Halderstone

Training module

ISMS Scope & Statement of Applicability

Define clear ISO/IEC 27001 ISMS scope and boundaries and maintain a defensible Statement of Applicability (SoA)

Is your information security scope vague, leaving boundaries and applicability decisions undefended?

Overview

Weak scope definitions and poorly justified applicability decisions undermine the credibility of an Information Security Management System.

This training module guides participants through drafting a defensible scope statement, identifying interfaces and dependencies, and connecting risk treatment outputs to control applicability. It explains how to structure a Statement of Applicability with rationale and implementation status and how to maintain the scope and SoA over time. Operational implementation differences are highlighted to avoid "documented but not done" gaps.

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)

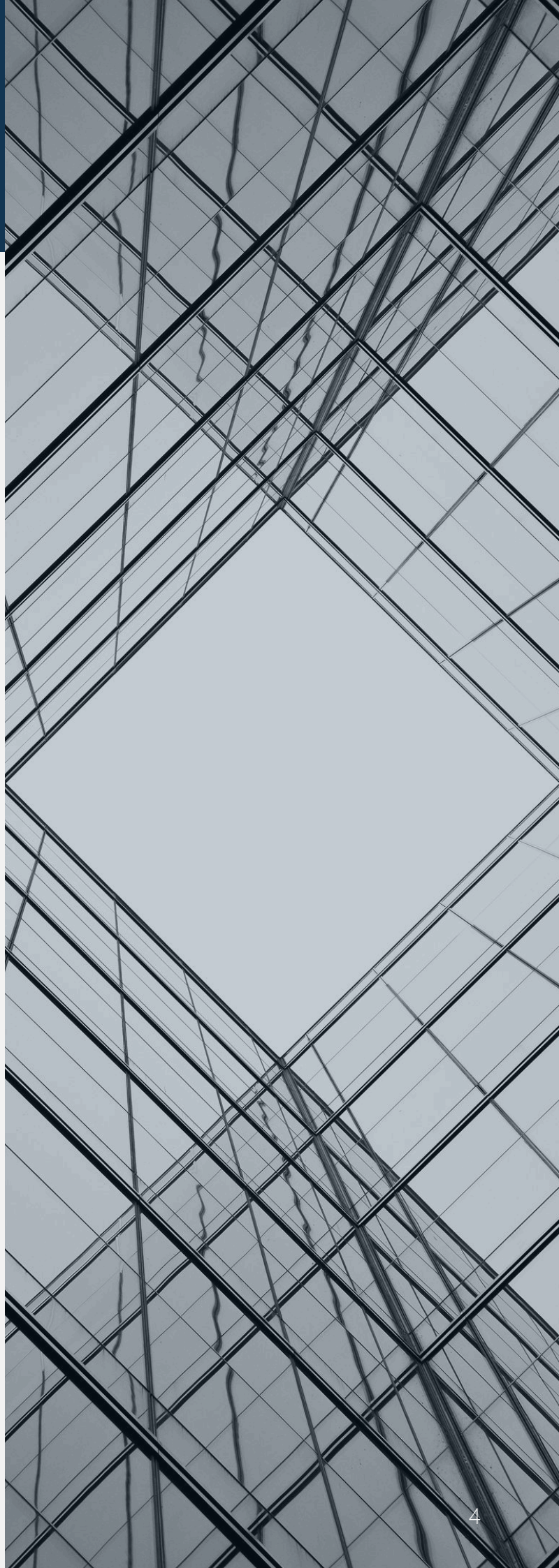
Is this module for you?

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

- are responsible for defining, maintaining, or defending an ISMS scope.
- struggle with vague, copied, or unstable Statements of Applicability.
- need scope and SoA decisions that are defensible in audits and incidents.
- must align ISMS boundaries with real organisational, technical, or supplier boundaries.
- want scope and applicability decisions that remain valid as the organisation changes.

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

- are only looking for a generic overview of ISO/IEC 27001.
- expect a risk assessment or control implementation course.
- want a template-only walkthrough without decision logic.
- already operate a clear, stable, and well-defended ISMS scope and SoA.



