

IT-Grundschutz Praktiker

Prüfungscode DBE-ITGS-PRA-01 · Fassung 1.1 · Stand 24.09.2026

Nachweis, dass du die IT-Grundschutz-Methodik des BSI kennst und an einem Sicherheitskonzept mitarbeiten kannst.

Die Prüfung im Überblick

Bearbeitungszeit 1 Stunde	Fragen 50
Bestehensgrenze 60 %	Fragetypen Einfach- und Mehrfachauswahl
Prüfungssprache Deutsch	Zertifikat gültig Unbegrenzt
Durchführung Online, zeitlich überwacht	Preis Kostenlos

Themenblöcke

Block	Thema	Gewichtung	Fragen
1	Einführung und Grundlagen der Informationssicherheit und rechtliche Rahmenbedingungen	4 %	2
2	Normen und Standards der Informationssicherheit	4 %	2
3	Einführung IT-Grundschutz	4 %	2
4	IT-Grundschutz-Vorgehensweise (Überblick)	4 %	2
5	IT-Grundschutz-Kompendium (Überblick)	4 %	2
6	Umsetzung der IT-Grundschutz-Vorgehensweise	16 %	8
7	IT-Grundschutz-Check	6 %	3
8	Risikoanalyse	10 %	5
9	Umsetzungsplanung	10 %	5
10	Aufrechterhaltung und kontinuierliche Verbesserung	10 %	5

11	Zertifizierung und Erwerb des IT-Grundschutz-Zertifikats auf Basis von ISO 27001	6 %	3
12	IT-Grundschutz-Profile	4 %	2
13	Vorbereitung auf ein Audit	6 %	3
14	Sicherheitsvorfallbehandlung	6 %	3
15	BCM-Prozess	6 %	3
Gesamt		100 %	50

Die Gewichtung gibt an, welchen Anteil ein Block an den Prüfungsfragen hat. Die Fragen werden beim Start zufällig und anteilig je Block aus dem Fragenpool gezogen.

BLOCK 1

4 % · 2 Fragen

Einführung und Grundlagen der Informationssicherheit und rechtliche Rahmenbedingungen

Begriffe und Grundwerte, Unterschied zwischen IT und OT sowie zwischen Security und Safety, gesetzliche Grundlagen.

- 1.1 Arten und Wichtigkeit von Informationen einordnen
Informationen als Werte einer Institution
- 1.2 Die Grundwerte unterscheiden
Vertraulichkeit, Integrität, Verfügbarkeit; dazu Authentizität und Verbindlichkeit
- 1.3 IT und OT sowie Security und Safety abgrenzen
Steuerungstechnik, funktionale Sicherheit
- 1.4 Gesetzliche Grundlagen kennen
BSI-Gesetz, IT-Sicherheitsgesetz, Vorgaben der Bundesnetzagentur für Netzbetreiber, Datenschutz

BLOCK 2

4 % · 2 Fragen

Normen und Standards der Informationssicherheit

Überblick über die ISO-2700x-Reihe und benachbarte Regelwerke, Synergien und integrierte Managementsysteme.

- 2.1 Zweck und Struktur der relevanten Normen erläutern
ISO/IEC 27001, 27002, 27005, 27019
- 2.2 Benachbarte Regelwerke einordnen
COBIT, ITIL, Verschlusssachenanweisung, C5, HV-Benchmark
- 2.3 Branchenspezifische Sicherheitsstandards und IT-Grundschutz-Profile einordnen
- 2.4 Synergien und integrierte Managementsysteme erkennen
gemeinsames Gerüst mehrerer Managementsystemnormen

Einführung IT-Grundschutz

Bestandteile des IT-Grundschutzes, Sicherheitsprozess, Rollen und Verantwortung sowie die Leitlinie.

- 3.1** Die Bestandteile des IT-Grundschutzes benennen
BSI-Standards 200-1 bis 200-4, Kompendium, Umsetzungshinweise
- 3.2** Den Sicherheitsprozess und seine Phasen beschreiben
- 3.3** Rollen, Verantwortung und Aufgaben zuordnen
Institutionsleitung, ISB, ICS-ISB, IS-Management-Team
- 3.4** Eine Leitlinie zur Informationssicherheit erstellen
Geltungsbereich, Sicherheitsziele, Sicherheitsniveau, Bekanntgabe, Aktualisierung

IT-Grundschutz-Vorgehensweise (Überblick)

Basis-, Kern- und Standard-Absicherung, die Anforderungsstufen und die Wahl der Vorgehensweise.

