Halderstone

Training module

Auditing Information Security Risk Management

Evaluate asset–threat–vulnerability logic, risk treatment decisions, and traceability to controls and the Statement of Applicability

Does your audit go beyond checking risk registers to judging risk reasoning and treatment choices?

Overview

ISO/IEC 27001 expects risk assessment and risk treatment to drive the information security management system (ISMS), not to exist as standalone documentation. In practice, auditors often encounter generic asset lists, recycled threat catalogues, inconsistent scoring, and a Statement of Applicability (SoA) that cannot be traced back to specific risks and treatment decisions.

This standard-specific auditing module focuses on how to audit ISMS risk management where information security logic materially matters: asset–threat–vulnerability reasoning, treatment decision quality, and traceability from risks to chosen controls (including Annex A) and the SoA. It does not re-teach generic risk management methods or generic audit techniques; it applies an audit judgement lens to ISO/IEC 27001 risk management expectations.

Target audience

- Aspiring auditors who want to audit against ISO/IEC 27001 following best practices
- Practising ISO/IEC 27001 auditors who want to strengthen their audit knowledge, judgement, and effectiveness

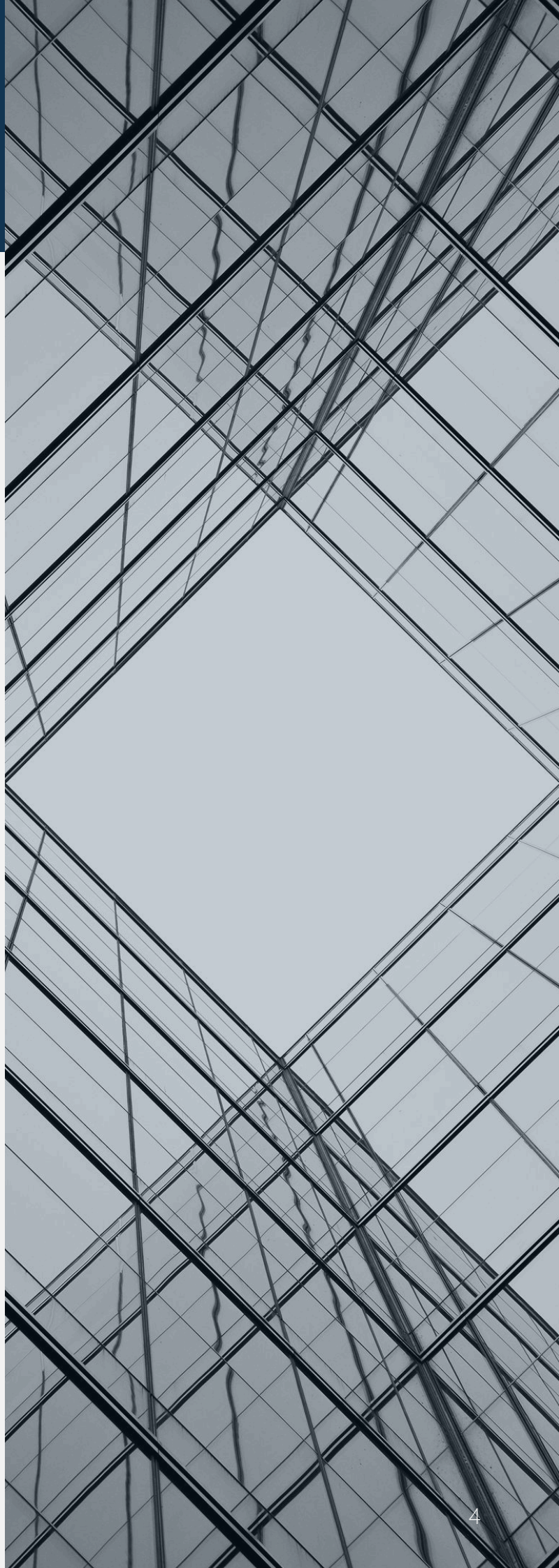
Is this module for you?

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

- aim to audit whether ISMS risk management actually drives security decisions.
- want to test asset–threat–vulnerability reasoning, not just risk register completeness.
- follow risks from context through treatment decisions to controls and the SoA.
- strengthen judgement on risk acceptance, prioritisation, and traceability.
- seek audit findings that reveal weak risk reasoning and systemic gaps.

