Halderstone

Training module

Auditing AI Risk & Impact Management

Evaluate harm, impact and risk reasoning, intended use alignment, and decision traceability in ISO/IEC 42001

Does your audit move beyond paperwork to defensible, traceable AI risk and impact decisions?

Overview

In ISO/IEC 42001 audits, weak AI risk and impact management rarely fails because an organisation used the wrong framework. It fails because the organisation cannot show a coherent line from intended use and stakeholders to impact reasoning, risk decisions, and documented acceptance of trade-offs. This creates false assurance: the system looks controlled on paper, while key harms, misuses, and operational realities remain unaddressed.

This standard-specific auditing module shows how to audit the quality of reasoning and documentation behind AI risk and impact decisions, without re-teaching generic risk methods or generic audit craft. It is designed to stand on its own in the ISO/IEC 42001 auditor pathway and is applicable to internal auditors and third-party auditors, including certification-body and independent assurance contexts.

Target audience

- Aspiring auditors who want to audit AI management systems against ISO/IEC 42001 following best practices
- Practising ISO/IEC 42001 auditors who want to strengthen their audit knowledge, judgement, and effectiveness

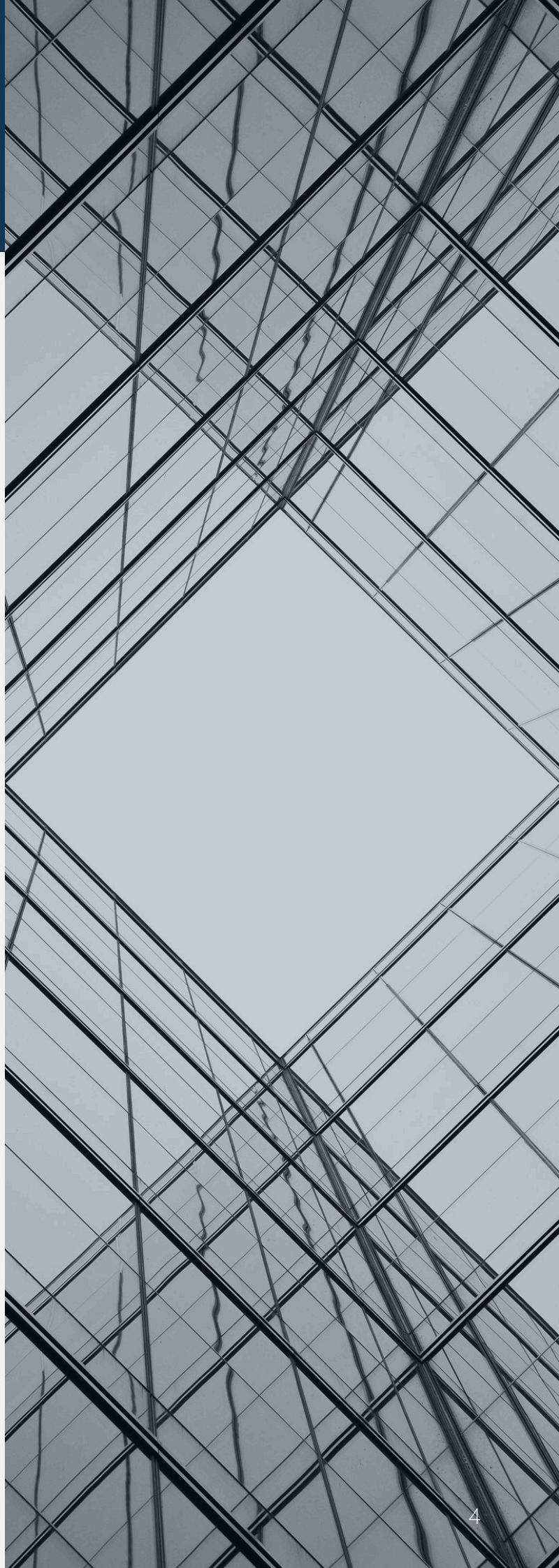
Is this module for you?

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

- seek to audit the quality of AI risk and impact reasoning.
- are aiming to judge alignment between intended use, impacts, and decisions.
- focus on traceability from risk reasoning to documented controls.
- are prepared to test whether decisions hold up under real use conditions.
- expect to strengthen audit conclusions on AI risk governance.

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

- prefer to design AI risk frameworks or impact assessment methods.
- are looking for guidance on harm analysis or ethical risk modelling.
- focus primarily on managing or mitigating AI risks yourself.
- do not intend to audit AI risk and impact management under ISO/IEC 42001.



