Halderstone

Training module

Operational Control in Information Security

Plan, implement & operate information security controls consistently in day-to-day activities in line with ISO/IEC 27001

Do your selected security controls drift from design to day-to-day operations?

Overview

Controls chosen in risk treatment and planning can lose effectiveness when implemented without clear roles, criteria and change management.

In this module, participants learn to translate risk treatment decisions into operational routines, define interfaces and handovers between control owners and operations, and integrate security-related change into business change processes. The module covers specifying what “operated and maintained” means for different control types, handling exceptions and compensating measures, identifying failure modes and documenting minimal evidence. It builds on risk, scope and preventive control foundations but does not re-teach those topics.

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)

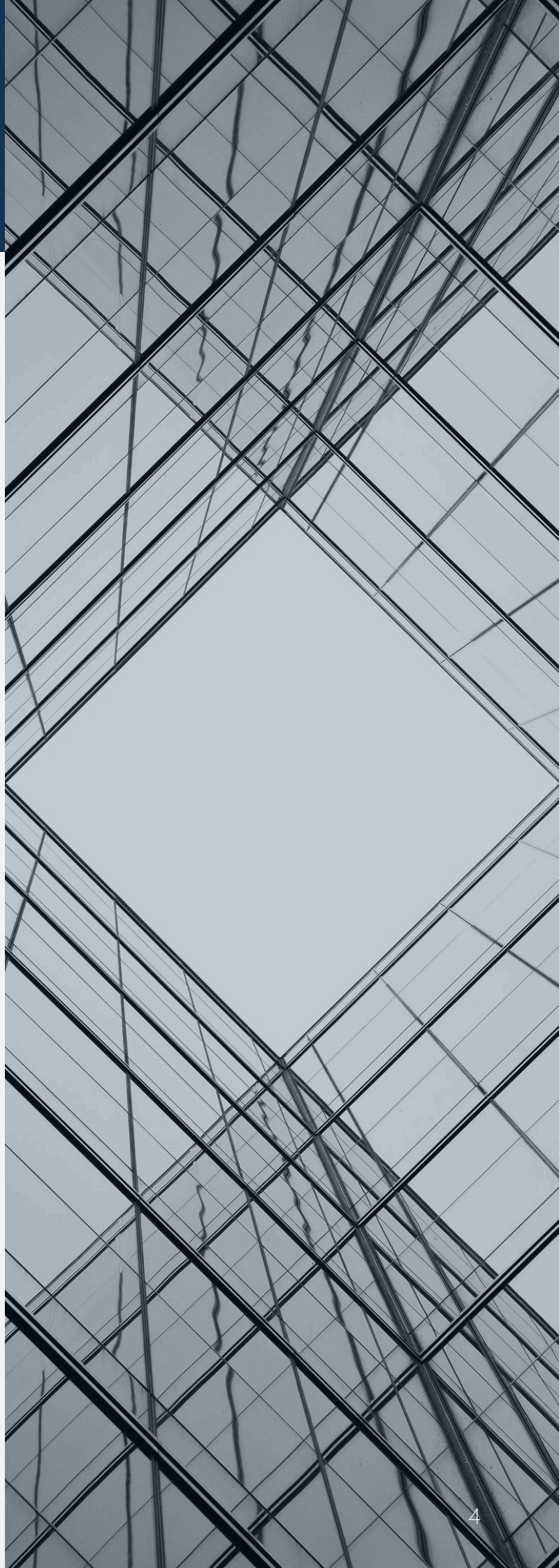
Is this module for you?

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

- run or oversee day-to-day ISMS operations and control execution.
- struggle with controls that exist on paper but drift in practice.
- need operational routines that keep security decisions traceable over time.
- manage control ownership, change, or handovers across teams or suppliers.
- want ISMS controls to hold up under real delivery pressure and incidents.

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

- are looking for control design, selection, or Annex A interpretation.
- expect technical hardening, configuration, or tooling guidance.
- want risk assessment, SoA design, or control objectives explained from scratch.
- already operate stable, well-owned, and consistently executed ISMS controls.



