Halderstone

Training module

Mechanisms of Detective & Corrective Security Controls

Core concepts in detective & corrective controls, including logging, monitoring, incident response, backup & recovery

Can you clearly explain how detection, response, and recovery controls work together?

Overview

This module explains how organizations detect security incidents, limit their impact, and restore systems and data to a secure state.

Participants learn how monitoring, alerting, incident response, backup, and disaster recovery mechanisms work together within an integrated control system. The module clarifies the role and limitations of these safeguards and how they complement preventive controls introduced in the Information Security Fundamentals I module.

Concepts are anchored in ISO/IEC 27001 Annex A. The focus is on structural understanding rather than operational tooling.

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

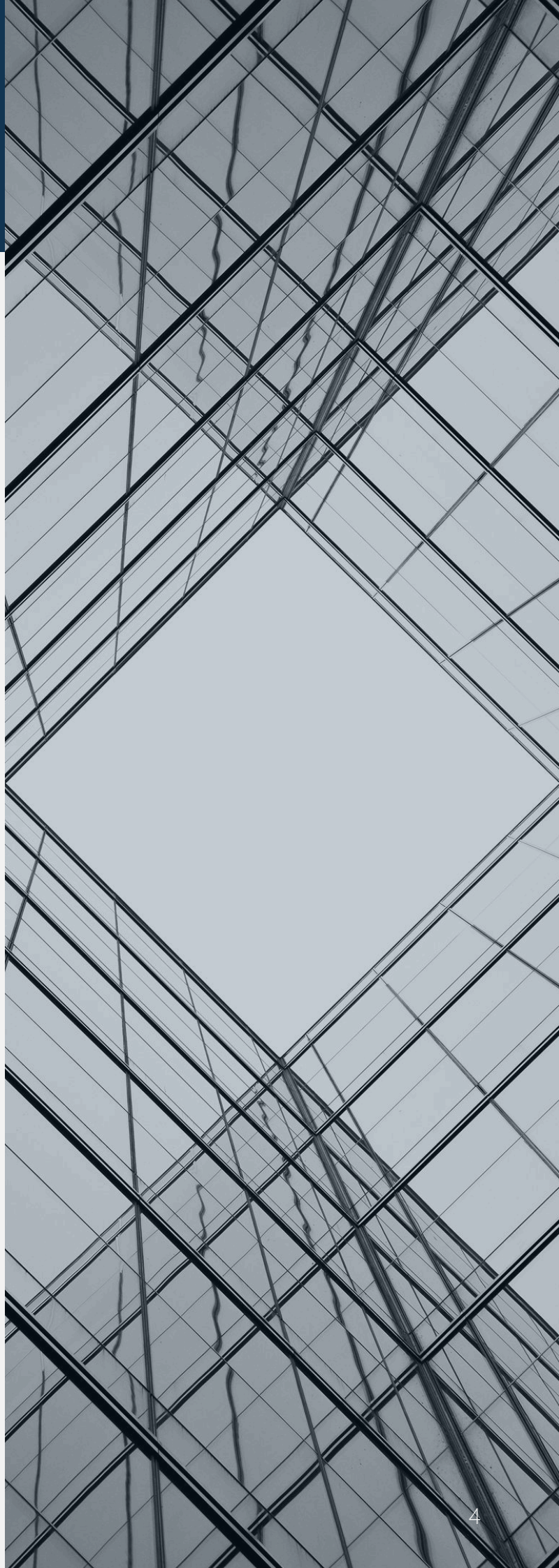
Is this module for you?

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

- want to understand what detection, response, and recovery mean conceptually.
- need clarity on what should be observable, measurable, and actionable in a security context.
- struggle to assess whether monitoring and response capabilities are coherent.
- want shared terminology across technical, governance, and advisory roles.
- need to judge whether detection and recovery mechanisms are meaningful or merely formal.

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

- are primarily looking for preventive controls rather than detection and recovery.
- expect tool configuration training (e.g., SIEM setup or hands-on log analysis).
- want a detailed incident response or crisis management playbook.
- already have a clear, shared conceptual understanding of detection and recovery controls.



