Halderstone

Training module

Auditing Information Security Controls

Evaluate control applicability, implementation evidence & common failure patterns across ISO/IEC 27001 Annex A control themes

Does your audit move beyond control-checklist auditing to traceable assurance about how security actually operates?

Overview

Many organisations can describe their Annex A controls but struggle to demonstrate why each control applies, how it is implemented, and whether it consistently operates across sites, teams, and suppliers. The result is an audit pattern of "policy evidence" without operational proof, and repeated findings that are symptoms of deeper system weaknesses.

This standard-specific auditing module focuses on Annex A control applicability and rationale (via the Statement of Applicability), evidence expectations by control theme, and typical systemic ISMS failures. It assumes information security fundamentals are already covered elsewhere and does not re-teach generic audit craft; it applies audit judgement to ISO/IEC 27001's control set for internal auditors and third-party auditors (e.g., certification bodies or independent assurance providers).

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

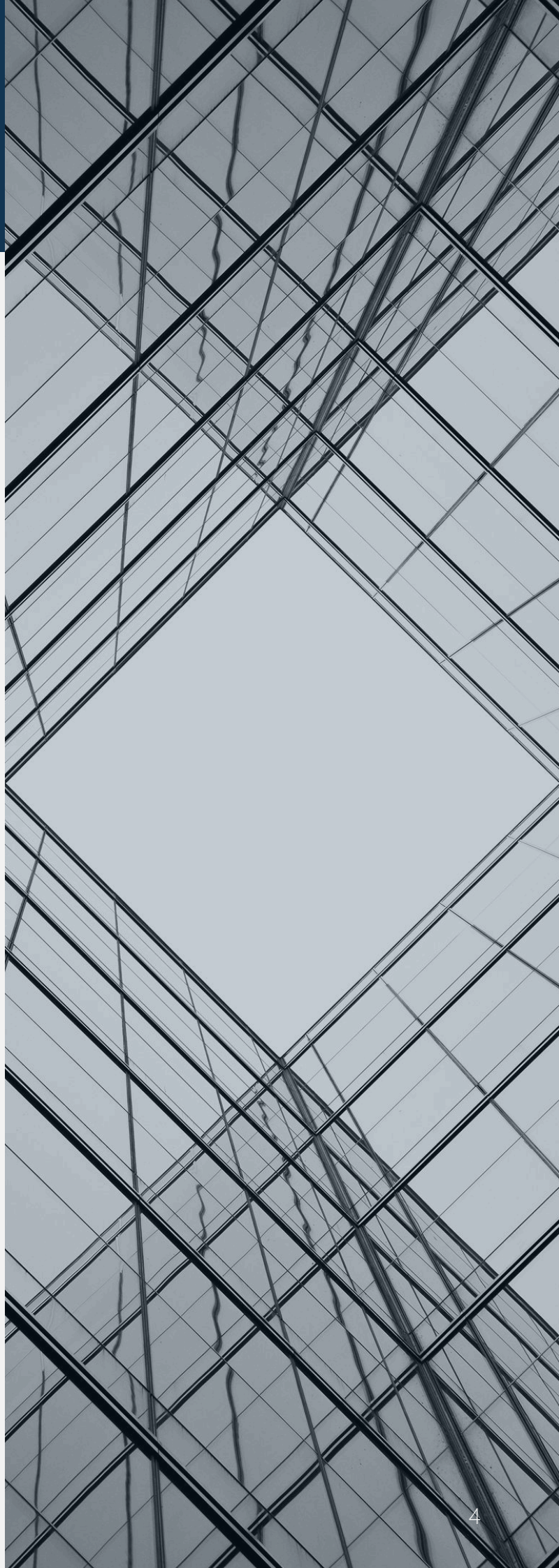
Is this module for you?

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

- aim to audit whether Annex A controls operate in practice, not just on paper.
- want to test control applicability and rationale via the Statement of Applicability.
- follow control claims end-to-end across policy, process, configuration, and records.
- strengthen evidence-based judgement across different control themes.
- seek audit findings that highlight systemic weaknesses, not checklist gaps.

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

- primarily want to design, implement, or improve security controls.
- expect control theory or technical implementation guidance.
- prefer audits limited to documentation or policy consistency checks.
- avoid challenging formally correct but weak control claims.



