Leitfaden zum Personenzertifizierungsprogramm
ISO 27001 Lead Auditor (TÜV®) / Auditor (TÜV®)

Inhalt

Herausgeber und Eigentümer:
TÜV NORD CERT GmbH
Zertifizierungsstelle für Personen
Am TÜV 1
45307 Essen
E-Mail: TNCERT-PZ@tuev-nord.de / perszert@tuev-nord.de

Rev. 03
Status: freigegeben, BM 06.05.2025
Gültig ab: 06.05.2025

Leitfaden zum Personenzertifizierungsprogramm ISO 27001 Lead Auditor (TÜV®) / Auditor (TÜV®)

1. Allgemein

Informationssicherheit soll gewährleisten, dass die Vertraulichkeit, Verfügbarkeit und Integrität der verarbeiteten Daten, Informationen sowie darunterliegenden Systemen und Anwendungen in ausreichendem Maß sichergestellt werden. Um diese Ziele erreichen zu können, gibt die Norm ISO 27001 Anforderungen und Maßnahmenziele für die Implementierung, den Betrieb, die Aufrechterhaltung sowie fortlaufende Verbesserung eines Informationssicherheitsmanagementsystems (ISMS) vor. Dabei richten sich die Maßnahmen in diesem Informationssicherheitsmanagementsystems innerhalb einer Organisation nach deren Bedürfnissen und Zielen, den Sicherheitsanforderungen, den organisatorischen Abläufen sowie nach Größe und Struktur der Organisation.

Als Auditor im Bereich des Informationssicherheitsmanagementsystems (ISMS) ist umfassendes Know-How zum Thema Informationssicherheit, allgemein zu Managementsystemen und im Spezifischen zum Auditprozess notwendig. Auditoren müssen wissen, wie Sie ein ISMS-Audit planen, durchführen und nachbereiten. Sicherheitsrisiken und Schwachstellen sind einzuschätzen, die relevanten Standards im Kontext eines Audits zu interpretieren.

Lead Auditoren müssen darüber hinaus eine entsprechende Ausbildung sowie umfassende praktische Erfahrungen einbringen.

2. Anwendungsbereich

Dieser Leitfaden gilt für alle Zertifizierungsverfahren zum Erlangen des Personenzertifikats ISO 27001 Lead Auditor (TÜV) / Auditor (TÜV) im Rahmen von anerkannten Lehrgängen. Die Lehrgänge können sowohl als Präsenzschulung, Blended Learning als auch Online anerkannt sein.

3. Eingangsvoraussetzungen zur Teilnahme an der Prüfung und zur Zertifikatserteilung

	Ausbildung / ersatzweise Berufserfahrung für fehlende Ausbildung	Berufserfahrung	fachbezogene Tätigkeit / bestandene Prüfung	Schulung im Zertifizierungsgebiet	praktische Erfahrung oder Auditerfahrung
ISO 27001 Auditor (TÜV®)	abgeschlossene Berufsausbildung / gleichwertig ersatzweise 5 Jahre Berufserfahrung	mindestens zweijährige praktische Vollzeitberufserfahrung im Bereich der Informationstechnologie/Informationssicherheit	Verständnis der Grundlagen zur Informationssicherheit und Vorgehensweise nach ISO 27001, nachzuweisen durch Schulungsnachweis.	fachbezogener Lehrgang mit mind. 5 Tagen (36 UE*). und erfolgreichem Abschluss	Keine (Einstieg in die Auditorentätigkeit)
ISO 27001 Lead Auditor (TÜV®)	berufliche Ausbildung oder Schulung auf einem mit einer universitären Ausbildung vergleichbaren Niveau / gleichwertig ersatzweise 10 Jahre Berufserfahrung	mindestens vierjährige praktische Vollzeitberufserfahrung im Bereich der Informationstechnologie/Informationssicherheit	Verständnis der Grundlagen zur Informationssicherheit und Vorgehensweise nach ISO 27001, nachzuweisen durch Schulungsnachweis.	fachbezogener Lehrgang mit mind. 5 Tagen (36 UE*). und erfolgreichem Abschluss	mindestens 2 interne/externe Audits (nach ISO 27001) mit einer Auditdauer von mind. 4 Personentagen (vor Ort / remote)

Hinweise zur Tabelle:

- 1 UE entspricht einer Unterrichtseinheit von 45 Minuten.
- „Erfolgreicher Abschluss“ bedeutet das Bestehen der zum Lehrgang bzw. zur Zertifizierung gehörenden Abschlussprüfung gemäß diesem Personenzertifizierungsprogramm.