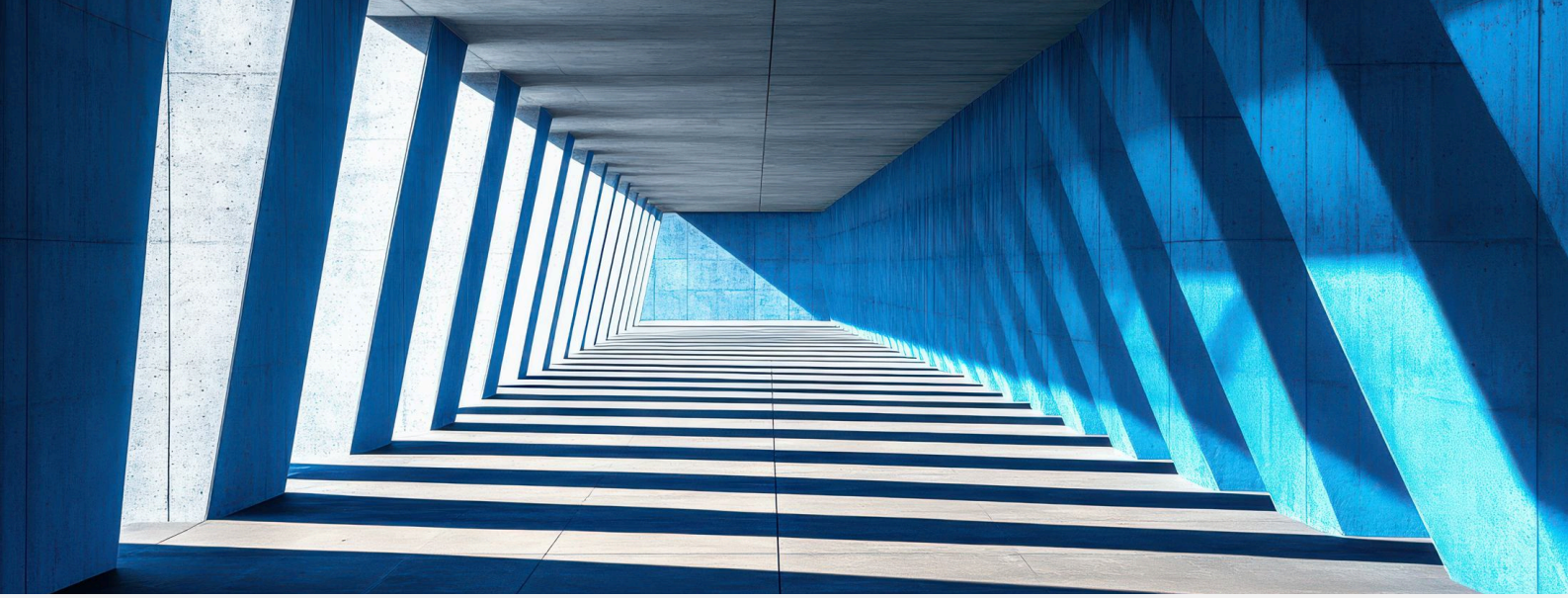
Learning outcomes

Key outcomes

- Explain the purpose, structure, and limits of detective and corrective controls
- Distinguish logging, monitoring, alerting, escalation, and incident management as separate control functions
- Describe containment and recovery concepts and their role in restoring secure operations

Additional capabilities

- Identify structural gaps and common failure points in detection and response chains
- Relate detective and corrective controls to ISO/IEC 27001 Annex A
- Assess whether detection and recovery mechanisms are coherent or merely formal
- Communicate detection and recovery requirements to technical and non-technical stakeholders



Agenda

Detective and corrective controls: purpose and limits

How to define what detective and corrective controls are intended to achieve, clarify their boundaries, and recognize structural gaps that reduce effectiveness

Logging foundations

How to determine which events must be logged, ensure sufficient identity, time, and context, and identify gaps that undermine detectability

Monitoring and alerting

How to translate logged events into actionable signals through monitoring and alerting logic, and avoid overload, latency, and missed escalation

Detection approaches and their constraints

How to distinguish core detection approaches, understand their strengths and weaknesses, and account for noise, adaptation, and incomplete visibility