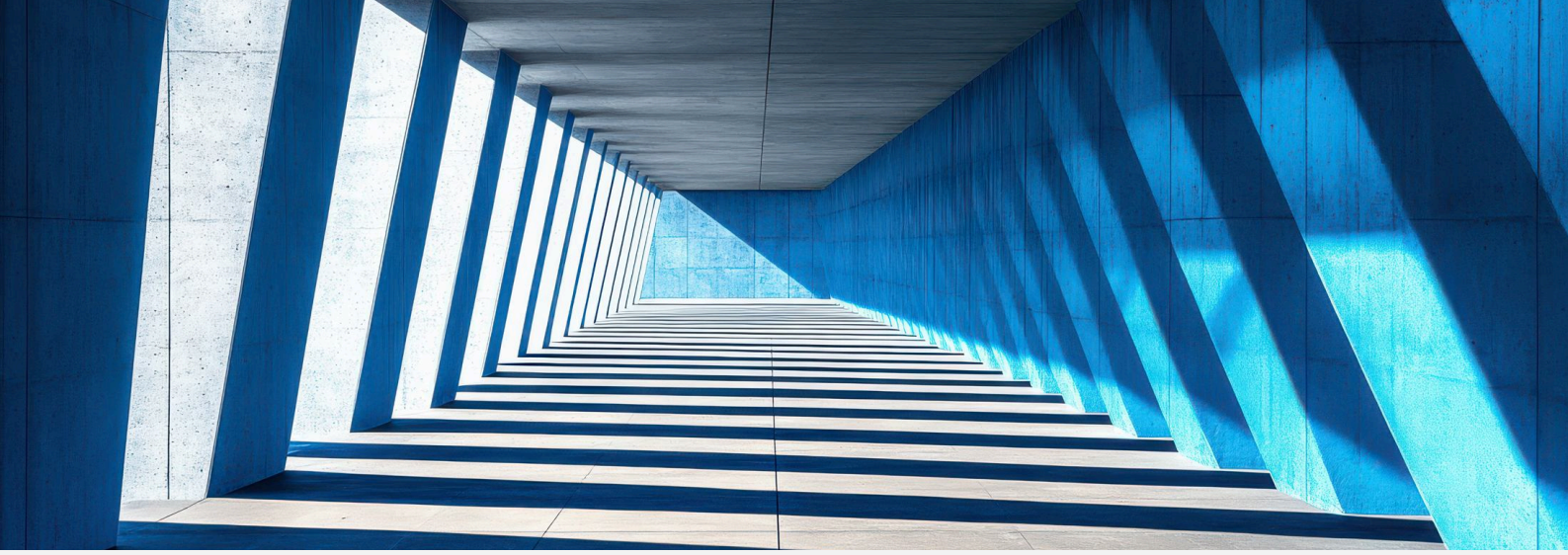
Learning outcomes

Key outcomes

- Challenge Annex A control applicability decisions using consistent tests for rationale quality and scope fit
- Distinguish control statement , implementation , and operation evidence, and identify which is missing
- Identify expected evidence types by Annex A control theme

Additional capabilities

- Build practical, traceable audit trails from control intent to operational proof across functions and suppliers
- Recognise recurring systemic ISMS failure patterns behind repeated control weaknesses
- Apply Annex A auditing judgement in both internal audits and third-party assurance contexts without reverting to checklist auditing



Agenda

Annex A in an audit context

Clarifies how Annex A controls are used to test assurance and operation, not as a checklist for document presence.

Control applicability and rationale

Tests the credibility of SoA inclusion, exclusion, and tailoring decisions, and how weak rationales surface as evidence gaps.

Evidence expectations by control theme (ISO/IEC 27001:2022)

Covers organisational controls (governance, ownership, routines), people controls (competence, JML, behavioural enforcement), and technological controls (configuration, access, logging, change), with focus on high-leverage audit signals.

Physical controls in real environments

Assesses site realities, shared spaces, visitor handling, and asset movement, including where physical and technical controls interact or fail.

Tracing one control end-to-end

Follows a single control claim through policy, process, configuration, and records, including interfaces with IT, HR, Facilities, suppliers, and shared platforms.

Paper control sets and drift patterns

Identifies declared controls without operational ownership, fragmented implementation across sites or tools, and risk-treatment drift where SoA and reality diverge over time.