4. Prüfungsgegenstand und Prüfungshilfsmittel

Die Präsenzprüfungen nach Präsenzlehrgängen finden in der Regel am letzten Lehrgangstag oder am Tag nach dem letzten Lehrgangstag am Ort des Lehrgangs statt.

Für Online-Prüfungen werden entsprechende separate Termine angeboten.

Aktuelle technische Voraussetzungen finden sich unter folgendem Link:
https://www.tuev-nord.de/de/unternehmen/bildung/unternehmensangebote/personenzertifizierung/pruefungs-informationen/
Einige Tage vor der Prüfung bekommen die Kandidatinnen und Kandidaten eine E-Mail mit den Zugangsvoraussetzungen, Links, Installationsanleitungen, der geltenden Prüfungsordnung für Online-Prüfungen und speziellen Informationen zur jeweiligen Prüfung. Darüber hinaus werden mit der Mail die notwendigen Passwörter zur Prüfung mitgeteilt.

Es sind keine Unterlagen als Hilfsmittel zugelassen.

5. Prüfungsübersicht

Prüfung ISO 27001 Lead Auditor (TÜV®) / Auditor (TÜV®)	schriftlich:
Dauer:	90 min.
Anzahl der Prüfungsaufgaben gesamt:	31
MC-Aufgaben:	30
Offene Aufgaben / Dokumentenprüfung:	0 / 1
Höchstpunktzahl:	50
Mindestpunktzahl:	30 (60 %)

Details s. Anlagen

6. Schriftliche Präsenzprüfung

Die Prüfungsaufgaben werden in einem separaten Aufgabenheft vorgelegt. Die Lösungen zu jeder Prüfungsaufgabe werden auf den Seiten des Einzelberichts eingetragen. Nur die Antworten auf dem Einzelbericht werden gewertet.

Die MC-Aufgaben sind im Singular formuliert, sodass ein Rückschluss auf die Anzahl der richtigen Lösungen nicht möglich ist. Es muss unter mehreren vorgegebenen Auswahlmöglichkeiten durch Ankreuzen jede richtige Lösung ausgewählt werden. Es können eine, mehrere oder alle Auswahlmöglichkeiten richtig sein. Für jede richtig beantwortete MC-Aufgabe gibt es einen Punkt. Eine Aufgabe ist richtig gelöst, wenn die Kreuze an den richtigen Stellen der Tabelle gesetzt sind. Gar nicht oder nicht vollständig richtig gelöste Aufgaben erhalten null Punkte. Es gibt keine Bruchteile von Punkten.

Bei der Dokumentenprüfung wird im Rahmen eines Audits ein Auszug aus einem Managementhandbuch auf Nonkonformitäten zu den relevanten Normen und auf Mängel untersucht. Der Befund wird in freier schriftlicher Form mit Erläuterungen bzw. Begründungen niedergelegt. Die Feststellungen müssen formale und inhaltliche Mängel mit Normenbezug enthalten. Die weitere Vorgehensweise als Auditor muss beschrieben werden. Die Sachverhalte werden vom Prüfer mit einer Mustervorlage verglichen und bewertet.

7. Schriftliche Online-Prüfung

Die Prüfungsaufgaben erscheinen einzeln auf dem Bildschirm. Die Lösungen zu jeder Prüfungsaufgabe werden direkt zur Aufgabe eingetragen.

Die MC-Aufgaben sind im Singular formuliert, sodass ein Rückschluss auf die Anzahl der richtigen Lösungen nicht möglich ist. Es muss unter mehreren vorgegebenen Antwortmöglichkeiten durch Anklicken jede richtige markiert werden. Es können eine, mehrere oder alle Auswahlmöglichkeiten richtig sein.
Für jede richtig beantwortete MC-Aufgabe gibt es einen Punkt. Eine Aufgabe ist richtig gelöst, wenn die Markierungen an den richtigen Stellen gesetzt sind. Gar nicht oder nicht vollständig richtig gelöste Aufgaben erhalten null Punkte. Es gibt keine Bruchteile von Punkten. Die Aufgaben werden automatisch gewertet.

