Halderstone

Training module

Mechanisms of Information Security Controls

Understand how preventive, detective and corrective controls work together across access, cryptography, monitoring, incident response, backup and recovery

Can you explain how information security controls work together?

Overview

This module explains how information security controls work together to prevent incidents, detect suspicious activity, limit impact and restore secure operation.

Participants learn how access management, cryptography, secure configuration, logging, monitoring, incident response, backup and recovery mechanisms connect within an integrated control architecture. The module clarifies the purpose, dependencies and limits of preventive, detective and corrective safeguards, and shows how they support confidentiality, integrity and availability.

Concepts are anchored in ISO/IEC 27001 Annex A. The focus is on structural understanding and decision-ready control logic rather than operational tool configuration or a clause-by-clause walkthrough.

Target audience

- Information security managers and ISMS implementers
- CIOs, CTOs, CISOs, and other technology executives
- IT service, platform, and application owners
- Compliance, risk, and governance professionals (ISO/IEC 27001)
- Security consultants and client-facing advisors
- Product, engineering, and operations leads

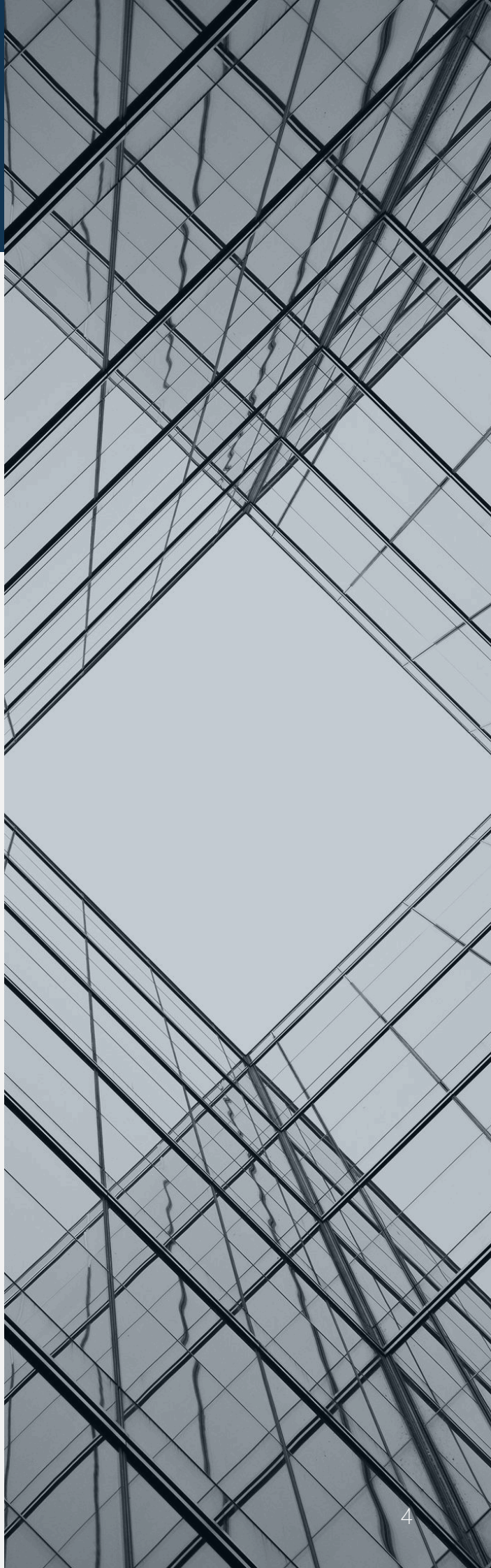
Is this module for you?

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

- want to understand how preventive, detective and corrective controls reduce risk together.
- need clarity on the intent, dependencies and limits of ISO/IEC 27001 Annex A safeguards.
- implement, assess or audit access, cryptography, configuration, monitoring, incident response or recovery controls.
- need a shared control vocabulary across security, IT, risk, governance and audit roles.
- want to judge whether information security controls are coherent, meaningful and proportionate in practice.

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

- expect hands-on tool configuration, SIEM setup, hardening labs or log analysis exercises.
- want a clause-by-clause walkthrough of ISO/IEC 27001 Annex A.
- are looking for a detailed incident response or crisis management playbook.
- already design and assess integrated information security control architectures confidently.



