What good ISMS risk statements look like in practice, including clarity, ownership, and affected information or processes, and which minimum fields are required to avoid orphan risks and untestable conclusions

Risk treatment expectations and artefacts

How ISO/IEC 27001 defines treatment options and evidencing decisions, and what proportionate treatment planning looks like in terms of owners, timelines, dependencies, and residual risk handling

Traceability to controls and the SoA interface

How treatment decisions drive control selection and justification, and how the SoA must show a defensible rationale for every included or excluded control linked back to risk treatment

Maintaining risk information over time

How changes, incidents, and performance signals trigger risk updates, and how risk and treatment artefacts stay aligned with operational reality and management review inputs

Case-based workshop

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

Included materials

Learning materials

- Slide deck
- Participant workbook

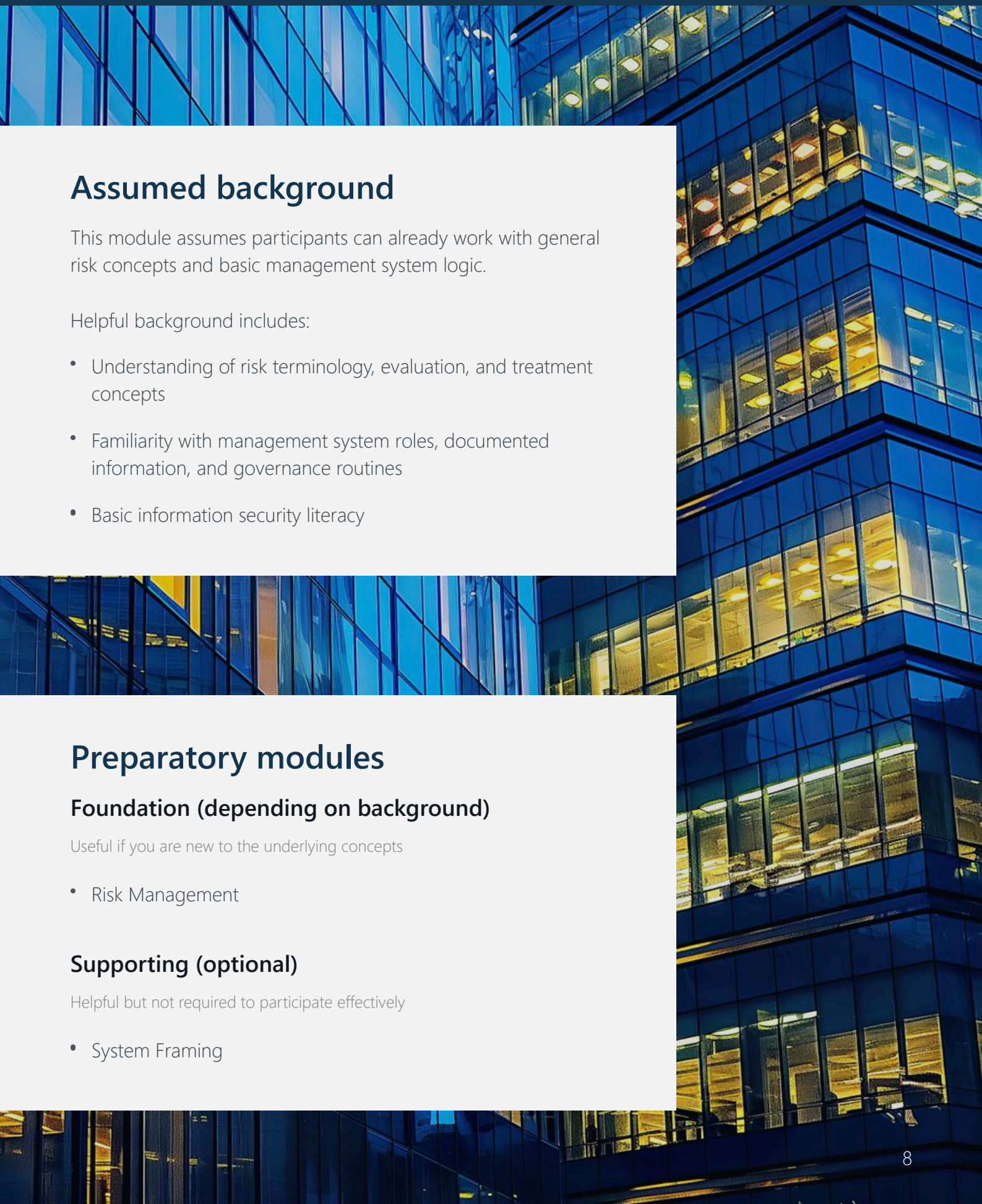
Templates & tools

- Information security risk management process
- Example information security risk register
- Risk criteria quality check list
- Risk treatment decision log
- Risk treatment plan template
- Supporting AI prompt set for typical use cases

Confirmation

- Confirmation of participation

Preparation guidance



Assumed background

This module assumes participants can already work with general risk concepts and basic management system logic.