Incident management fundamentals

How to structure incident management with clear escalation logic, defined authority, containment decisions, evidence handling, and structured learning after incidents

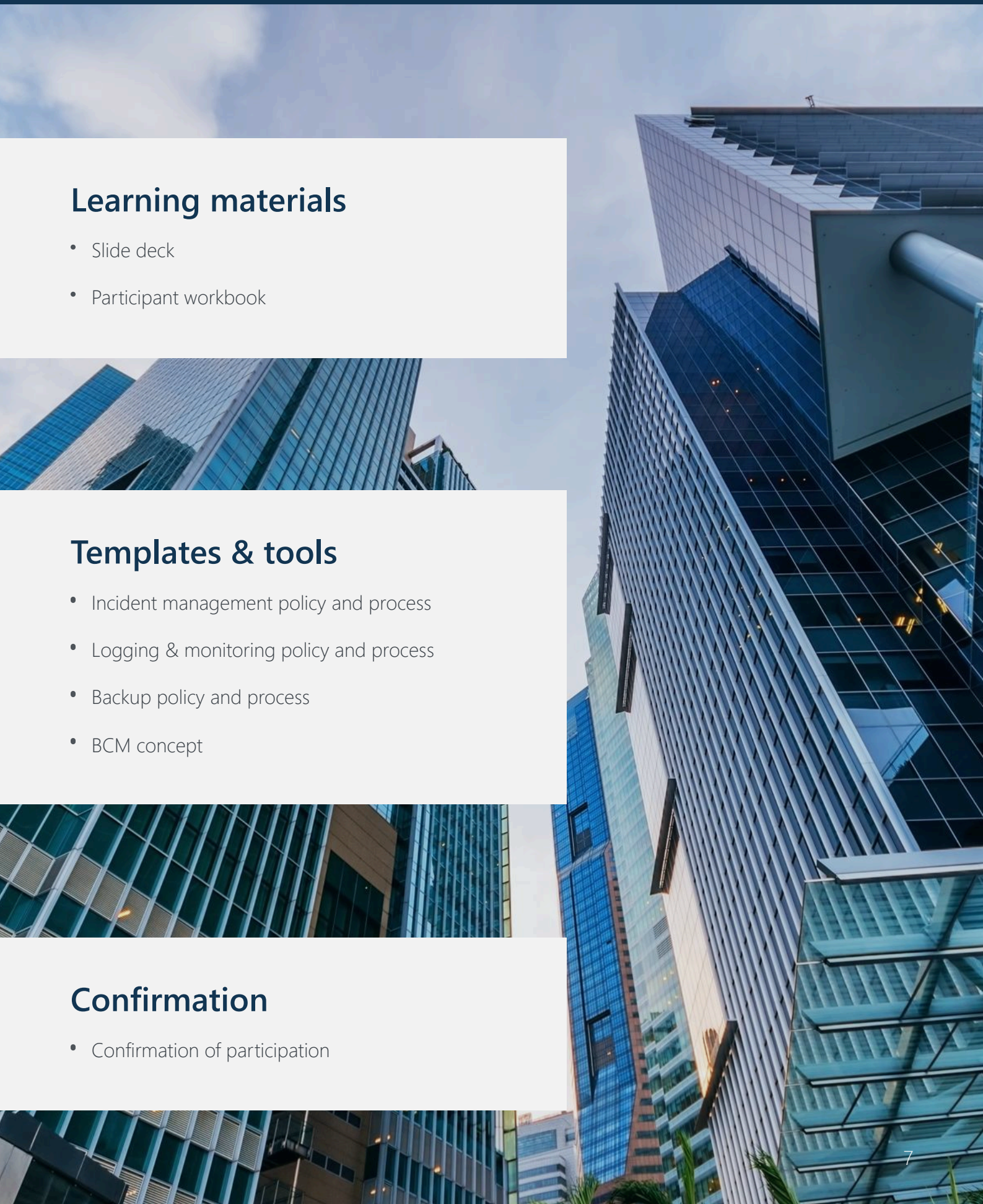
Containment, continuity, and recovery

How to design containment and recovery measures that balance isolation and operational continuity, define recovery expectations through BIA, RTO, and RPO concepts, and ensure backup and restore capabilities are realistic

