
SELF-ASSESSMENT WORKSHEET

ISO/IEC 27701:2025 — Privacy Information Management

Work through each clause, record what you do today, rate where you are and agree the actions that close the gap.

ORGANISATION

COMPLETED BY

DATE

How to rate: 0 = nothing in place 1 = partly in place 2 = in place, little evidence 3 = in place and evidenced
Fill in on screen or print. Always work from the current published standard.

How to complete this worksheet

1

Get the right people together

Ask the person who runs each area to help. Allow 1–2 hours per sitting; you don't have to finish in one go.

2

Read each clause and the evidence prompt

The grey box tells you what an auditor will look for. The examples underneath show the kind of records that count.

3

Write what you actually do today

Describe the real practice, not what you'd like to happen. Name the document, system or record and where it's kept, e.g. 'Training matrix — SharePoint/HR, updated monthly'.

4

Rate honestly from 0 to 3

0 nothing in place · 1 partly in place or informal · 2 in place but little written proof · 3 in place, followed and evidenced with records. If you can't show it, it isn't a 3.

5

Agree actions, owners and due dates

For anything rated 0–2, write the next practical step, who will do it and by when. Small, specific actions get done.

6

Summarise and review

List your top three priorities on the final page. Revisit the worksheet every few months to track progress.

What counts as good evidence?

- Good evidence is current, approved, dated and actually used — a policy nobody follows isn't evidence.
- Records beat documents: a completed checklist proves more than the procedure that describes it.
- Photos, screenshots, emails and system exports all count if they show the activity happening.
- Leave a box blank rather than guess — blanks show you where to look first.

CLAUSES 1-3

Scope, references and definitions

These opening clauses explain what ISO/IEC 27701:2025 covers, list any documents it relies on and define its key terms. They contain no requirements you are audited against.

Evidence to look for: Read the definitions once — words like 'shall', 'interested party' and 'documented information' have precise meanings in an audit.

Examples of suitable evidence

- ✓ Copy of the current ISO/IEC 27701:2025 standard
- ✓ Reference list of documents cited by the standard
- ✓ Staff glossary of privacy terms and definitions
- ✓ Briefing notes explaining the standard's scope

What we do today / evidence we hold**Actions to close the gap****Owner**

Due

Rating
☐ 0

☐ 1

☐ 2

☐ 3

CLAUSE 4

Context of the organisation

Understand your role as a PII controller and/or processor, privacy legislation that applies (such as UK GDPR) and define the privacy information management system scope.

Evidence to look for: A record of processing activities and a scope naming controller and processor roles.

Examples of suitable evidence

- ✓ Approved privacy information management system scope statement
- ✓ Processing register identifying controller and processor roles
- ✓ Legal obligations register covering UK GDPR and the Data Protection Act 2018
- ✓ Context review minutes recording stakeholder privacy requirements

What we do today / evidence we hold**Actions to close the gap****Owner**

Due

Rating
☐ 0

☐ 1

☐ 2

☐ 3

CLAUSE 5

Leadership

Top management must own the privacy system: set the policy, assign roles and responsibilities, provide resources and make it part of normal business decisions. Responsibility can be delegated; accountability cannot.

Evidence to look for: Directors can explain the policy, review results at board level and remove obstacles. A signed policy alone is not enough.

Examples of suitable evidence

- ✓ Privacy policy approved by the managing director
- ✓ Signed privacy roles and responsibilities matrix
- ✓ Board minutes approving privacy staffing and budget
- ✓ Project approval minutes recording management decisions on privacy risks

What we do today / evidence we hold

Actions to close the gap

Owner		Due		Rating	0	1	2	3
-------	--	-----	--	--------	---	---	---	---

CLAUSE 6

Planning

Assess privacy risks to individuals as well as to the business, select controls and record them in a Statement of Applicability, and set privacy objectives.

Evidence to look for: Data protection impact assessments (DPIAs) linked to the risk register.