Learning outcomes

Key outcomes

- Draft an ISO/IEC 27001-aligned scope statement with clear boundaries and rationale
- Identify interfaces, dependencies and assumptions that influence the scope
- Use risk treatment outputs to decide which controls are applicable and justify those decisions

Additional capabilities

- Structure a Statement of Applicability with clear rationale and implementation status
- Distinguish between documented applicability and operational implementation to spot gaps
- Define maintenance rules and triggers to keep the scope and SoA current over time

Agenda

What ISO/IEC 27001 expects from scope and boundaries

How ISMS scoping is understood as credible coverage rather than formal exclusion, and why organisational charts, locations, or tooling alone create false assurance

Applying scoping logic to the ISMS

How organisational context, services, and delivery models translate into ISMS boundaries, including internal interfaces, shared platforms, and external providers

Building an operationally usable scope statement

How a scope statement clearly communicates coverage, exclusions, and interfaces, and how multi-site, multi-service, and group structures are handled without overpromising

From risk treatment decisions to control applicability

How risk treatment outputs are used as inputs to control applicability decisions, and what makes "applicable" and "not applicable" positions defensible in practice

Statement of Applicability: structure and traceability

How the SoA functions as a decision record covering rationale, implementation status, and references, and how it remains consistent with policies, controls, and evidence reality

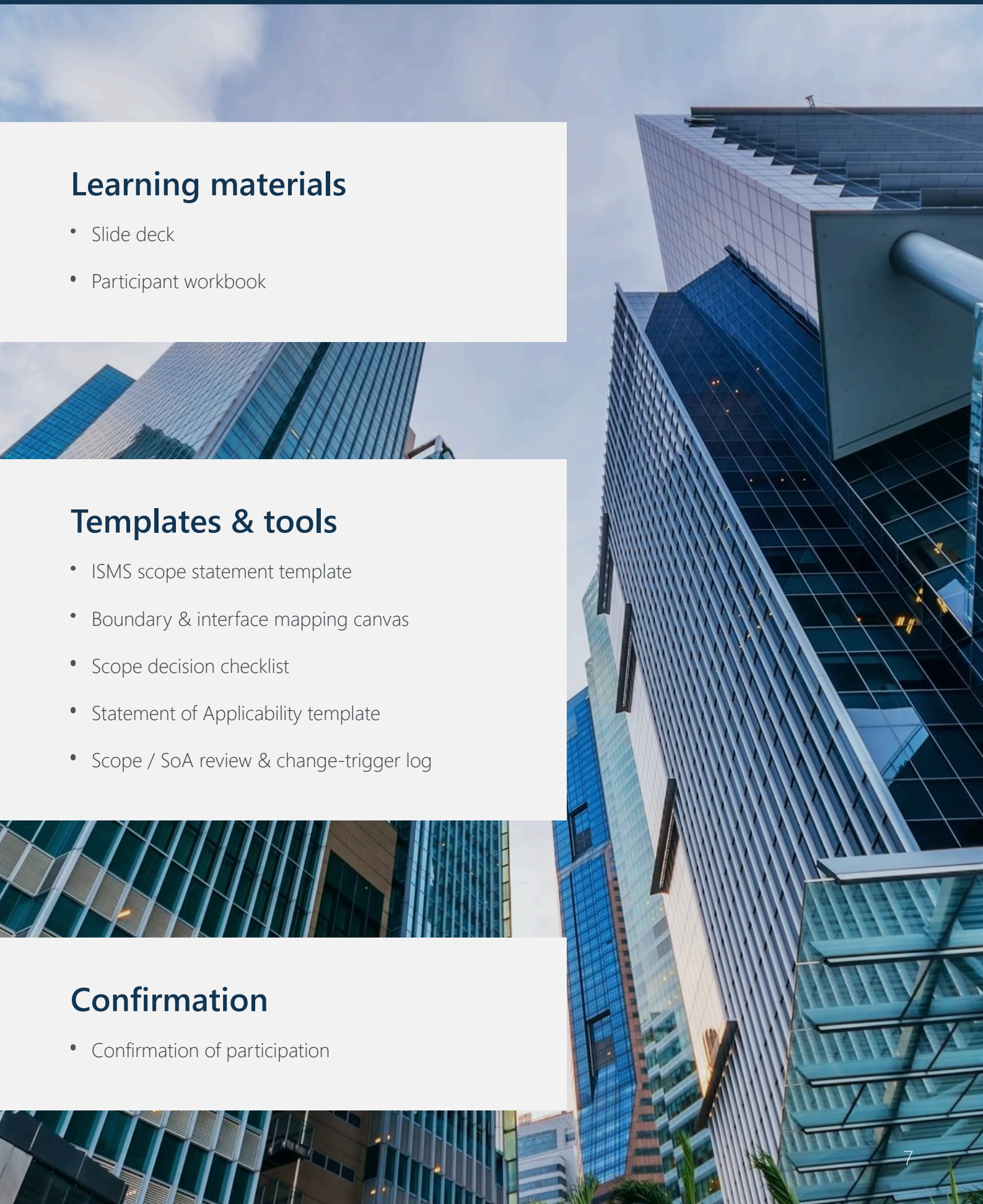
Maintaining scope and SoA over time

How organisational change, supplier shifts, platform changes, and incidents trigger scope updates, and how ownership and review cadence integrate into management routines

