Leitfaden zum Personenqualifizierungsprogramm

IT-Grundschutz-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. 00
Status: freigegeben, 24.06.2019 BM

Leitfaden zum Personenqualifizierungsprogramm IT-Grundschutz-Personal (TÜV®)

1. Allgemein

Informationen sind wesentliche Werte für Unternehmen und Behörden. Sie erfordern es, in angemessener Art und Weise geschützt zu werden. Innerhalb von Betriebs- und Geschäftsprozessen werden diese Informationen zumeist mit Hilfe der Informationstechnik verarbeitet, gespeichert bzw. übertragen. Eine sichere und zuverlässige Informationstechnik ist daher ebenso wie der vertrauenswürdige Umgang mit Informationen unerlässlich.

Über die Funktion und Aufrechterhaltung des Betriebs und wesentlicher Geschäftsprozesse hinaus ist die Vertraulichkeit von Informationen (z. B. Datenschutz bei Gesundheitsdaten) und deren Integrität (Korrektheit) von hoher Bedeutung. Unzureichend geschützte Informationen stellen einen Risikofaktor dar, der im Schadensfall existenzbedrohend sein kann.

Ein effektives und nachhaltiges Management der Informationssicherheit wirkt risikomindernd und gewährleistet die Informationssicherheit sowohl in Unternehmen als auch in Behörden. Dazu ist ein koordinierter Sicherheitsprozess zu etablieren und ein Sicherheitskonzept zu erstellen. Hierbei ist es zweckmäßig, auf anerkannte Standards wie den IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI) aufzubauen und damit vorhandene Erfahrung und Praxiswissen zu nutzen.

Mit der Modernisierung des IT-Grundschutzes sind die Standards nach BSI 200-x nicht nur für die öffentliche Verwaltung und Behörden, sondern auch zunehmend für die Industrie und freie Wirtschaft interessant geworden. Damit einhergehend wächst die Anzahl gefragter Personen mit entsprechender Fachexpertise.

IT-Grundschutz-Personal unterstützt Behörden und Unternehmen bei der Entwicklung von Sicherheitskonzepten und begleiten die Einführung eines Managementsystems für Informationssicherheit (ISMS). In Zusammenarbeit mit den verantwortlichen Mitarbeitern werden Konzepte definiert und Maßnahmen nach IT-Grundschutz benannt und entwickelt. Zertifiziertes IT-Grundschutz-Personal können die Behörden und Unternehmen zudem dabei unterstützen, ein ISO 27001 Audit auf Basis von IT-Grundschutz vorzubereiten.

2. Geltungsbereich

Dieser Leitfaden gilt für alle Zertifizierungsverfahren zum Erlangen des Zertifikats IT-Grundschutz-Praktiker (TÜV®) im Rahmen von anerkannten Lehrgängen, sowie der Ausbildung zum IT-Grundschutz- Berater zur Prüfungszulassung beim BSI.

3. Eingangsvoraussetzungen zur Teilnahme an der Prüfung und zur Zertifikatserteilung

	Ausbildung / ersatzweise Berufserfahrung für fehlende Ausbildung	fachbezogene Tätigkeit/ bestandene Prüfung	Schulung im Zertifizierungsgebiet	praktische Erfahrung oder Auditerfahrung
IT-Grundschutz-Praktiker	abgeschlossene Berufsausbildung oder vergleichbarer Abschluss		fachbezogener Lehrgang mit mind. 24 UE*. und erfolgreichem Abschluss	2 Jahre Berufserfahrung auf dem Gebiet der Informationstechnologie oder in einem sonstigen IT- oder sicherheitsrelevanten Umfeld, alternativ 5 Jahre Berufserfahrung ohne Spezifikation
IT-Grundschutz-Berater	abgeschlossene Berufsausbildung oder vergleichbarer Abschluss	erfolgreich abgelegte Prüfung zum IT-Grundschutzpraktiker	fachbezogener Lehrgang mit mind. 16 UE*.	2 Jahre Berufserfahrung auf dem Gebiet der Informationstechnologie oder in einem sonstigen IT- oder sicherheitsrelevanten Umfeld, alternativ 5 Jahre Berufserfahrung ohne Spezifikation

IT-Grundschutz-Praktiker können im nächsten Schritt an einer Aufbauschulung teilnehmen, um eine Personenzertifizierung zum IT-Grundschutz-Berater zu erhalten. Neben der Aufbauschulung müssen Teilnehmer auch weitere Berufs- und Praxiserfahrung nachweisen. Nach der Teilnahme an der Aufbauschulung besteht die Möglichkeit, sich für die Prüfung zum IT-Grundschutz-Berater beim Bundesamt für Sicherheit in der Informationstechnik (BSI) anzumelden.