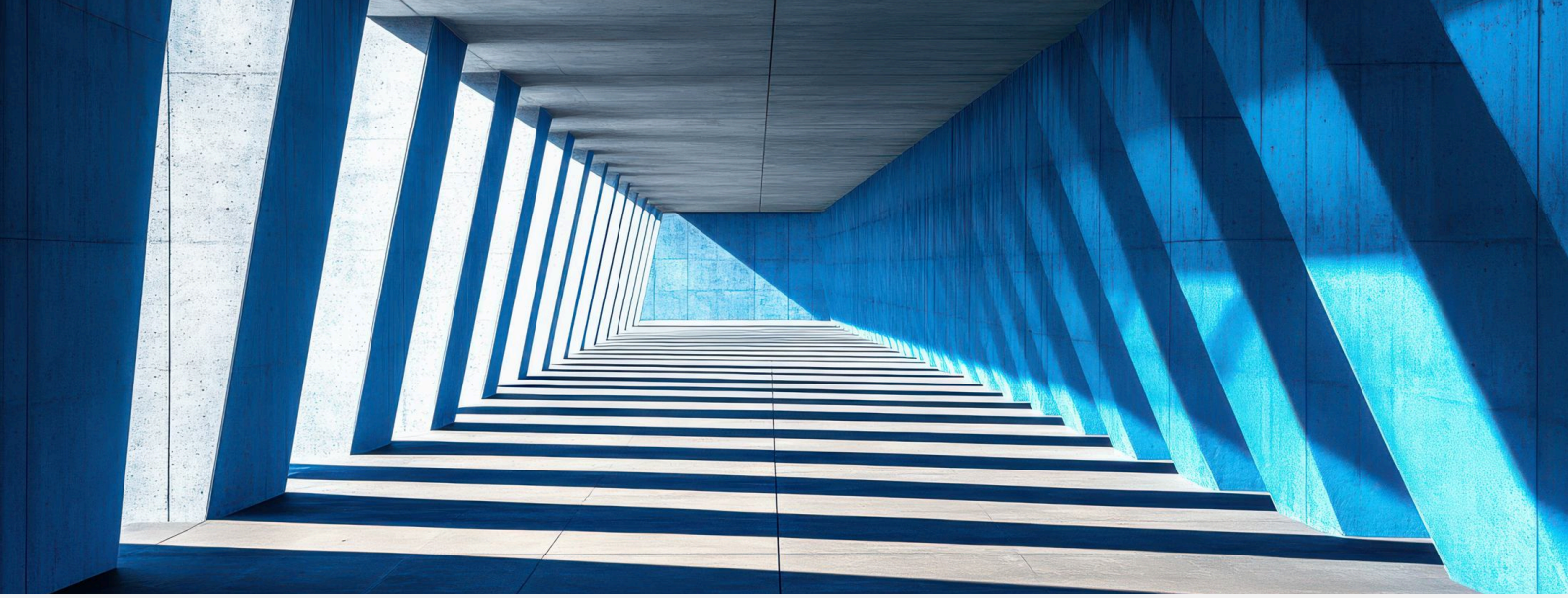
Learning outcomes

Key outcomes

- Translate risk treatment decisions into operational control routines with clear tasks and timing
- Define interfaces and handovers between control owners, IT operations and service management
- Integrate security-related change into general change management processes

Additional capabilities

- Specify what “operated and maintained” means for different control types and evidence needed
- Handle exceptions and compensating measures without undermining control intent
- Identify control failure modes and produce minimal evidence for governance and assurance



Agenda

What operational control means in ISO/IEC 27001 practice

How operational control translates ISMS intent into repeatable execution and where it typically breaks down through drift, informal exceptions, unclear ownership, or silent change

Planning and controlling ISMS operations

How selected controls and requirements are translated into concrete operational routines with defined owners, triggers, and frequencies without re-scoping the ISMS

Controlled change in information security operations

How security-relevant changes are identified, assessed, approved, and integrated into existing change processes without creating parallel security workflows

Operating Annex A controls without re-teaching the controls

How Annex A controls are practically "operated and maintained" through routines, checks, and minimal traceable evidence rather than re-documentation

Outsourced and supplier-operated controls

How supplier-operated controls are made auditable and manageable through clear interfaces, responsibilities, and operational verification points

Operational deviations, incidents, and corrective follow-up

How operational deviations and incidents are distinguished, escalated, contained, and fed into corrective action without blurring responsibilities