Learning outcomes

Key outcomes

- Explain how preventive, detective and corrective controls work together as an integrated information security control system
- Describe access, cryptography, configuration, logging, monitoring, incident response, backup and recovery as complementary safeguards
- Relate information security control mechanisms to ISO/IEC 27001 Annex A and to confidentiality, integrity and availability

Additional capabilities

- Identify dependency gaps, visibility gaps and common failure points across information security control chains
- Assess whether detection, response and recovery mechanisms meaningfully complement preventive safeguards
- Communicate control logic and control limitations across technical, governance, risk and audit roles
- Select proportionate questions and evidence targets when reviewing information security controls

Agenda

How information security controls work as a system

How preventive, detective and corrective controls reduce exposure, create visibility, limit impact and restore secure operation as connected control functions

Preventive control logic and exposure reduction

How access management, secure configuration, segmentation and protective design reduce attack opportunities before harm occurs

Identity and access management fundamentals

How authentication, authorisation, session control, least privilege and segregation of duties support secure access across users, administrators and services

Cryptography and information protection

How cryptographic mechanisms, key management, classification, handling rules and data loss prevention protect confidentiality, integrity and authenticity

Logging foundations and observability

How to determine which events must be logged, preserve identity, time and context, and avoid gaps that undermine detectability

Monitoring, alerting and detection approaches

How logged events become actionable signals, how detection approaches differ, and how to manage noise, latency, escalation and incomplete visibility

Incident response and containment

How to structure incident response with clear escalation, authority, containment decisions, evidence handling and learning after incidents

Backup, continuity and recovery

How backup, restore, continuity and recovery measures support secure operation, and how BIA, RTO and RPO concepts shape recovery expectations

Case-based control-chain workshop

Applying the learned concepts to a realistic scenario that connects prevention, detection, response and recovery decisions

