

ISO/IEC 27001:2022 (whole Part)

Audit Checklist

219 audit questions across **11** 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 27001:2022 (whole Part) (219 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

Organisational controls

Q1 ANNEX

ISO-27001 A.5.1

Has the entity defined an information-security policy and topic-specific policies — approved by management, published, communicated to and acknowledged by relevant personnel and interested parties, and reviewed at planned intervals and on significant changes?

SOURCE VERBATIM

Cite ISO/IEC 27001:2022 Annex A.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

- Approved policy + topic-specific policies
- Acknowledgement records
- Review log

MANAGEMENT SYSTEM REFERENCE:

FINDINGS / NOTES:

Are information-security roles and responsibilities defined and allocated according to the organisation's needs?

SOURCE VERBATIM

Cite ISO/IEC 27001:2022 Annex A.5.2.

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

- Roles + responsibilities matrix (RACI)
- Allocation evidence

MANAGEMENT SYSTEM REFERENCE:

FINDINGS / NOTES:

Are conflicting duties and conflicting areas of responsibility segregated?

SOURCE VERBATIM

Cite ISO/IEC 27001:2022 Annex A.5.3.

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

- Conflicting-duty register
- Segregation enforcement evidence (system + process)

MANAGEMENT SYSTEM REFERENCE:

FINDINGS / NOTES: