Leitfaden zum Personenqualifizierungsprogramm

Information Security Personal (TÜV®)

Inhalt

Herausgeber und Eigentümer:
TÜV NORD CERT GmbH
Personenzertifizierungsstelle
Langemarckstr. 20
45141 Essen
E Mail: TNCERT-PZ@tuev-nord.de / perszert@tuev-nord.de

Rev. 02
Status: freigegeben, BM 18.04.2018

Leitfaden zum Personenqualifizierungsprogramm Information Security Personal (TÜV®)

1. Allgemein

Die Informationssicherheit hat zum Ziel die Verarbeitung, Speicherung und Kommunikation von Informationen so zu gestalten, dass die Vertraulichkeit, Verfügbarkeit und Integrität der Informationen und Systeme in ausreichendem Maß sichergestellt wird. Die Herstellung der Informationssicherheit in Unternehmen und Einrichtungen ist Gemeinschaftsaufgabe aller im Betrieb beschäftigten Mitarbeiter. Der Unternehmer bzw. der Leiter einer Organisation trägt jedoch die Verantwortung für die Erfüllung dieser Aufgabe in seinem Bereich. Die vielfältigen und umfangreichen Aufgaben machen es erforderlich, zur Unterstützung der oder des Verantwortlichen innerhalb der Sicherheitsorganisation des Betriebes einen oder mehrere Verantwortliche zu bestellen, dem oder denen diese Aufgaben in wesentlichen Teilen übertragen werden.

Der Information Security Officer (ISO) muss mit den Grundlagen und Normen des Informationssicherheitsmanagements vertraut sein und er muss die Prinzipien, Methoden und Verfahren des Informationssicherheitsmanagements entsprechend den Belangen der Wirtschaft beherrschen. Er muss die Kompetenz besitzen, um beim Aufbau und bei der Aufrechterhaltung eines Informationssicherheitsmanagements Unterstützung zu leisten.

Der Chief Information Security Officer (CISO) muss die Qualifikation des ISO haben und kompetent sein, ein Informationssicherheitsmanagementsystem aufzubauen und anzuwenden. Er kann 1st- und 2nd-Party Audits organisieren und ein Informationssicherheitsmanagementsystem im Rahmen eines Verbesserungsprozesses weiterentwickeln.

2. Geltungsbereich

Dieser Leitfaden gilt für alle Zertifizierungsverfahren zum Erlangen des Zertifikats Information Security Officer (TÜV®) bzw. Chief Information Security Officer (TÜV®) im Rahmen von anerkannten Lehrgängen.

3. Eingangsvoraussetzungen zur Teilnahme an der Prüfung und zur Zertifikatserteilung

	Ausbildung / ersatzweise Berufserfahrung für fehlende Ausbildung:	Berufserfahrung	bestandene Prüfung	Schulung im Zertifizierungsgebiet	praktische Erfahrung oder Auditerfahrung
Information Security Officer	abgeschlossene Berufsausbildung oder höherwertig, ersatzweise drei Jahre Berufserfahrung	3 Jahre		fachbezogener Lehrgang mit mind. 32 UE*. und erfolgreichem Abschluss	1 Jahr im Bereich der Informationssicherheit
Chief Information Security Officer	abgeschlossene Berufsausbildung oder höherwertig, ersatzweise drei Jahre Berufserfahrung	3 Jahre	zum Information Security Officer	fachbezogener Lehrgang mit mind. 32 UE*. und erfolgreichem Abschluss.	1 Jahr im Bereich der Informationssicherheit

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 Zertifizierungsprogramm.

4. Prüfungsgegenstand und Prüfungshilfsmittel

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

Als Hilfsmittel sind Lehrgangsunterlagen, Lehrbücher, die relevanten normativen Dokumente, eigene Aufzeichnungen und bei Bedarf Taschenrechner zugelassen. Weitere elektronische Hilfsmittel sind nicht zulässig.