Case-based audit simulation

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

Included materials

Learning materials

- Slide deck
- Participant workbook

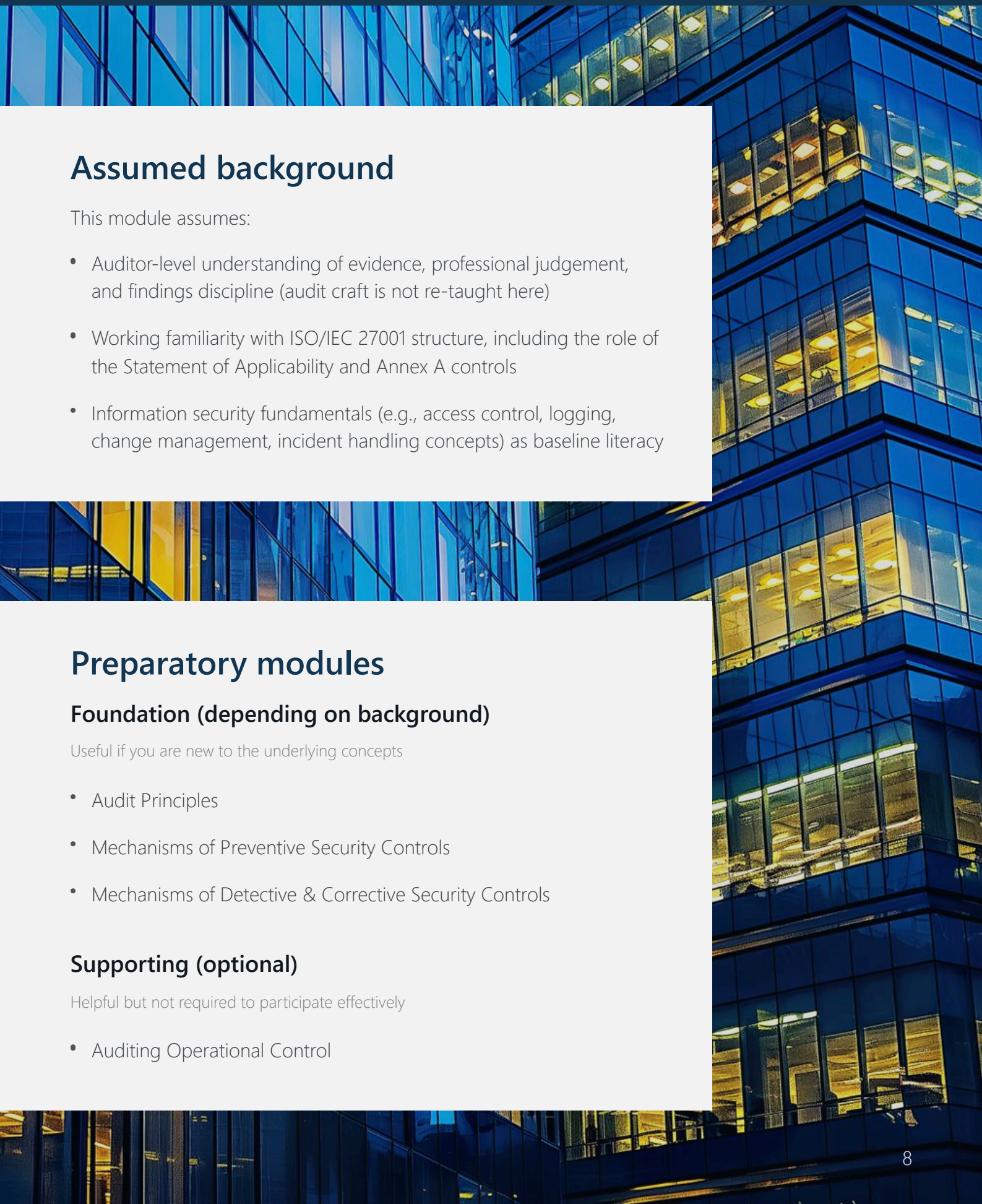
Templates & tools

- 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:

- Auditor-level understanding of evidence, professional judgement, and findings discipline (audit craft is not re-taught here)
- Working familiarity with ISO/IEC 27001 structure, including the role of the Statement of Applicability and Annex A controls
- Information security fundamentals (e.g., access control, logging, change management, incident handling concepts) as baseline literacy