- 4.1** Die drei Vorgehensweisen unterscheiden
Basis-, Kern- und Standard-Absicherung
- 4.2** Die Leitfragen zur Wahl der Vorgehensweise anwenden
- 4.3** Die Anforderungsstufen unterscheiden
Basis-Anforderungen, Standard-Anforderungen, Anforderungen bei erhöhtem Schutzbedarf

IT-Grundschutz-Kompendium (Überblick)

Aufbau und Anwendung des Kompendiums, Prozess- und System-Bausteine, Umsetzungshinweise.

- 5.1** Aufbau und Anwendung des Kompendiums erläutern
Schichten, Aufbau eines Bausteins
- 5.2** Prozess- und System-Bausteine unterscheiden
ISMS, ORP, CON, OPS, DER sowie APP, SYS, IND, NET, INF
- 5.3** Umsetzungshinweise einordnen
- 5.4** Einen benutzerdefinierten Baustein erstellen
wenn kein Baustein passt

Umsetzung der IT-Grundschutz-Vorgehensweise

Strukturanalyse, Schutzbedarfsfeststellung mit Vererbung und Modellierung des Informationsverbunds.

- 6.1** Eine Strukturanalyse durchführen
Netzplan, Geschäftsprozesse, Anwendungen, IT-Systeme, Räume, Kommunikationsverbindungen, Gruppenbildung
- 6.2** Den Schutzbedarf feststellen und begründen
Kategorien normal, hoch und sehr hoch; Schadensszenarien
- 6.3** Den Schutzbedarf vererben
Maximumprinzip, Kumulationseffekt, Verteilungseffekt
- 6.4** Den Informationsverbund modellieren
Bausteine zuordnen, Reihenfolge, Dokumentation, Anforderungen anpassen
- 6.5** Ausgelagerte Zielobjekte berücksichtigen
Dienstleister in Strukturanalyse und Modellierung

IT-Grundschutz-Check

Soll-Ist-Vergleich: Vorbereitung, Durchführung im Interview, Umsetzungsstatus und Dokumentation.

- 7.1** Zweck und Umfang des Checks beschreiben
Soll-Ist-Vergleich der modellierten Anforderungen
- 7.2** Den Check vorbereiten und durchführen
Dokumente sichten, Ansprechpersonen, Interviews, Stichproben
- 7.3** Den Umsetzungsstatus vergeben
entbehrlich, ja, teilweise, nein; jeweils mit Begründung
- 7.4** Die Ergebnisse dokumentieren
Stamminformationen, Begründung, Verantwortung, Termin

Risikoanalyse

Risikoanalyse nach BSI-Standard 200-3: Gefährdungsübersicht, Einstufung und Behandlung.

- 8.1** Erkennen, wann eine Risikoanalyse nötig ist
hoher Schutzbedarf, kein passender Baustein, untypisches Einsatzszenario
- 8.2** Die elementaren Gefährdungen anwenden
G 0.1 bis G 0.47, weitere Gefährdungsübersichten

- 8.3** Risiken einstufen
Eintrittshäufigkeit und Schadensauswirkung, Risikomatrix
- 8.4** Risiken behandeln und Restrisiken dokumentieren
vermeiden, reduzieren, übertragen, akzeptieren

BLOCK 9

10 % · 5 Fragen

Umsetzungsplanung

Aus den offenen Anforderungen einen Maßnahmenplan mit Aufwand, Reihenfolge und Verantwortung machen.

- 9.1** Maßnahmen sichten und konsolidieren
- 9.2** Aufwände schätzen
einmalige und laufende Kosten, Personalaufwand
- 9.3** Umsetzungsreihenfolge und Verantwortung festlegen
- 9.4** Begleitende Maßnahmen planen
Sensibilisierung, Schulung, Kommunikation

BLOCK 10

10 % · 5 Fragen

Aufrechterhaltung und kontinuierliche Verbesserung

Überprüfung des erreichten Niveaus, Kennzahlen, Reifegrade und der Verbesserungsprozess.