Case-based workshop

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

Included materials

Learning materials

- Slide deck
- Participant workbook

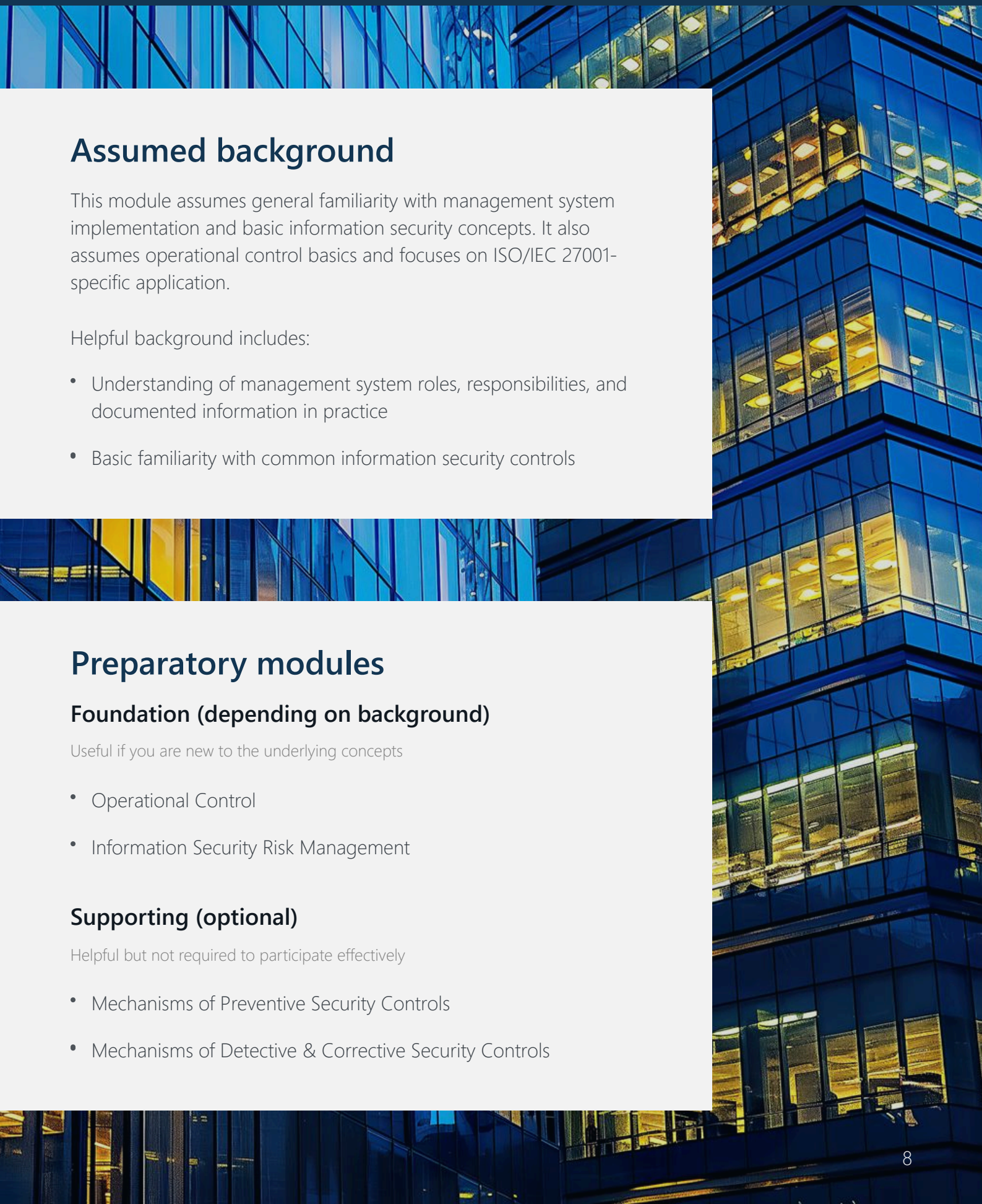
Templates & tools

- ISMS operational control map
- Operational routine specification template
- Security-relevant change impact checklist
- Exception and compensating measure log template
- Supplier control interface worksheet
- Minimum operational evidence set guide

Confirmation

- Confirmation of participation

Preparation guidance



Assumed background

This module assumes general familiarity with management system implementation and basic information security concepts. It also assumes operational control basics and focuses on ISO/IEC 27001-specific application.