5. Prüfungsübersicht

Prüfung Information Security Officer	schriftlich:	praktisch
Dauer:	75 min.	
Anzahl der Prüfungsaufgaben gesamt:	32	
MC-Aufgaben:	30	
Offene Aufgaben:	2	
Höchstpunktzahl:	40	
Mindestpunktzahl:	24 (60 %)	
Prüfung Chief Information Security Officer	**schriftlich:**	**praktisch**
Dauer:	75 min.	4 Wochen
Anzahl der Prüfungsaufgaben gesamt:	32	
MC-Aufgaben:	30	
Offene Aufgaben / Dokumentenprüfung:	2 / 0	
Höchstpunktzahl:	38	50
Mindestpunktzahl:	23 (60 %)	30

Details s. Anlagen

6. Schriftliche Prüfung

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

Bei den MC-Aufgaben wird unter mehreren vorgegebenen Lösungen durch Ankreuzen jede richtige ausgewählt. 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 den offenen Aufgaben formuliert der Kandidat die Antworten in freier, knapper Form und schreibt diese jeweils in das Feld im Einzelbericht. Für jede vollständig und richtig beantwortete Aufgabe gibt es vier (CISO) bzw. fünf (ISO) Punkte. Eine teilweise richtige Lösung erhält Teilpunkte im Verhältnis zur richtigen Gesamtlösung. Hierbei ist eine Punktstückelung von halben (½) Punkten möglich.

7. Praktische Prüfung

Die praktische Prüfung erfolgt in Form der Erstellung einer Fallstudie. Die Aufgabenstellung für die praktische Prüfung wird direkt im Anschluss der schriftlichen Prüfung ausgegeben. Für die Erstellung der Fallstudie hat der Kandidat vier Wochen Zeit (24 Werktage). Details s. Anlage 2b.

8. Gesamtbewertung

Die Prüfung Information Security Officer (TÜV®) ist bestanden, wenn die schriftliche Prüfung bestanden ist.

Die Prüfung Chief Information Security Officer (TÜV®) ist bestanden, wenn die schriftliche und praktische Prüfung bestanden sind.

Es erfolgt keine Mitteilung über Einzel- oder Punkteergebnisse.

9. Zertifikaterteilung

Dem Kandidaten wird bei bestandener Prüfung und Erfüllung der weiteren Anforderungen durch die TÜV NORD CERT ein Zertifikat ausgestellt.

Das Zertifikat enthält folgende Angaben:

a) Personalien des Kandidaten (Titel, Vorname, Name, Geburtsdatum
Geburtsort, ggf. mit Länderangabe)
b) Bezeichnung der Qualifikation
c) Prüfungsinhalte
d) Ausbildungsträger
e) Unterschrift der Fachleitung Personenzertifizierung
f) Ausstellungsdatum

Jedes Zertifikat erhält eine eindeutige Nummer:

44-02-IT-ISO-tt.mm.jj- DE02-32157 (Beispiel)

Die Nummer setzt sich wie folgt zusammen:

44	TÜV NORD CERT GmbH-Personenzertifizierung
02	Zertifikat
IT-ISO	Kurzkennzeichnung des Zertifizierungsgebietes
tt.mm.jjj	Tag der Prüfung
DE02	Kennzahl des Prüfungszentrums
032567	Prüfungszentrumsspezifische Kandidatenidentifikationsnummer

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

10. Mitgeltende Unterlagen

Allgemeine Prüfungsordnung (TÜV®)

Gebührenordnung für Prüfungen (TÜV®)