- 10.1** Die Leitfragen für die Überprüfung anwenden
- 10.2** Überprüfungsverfahren unterscheiden
Selbsteinschätzung, interne Audits, Übungen, externe Prüfung
- 10.3** Kennzahlen bilden und bewerten
Messgröße, Quelle, Turnus
- 10.4** Reifegradmodelle anwenden und den Verbesserungsprozess steuern

BLOCK 11

6 % · 3 Fragen

Zertifizierung und Erwerb des IT-Grundschutz-Zertifikats auf Basis von ISO 27001

Auditarten, Akkreditierung und Zertifizierung sowie der Ablauf des BSI-Zertifizierungsverfahrens.

- 11.1** Arten von Audits unterscheiden
System-, Prozess- und Produktaudit
- 11.2** Die Grundsätze der Auditierung kennen
Erst-, Zweit- und Drittparteien-Audit

- 11.3 Das Modell von Akkreditierung und Zertifizierung erläutern
- 11.4 Den Ablauf des BSI-Zertifizierungsverfahrens beschreiben
Antrag, Dokumentenprüfung, Umsetzungsprüfung, Laufzeit, Überwachungsaudits

BLOCK 12

4 % · 2 Fragen

IT-Grundschutz-Profil

Aufbau, Nutzung und Erstellung eines IT-Grundschutz-Profiles als Muster-Sicherheitskonzept.

- 12.1 Den Aufbau eines Profils beschreiben
- 12.2 Ein veröffentlichtes Profil nutzen und anpassen
- 12.3 Die Grenzen eines Profils kennen
ersetzt weder Strukturanalyse noch IT-Grundschutz-Check

BLOCK 13

6 % · 3 Fragen

Vorbereitung auf ein Audit

Auditplan, Referenzdokumente, Nichtkonformitäten, Berichtswesen, Folgemaßnahmen und Qualifikation der Auditierenden.

- 13.1 Ein Audit planen und vorbereiten
Rollen, Unabhängigkeit, Auditplan, Checklisten, Kombination von Audits
- 13.2 Die Aktivitäten im Auditprozess kennen
Auditteam, Referenzdokumente, Vor-Ort-Audit, Nichtkonformitäten
- 13.3 Das Berichtswesen beschreiben
Inhalt und Aufbau, Genehmigung, Verteilung, Aufbewahrung, Vertraulichkeit
- 13.4 Folgemaßnahmen und die Qualifikation von Auditierenden einordnen
Voraudit, Überwachungsaudit, Korrekturmaßnahmen

BLOCK 14

6 % · 3 Fragen

Sicherheitsvorfallbehandlung

Vorfälle erkennen, einstufen, behandeln und auswerten.

- 14.1 Störung, Sicherheitsvorfall und Notfall abgrenzen
- 14.2 Meldewege und Eskalation festlegen
Vorgaben des Bausteins DER.2.1
- 14.3 Einen Vorfall behandeln
Erstreaktion, Eindämmung, Beseitigung, Wiederherstellung

14.4 Vorfälle nachbereiten

Ursachenanalyse, Lessons Learned, Rückkopplung in das Sicherheitskonzept

BLOCK 15

6 % · 3 Fragen

BCM-Prozess

Überblick über BSI-Standard 200-4 und den BCM-Prozess, angelehnt an den Baustein DER.4.

15.1 Zweck und Abgrenzung des BCM erläutern

Unterschied zu Vorfallbehandlung und Krisenmanagement

15.2 Die Kenngrößen kennen

maximal tolerierbare Ausfallzeit, Wiederanlaufzeit, tolerierbarer Datenverlust

15.3 Die Business-Impact-Analyse beschreiben

zeitkritische Prozesse und ihre Ressourcen

15.4 Den BCM-Prozess und den Baustein DER.4 einordnen

Stufenmodell, Notfallhandbuch, Übungen und Tests

Institut für Webentwicklung · unabhängiges Lernangebot ohne Verbindung zu den genannten Technologieanbietern. Maßgeblich ist die Fassung auf der Zertifizierungsseite.