

Halderstone



Training module

Auditing Operational Privacy Controls

Evaluate whether privacy controls are implemented effectively and applied consistently across personal data processing activities



Do privacy controls exist on paper while data handling practices quietly diverge?

Overview

Operational privacy controls translate privacy policies and risk decisions into day-to-day handling of personal data. These controls govern how personal data is collected, accessed, processed, shared, retained, and deleted across organisational processes and technical systems.

In practice, privacy controls often appear complete in policies and procedures while operational evidence reveals inconsistent application, unclear ownership, or gaps across systems and third-party processors. Audits therefore need to test whether privacy controls actually operate as intended in real processing environments.

This module develops the capability to audit operational privacy controls in a privacy information management system aligned with ISO/IEC 27701. Participants review how privacy operational controls function within a PIMS and then learn how auditors test implementation, trace operational evidence, and detect typical failure patterns without drifting into privacy control design or engineering.



Target audience

- Aspiring auditors who want to audit privacy information management systems against ISO/IEC 27701 following best practices
- Practising ISO/IEC 27701 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...

- audit operational privacy controls in a privacy information management system.
- seek to judge whether privacy requirements are applied consistently in practice.
- need to evaluate how personal data processing activities are controlled operationally.
- want to follow evidence trails across systems, teams, and third-party processors.
- expect to strengthen audit conclusions on privacy control effectiveness.

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

- prefer to design privacy controls or safeguards yourself.
- are looking for methods to implement privacy programs or governance frameworks.
- focus primarily on privacy engineering or control implementation.
- do not intend to audit operational privacy controls.

Learning outcomes

Key outcomes

- Assess whether privacy operational controls are implemented consistently across processing activities
- Test whether privacy requirements are reflected in operational practices and system behaviour
- Trace operational privacy controls across systems, records, and organisational roles

Additional capabilities

- Evaluate whether privacy controls function across organisational and third-party processing boundaries
- Detect common failure patterns such as policy-only controls or inconsistent implementation
- Select meaningful sampling targets when auditing privacy operational controls
- Formulate defensible audit conclusions on privacy control effectiveness



Agenda

Operational privacy controls in a PIMS

How privacy requirements are translated into operational controls governing personal data collection, processing, sharing, retention, and deletion

Effective auditing of privacy operational controls

How auditors judge whether privacy controls operate effectively rather than relying on policy statements or procedural descriptions

Operational control implementation

How to evaluate whether privacy requirements are implemented in systems, workflows, and operational processes handling personal data

Evidence of control operation

How to test operational evidence such as system configurations, processing records, and employee practices to determine whether controls function in practice

Third-party processing and shared responsibility

How to audit privacy control implementation across external processors, service providers, and shared operational environments

Detecting operational control failure patterns

How to recognise common weaknesses such as policy-only controls, inconsistent system enforcement, or informal workarounds

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 participants can perform basic audit activities and apply evidence-based judgement.

Helpful background includes:

- General understanding of privacy concepts and personal data processing
- Ability to follow audit trails across systems, documentation, and organisational processes
- Basic familiarity with privacy policies, procedures, and operational data handling practices

Preparatory modules

Foundation (depending on background)

Useful if you are new to the underlying concepts

- Audit Principles
- Data Protection Principles

Supporting (optional)

Helpful but not required to participate effectively

- Auditing Operational Control

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