Bei der Dokumentenprüfung wird im Rahmen eines Audits ein Auszug aus einem Managementhandbuch auf Nonkonformitäten zu den relevanten Normen und auf Mängel untersucht. Der Befund wird in freier schriftlicher Form mit Erläuterungen bzw. Begründungen niedergelegt. Die Feststellungen enthalten formale und inhaltliche Mängel mit Normenbezug. Die weitere Vorgehensweise als Auditor muss beschrieben werden. Die Sachverhalte werden vom Prüfer mit einer Mustervorlage verglichen und bewertet.

8. Gesamtbewertung

Die Prüfung ISO 27001 Lead Auditor (TÜV) / Auditor (TÜV) ist bestanden, wenn die schriftliche Prüfung bestanden ist.

Es erfolgt keine Mitteilung über Einzelergebnisse oder Punktzahlen.

Maßgeblich für die Bewertung sind bei nachträglichen Korrekturen, die erreichten 60 %, nicht die auf- oder abgerundete Punktzahl.

9. Zertifizierungsentscheidung und Zertifikatserteilung

Bei bestandener Prüfung wird durch die TÜV NORD CERT ein Personenzertifikat ausgestellt.

Das Personenzertifikat enthält folgende Angaben:

a) Personalien der zertifizierten Person (Titel, Vorname, Name, Geburtsdatum, Geburtsort, ggf. mit Länderangabe)
b) Bezeichnung der Qualifikation
c) Prüfungsinhalte
d) Unterschrift der Fachleitung Personenzertifizierung
e) Ausstellungsdatum
f) Gültigkeit
g) Datum der Erstzertifizierung (bei Rezertifizierung)

Jedes Personenzertifikat erhält eine eindeutige Nummer:

44-01-A10201255-tt.mm.jjjj- DE02-32157 (Beispiel)

Die Nummer setzt sich wie folgt zusammen:

44	TÜV NORD CERT GmbH-Personenzertifizierung
01	Personenzertifikat
A10201255	A=Auditor, LA=Lead Auditor, Kurzkennzeichnung des Zertifizierungsgebietes
tt.mm.jjjj	Tag des Ablaufdatums
DE02	Kennzahl des Prüfungszentrums
32157	Prüfungszentrumsspezifische Kandidatenidentifikationsnummer

Das Personenzertifikat darf nur in der zur Verfügung gestellten Form verwendet werden. Es darf nicht nur teil- oder auszugsweise benutzt werden. Änderungen des Personenzertifikats dürfen nicht vorgenommen werden. Das Personenzertifikat darf nicht irreführend verwendet werden.

10. Rezertifizierung von Personenzertifikaten

Gültigkeit der Personenzertifikate

Das jeweilige Personenzertifikat ist 3 Jahre gültig.

Die Gültigkeit eines in der Erstzertifizierung erlangten Zertifikats beginnt mit dem Tag der positiven Zertifizierungsentscheidung und gilt bis 3 Jahre nach erfolgreicher Prüfung minus 1 Tag.

11. Anforderungen an die Rezertifizierung

Bei Ablauf der Gültigkeit des Personenzertifikats kann auf Antrag der zertifizierten Person eine Rezertifizierung erfolgen.

Hierzu muss die zertifizierte Person der Zertifizierungsstelle für Personen Folgendes nachweisen:

	Nachweis der Praktischen Tätigkeit	Schulung im Zertifizierungsgebiet	Nachweis der Audittätigkeit
ISO 27001 Auditor (TÜV®)	im zurückliegenden Zeitraum mind. 2 Jahre Tätigkeit im zertifizierten Bereich	jährlich mindestens eine 1-tägige fachspezifische Weiterbildung/Schulung/Konferenz/Erfahrungsaustausch, mit Schwerpunkt Informationstechnologie/Informationssicherheit.	Im Gültigkeitszeitraum mind. 2 externe/interne Audits (nach ISO 27001) mit einer Auditdauer von mind. 2 Personentagen (vor Ort / remote) als Auditor.
ISO 27001 Lead Auditor (TÜV®)	im zurückliegenden Zeitraum kontinuierliche Tätigkeit im zertifizierten Bereich	jährlich mindestens eine 1-tägige fachspezifische Weiterbildung/Schulung/Konferenz/Erfahrungsaustausch, mit Schwerpunkt Informationstechnologie/Informationssicherheit.	Im Gültigkeitszeitraum mind. 3 externe/interne Audits (nach ISO 27001) mit einer Auditdauer von mind. 3 Personentagen (vor Ort / remote) als Leadauditor.