Hinweise zur Tabelle:

- 1 UE entspricht einer Unterrichtseinheit von 60 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.

Es sind keine Hilfsmittel zugelassen.

5. Prüfungsübersicht

Prüfung zum IT-Grundschutz-Praktiker	schriftlich:
Dauer:	60 min.
Anzahl der Prüfungsaufgaben gesamt:	50
MC-Aufgaben:	50
Höchstpunktzahl:	50
Mindestpunktzahl:	30 (60 %)

Details s. Anlage

Prüfung zum IT-Grundschutz-Berater
Nach Teilnahme an der Aufbauschulung können sich Interessierte für die Prüfung zum IT-Grundschutz-Berater beim Bundesamt für Sicherheit in der Informationstechnik (BSI) anmelden. Wurde die Prüfung erfolgreich absolviert und alle erforderlichen Nachweise erbracht, erfolgt die Personenzertifizierung. Link: https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Personenzertifizierung/GS-Berater/GS-Berater_node.html Das Bundesamt für Sicherheit in der Informationstechnik (BSI) legt die Prüfungs- und Zertifizierungsbedingungen für IT-Grundschutz-Berater fest. Offizielle Angaben hierzu lagen bei Freigabe des Leitfadens noch nicht vor und können ggf. beim BSI erfragt werden.

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.

7. Gesamtbewertung

Die Prüfung IT-Grundschutz-Praktiker (TÜV®) ist bestanden, wenn die schriftliche Prüfung bestanden ist.

Es erfolgt keine Mitteilung über Einzel- oder Punkteergebnisse.

8. 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-BSI-tt.mm.jjjj- DE02-32157 (Beispiel)

Die Nummer setzt sich wie folgt zusammen:

44	TÜV NORD CERT GmbH-Personenzertifizierung
02	Zertifikat
BSI	Kurzkennzeichnung des Zertifizierungsgebietes
tt.mm.jjjj	Tag der Prüfung
DE02	Kennzahl des Prüfungszentrums
32157	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.

9. Wiederholung der Prüfung

Abweichend zu Punkt 10 der allgemeinen Prüfungsordnung gilt für die Prüfungswiederholung Folgendes:

Im Falle des Nichtbestehens kann die Prüfung in Form einer einmaligen Nachprüfung wiederholt werden.

Wird die Prüfung zum zweiten Mal nicht bestanden, muss eine erneute Schulung absolviert werden.

Die Anmeldung hat innerhalb eines Jahres zu erfolgen. Ausnahmen bedürfen der Zustimmung der Personenzertifizierungsstelle.

Termine für Wiederholungsprüfungen werden vom Prüfungszentrum in Abstimmung mit Bildungsträger und Personenzertifizierungsstelle bedarfsorientiert festgelegt.

10. Mitgeltende Unterlagen

Allgemeine Prüfungsordnung (TÜV®)

Gebührenordnung für Prüfungen (TÜV®)

Anlagen

11. Anlage 1:Themen des Lehrgangs und Prüfungsmodalitäten der schriftlichen Prüfung IT-Grundschutz-Praktiker (TÜV®)

Themenbereich und Lerninhalte	Anzahl der UE*	Anzahl der Aufgaben MC*/o*
1. Einführung und Grundlagen der IT-Sicherheit und rechtlicher Rahmenbedingungen (I + II) • Begriffe (Arten und Wichtigkeit von Informationen, Aspekte der Integrität, Verfügbarkeit, Vertraulichkeit usw.) • Unterschied zwischen IT und OT sowie Security und Safety • Gesetzliche Grundlagen (BSIG, IT-SiG usw.)	**2 UE**	**2 MC**
2. Normen und Standards der Informationssicherheit (I) • Überblick, Zweck und Struktur über relevante Normen und Richtlinien z.B. ISO 2700x usw.) • Cobit, ITIL usw. • IT-Grundschutz-Kompendium • Branchenspezifische Sicherheitsstandards und IT-Grundschutz-Profile	**2 UE**	**2 MC**
3. Einführung It-Grundschutz (II) • IT-Grundschutz – Bestandteile • Sicherheitsprozess • Rollen, Verantwortung und Aufgaben (Leitung, Informationssicherheitsbeauftragte, ICS-Informationssicherheitsbeauftragte, Information-Management-Team usw.) • Sicherheitskonzept • Leitlinie erstellen	**2 UE**	**2 MC**
4. IT-Grundschutz-Vorgehensweise (Überblick) (I + II) • Leitfragen zur IT-Grundschutz-Absicherung • Basis-Anforderungen • Standard-Anforderungen • Anforderungen für den erhöhten Schutzbedarf • Wahl der Vorgehensweise am Praxisbeispiel	**1 UE** **1 UE**	**1 MC**
5. Kompendium (Überblick) (I + II) • Aufbau und Anwendung des Kompendiums • ISMS (Informationssicherheitsmanagement) • Prozess-Bausteine • System-Bausteine • Umsetzungshinweise • Erstellung eines Bausteins	**1 UE**	**1 MC**

