# Fragebogen

| | |
|---|---|
| Name: | _____ |
| Matrikelnummer: | _____ |
| Unterschrift: | _____ |

Für den Erhalt des ISMS 27001 Foundation Prüfungszertifikates muss die im Multiple-Choice-Verfahren gehaltene Prüfung erfolgreich bestanden werden.

**Version:** ISO/IEC 27001:2013 + Cor. 1:2014

**Sprache:** Deutsch

**Dauer:** 45 Minuten

**Format:** 30 Multiple-Choice-Fragen; mit zwei oder drei Antwortmöglichkeiten, von denen eine, zwei oder auch alle drei Antworten korrekt sein können.

**min. Punkte:** 20 von 30
Jede komplett richtig beantwortete Frage gibt einen Punkt. Bei falsch beantworteten Fragen gibt es 0 Punkte (aber keinen Punktabzug). Als falsch beantwortet gilt eine Frage, wenn eine falsche Antwort markiert ist, oder nicht alle richtigen angekreuzt wurden.

**AUSFÜLLHILFE FÜR DEN ANTWORTBOGEN**

**Wie markiere ich richtig?**
Für diese Prüfung erhalten Sie einen Fragebogen und einen Antwortbogen. Die Antworten sind durch entsprechende Markierungen auf dem Antwortbogen vorzunehmen. Dieser wird maschinell ausgewertet, handschriftliche Anmerkungen werden nicht berücksichtigt. Ankreuzungen auf dem Fragebogen werden nicht ausgewertet! Verwenden Sie für Ihre Markierungen ausschließlich einen schwarzen oder blauen Kugelschreiber von normaler Schriftstärke. Die Markierungen müssen deutlich und positionsgenau durch ein Kreuz erfolgen. Wenn Sie eine Ankreuzung korrigieren möchten, füllen Sie das Kästchen vollkommen aus, dadurch wird diese Markierung wie ein leeres Kästchen gewertet. Eine neuerliche Korrektur ist dann nicht mehr möglich!

**Ausfüllen der Matrikelnummer**:
Tragen Sie zu Beginn der Prüfung Ihre 9-stellige Matrikelnummer auf dem Antwortbogen in das dafür vorgesehene Feld ein. Übertragen Sie dann Ihre Matrikelnummer mit Kreuzen in die darunter befindlichen Kästchen, die von 0 bis 9 nummeriert sind. Die erste Spalte entspricht der 1. Ziffer Ihrer Matrikelnummer, die zweite Spalte entspricht der 2. Ziffer Ihrer Matrikelnummer usw.

**Übertragen der richtigen Gruppe:**
Bitte übertragen Sie die Gruppe, die Sie in der Kopfzeile des Fragebogens finden, in das entsprechende Feld auf dem Antwortbogen.

**Viel Erfolg bei der Prüfung!**

**1)** Welche Eigenschaften von Informationen sollen im Rahmen der Informationssicherheit aufrechterhalten werden?

a) Vertraulichkeit
b) Unverletzbarkeit
c) Integrität

**2)** Was muss eine Organisation gemäß ISO/IEC 27001 im Rahmen ihres Prozesses zur Behandlung von Informationssicherheitsrisiken tun?

a) Die Informationssicherheitsrisiken bewerten
b) Einen Plan für die Behandlung von Informationssicherheitsrisiken formulieren
c) Maßnahmen, die zur Umsetzung der gewählte(n) Option(en) für die Behandlung von Informationssicherheitsrisiken erforderlich sind, festlegen

**3)** Was ist in der Phase "Verbesserung" nach ISO/IEC 27001 fortlaufend zu optimieren?

a) Die Wirksamkeit des ISMS
b) Die Genauigkeit des ISMS
c) Die Gesetzmäßigkeit des ISMS

**4)** Welche der folgenden Aussagen zu internen Audits und Managementbewertungen sind korrekt?

a) Interne Audits werden durch die oberste Leitung (Top-Management) durchgeführt
b) Managementbewertungen müssen in geplanten Abständen durchgeführt werden
c) Eine Managementbewertung wird durch die oberste Leitung (Top-Management) durchgeführt