Case-based workshop

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

Included materials



Learning materials

- Slide deck
- Participant workbook

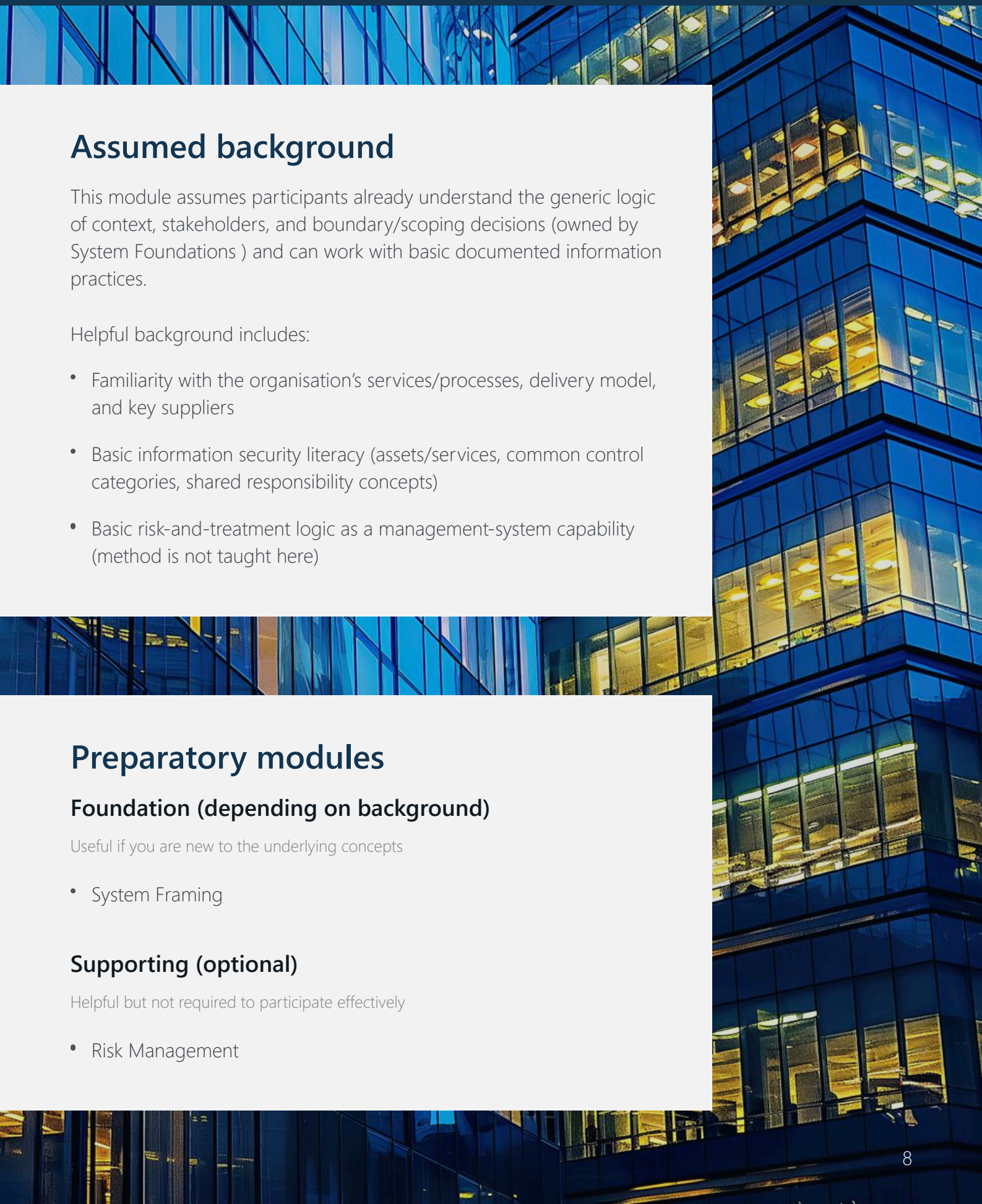
Templates & tools

- ISMS scope statement template
- Boundary & interface mapping canvas
- Scope decision checklist
- Statement of Applicability template
- Scope / SoA review & change-trigger log

Confirmation

- Confirmation of participation

Preparation guidance



Assumed background

This module assumes participants already understand the generic logic of context, stakeholders, and boundary/scoping decisions (owned by System Foundations) and can work with basic documented information practices.