Case-based workshop

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

Included materials



Learning materials

- Slide deck
- Participant workbook

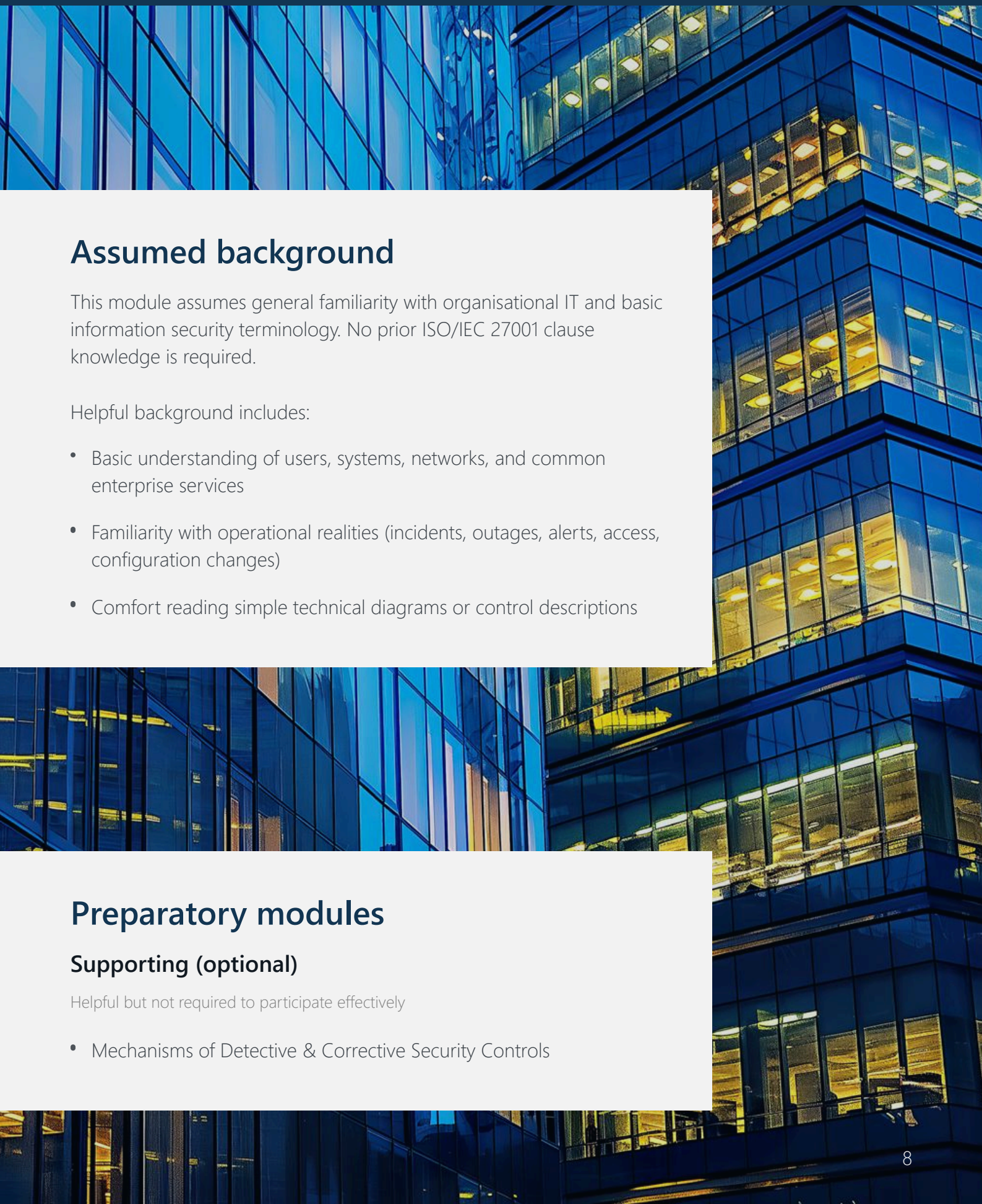
Templates & tools

- Incident management policy and process
- Logging & monitoring policy and process
- Backup policy and process
- BCM concept