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

- primarily want to design or improve risk assessment or treatment methods.
- expect generic risk management frameworks or scoring models.
- focus on facilitating workshops or producing risk documentation.
- are unwilling to challenge formally complete but weak risk rationales.



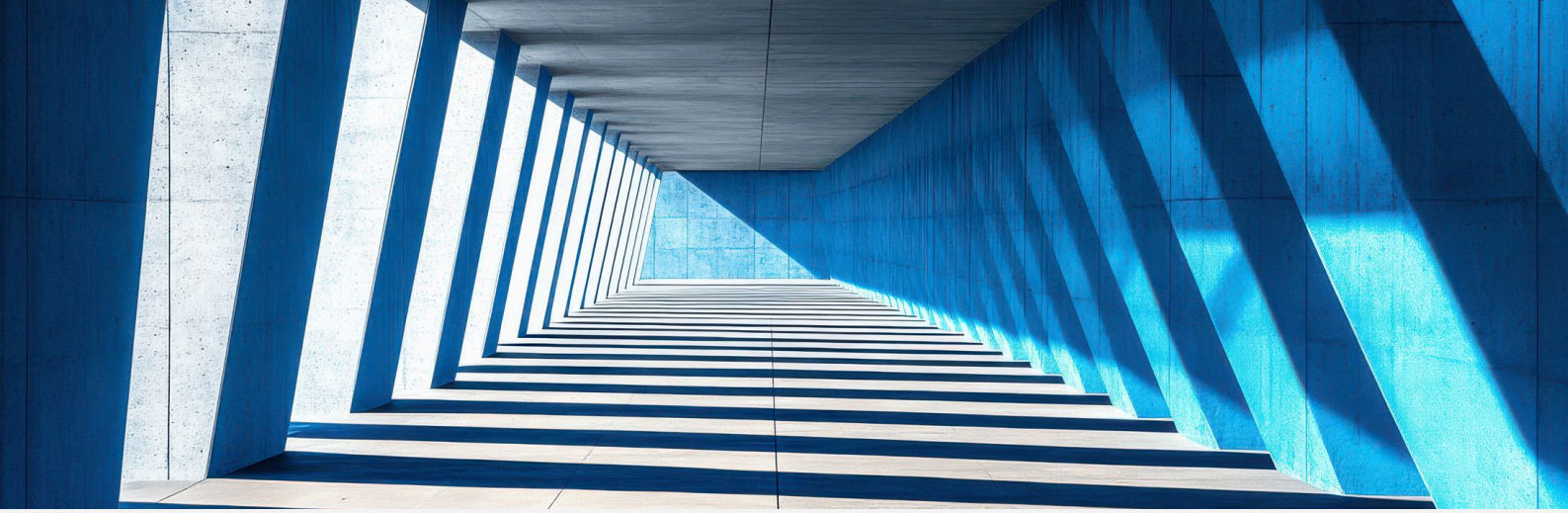
Learning outcomes

Key outcomes

- Evaluate whether asset–threat–vulnerability logic is credible and fit for decision-making in an ISMS
- Test internal consistency of risk assessment results using practical audit checks and targeted sampling heuristics
- Assess whether risk treatment decisions are explainable, authorised, and reviewable

Additional capabilities

- Verify end-to-end traceability from risks to controls and to the Statement of Applicability (SoA)
- Identify common systemic failure modes in ISO/IEC 27001 risk management and recognise early warning signals
- Build effective audit trails and evidence requests that connect risk documentation to operational control reality



Agenda

What makes ISMS risk management audit-ready

Assesses whether risk management functions as a decision and traceability system, not whether a risk register exists or “looks complete”.

Testing asset–threat–vulnerability reasoning

Tests plausibility of assets in scope, realistic threat paths, and meaningful vulnerabilities, including boundary and dependency risks from shared services, cloud, suppliers, and shadow assets.

Risk assessment outputs that hold under audit

Checks internal consistency across scope, assets, incidents, weaknesses, and results, and uses targeted sampling to expose weak or convenience-driven reasoning.

Judging risk treatment decisions

Evaluates whether treatment choices (reduce, retain, avoid, share) are coherent, authorised, and documented, and whether risk acceptance is credible in terms of authority, rationale, residual risk, and review triggers.

Traceability to controls and the Statement of Applicability (SoA)

Verifies traceability from risks to control selection and applicability rationale, and tests SoA completeness and indicators of “control theatre”.