Helpful background includes:

- Familiarity with the organisation's services/processes, delivery model, and key suppliers
- Basic information security literacy (assets/services, common control categories, shared responsibility concepts)
- Basic risk-and-treatment logic as a management-system capability (method is not taught here)

Preparatory modules

Foundation (depending on background)

Useful if you are new to the underlying concepts

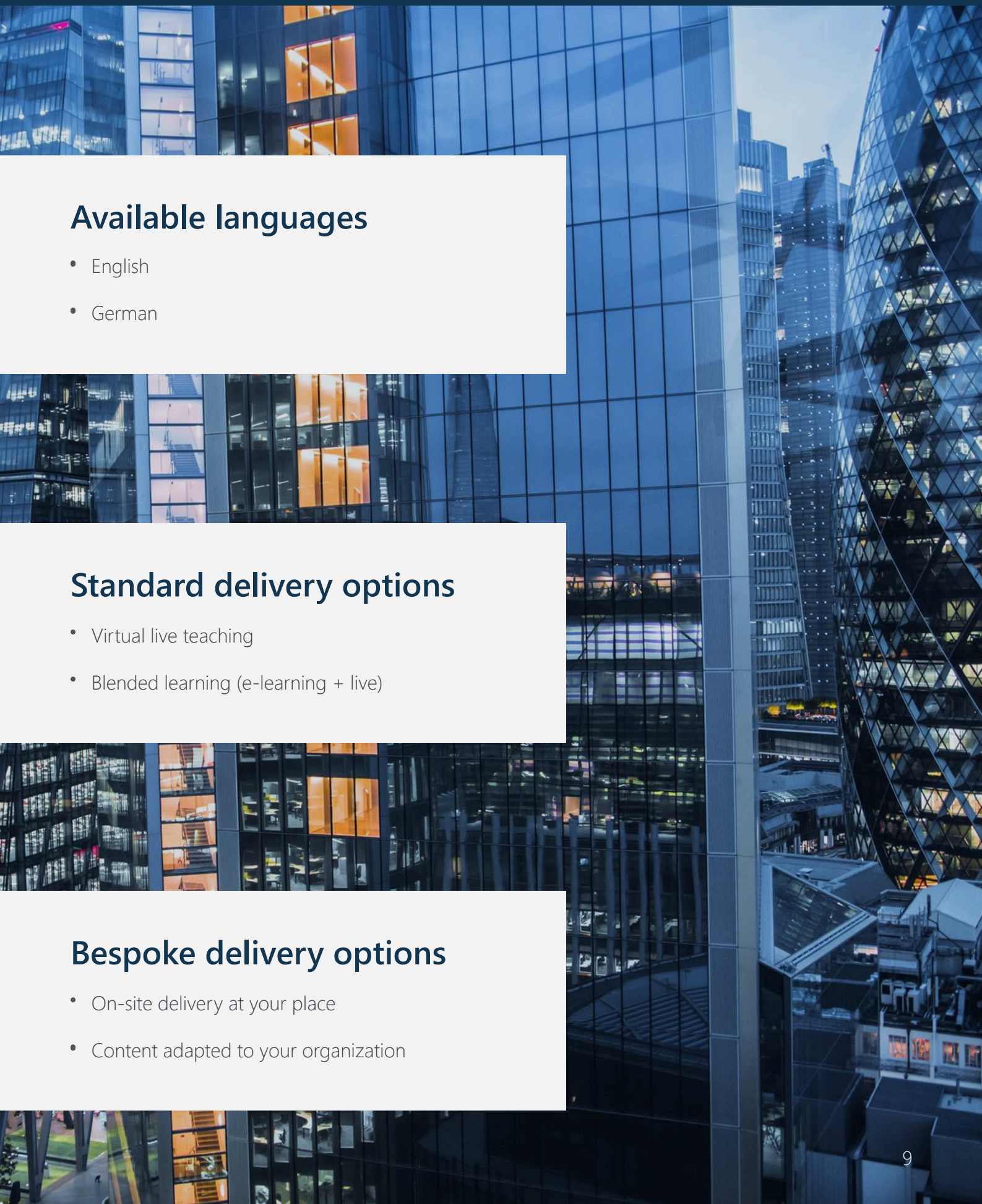
- System Framing

Supporting (optional)

Helpful but not required to participate effectively

- 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