Confirmation

- Confirmation of participation

Preparation guidance



Assumed background

This module assumes general 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 (incidents, outages, alerts, access, configuration changes)
- Comfort reading simple technical diagrams or control descriptions

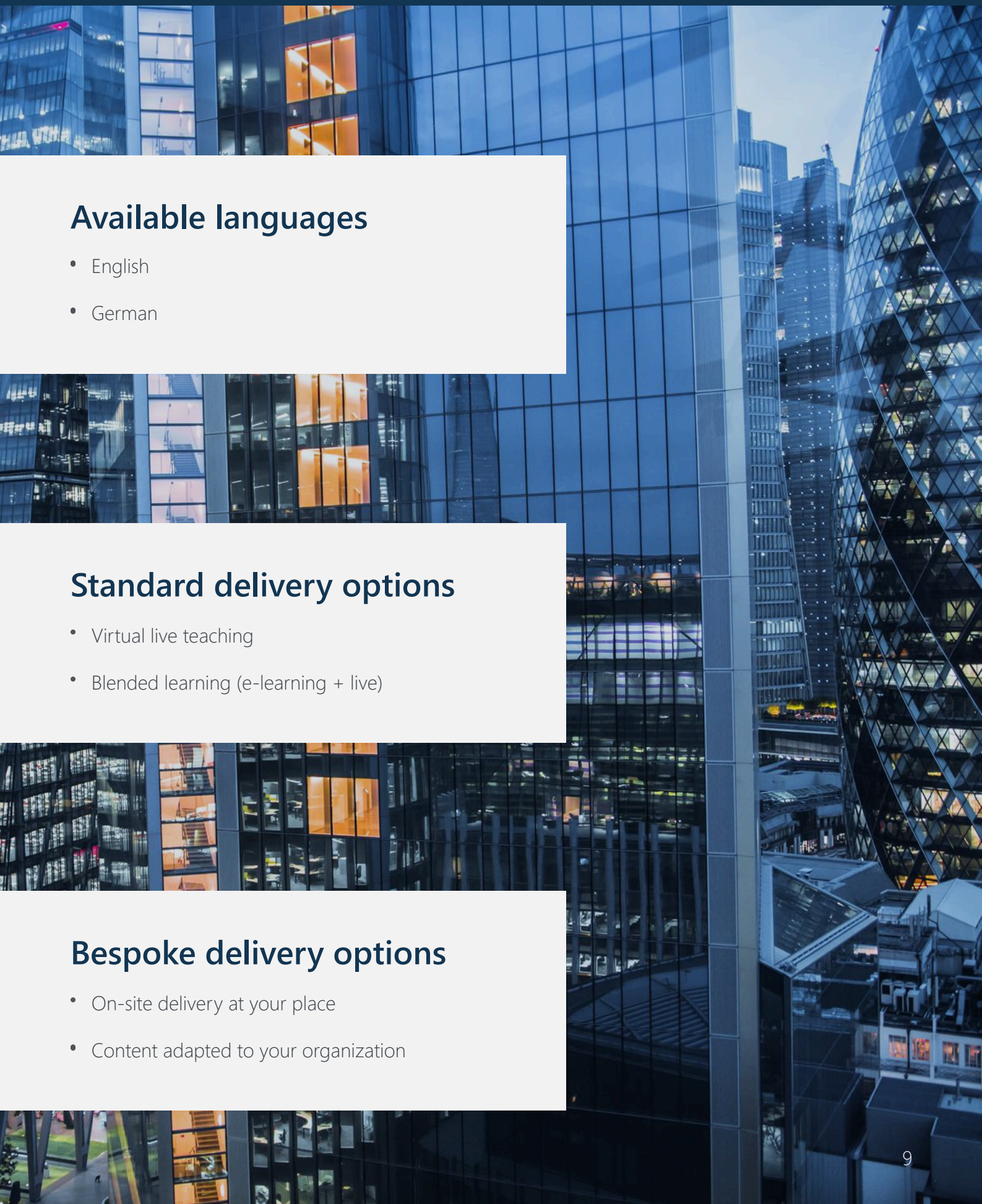
Preparatory modules

Supporting (optional)

Helpful but not required to participate effectively

- 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