6. Umsetzung der IT-Grundschutz-Vorgehensweise (II) • Netzplan erstellen • Geschäftsprozess und zugehörige Anwendungen sowie IT-Systeme, Räume erfassen • Schutzbedarfskategorien, Vorgehen und Vererbung • Modellierung gemäß IT-Grundschutz (Vorgehen, Dokumentation, Anforderungen anpassen)	**1 UE**	**5 MC**
7. IT-Grundschutz-Check (II) • Was wird geprüft? • Vorbereitung und Durchführung • IT-Grundschutz-Check dokumentieren • Entscheidungskriterien • Beispiel für die Dokumentation • Beispiel für die Durchführung	**1 UE** **1 UE** **1 UE**	**5 MC**
8. Risikoanalyse (II) • Die elementaren Gefährdungen sowie andere • Gefährdungsübersichten • Vorgehen bei der Risikobewertung und Risikobehandlung • Beispiel für die Risikobewertung	**1 UE** **1 UE**	**5 MC**
9. Umsetzungsplanung (II) • Maßnahmenplan entwickeln und dokumentieren, Aufwand schätzen, Umsetzungsreihenfolge und Verantwortlichkeit bestimmen, begleitende Maßnahmen planen • Aufwände schätzen	**1 UE**	**5 MC**
10. Aufrechterhaltung und kontinuierliche Verbesserung (II) • Leitfragen für die Überprüfung • Überprüfungsverfahren • Kennzahlen • Reifegradmodelle • Beispiel für Anwendung kontinuierlicher Verbesserungsprozess (KVP)	**1 UE**	**5 MC**
11. Zertifizierung und Erwerb des IT-Grundschutz-Zertifikats auf Basis von ISO 27001 (I) • Arten von Audits z.B. Prozess und Produkt Audit • Grundsätze der Auditierung 1st, 2nd, 3rdParty Auditoren • Modell der Akkreditierung und Zertifizierung • Ablauf des BSI-Zertifizierungsprozesses	**1 UE**	**5 MC**
12. IT-Grundschutzprofile (I + II) • Aufbau eines Profils • Erstellung eines Profils • Anwendung bzw. Nutzungsmöglichkeit veröffentlichter Profile	**1 UE**	**2 MC**

13. Vorbereitung auf ein Audit (II) • Planung und Vorbereitung (Rollen und Verantwortlichkeiten, Unabhängigkeit, Auditplan, Checklisten, Kombination von Audits, Synergieeffekte) • Auditprozess-Aktivitäten (Zusammenstellung eines Team, Dokumente vorbereiten, Planung des Vor-Ort-Audits, Umgang mit Nichtkonformitäten) • Berichtswesen (Inhalt und Aufbau eines Berichtes, Genehmigung und Verteilung, Aufbewahrung und Vertraulichkeit) • Folgemaßnahmen (Vor-Audit, Wiederholungsaudit, Überwachung, Korrekturmaßnahmen) • Qualifikation von Auditoren (Berufserfahrung, Schulung, persönliche Eigenschaften, Aufrechterhaltung der Qualifikation)	**1 UE**	**5 MC**
14. Notfallmanagement (II) • Überblick über den BSI-Standard 100-4 • Notfallmanagement Prozess (initiieren, analysieren, einführen, üben, verbessern) • Business-Impact-Analyse (BIA) • Notfälle bewältigen (Umgang mit Sicherheitsvorfällen) • Vorgehensweise bei Sicherheitsvorfall und Meldeweg erarbeiten	**2 UE** **1 UE**	**5 MC**
15. Zusammenfassung und Prüfungsvorbereitung (I)	**1 UE**	
16. Abschlussprüfung		
schriftlich		**50 MC**
	24 UE	

*

UE: Unterrichtseinheit à 60 Minuten

MC: Multiple Choice Aufgaben

Es wird je nach Qualifikation zwischen den folgenden Vertiefungsstufen unterschieden:

I: „Kenntnisse, die verstanden sind und erläutert werden können“. (Reproduktion)