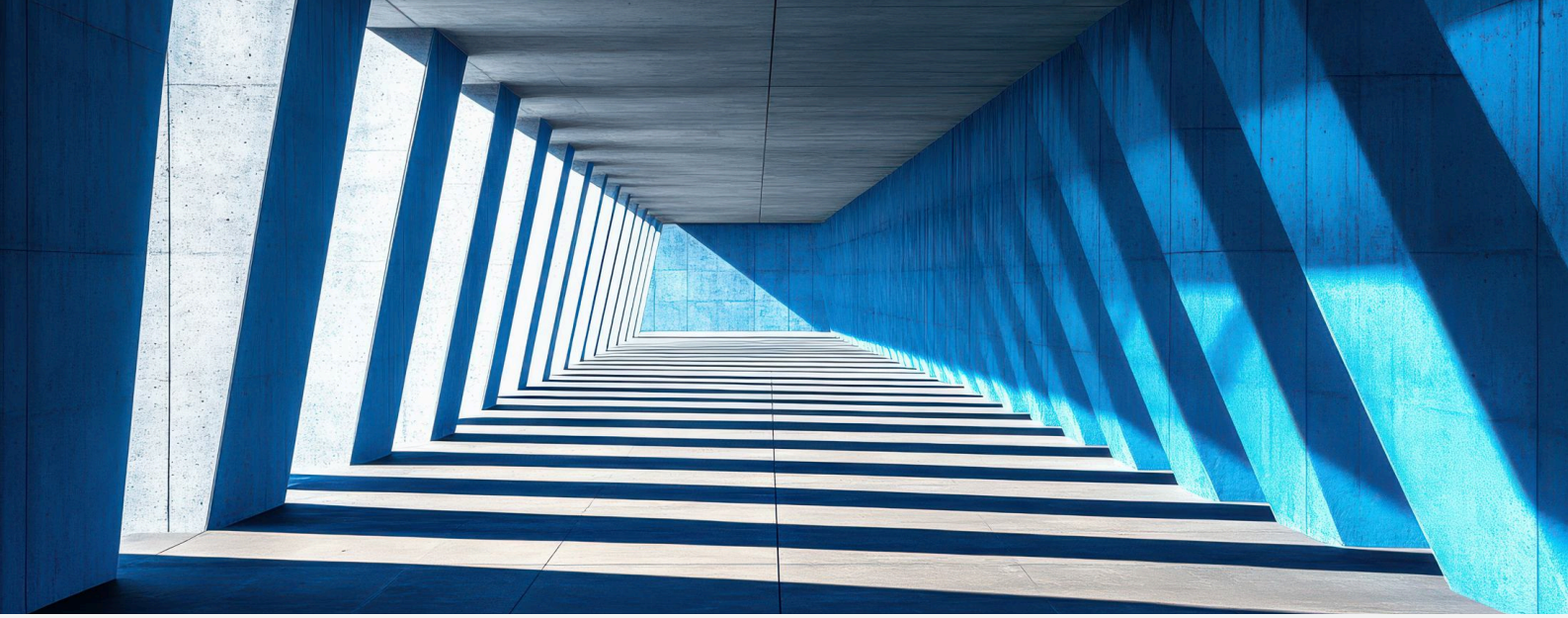
Learning outcomes

Key outcomes

- Evaluate whether harm/impact reasoning is specific, complete enough for decisions, and consistent across artefacts
- Test traceability from intended use and stakeholder considerations to impact assessment, risk decisions, and controls
- Assess whether risk and impact decisions are documented in a way that supports accountability and later review

Additional capabilities

- Identify and prioritise evidence sources that demonstrate real operation (not just planned intent)
- Recognise common ISO/IEC 42001 risk/impact audit red flags that indicate false assurance
- Define focused audit tests for decision quality without substituting for generic audit planning or interviewing techniques



Agenda

AI risk and impact management in an ISO/IEC 42001 audit

What auditors judge: coherence, traceability, and operational credibility of AI risk and impact decisions. Scope boundary: no generic risk frameworks, no audit-craft re-teaching.

Testing harm and impact reasoning

Assesses whether harms and impacts are defined in a usable, decision-ready way (who/what is affected, how, why it matters), and whether severity, likelihood, and uncertainty are treated consistently and transparently.

Intended use integrity and stakeholder alignment

Tests alignment between intended and actual use, including scope drift, misuse paths, and silent expansion via configuration or integration. Verifies that affected stakeholders and obligations were substantively considered, not just listed.

Decision documentation quality

Evaluates decision records for rationale, trade-offs, approvals, and residual risk acceptance. Checks cross-document consistency across impact assessments, risk decisions, controls, monitoring triggers, and incident learning.