Examples of suitable evidence

- ✓ Privacy risk assessments covering harm to individuals and business impacts
- ✓ Privacy risk treatment plan with named owners and deadlines
- ✓ Approved Statement of Applicability recording control selections and exclusions
- ✓ Privacy objectives register with measurable targets and review dates

What we do today / evidence we hold

Actions to close the gap

Owner		Due		Rating	0	1	2	3
-------	--	-----	--	--------	---	---	---	---

CLAUSE 7**Support**

Provide the people, competence, awareness, communication, infrastructure and controlled documents and records the privacy system needs.

Evidence to look for: Training is based on the work people actually do, current instructions are easy to find and old versions are withdrawn.

Examples of suitable evidence

- ✓ Privacy training attendance records and staff competence assessments
- ✓ Privacy communications plan naming audiences, channels and responsible staff
- ✓ IT maintenance logs for systems supporting privacy controls
- ✓ Controlled document register showing owners, versions and approval dates

What we do today / evidence we hold**Actions to close the gap****Owner**

Due

Rating
☐ 0

☐ 1

☐ 2

☐ 3
CLAUSE 8**Operation**

Operate controls for lawful basis, consent, data subject rights, privacy by design, retention, transfers and processor obligations.

Evidence to look for: Rights-request logs, retention schedules and processor contracts.

Examples of suitable evidence

- ✓ Lawful basis register linked to consent records
- ✓ Data subject request log recording identity checks and response dates
- ✓ Completed privacy impact assessment documenting design changes and retention controls
- ✓ Signed processor agreements with documented international transfer safeguards

What we do today / evidence we hold**Actions to close the gap****Owner**

Due

Rating
☐ 0

☐ 1

☐ 2

☐ 3

CLAUSE 9**Performance evaluation**

Decide what to monitor and measure for privacy, analyse the results, run a planned programme of impartial internal audits and hold management reviews at planned intervals.

Evidence to look for: Use a handful of meaningful indicators, audit real work rather than paperwork, and minute the decisions management review actually takes.

Examples of suitable evidence

- ✓ Monthly privacy performance dashboard with targets and trend analysis
- ✓ Internal audit programme naming auditors independent of activities reviewed
- ✓ Completed privacy internal audit reports with findings and supporting evidence
- ✓ Management review minutes recording privacy performance, decisions and assigned actions

What we do today / evidence we hold**Actions to close the gap**

Owner		Due		Rating	☐	☐	☐	☐
					0	1	2	3

CLAUSE 10**Improvement**

When something goes wrong, deal with the immediate effect, find the root cause, take action so it does not recur and check the action worked. Keep improving the system over time.

Evidence to look for: A nonconformity is only closed when you have evidence the cause was fixed — not when the form is completed.

Examples of suitable evidence

- ✓ Privacy incident log recording immediate containment and remedial actions
- ✓ Root cause analysis report for a missed deletion deadline
- ✓ Corrective action register with owners, deadlines and effectiveness checks
- ✓ Improvement log recording completed changes and measured privacy benefits

What we do today / evidence we hold**Actions to close the gap**

Owner		Due		Rating	☐	☐	☐	☐
					0	1	2	3

NOTE

2025 edition

The 2025 edition can operate as a standalone management system standard rather than only as an extension to ISO/IEC 27001.

Evidence to look for: Organisations certified to the 2019 version should plan their transition.

Examples of suitable evidence

- ✓ Copy of the published ISO/IEC 27701:2025 standard
- ✓ Edition comparison briefing explaining the standalone management system structure
- ✓ Gap assessment comparing existing privacy arrangements against the 2025 edition
- ✓ Management meeting minutes discussing adoption of the standalone privacy management system

What we do today / evidence we hold

Actions to close the gap

Owner		Due		Rating	0	1	2	3
-------	--	-----	--	--------	------------------------------------	------------------------------------	------------------------------------	------------------------------------

Summary and next steps

Top three priorities

Resources or support needed

Target date for certification or review

Want a second pair of eyes?

Send your completed worksheet to our success team for a free review call.

success@isology.co.uk · www.isology.co.uk/contact