

## Leitfaden zum Personenqualifizierungsprogramm **ISO 27001 Lead Auditor (TÜV®) / Auditor (TÜV®)**

### Inhalt

|     |                                                                                                                                    |   |
|-----|------------------------------------------------------------------------------------------------------------------------------------|---|
| 1.  | Allgemein                                                                                                                          | 2 |
| 2.  | Geltungsbereich                                                                                                                    | 2 |
| 3.  | Eingangsvoraussetzungen zur Teilnahme an der Prüfung und zur Zertifikatserteilung                                                  | 3 |
| 4.  | Prüfungsgegenstand und Prüfungshilfsmittel                                                                                         | 3 |
| 5.  | Prüfungsübersicht                                                                                                                  | 4 |
| 6.  | Schriftliche Präsenzprüfung                                                                                                        | 4 |
| 7.  | Schriftliche Online-Prüfung                                                                                                        | 4 |
| 8.  | Gesamtbewertung                                                                                                                    | 5 |
| 9.  | Zertifikatserteilung                                                                                                               | 5 |
| 10. | Rezertifizierung von Personenzertifikaten                                                                                          | 6 |
| 11. | Anforderungen an die Rezertifizierung                                                                                              | 6 |
| 12. | Mitgeltende Unterlagen                                                                                                             | 6 |
| 13. | Anlage 1: Themen des Lehrgangs und Prüfungsmodalitäten der schriftlichen Prüfung<br>ISO 27001 Lead Auditor (TÜV®) / Auditor (TÜV®) | 7 |

### Herausgeber und Eigentümer:

TÜV NORD CERT GmbH

Personenzertifizierungsstelle

Am TÜV 1

45307 Essen

E-Mail: [TNCERT-PZ@tuev-nord.de](mailto:TNCERT-PZ@tuev-nord.de) / [perscert@tuev-nord.de](mailto:perscert@tuev-nord.de)

Rev. 02

Status: freigegeben, BM 08.05.2024

# Leitfaden zum Personenqualifizierungsprogramm 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. Geltungsbereich

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 Präsenzschiung, Blended Learning als auch Online anerkannt sein.

### 3. Eingangsvoraussetzungen zur Teilnahme an der Prüfung und zur Zertifikatserteilung

|                                               | Ausbildung /<br>ersatzweise<br>Berufserfahrung<br>für fehlende<br>Ausbildung                                                                                                                         | Berufserfahrung                                                                                                                                          | fachbezogene<br>Tätigkeit / bestan-<br>dene Prüfung                                                                                                        | Schulung im<br>Zertifizie-<br>rungsgebiet                                                                        | Audittätigkeit                                                                                                                                               |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ISO 27001<br/>Auditor<br/>(TÜV)</b>        | abgeschlossene<br>Berufsausbildung<br>/ gleichwertig<br>ersatzweise 5<br>Jahre Berufser-<br>fahrung                                                                                                  | mindestens zwei-<br>jährige praktische<br>Vollzeitberufser-<br>fahrung im Be-<br>reich der Informa-<br>tionstechnolo-<br>gie/Informations-<br>sicherheit | Verständnis der<br>Grundlagen zur<br>Informationssi-<br>cherheit und<br>Vorgehensweise<br>nach ISO 27001,<br>nachzuweisen<br>durch Schulungs-<br>nachweis. | fachbezoge-<br>ner Lehr-<br>gang mit<br>mind. 5 Ta-<br>gen (36<br>UE*). und<br>erfolgrei-<br>chem Ab-<br>schluss | Keine<br><br>(Einstieg in<br>die Auditoren-<br>tätigkeit)                                                                                                    |
| <b>ISO 27001<br/>Lead Audi-<br/>tor (TÜV)</b> | berufliche Ausbil-<br>dung oder Schu-<br>lung auf einem<br>mit einer univer-<br>sitären Ausbil-<br>dung vergleich-<br>baren Niveau<br>/ gleichwertig<br>ersatzweise 10<br>Jahre Berufser-<br>fahrung | mindestens vier-<br>jährige praktische<br>Vollzeitberufser-<br>fahrung im Be-<br>reich der Informa-<br>tionstechnolo-<br>gie/Informations-<br>sicherheit | Verständnis der<br>Grundlagen zur<br>Informationssi-<br>cherheit und<br>Vorgehensweise<br>nach ISO 27001,<br>nachzuweisen<br>durch Schulungs-<br>nachweis. | fachbezoge-<br>ner Lehr-<br>gang mit<br>mind. 5 Ta-<br>gen (36<br>UE*). und<br>erfolgrei-<br>chem Ab-<br>schluss | mindestens 2<br>interne/ex-<br>terne Audits<br>(nach ISO<br>27001) mit<br>einer Audit-<br>dauer von<br>mind. 4 Per-<br>sonentagen<br>(vor Ort / re-<br>mote) |

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 Personenqualifizierungsprogramm.

### 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 entsprechend separate Termine angeboten.

Aktuelle technische Voraussetzungen finden sich unter folgendem Link:

<https://www.tuev-nord.de/de/unternehmen/bildung/personenzertifizierung/pruefungsinformationen-1/>

Einige Tage vor der Prüfung bekommen die Kandidaten eine E-Mail mit den Zugangsvoraussetzungen, Links, Installationsanleitungen, der geltenden Prüfungsordnung für Online-Prüfungen und speziellen Informationen zur jeweiligen Prüfung. Darüber hinaus werden den Kandidaten mit der E-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, so dass ein Rückschluss auf die Anzahl der richtigen Lösungen nicht möglich ist. Es muss unter mehreren vorgegebenen Lösungen durch Ankreuzen jede richtige ausgewählt werden. Es sind immer eine, mehrere oder alle richtigen Lösungen zu kennzeichnen. 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 werden zu jeder Prüfungsaufgabe direkt zur Aufgabe eingetragen.