Evidence trails from documentation to operation

Follows evidence from treatment decisions into projects, control implementation, and operational reality, and identifies disconnects between plans, controls, and actual operation.

Case-based audit simulation

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

Included materials

Learning materials

- Slide deck
- Participant workbook

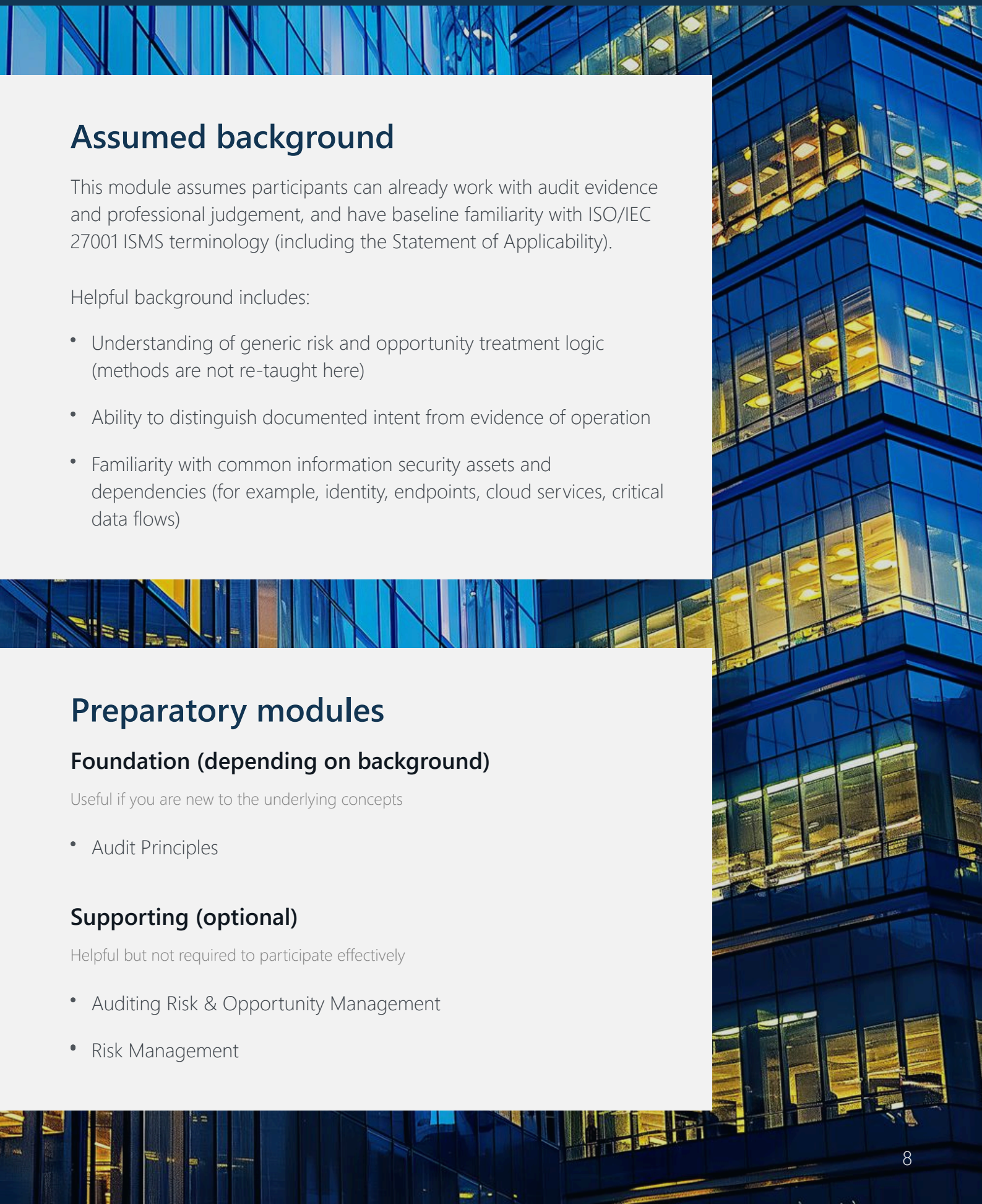
Templates & tools

- 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 already work with audit evidence and professional judgement, and have baseline familiarity with ISO/IEC 27001 ISMS terminology (including the Statement of Applicability).

