

Leitfaden zum Personenqualifizierungsprogramm **IT-Grundschutzexperte (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	3
6.	Schriftliche Prüfung	4
7.	Gesamtbewertung	4
8.	Zertifikaterteilung	4
9.	Mitgeltende Unterlagen	5
10.	Anlage 1:Themen des Lehrgangs und Prüfungsmodalitäten der schriftlichen Prüfung IT-Grundschutzexperte (TÜV®)	6

Herausgeber und Eigentümer:

TÜV NORD CERT GmbH

Personenzertifizierungsstelle

Langemarckstr. 20

45141 Essen

E Mail: TNCERT-PZ@tuev-nord.de / perscert@tuev-nord.de

Rev. 00

Status: freigegeben, 12.02.2018 BM

Leitfaden zum Personenqualifizierungsprogramm IT-Grundschutzexperte (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. im Datenschutz) und deren Integrität (Unverändertheit) von hoher Bedeutung. Unzureichend geschützte Informationen stellen in Wirtschaft und Verwaltung einen Risikofaktor dar, der im Schadensfall existenzbedrohend sein kann.

Ein effektives und nachhaltiges Management der Informationssicherheit wirkt risikomindernd und gewährleistet die Informationssicherheit in Unternehmen als auch 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.

Die vom BSI entwickelte IT-Grundschutz-Methodik besteht aus der Kombination des BSI-Standard 100 und den IT-Grundschutz-Katalogen. Sie zeichnet sich unter anderem dadurch aus, dass anwendbare Sicherheitsmaßnahmen in themenbezogenen Bausteinen gebündelt sind und so bereits mit verhältnismäßig geringem finanziellen und zeitlichen Aufwand ein „normales“ Schutzniveau zu erreichen ist.

Bei höheren Risiken werden zusätzliche Analysen erforderlich, die durch die BSI-Standardreihe 100 unterstützt werden. Damit ist die IT-Grundschutz-Methodik kompatibel zur international anerkannten Norm ISO 27001 für Informationssicherheitsmanagementsysteme und liefert weitere umfangreiche, detaillierte Empfehlungen und konkrete Vorgehensweisen.

Erfahrungen zeigen, dass qualifizierte Experten für IT-Grundschutz einen wesentlichen Erfolgsfaktor für den Aufbau und Betrieb eines Informationssicherheitsmanagementsystems auf Basis des IT-Grundschutzes darstellen.

2. Geltungsbereich

Dieser Leitfaden gilt für alle Zertifizierungsverfahren zum Erlangen des Zertifikats IT-Grundschutzexperte (TÜV®) im Rahmen von anerkannten Lehrgängen.

3. Eingangsvoraussetzungen zur Teilnahme an der Prüfung und zur Zertifikatserteilung

	Ausbildung / ersatzweise Berufserfahrung für fehlende Ausbildung:	Schulung im Zertifizierungsgebiet	praktische Erfahrung oder Auditerfahrung
IT-Grundschutz-experte	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

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 zum IT-Grundschutzexperten	schriftlich:
Dauer:	60 min.
Anzahl der Prüfungsaufgaben gesamt:	24
MC-Aufgaben:	20
Offene Aufgaben:	4
Höchstpunktzahl:	40
Mindestpunktzahl:	24 (60 %)

Details s. Anlage

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 fünf Punkte. Eine teilweise richtige Lösung erhält Teilpunkte im Verhältnis zur richtigen Gesamtlösung. Hierbei ist eine Punktstückelung von halben ($\frac{1}{2}$) Punkten möglich.

7. Gesamtbewertung

Die Prüfung IT-Grundschutzexperte (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-BSI100-tt.mm.jjjj- DE02-32157 (Beispiel)

Die Nummer setzt sich wie folgt zusammen:

44	TÜV NORD CERT GmbH-Personenzertifizierung
02	Zertifikat
BSI100	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. Mitgeltende Unterlagen

Allgemeine Prüfungsordnung (TÜV®)

Gebührenordnung für Prüfungen (TÜV®)

Anlagen

10. Anlage 1: Themen des Lehrgangs und Prüfungsmodalitäten der schriftlichen Prüfung IT-Grundschutzexperte (TÜV®)

Themenbereich und Lerninhalte	Anzahl der UE*	Anzahl der Aufgaben MC*/o*
1. Grundlagen der Informationssicherheit (IS) <ul style="list-style-type: none"> • Aktuelle Herausforderungen und Erwartungen an die Informationssicherheit • Motivation und Grundsätze der Informationssicherheit • Bedrohungen und Schwachstellen • Informationssicherheit als Prozess • Modelle und Standards für ganzheitliche Informationssicherheit • Grundlagen des Sicherheitsmanagements nach 27001 	5 UE	5 MC/1 o
2. Die BSI-Standards zur Informationssicherheit (BS) <ul style="list-style-type: none"> • Informationssicherheits-Managementsysteme nach ISO 27001 und BSI-Standard 100-1 • Sicherheitskonzeption nach IT-Grundschutz (BSI-Standard 100-2, IT-Grundschutzkataloge) • Risikoanalysestrategien und Notfallvorsorge (BSI-Standards 100-3 und 100-4, ISO 27005) • Prüfung und Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz 	12 UE	10 MC/2 o
3. Praktische Aspekte der Arbeit mit den BSI-Standards zur Informationssicherheit (PB) <ul style="list-style-type: none"> • Strukturanalyse • Schutzbedarfsfeststellung • Auswahl und Anpassung von Maßnahmen (Modellierung nach IT-Grundschutz) • Planung und Durchführung von Basis-Sicherheitschecks • Ergänzende Sicherheitsanalyse und Risikoanalyse • Toolbasiertes Informationssicherheitsmanagement am Beispiel von GSTOOL und verinice 	7 UE	5 MC/1 o
4. Abschlussprüfung		20 MC/4 o
schriftlich	60 min.	

*

UE: Unterrichtseinheit à 45 Minuten

MC: Multiple Choice Aufgaben

o: offene Aufgaben