Included materials

Learning materials

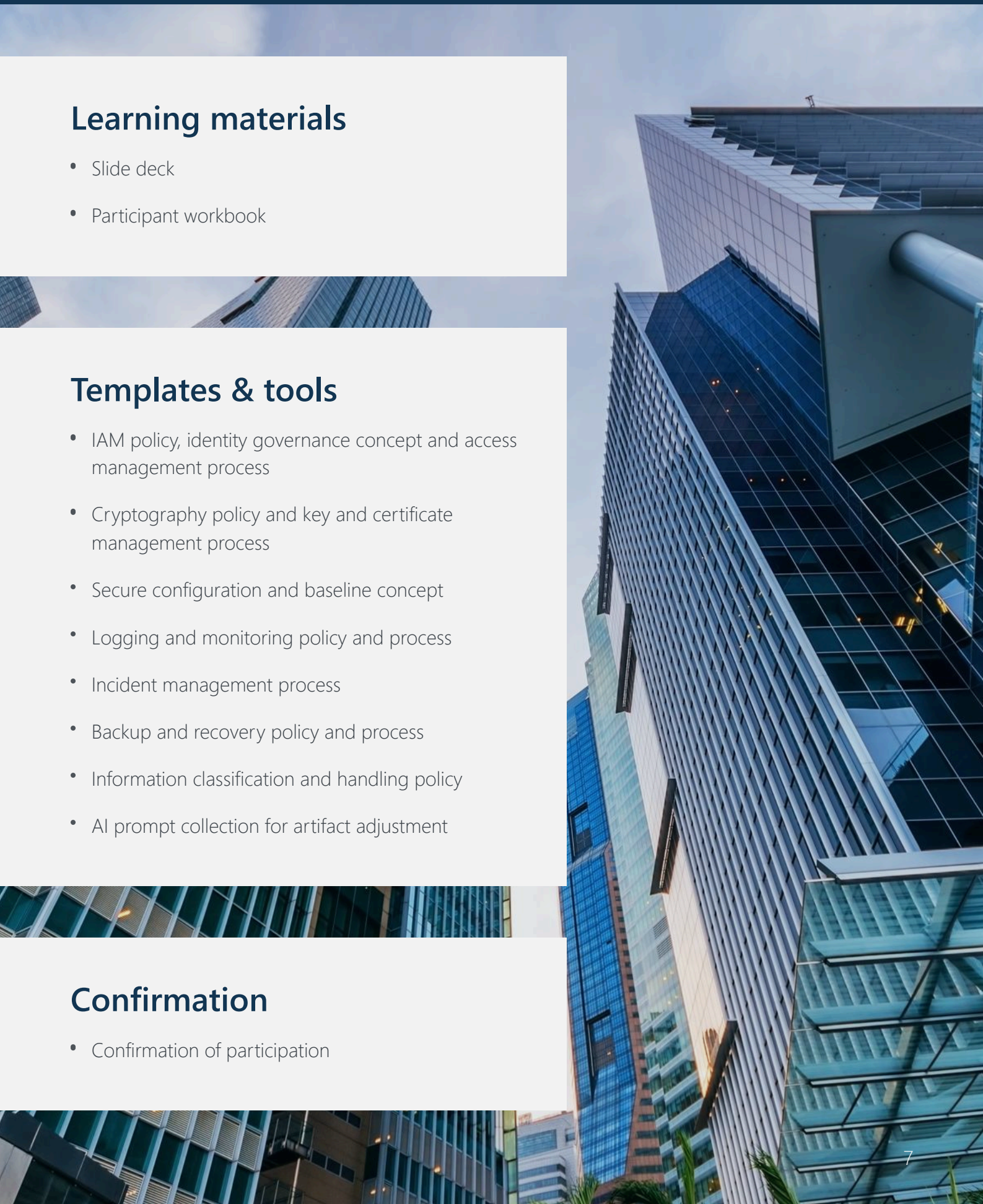
- Slide deck
- Participant workbook

Templates & tools

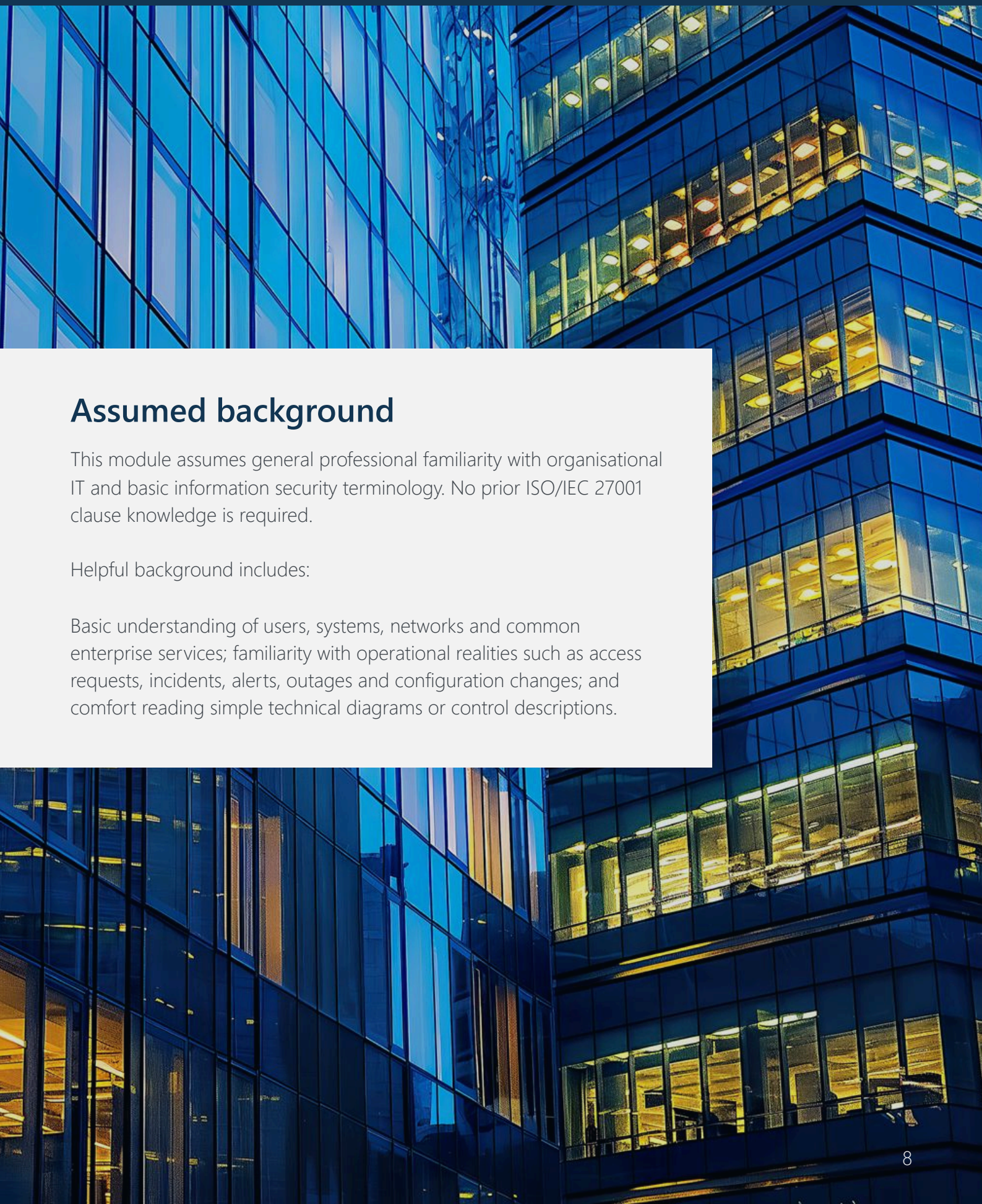
- IAM policy, identity governance concept and access management process
- Cryptography policy and key and certificate management process
- Secure configuration and baseline concept
- Logging and monitoring policy and process
- Incident management process
- Backup and recovery policy and process
- Information classification and handling policy
- AI prompt collection for artifact adjustment

