ISO/IEC 27701:2019

ISO/IEC 27701:2019 (whole Part)

Audit Checklist

88 audit questions across **4** sections.

HOW TO USE THIS CHECKLIST

Each question has three boxes the auditor fills in during the audit:

1. **Compliance** — the binary headline: Compliant / Non-compliant.
2. **Classification** — where the gap is, four-state grid: Documented / Implemented matrix.
3. **Finding level** — severity: Maj / Min / Obs (Major nonconformity / Minor nonconformity / Observation).

Severity is the auditor's call on the day, against the real finding — no severity is pre-suggested per question.

auditchecklists.org Audit Checklist Licence

Product:	ISO/IEC 27701:2019 (whole Part) (88 questions)
Regulation:	
Issued:	[YYYY-MM-DD — STAMPED AT ISSUE]

Licensed to:	[ORG NAME — STAMPED AT ISSUE]
Licensee email:	[EMAIL — STAMPED AT ISSUE]
Order:	[AVI-YYYY-NNNNN — STAMPED AT ISSUE]

Licence terms

This audit checklist is licensed for use within the organisation named above by the licensee email named above. Use is permitted by employees and contractors of the named organisation in the course of their work for that organisation, including printing, internal distribution within the organisation, annotation during audits, and incorporation into the organisation's management-system documentation as a working reference.

Not for redistribution. Sharing this document, or any derivative or extract of it, with any party outside the named organisation is a breach of this licence. This includes posting to file-sharing networks, internal wikis or knowledge bases accessible to other organisations, vendor portals, supplier-facing GRC systems, and email forwarding to colleagues at other firms. Quoting individual audit questions in regulator submissions or internal training materials is permitted; reproducing the structured checklist as a whole is not.

Each additional organisation or operating site requires a separate licence. If a sister organisation in the same group, or a separate operating entity, requires the same checklist, contact licences@auditchecklists.org for a multi-site licence quote. Holding companies licensing for multiple subsidiaries are eligible for group-licence pricing.

Licence transfers. This licence does not transfer with sale, merger, or organisational restructure without written consent. auditchecklists.org may, at its discretion, transfer the licence to the successor organisation on request — usually a formality, contact licences@auditchecklists.org.

Defects and amendments. If you identify a defect in this checklist — wrong content, mistranscribed regulation, factual error — email support@auditchecklists.org. We will verify the defect, correct it, and reissue the affected artefacts to you within a reasonable timeframe at no further charge. Regulatory amendments published during your 12-month update

§Clause 5

PIMS-specific requirements related to ISO/IEC 27001

Q1 CLAUSE ISO-27701 §5.1

Has the organisation extended the requirements of ISO/IEC 27001 that mention "information security" to the protection of privacy as potentially affected by the processing of PII (i.e. reading "information security" as "information security and privacy")?

SOURCE VERBATIM

Cite ISO/IEC 27701:2019 Clause 5.1.

COMPLIANCE

☐ Compliant ☐ Non-compliant

CLASSIFICATION (FOUR-STATE)

☐ Documented and Implemented
☐ Documented Not Implemented
☐ Not Documented but Implemented
☐ Not Documented and Not Implemented

FINDING LEVEL

☐ Maj ☐ Min ☐ Obs

Maj = Major nonconformity · Min = Minor nonconformity · Obs = Observation

SUGGESTED EVIDENCE TO REQUEST

- PIMS scoping/interpretation statement extending 27001 to privacy

MANAGEMENT SYSTEM REFERENCE:

FINDINGS / NOTES:

Q2 CLAUSE ISO-27701 §5.2.1#role

Has the organisation determined its role as a PII controller (including joint controller) and/or a PII processor — with separate roles determined where it acts in both, each the subject of a separate set of controls?

SOURCE VERBATIM

Cite ISO/IEC 27701:2019 Clause 5.2.1.

COMPLIANCE

☐ Compliant ☐ Non-compliant

CLASSIFICATION (FOUR-STATE)

☐ Documented and Implemented
☐ Documented Not Implemented
☐ Not Documented but Implemented
☐ Not Documented and Not Implemented

FINDING LEVEL

☐ Maj ☐ Min ☐ Obs

Maj = Major nonconformity · Min = Minor nonconformity · Obs = Observation

SUGGESTED EVIDENCE TO REQUEST

- Documented determination of PII roles per processing activity

MANAGEMENT SYSTEM REFERENCE:

FINDINGS / NOTES:

Q3 CLAUSE ISO-27701 §5.2.1#factors

Has the organisation determined the external and internal factors relevant to its context that affect its PIMS — such as applicable privacy legislation, regulations, judicial/administrative decisions, organisational context and contractual requirements?

SOURCE VERBATIM

Cite ISO/IEC 27701:2019 Clause 5.2.1.

COMPLIANCE

☐ Compliant ☐ Non-compliant

CLASSIFICATION (FOUR-STATE)

☐ Documented and Implemented
☐ Documented Not Implemented
☐ Not Documented but Implemented
☐ Not Documented and Not Implemented

FINDING LEVEL

☐ Maj ☐ Min ☐ Obs
Maj = Major nonconformity · Min = Minor nonconformity · Obs = Observation

SUGGESTED EVIDENCE TO REQUEST

- PIMS context document covering privacy legislation, regulation and contractual factors

MANAGEMENT SYSTEM REFERENCE:

FINDINGS / NOTES: