PENTESTERRA

ISO/IEC 27701:2019 GAP ASSESSMENT

Is Your Privacy Extension as Ready as You Think?

Gap assessment across 21 ISO/IEC 27701 controls - the privacy extension (PIMS) to ISO 27001 - for organizations that want to cover privacy with the same rigor as security.

IN SHORT

Covers the 21 key controls of ISO/IEC 27701:2019, organized across the standard's 4 structural parts: PIMS requirements tied to ISO 27001, PIMS-specific guidance, and the additional controls for controllers and processors.

21	PIMS	+ ISO 27001
PIMS controls covered	Privacy Information Management System	A natural extension for the already-certified

THE SITUATION TODAY

WHO YOU ARE

You're the DPO or CISO of an organization already certified (or being certified) to ISO 27001 that wants to formally extend privacy management with the same rigor used for security.

WHAT HAPPENED

A client or an audit asks for evidence of a structured privacy management system - not just a generic GDPR policy.

WHY IT HURTS

Without a structured PIMS, every privacy evidence request becomes a manual collection exercise from scratch - slow, incomplete, and hard to repeat at the next audit.

WHERE YOU WANT TO GET TO

DESIRED OUTCOME	You want to know, control by control, what's satisfied, what's partial, and what's missing - with real technical evidence attached to every answer, not an optimistic claim nobody has verified.
THE SOLUTION	Pentesterra's ISO/IEC 27701:2019 Gap Assessment: a structured assessment across every control, with technical controls auto-filled from vulnerability scanning, penetration testing, OSINT and External Exposure monitoring wherever evidence exists.
WHY IT'S DIFFERENT	You're not buying another self-assessment questionnaire, and this isn't a legal opinion. You're working with [YOUR COMPANY NAME] - a certified provider with a long track record in information security. You've likely worked with us already, directly or through someone you know - a colleague, a supplier, a competitor. And the gap assessment doesn't stop at a paper checklist: technical controls are auto-filled from evidence already on file, with cross-standard mapping to the other 12 frameworks the platform supports, so a second audit never starts from zero.
CONCRETE PROOF	The result is a complete, ready-to-deliver PDF report covering every control, with a direct reference to the legal/regulatory basis. If gaps come up, we propose the additional services to close them: vulnerability assessment, network or application penetration testing, phishing training and simulation.

WHAT'S ACTUALLY INCLUDED

Not a generic checklist - the real controls of ISO/IEC 27701:2019, grouped the way you'll see them in the platform.

Clause 5 - PIMS requirements tied to ISO 27001

The management-system layer, integrated with your existing ISMS.

- Extending context and leadership to privacy
- PIMS-specific planning and objectives
- Integration with existing ISO 27001 controls

Clause 6 - PIMS-specific guidance

Privacy extensions to the existing ISO 27002 controls.

- Conditions for collection and processing
- Obligations toward data subjects
- Privacy by design in IT projects

Clause 7 - PII controllers

Additional controls specific to those who determine the purposes and means of processing.

- Identifying the lawful basis
- Managing consent and data subject rights
- Sharing, transfer and disclosure of data

Clause 8 - PII processors

Additional controls specific to those who process data on behalf of others.

- Contractual agreements with the controller
- Processing in line with received instructions
- Returning or deleting data at contract end

WHAT YOU GET

- ✓ An exportable XLSX control matrix, with the status of every individual control
- ✓ An editable DOCX gap report, ready for your auditor or your board
- ✓ Technical controls auto-filled from evidence the platform already collected
- ✓ Guided applicability check by sector, country, and company size
- ✓ Cross-standard mapping to the other 12 frameworks the platform supports - answer once, reuse across standards
- ✓ A one-click auditor package: questionnaire, technical evidence and gap report together
- ✓ Prioritized remediation recommendations for the gaps found

HOW IT WORKS

1

We define the scope

Assessment boundary, systems and processes involved - we set the scope together.

2

We collect the evidence

Technical controls are auto-filled from evidence the platform already collected.

3

We complete the questionnaire

Non-technical controls are verified with your team.

4

We deliver the report

A complete PDF with the gaps found and the actions to take.

Find out how ready you are for ISO/IEC 27701:2019

A complete report, ready to present to clients, auditors, or your board.

Request your ISO/IEC 27701:2019 Gap Assessment →

info@pentesterra.com · pentesterra.com/solutions/compliance