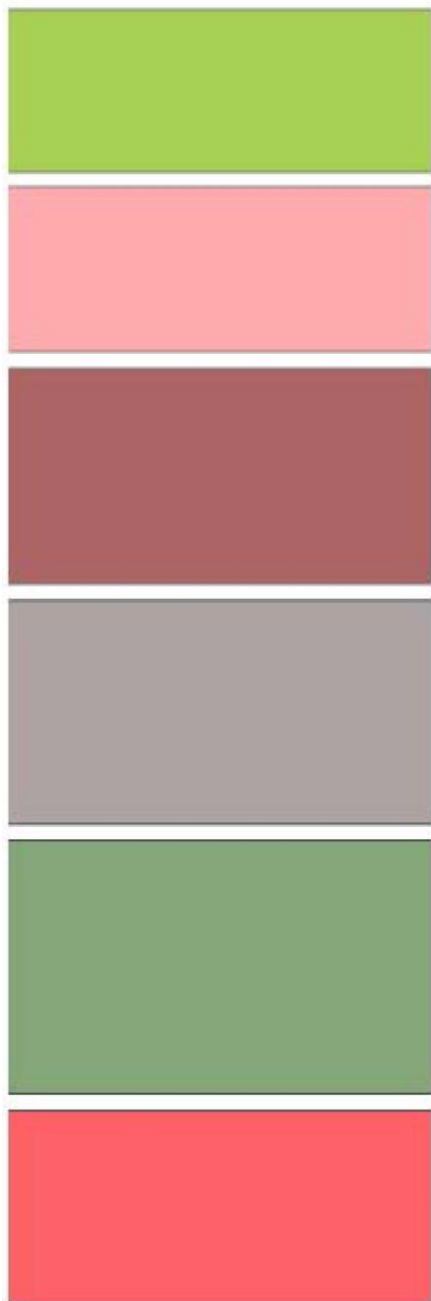




Einleitung

Audit -

Fragenkatalog

DIN EN ISO IEC

27001:2024

[hier können Sie den
gesamten Fragenkatalog bestellen](#)

QUMsult GmbH & Co. KG
Eisenbahnstraße 41
79098 Freiburg
Tel. 07 61 / 29286-50
Fax 07 61 / 29286-77
E-mail info@qumsult.de
www.qumsult.de



Zur Handhabung des Audit-Fragenkatalogs

Der Audit-Fragenkatalog ist ein Arbeitspapier, in das Sie Ihre Antworten und Nachweise direkt eintragen können.

Es gibt offene und geschlossene Fragen.

- Tragen Sie bei offenen Fragen Ihre Antworten ein. Bei geschlossenen Fragen stehen Ankreuzmöglichkeiten zur Verfügung
- Mit „**Frage nicht relevant**“ können Sie die für Sie nicht relevanten Fragen kenntlich machen.
- „**Anforderung erfüllt**“ kreuzen Sie an, wenn alle Anforderungen bezüglich der Fragestellung erfüllt sind.
- „**Handlungsbedarf**“ ist immer dann gegeben, wenn Sie Schwachstellen aufdecken, die behoben werden müssen.

Zu den Frageneigenschaften in der Kopfzeile

Basis/Norm

Hier wird die Herkunft der Frage eingegeben. Dies können z.B. die ISO xxx oder eigene unternehmensspezifische Fragentabellen sein.

Nummer

Beispiel: **04.2.1-01**

erste 3 Ziffern = Kapitel der Norm

letzte Ziffer = Zähler innerhalb dieses Kapitels

Prozess/Kapitel/Thema

Diese Felder enthalten die Angaben aus den Inhaltsverzeichnissen: 1. Überschrift/2. Überschrift/3. Überschrift

Hier sehen Sie ein Beispiel für eine Audit - Frage:

Fortlaufende Nummer
(Siehe Norm)

Prozess
(Hauptkapitel der Norm)

Vorgegebene Themen
(Normunterkapitel)

Kapitel
der Norm

Fragenkatalog "ISO IEC 27001:2024"

NUMSULT
BERATUNG UND SOFTWARE

Nummer	04.1-01	Basis/Norm	ISO IEC 27001:2024
Prozess	Kontext der Organisation	Thema	
Kapitel	Verstehen der Organisation und ihres Kontextes		

Frage Hat die Organisation externe und interne Themen bestimmt, die für ihren Zweck und ihre strategische Ausrichtung relevant sind und sich auf ihre Fähigkeit auswirken, die beabsichtigten Ergebnisse ihres Informationssicherheitsmanagementsystems zu erreichen? Frage nicht relevant ☐

Antwort Anforderung erfüllt ☐
Handlungsbedarf ☐

Nachweise

§§ / Hinweise 4 Kontext der Organisation
4.1 Verstehen der Organisation und ihres Kontextes

ANMERKUNG Die Themenbestimmung bezieht sich auf die Festlegung des internen und externen Kontextes des Unternehmens, wie in ISO 31000:2009 (5), 5.3, beschrieben.

Ggf. nützliche Hinweise (aus der Norm)

Inhalt / Kapitel der DIN ISO IEC 27001:2024

4 Kontext der Organisation

4.1 Verstehen der Organisation und ihres Kontextes

4.2 Verstehen der Erfordernisse und Erwartungen interessierter Parteien

4.3 Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystems

4.4 Informationssicherheitsmanagementsystems

5 Führung

5.1 Führung und Verpflichtung

5.2 Politik

5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation

6 Planung

6.1 Maßnahmen zum Umgang mit Risiken und Chancen

6.2 Informationssicherheitsziele und Planung zu deren Erreichung

7. Unterstützung

7.1 Ressourcen

7.2 Kompetenz

7.3 Bewusstsein

7.4 Kommunikation

7.5 Dokumentierte Information

8 Betrieb

8.1 Betriebliche Planung und Steuerung

8.2 Informationssicherheitsrisikobeurteilung

8.3 Informationssicherheitsrisikobehandlung

9. Bewertung der Leistung

9.1 Überwachung, Messung, Analyse und Bewertung

9.2 Internes Audit

9.3 Managementbewertung

10 Verbesserung

10.1 Nichtkonformität und Korrekturmaßnahmen

10.3 Fortlaufende Verbesserung

Anhang A (normativ)

Referenzmaßnahmenziele und -maßnahmen

Der vorliegende Fragenkatalog orientiert sich an den Anforderungen der DIN ISO IEC 27001:2024. Alle Anforderungen sind als Fragen formuliert.

Auf Vollständigkeit besteht kein Anspruch.

Rechtsansprüche aus dem Fragenkatalog sind nicht abzuleiten.

Alle Rechte, insbesondere das Recht der Vervielfältigung und Verbreitung sowie der Übersetzung, bleiben vorbehalten.