Helpful background includes:

- Understanding of generic risk and opportunity treatment logic (methods are not re-taught here)
- Ability to distinguish documented intent from evidence of operation
- Familiarity with common information security assets and dependencies (for example, identity, endpoints, cloud services, critical data flows)

Preparatory modules

Foundation (depending on background)

Useful if you are new to the underlying concepts

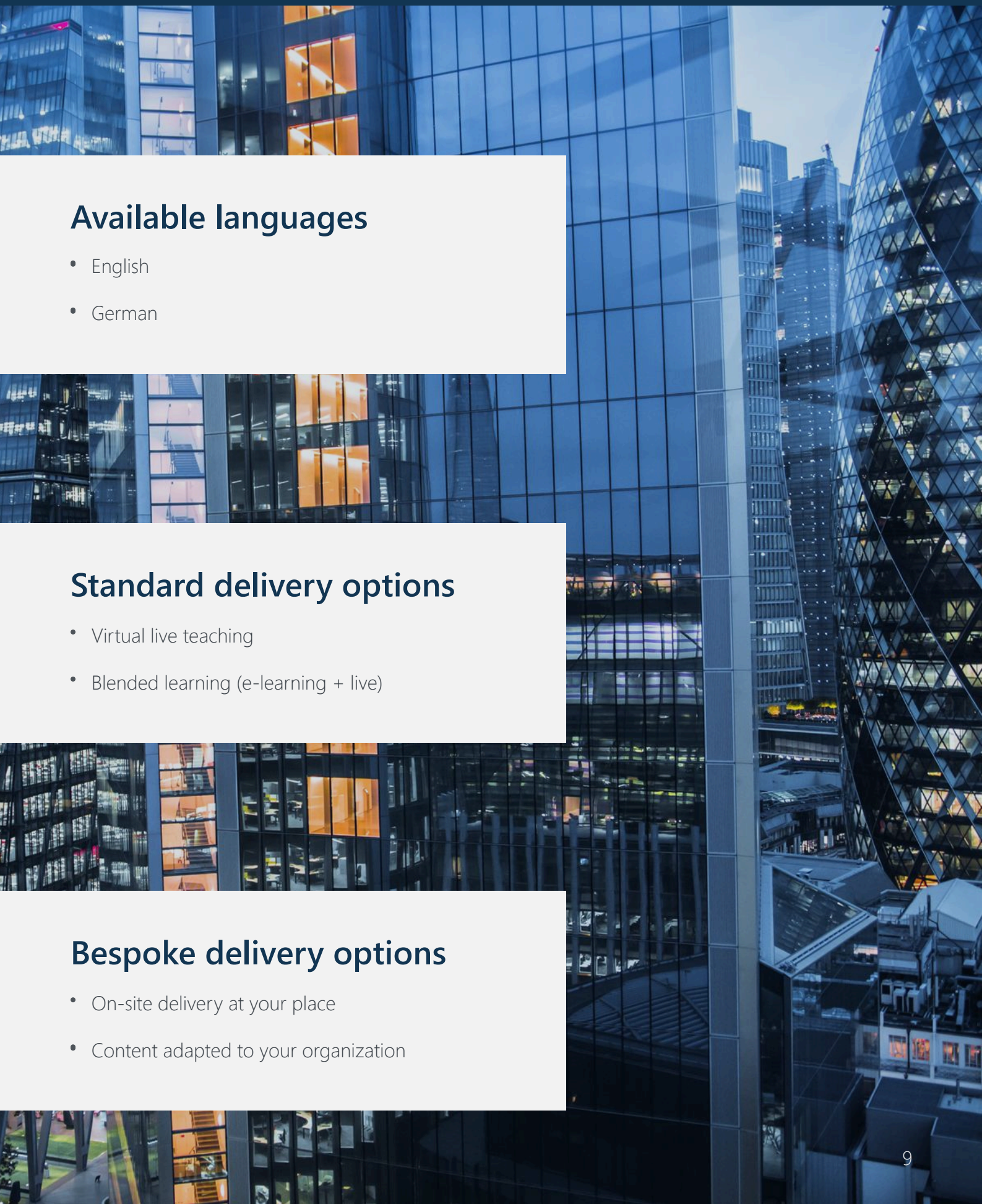
- Audit Principles

Supporting (optional)

Helpful but not required to participate effectively

- Auditing Risk & Opportunity Management
- 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