Helpful background includes:

- Understanding of management system roles, responsibilities, and documented information in practice
- Basic familiarity with common information security controls

Preparatory modules

Foundation (depending on background)

Useful if you are new to the underlying concepts

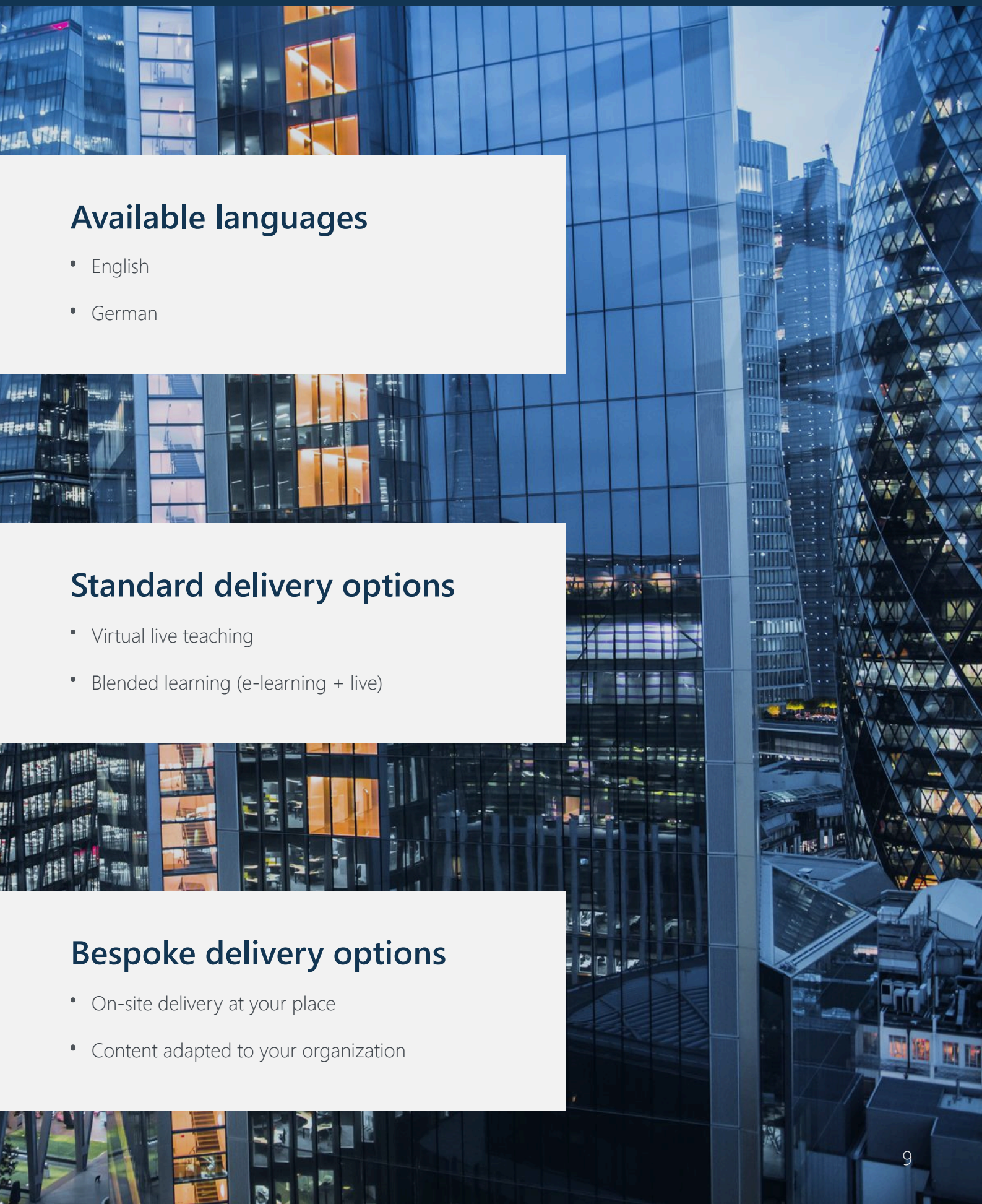
- Operational Control
- Information Security Risk Management

Supporting (optional)

Helpful but not required to participate effectively

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

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