Evidence trails, sampling focus, and red flags

Identifies where evidence actually sits in governance routines and operational records. Flags template compliance, post-hoc rationales, unowned residual risks, and undocumented trade-offs.

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 auditors can already apply core audit evidence and judgement concepts and are familiar with management system basics. It does not teach generic audit craft or generic risk methodology.

Helpful background includes:

- Practical ability to evaluate evidence, sampling rationale, and professional judgement
- General understanding of how management systems use documented information to support governance decisions

Preparatory modules

Foundation (depending on background)

Useful if you are new to the underlying concepts

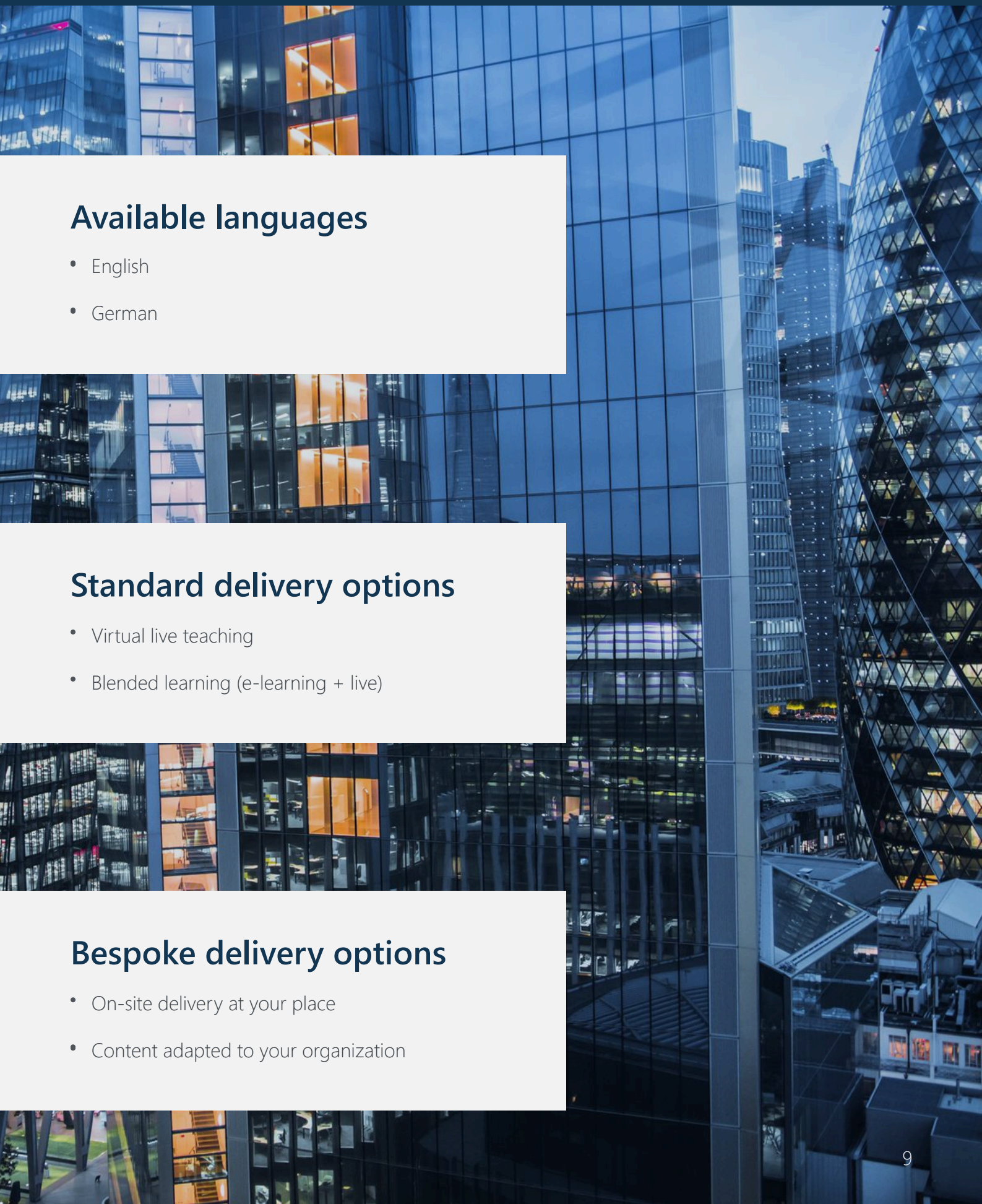
- Audit Principles
- AI Limitations & Failure Modes

Supporting (optional)

Helpful but not required to participate effectively

- AI Systems & Architectures
- Auditing Risk & Opportunity 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