ISO 31000:2018

ISO 31000:2018 (whole Part)

Audit Checklist

21 audit questions across **3** 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.

SAMPLE

Licensed to [ORG NAME — STAMPED AT ISSUE] ([EMAIL — STAMPED AT ISSUE]) · order [AVI-YYYY-NNNNN — STAMPED AT ISSUE] · Single-organisation use · Not for redistribution · © Contenza K/S

auditchecklists.org Audit Checklist Licence

Product:	ISO 31000:2018 (whole Part) (21 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]

SAMPLE

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 4

Principles

Q1 CLAUSE ISO 31000 Cl.4

Are the eight ISO 31000 principles reflected in the organisation's risk-management framework and processes — i.e. risk management that is integrated into all organisational activities; structured and comprehensive; customised and proportionate to the organisation's context and objectives; inclusive (appropriate, timely stakeholder involvement); dynamic (anticipating and responding to change); based on the best available information (with its limitations and uncertainties made explicit); accounting for human and cultural factors; and continually improved — so that it serves the purpose of creating and protecting value?

SOURCE VERBATIM

> Cite ISO 31000:2018 Clause 4.

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

- Risk-management framework/policy demonstrating the principles (integration, customisation, inclusiveness, dynamism, information quality, human/cultural factors, improvement)
- Evidence the framework is designed with the principles explicitly in mind

MANAGEMENT SYSTEM REFERENCE: _____

FINDINGS / NOTES:

SAMPLE

Licensed to [ORG NAME — STAMPED AT ISSUE] ([EMAIL — STAMPED AT ISSUE]) · order [AVI-YYYY-NNNNN — STAMPED AT ISSUE] · Single-organisation use · Not for redistribution · © Contenza K/S

§Clause 5

Framework

Q1 CLAUSE ISO 31000 Cl.5.2

Do top management and oversight bodies (where applicable) ensure that risk management is integrated into all organisational activities and demonstrate leadership and commitment — by customising and implementing all components of the framework, issuing a statement or policy establishing the risk-management approach, ensuring necessary resources are allocated, and assigning authority, responsibility and accountability at appropriate levels?

SOURCE VERBATIM

> Cite ISO 31000:2018 Clause 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

- Risk-management policy/statement issued by top management
- Evidence of resource allocation and assigned authority/responsibility/accountability

MANAGEMENT SYSTEM REFERENCE: _____

FINDINGS / NOTES:

SAMPLE

Licensed to [ORG NAME — STAMPED AT ISSUE] ([EMAIL — STAMPED AT ISSUE]) · order [AVI-YYYY-NNNNN — STAMPED AT ISSUE] · Single-organisation use · Not for redistribution · © Contenza K/S

Q2 CLAUSE ISO 31000 Cl.5.3

Does the organisation integrate risk management into its structure and activities — recognising that risk is managed in every part of the structure, that everyone has responsibility for managing risk, and that risk management is a part of (not separate from) organisational purpose, governance, leadership, strategy, objectives and operations — customised to the organisation's needs and culture?

SOURCE VERBATIM

> Cite ISO 31000:2018 Clause 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

- Evidence risk management is embedded across structures, governance and operations (not run as a silo)

MANAGEMENT SYSTEM REFERENCE:

FINDINGS / NOTES:

SAMPLE

Licensed to [ORG NAME — STAMPED AT ISSUE] ([EMAIL — STAMPED AT ISSUE]) · order [AVI-YYYY-NNNNN — STAMPED AT ISSUE] · Single-organisation use · Not for redistribution · © Contenza K/S