Anlagen

11. Anlage 1:Themen des Lehrgangs und Prüfungsmodalitäten der schriftlichen Prüfung Information Security Officer (TÜV®)

Themenbereich und Lerninhalte	Anzahl der UE*	Anzahl der Aufgaben MC*/o*
1. Grundlagen der Informationssicherheit (IM) • Informationssicherheit: Begriffe, Spektrum, Abgrenzung Notwendigkeit und strategische Bedeutung von IS Anforderungen an IS IS-Strategie Standards der Informationssicherheit • Aktuelle Themen und Gefährdungslage Gefahrenpotential Bedrohungen und ihre Einschätzung Angriffe, Angriffsziele und -methoden Schwachstellen • Anforderungs- und Risikomanagement Grundbegriffe und Klassifizierung Typische IT-Sicherheitsrisiken Risikoanalyse und -strategien Der Prozess „Risikomanagement“ Schutzbedarfsfeststellung	**5 UE**	**5 MC**
2. Informationssicherheitsmanagement (IS) • Aufgaben und Rollen in der Sicherheitsorganisation Ebenen der Sicherheitsorganisation Projekt- und Konfliktmanagement • Der Information Security Officer Notwendigkeit des ISO Stellung und Aufgaben des ISO Anforderungsprofil	**3 UE**	**4 MC8 MC**
3. IS-Management nach ISO 27001 (ISO) • Einführung in die ISO 27001 • Aufbau, Inhalt und Methodik • Umsetzungshilfen	**6 UE**	**6 MC**
4. IS-Management nach BSI IT-Grundschutz (GS) Vorgehensweisen nach BSI 200-x Strukturanalyse Schutzbedarfsfeststellung Risikoanalyse nach BSI 200-3 Auswertung der Ergebnisse Schichtenmodell und Bausteine IT-GS-Kompendium Realisierungsplanung	**6 UE**	**6 MC**

5. Übergreifende Informationssicherheitskonzepte (KON) • Aufbau der ISMS Dokumentation • Basis-Sicherheitskonzepte Datensicherung und Archivierung Schutz vor Schadprogrammen Incident Management User- und Berechtigungsmanagement • Infrastruktursicherheit Zutrittskontrollen, Sicherheitszonen, bauliche Sicherheit, Schutz vor Brand, Wasser, Einbruch etc. Überblick: IT-GS Maßnahmen in der Schicht „Sicherheit der Infrastruktur“	**5 UE**	**5 MC**
6. Kryptographische Verfahren, Sicherheit im Netzwerk, System- und Anwendungssicherheit (IT) • SystemsicherheitSystemsicherheit Server-Sicherheit Client-Sicherheit Speichersysteme und Speichernetze Virtualisierung • Kryptographische Verfahren Grundlagen der Verschlüsselung Signaturen und Hash-Funktionen Key Management und Zertifikate Public Key Infrastructure (PKI) • Sicherheitsaspekte der TCP/IP-Kommunikation ISO/OSI-Referenzmodell IP-Protokollsuite Sicherheitslecks der IP-Protokolle IP-Netzdienste und Sicherheit Analysemethoden und -tools • Anwendungssicherheit E-Mail	**7 UE**	**4 MC**
6. Themenübergreifendes Verständnis		**2 o**
7. Abschlussprüfung		**30 MC/2 o**
schriftlich	**75 min.**	

12. Anlage 2a:Themen des Lehrgangs und Prüfungsmodalitäten der schriftlichen Prüfung Chief Information Security Officer (TÜV®)

Themenbereich und Lerninhalte	Anzahl der UE*	Anzahl der Aufgaben MC*/o*
1. Steuerung der Informationssicherheit (SIS) • Die Rolle des CISO im IS-Management • Zielsetzung • Steuerungsinstrumente • Indikatoren • Kontrolle, Überwachung • Management-Bewertung des ISMS und kontinuierliche Verbesserung (KVP) • Sicherheitsvorfallbehandlung im Rahmen der kontinuierlichen Verbesserung	**5 UE**	**5 MC**

2. Risikomanagement (RM)
• Standards und Methoden
  • ISO 27005
  • ISO31000
  • BSI 100-3
  • FMEA
• Einbindung in das unternehmensweite Risikomanagement
• Übung zur Erstellung einer Risikoanalyse:
  • Ermittlung von Bedrohungsszenarien und Schwachstellen für ein gegebenes Asset (Informationswert)
  • Bewertung des Risikos für:
  • Vertraulichkeit
  • Verfügbarkeit und
  • Integrität des Assets
  • Ermittlung eines Risikowertes unter Anwendung der ISO 27005
• Ableitung von Handlungsempfehlungen zur Risikobehandlung
	4 UE	**4 MC**