Confirmation

- Confirmation of participation



Preparation guidance



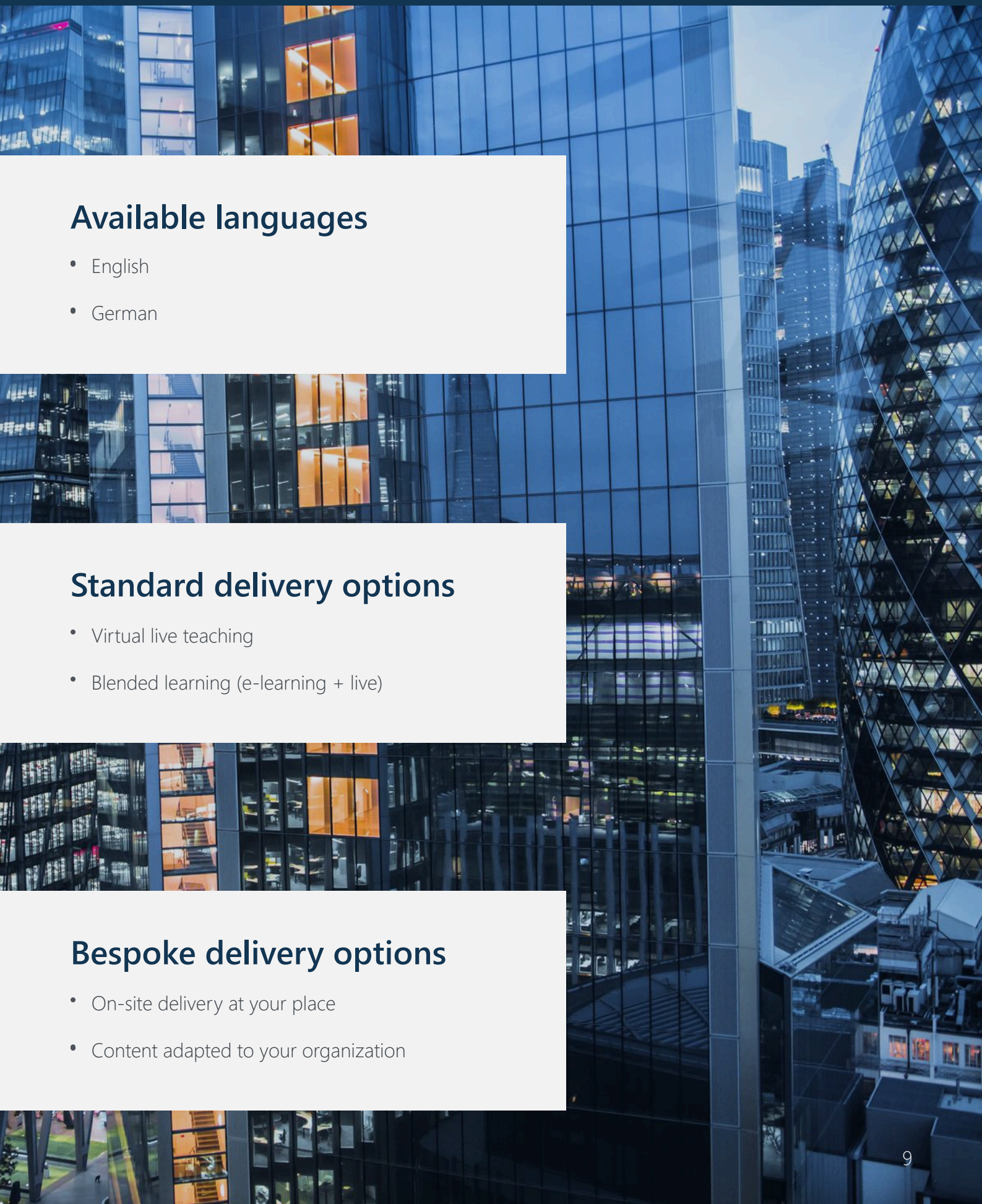
Assumed background

This module assumes general professional familiarity with organisational IT and basic information security terminology. No prior ISO/IEC 27001 clause knowledge is required.

Helpful background includes:

Basic understanding of users, systems, networks and common enterprise services; familiarity with operational realities such as access requests, incidents, alerts, outages and configuration changes; and comfort reading simple technical diagrams or control descriptions.

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