Die MC-Aufgaben sind im Singular formuliert, sodass ein Rückschluss auf die Anzahl der richtigen Lösungen nicht möglich ist. Bei den MC-Aufgaben muss unter mehreren vorgegebenen Lösungen durch Anklicken jede richtige markiert werden. Es sind immer eine, mehrere oder alle richtige Lösungen zu kennzeichnen. 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 wird beschrieben. 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. Zertifikatserteilung

Dem Kandidaten wird bei bestandener Prüfung durch die TÜV NORD CERT ein Personenzertifikat ausgestellt.

Das Personenzertifikat enthält folgende Angaben:

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

Jedes Personenzertifikat erhält eine eindeutige Nummer:

**44-01-LA10201255-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, Produktnummer                   |
| tt.mm.jjjj | Tag des Ablaufdatums                                        |
| DE01/02    | 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 und Eindeutigkeit 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 dem Tag der erfolgreichen Prüfung minus 1 Tag.

## 11. Anforderungen an die Rezertifizierung

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

Hierzu muss der Zertifikatsinhaber der Personenzertifizierungsstelle Folgendes nachweisen:

|                                      | Nachweis der praktischen Tätigkeit                                              | Schulung im Zertifizierungsgebiet                                                                                                                                       | Nachweis der Audittätigkeit                                                                                                                               |
|--------------------------------------|---------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ISO 27001 Auditor (TÜV®)</b>      | im zurückliegenden Zeitraum min. 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.     |
| <b>ISO 27001 Lead Auditor (TÜV®)</b> | 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 des Antragstellers im Audit und Name der auditierten Organisation durch den Arbeitgeber oder Auditauftraggeber schriftlich zu bestätigen.

Bei Unklarheiten ist die Personenzertifizierungsstelle berechtigt, weitere Nachweise anzufordern und/oder den Zertifikatsinhaber 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®)**

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Anzahl der<br>UE* | Anzahl der<br>Aufgaben<br>MC*/o* |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|----------------------------------|
| <b>Themenbereich und Lerninhalte</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                   |                                  |
| <b>1. Informationssicherheit (IS)</b> <ul style="list-style-type: none"> <li>• Relevante Standards, wie ISO/IEC 27001, ISO/IEC 27002 und weitere, ISO 31000, ISO 17021 und ISO 19011</li> <li>• Cyber-Security-Gesetzgebung</li> <li>• Informationssicherheit und ihre Bedeutung</li> <li>• Einschätzen von Sicherheitslücken und -gefährdungen</li> <li>• Management von Informationssicherheitsrisiken</li> <li>• Auswahl von Sicherheitskontrollen und -maßnahmen</li> <li>• Einsatz von Software bzw. Tools zur Effektivitäts- und Effizienzsteigerung</li> </ul>                                                                                                                                                                                          | <b>4 UE</b>       | <b>4 MC</b>                      |
| <b>2. Managementsystem (MS)</b> <ul style="list-style-type: none"> <li>• Informationssicherheit und Datenschutz in Managementsystemen (spezielle Kenntnisse)</li> <li>• Prozessorientierter Ansatz (PDCA: Plan-Do-Check-Act)</li> <li>• ISMS-Prozesslandschaft und -Regelungen</li> <li>• Implementierung, Betrieb, Überwachung, Überprüfung und Verbesserung eines ISMS nach ISO/IEC 27001:2022</li> <li>• Zusammenhänge und Wechselbeziehungen der ISO/IEC 2700x-Reihe mit ISO 31000 und ISO 22301 sowie rechtlicher Rahmen eines ISMS und ISO 17021 und ISO 19011</li> </ul>                                                                                                                                                                                | <b>8 UE</b>       | <b>8 MC</b>                      |
| <b>3. Auditprozess (incl. praktischer Übungen) (AP)</b> <ul style="list-style-type: none"> <li>• Auditprinzipien, -verfahren und -techniken</li> <li>• Auditvorbereitung, -nachbereitung und -durchführung</li> <li>• Aufgaben und Fähigkeiten eines Auditors (unter Beachtung ISO 27006)</li> <li>• Kommunikationstechniken und Auditarten</li> <li>• Anforderungen der ISO/IEC 27001:2022 im Kontext mit einem ISMS-Audit interpretieren</li> <li>• Nachweise sammeln und bewerten (Auditfeststellungen)</li> <li>• Management und Leiten eines ISO/IEC-27001:2022-Audit-Teams</li> <li>• Umgang mit schwierigen Auditsituationen, Auditrisiken</li> <li>• Normen- und Organisationsverständnis sowie gesetzlichen Anforderungen und Vorschriften</li> </ul> | <b>24 UE</b>      | <b>18 MC</b>                     |
| <b>4. Abschlussprüfung</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                   |                                  |
| <b>schriftlich</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | <b>90 Minuten</b> | <b>30 MC<br/>1 Doku</b>          |

\*

UE: Unterrichtseinheit à 45 Minuten

MC: Multiple-Choice-Aufgaben

Doku: Dokumentenprüfung

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 Teilnehmer, Vorkenntnisse und Teilnehmerzahl geringfügig abweichen können. Die hier dargestellte Reihenfolge der Themen muss nicht der Reihenfolge der Themen des Lehrgangs entsprechen.