3. Personelle Aspekte der Informationssicherheit (PA)
• Der Personalprozess nach ISO 27001, A.8
  • Personalauswahl, Vertrauenswürdigkeit
  • Einstellung
  • Rollenwechsel und
  • Ausscheiden von Mitarbeitern
• Sensibilisierung für Informationssicherheit, Aufrechterhaltung der Sensibilisierung
• Assetverwaltung im Personalprozess
• Umgang mit organisationseigenen Assets
	2 UE	**3 MC**

4. Auslagerung von Prozessen und Diensten (APD)
• Grundsätzliche Erwägungen zur Auslagerung von Diensten
• Fallunterscheidungen
  • Outtasking
  • Outsourcing
  • Cloud-Dienstleistungen
	3 UE	**3 MC**

5. Informationssicherheit im Kontext weiterer, relevanter Standards (RS) • ISO 27000 Familie • BSI-100 Familie • ITIL • CoBit • ISF: The Standard • Common Criteria (ISO 15408) • FIPS (Federal Information Processing Standard) • ISO 9001 IS-Anforderungen aus dem Qualitätsmanagement	**2 UE**	**2 MC**

6. Business Continuity Management (BCM)
• Grundlagen des Notfallmanagements
• BCM als Organisationsaufgabe, Verzahnung mit dem Informationssicherheitsmanagement
• Relevante Standards des Notfallmanagements
  • ISO 22301
  • BSI 100-4
• Notfallorganisation
• Testen von Notfallplänen
	4 UE	**4 MC**

7. Auditierung (AUD)
• Planung eines internen Auditprogramms (ISO 19011)
  • Methoden der internen Auditierung
  • Risikoorientierung
  • Dokumentation und Aufzeichnungen
• Organisation externer Audits
  • Die Rolle des CISO bei der Organisation und Durchführung externer Audits
  • Anforderungen des Auditteams und organisatorische Rahmenbedingungen
	4 UE	**4 MC**

8. Compliance Aspekte der Informationssicherheit (CIS)
• Rechtsgrundlagen der Informationssicherheit und Compliance
• Verantwortung für die IS:
  • Pflichten der Geschäftsleitung
  • Haftung der Geschäftsleitung
• Der Chief Information Security Officer:
  • Rolle
  • Anforderungen
  • Haftung
  • Pflichten
• Datenschutz
• IS-Management
• Compliance-Management
• Anforderungsmanagement
	8 UE	**5 MC**

9. Themenübergreifendes Verständnis		**2 o**
6. Abschlussprüfung		**30 MC/2 o**
schriftlich	**75 min.**	
praktisch	**4 Wochen**	

*

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

13. Anlage 2b:Themen und Prüfungsmodalitäten für die praktische Prüfung Chief Information Security Officer (TÜV®): Erstellung einer Fallstudie

In der praktischen Prüfung stellt der Kandidat sein Fachwissen und seine Methodik in Form einer schriftlichen Fallstudie dar. Hierbei sind konkrete Aufgabestellungen aus dem Arbeitsumfeld des Kandidaten zu bearbeiten. Die Bearbeitungszeit beträgt vier Wochen (24 Werktage). Der Umfang der eingereichten Arbeit sollte ca. 15 Seiten umfassen, jedoch 20 Seiten nicht überschreiten.

Dem Kandidaten wird eine Aufgabestellung zu den Themen

- Informationssicherheit im Unternehmen
- Übergreifende IT-Sicherheitskonzeption
- Sicherheit von IT-Systemen und Anwendungen

vorgelegt, die von ihm eigenständig zu bearbeiten ist.

Es werden bei der Prüfung der Fallstudie die Kriterien

- Beantwortung der Aufgabestellung und Erreichung der sicherheitstechnischen Zielstellung mit maximal 15 Punkten (30 %),
- Inhaltliche Richtigkeit der Aussagen bezüglich formaler Regelungen, Themenbezug und logische Stringenz, Darstellung des Sachverhalts mit maximal 15 Punkten (30 %),
- Fachliche Schlüssigkeit und Struktur mit maximal 10 Punkten (20 %) und
- Niveau und Anschaulichkeit der Darstellung (Grammatik, Grafiken, Tabellen, Verweise, Zitate) mit maximal 10 Punkten (20 %) bewertet.