Die Erfüllung der Anforderungen muss durch objektive Nachweise bestätigt werden.

Z. B. sind interne bzw. externe Audits bzgl. Zeitpunkt, Dauer, Art des Audits, Funktion der zertifizierten Person im Audit und Name der auditierten Organisation durch den Arbeitgeber oder Auditauftraggeber schriftlich zu bestätigen.

Bei Unklarheiten ist die Zertifizierungsstelle für Personen berechtigt, weitere Nachweise anzufordern und/oder die zertifizierte Person zu einem Gespräch einzuladen.

12. Mitgeltende Unterlagen

Allgemeine Prüfungsordnung (TÜV®)

Gebührenordnung für Prüfungen (TÜV®)

Zertifizierungsantrag

13. Anlage 1: Themen des Lehrgangs und Prüfungsmodalitäten der schriftlichen Prüfung ISO 27001 Lead Auditor (TÜV®) / Auditor (TÜV®)

Themenbereich und Lerninhalte	Anzahl der UE*	Anzahl der Aufgaben MC*/o*
1. Informationssicherheit (IS) • Relevante Standards, wie ISO/IEC 27001, ISO/IEC 27002 und weitere, ISO 31000, ISO 17021 und ISO 19011 • Cyber-Security-Gesetzgebung • Informationssicherheit und ihre Bedeutung • Einschätzen von Sicherheitslücken und -gefährdungen • Management von Informationssicherheitsrisiken • Auswahl von Sicherheitskontrollen und -maßnahmen • Einsatz von Software bzw. Tools zur Effektivitäts- und Effizienz-steigerung	**4 UE**	**4 MC**
2. Managementsystem (MS) • Informationssicherheit und Datenschutz in Managementsystemen (spezielle Kenntnisse) • Prozessorientierter Ansatz (PDCA: Plan-Do-Check-Act) • ISMS-Prozesslandschaft und -Regelungen • Implementierung, Betrieb, Überwachung, Überprüfung und Ver-besserung eines ISMS nach ISO/IEC 27001:2022 • Zusammenhänge und Wechselbeziehungen der ISO/IEC 2700x-Reihe mit ISO 31000 und ISO 22301 sowie rechtlicher Rahmen ei-nes ISMS und ISO 17021 und ISO 19011	**8 UE**	**8 MC**
3. Auditprozess (inkl. praktischer Übungen) (AP) • Auditprinzipien, -verfahren und -techniken • Auditvorbereitung, -nachbereitung und -durchführung • Aufgaben und Fähigkeiten eines Auditors (unter Beachtung ISO 27006) • Kommunikationstechniken und Auditarten • Anforderungen der ISO/IEC 27001:2022 im Kontext mit einem ISMS-Audit interpretieren • Nachweise sammeln und bewerten (Auditfeststellungen) • Management und Leiten eines ISO/IEC-27001:2022-Audit-Teams • Umgang mit schwierigen Auditsituationen, Auditrisiken • Normen- und Organisationsverständnis sowie gesetzlichen Anfor-derungen und Vorschriften	**24 UE**	**18 MC**
4. Abschlussprüfung		
schriftlich	**90 Minuten**	**30 MC** **1 Doku**

*

UE: Unterrichtseinheit à 45 Minuten
MC: Multiple-Choice-Aufgaben
o: offene Aufgaben

In der Tabelle „Themen des Lehrgangs und Prüfungsmodalitäten der schriftlichen Prüfung“ handelt es sich bei den Angaben der Unterrichtseinheiten um Richtwerte, die in Einzelfällen bedingt durch Zusammensetzung der Teilnehmenden, Vorkenntnisse und Teilnehmerzahl geringfügig abweichen können. Die hier dargestellte Reihenfolge der Themen muss nicht der Reihenfolge der Themen des Lehrgangs entsprechen.