Helpful background includes:

- Understanding of risk terminology, evaluation, and treatment concepts
- Familiarity with management system roles, documented information, and governance routines
- Basic information security literacy

Preparatory modules

Foundation (depending on background)

Useful if you are new to the underlying concepts

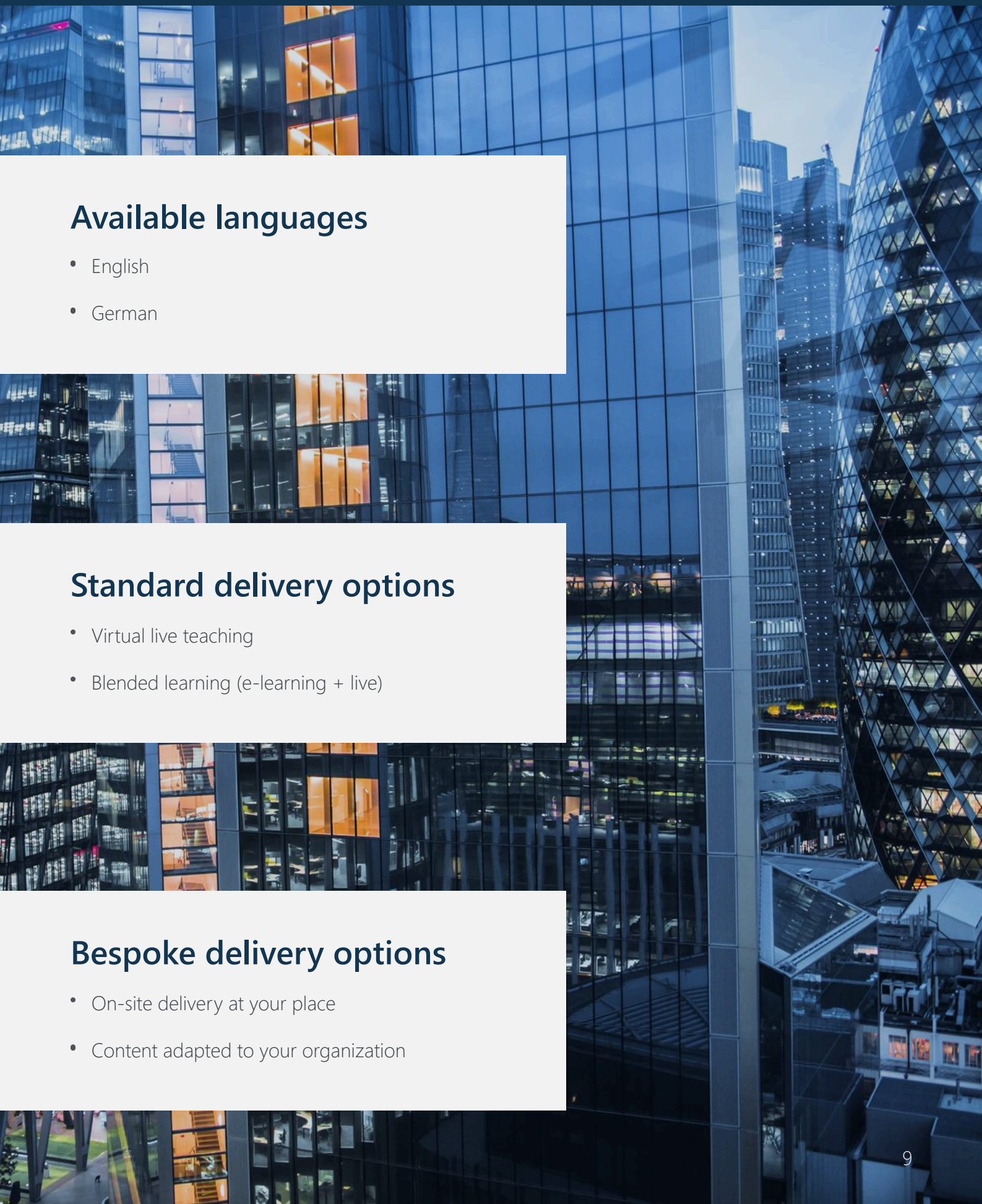
- Risk Management

Supporting (optional)

Helpful but not required to participate effectively

- System Framing

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