II: „Kenntnisse und Fertigkeiten, die auf eigene Prozesse und Komponenten angewendet und umgesetzt werden können“. (Transfer)

III: „Analysen und Methoden, die auf andere Institutionen, Prozesse und Komponenten angewendet und bewertet werden können“. (Reflexion)

12. Anlage 2: Themen des Lehrgangs IT-Grundschutz-Berater zur möglichen Prüfung beim Bundesamt für Sicherheit in der Informationstechnik (BSI)

Themenbereich und Lerninhalte	Anzahl der UE*	Anzahl der Aufgaben MC*/o*
1. Einführung und Grundlagen der IT-Sicherheit und rechtlicher Rahmenbedingungen	0 UE	
2. Normen und Standards der Informationssicherheit (II + III) • Überblick, Zweck und Struktur über relevante Normen und Richtlinien z.B. ISO 2700x usw.) • Cobit, ITIL usw. • IT-Grundschutz-Kompendium • Branchenspezifische Sicherheitsstandards und IT-Grundschutz-Profile	**1 UE**	
3. Einführung It-Grundschutz	0 UE	
4. IT-Grundschutz-Vorgehensweise (Überblick) (III) • Leitfragen zur IT-Grundschutz-Absicherung • Basis-Anforderungen • Standard-Anforderungen • Anforderungen für den erhöhten Schutzbedarf • Wahl der Vorgehensweise am Praxisbeispiel	**1 UE** **1 UE**	
5. Kompendium (Überblick) (I + II) • Aufbau und Anwendung des Kompendiums • ISMS (Informationssicherheitsmanagement) • Prozess-Bausteine • System-Bausteine • Umsetzungshinweise • Erstellung eines Bausteins	**1 UE** **1 UE**	
6. Umsetzung der IT-Grundschutz-Vorgehensweise (II)	0 UE	
7. IT-Grundschutz-Check (II) • Beispiel für die Durchführung	**1 UE**	
8. Risikoanalyse (II) • Beispiel für die Risikobewertung	**1 UE**	
9. Umsetzungsplanung (II)	0 UE	
10. Aufrechterhaltung und kontinuierliche Verbesserung (II) • Beispiel für Anwendung kontinuierlicher Verbesserungsprozess (KVP)	**1 UE**	
11. Zertifizierung und Erwerb des IT-Grundschutz-Zertifikats auf Basis von ISO 27001 (I)	0 UE	
12. IT-Grundschutzprofile (I + III)	**2 UE**	

• Aufbau eines Profils • Erstellung eines Profils • Anwendung bzw. Nutzungsmöglichkeit veröffentlichter Profile		
13. Vorbereitung auf ein Audit (II + III) • Planung und Vorbereitung (Rollen und Verantwortlichkeiten, Unabhängigkeit, Auditplan, Checklisten, Kombination von Audits, Synergieeffekte) • Auditprozess-Aktivitäten (Zusammenstellung eines Team, Dokumente vorbereiten, Planung des Vor-Ort-Audits, Umgang mit Nichtkonformitäten) • Berichtswesen (Inhalt und Aufbau eines Berichtes, Genehmigung und Verteilung, Aufbewahrung und Vertraulichkeit) • Folgemaßnahmen (Vor-Audit, Wiederholungsaudit, Überwachung, Korrekturmaßnahmen) • Qualifikation von Auditoren (Berufserfahrung, Schulung, persönliche Eigenschaften, Aufrechterhaltung der Qualifikation)	**2 UE**	
14. Notfallmanagement (II + III) • Überblick über den BSI-Standard 100-4 • Notfallmanagement Prozess (initiieren, analysieren, einführen, üben, verbessern) • Business-Impact-Analyse (BIA) • Notfälle bewältigen (Umgang mit Sicherheitsvorfällen) • Vorgehensweise bei Sicherheitsvorfall und Meldeweg erarbeiten	**2 UE** **1 UE**	
15. Zusammenfassung und Prüfungsvorbereitung (I)	**1 UE**	
16. Abschlussprüfung durch BSI		
	16 UE	

*

UE: Unterrichtseinheit à 60 Minuten
MC: Multiple Choice Aufgaben

Es wird je nach Qualifikation zwischen den folgenden Vertiefungsstufen unterschieden:

I: „Kenntnisse, die verstanden sind und erläutert werden können“. (Reproduktion)

II: „Kenntnisse und Fertigkeiten, die auf eigene Prozesse und Komponenten angewendet und umgesetzt werden können“. (Transfer)

III: „Analysen und Methoden, die auf andere Institutionen, Prozesse und Komponenten angewendet und bewertet werden können“. (Reflexion)