Preparatory modules

Foundation (depending on background)

Useful if you are new to the underlying concepts

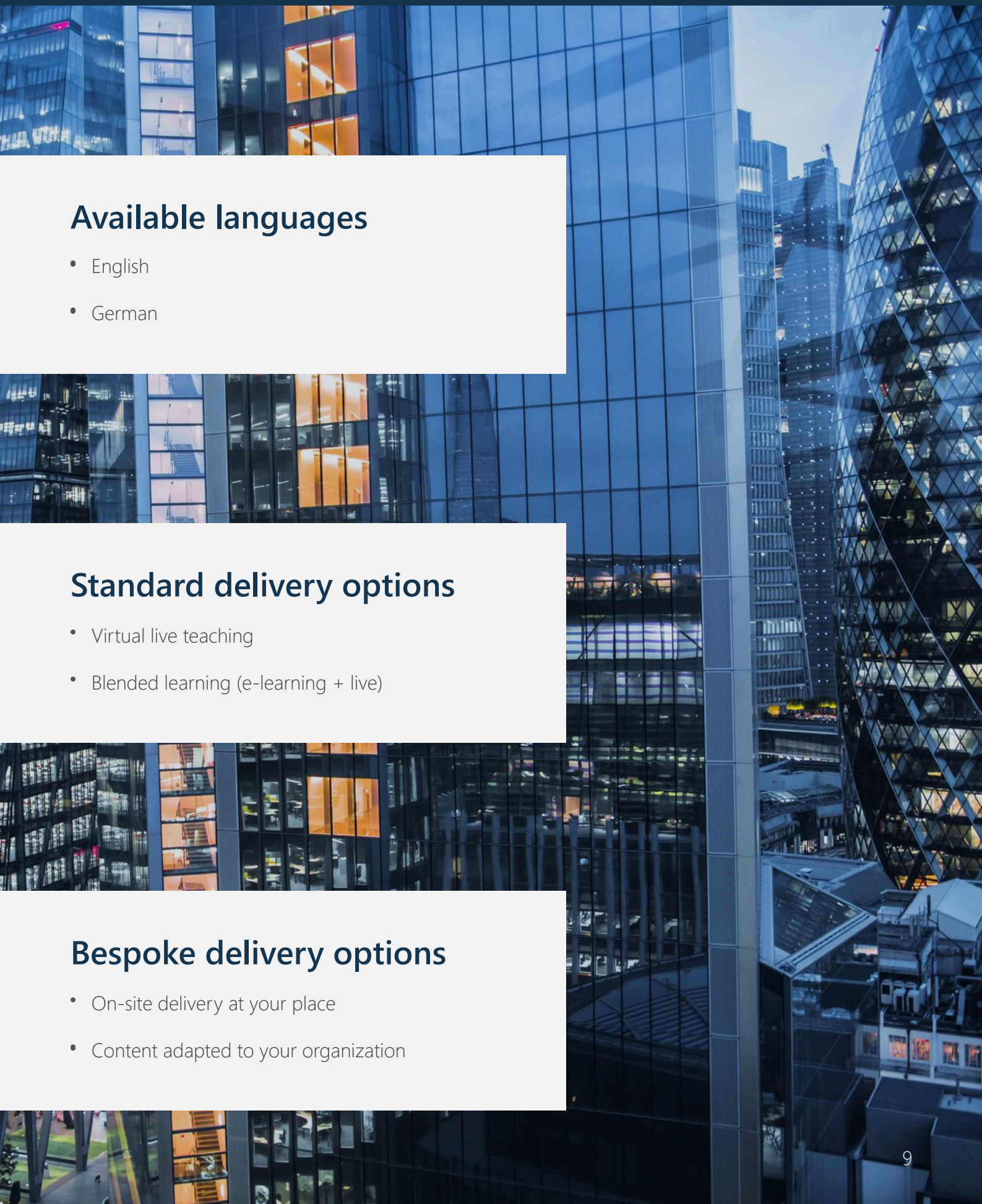
- Audit Principles
- Mechanisms of Preventive Security Controls
- Mechanisms of Detective & Corrective Security Controls

Supporting (optional)

Helpful but not required to participate effectively

- Auditing Operational Control

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