**5)** Was trifft im Kontext des Standards ISO/IEC 27000 auf Maßnahmen (Controls) zu?

a) ISO/IEC 27002 behandelt die gleichen Maßnahmen (Controls), die auch im Anhang A der Norm ISO/IEC 27001 definiert sind
b) Im Anhang A der Norm ISO/IEC 27001 sind immer ein oder mehrere Maßnahmenziele (Control Objectives) einer Maßnahme (Control) zugeordnet
c) Maßnahmen (Controls) sind in Anhang A der Norm ISO/IEC 27001 definiert

**6)** Ein Audit ist ein Prozess, mit dem bestimmt werden soll, inwieweit Auditkriterien erfüllt sind. Welche der folgenden Eigenschaften muss dieser Prozess gemäß ISO/IEC 27000 unter anderem aufweisen?

a) Er muss systematisch sein
b) Er muss durch eine externe Partei gesteuert werden
c) Er muss dokumentiert sein

**7)** Welche der folgenden Aussagen zum Anhang A der Norm ISO/IEC 27001 sind korrekt?

a) Der Anhang A ist normativ, und sofern Ausschlüsse vorgenommen werden, müssen diese begründet werden.
b) Der Anhang A enthält Bedrohungs- und Gefährdungskataloge.
c) Im Anhang A sind Maßnahmenziele (Control Objectives) definiert.

**8)** Was trifft auf auf den Standard ISO/IEC 27001 zu?

a) Er formuliert die minimalen Anforderungen an ein Informationssicherheitsmanagementsystem (ISMS)
b) Er legt Anforderungen an Konformitätsbewertungstellen fest
c) Er ist Teil einer größeren Standardfamilie

**9)** Was ist Vetraulichkeit?

a) Eigenschaft, dass eine Information wohlbekannt und kommuniziert ist
b) Eigenschaft, dass eine Entität das ist, was sie vorgibt zu sein
c) Eigenschaft, dass Information unbefugten Parteien nicht verfügbar gemacht oder offengelegt wird

**10)** In welchen der folgenden Fälle liegt eine Verletzung der Integrität vor?

a) Einem Dokument wurden unberechtigterweise weitere Informationen hinzugefügt.
b) Ein Dokument ist unverschlüsselt.
c) Auf ein Dokument wurde unberechtigterweise zugegriffen.

**11)** ISO/IEC 27001 definiert Maßnahmen (Controls) und Maßnahmenziele (Control Objectives) zu / zur ...

a) Verwaltung der Werte (Asset management) einer Organisation
b) Personalsicherheit (Human resource security)
c) physischen und umgebungsbezogenen Sicherheit (Physical and environmental security)

**12)** Worüber müssen sich Personen, die Tätigkeiten für eine Organisation ausüben, die Konformität mit ISO/IEC 27001 beansprucht, bewusst sein?

a) Über Folgen einer Nichterfüllung der Anforderungen des ISMS
b) Über ihren Beitrag zur Wirksamkeit des ISMS
c) Über alle Maßnahmen zur Behandlung von Informationssicherheitsrisiken gemäß Risikobehandlungsplan

**13)** Wobei handelt es sich um Kriterien, die gemäß ISO/IEC 27001 im Rahmen des Prozesses zur Beurteilung von Informationssicherheitsrisiken festgelegt und angewendet werden müssen?

a) Kriterien für die Risikodokumentation
b) Kriterien zur Maßnahmenbewertung
c) Kriterien zur Risikoakzeptanz

**14)** Was trifft auf Prozesse im Kontext der ISO/IEC 27000 Standardfamilie zu?

a) Prozesse stellen einen Teil bzw. Teile eines Managementsystems dar
b) ISO/IEC 27002 definiert 14 Informationssicherheitsprozesse, um das Erreichen der Maßnahmenziele des Anhangs A der Norm ISO/IEC 27001 sicherzustellen
c) ISO/IEC 27000 definiert einen Prozess als einen Satz zusammenhängender und sich gegenseitig beeinflussender Tätigkeiten, der Eingaben in Ergebnisse umwandelt

**15)** Wodurch zeichnet sich ein führungsstarkes Top-Management im Zusammenhang mit einem ISMS aus?

a) Durchführung von Auditgesprächen mit allen Mitarbeitern
b) Beurteilung aller Informationssicherheitsrisiken
c) Klares Bekenntnis zu Informationssicherheitszielen

**16)** Worüber sollen interne Audits Informationen liefern?

a) Darüber, ob das ISMS die Anforderungen der Organisation erfüllt
b) Darüber, ob das ISMS wirksam umgesetzt und aufrechterhalten wird
c) Darüber, welche Informationssicherheitsvorfälle vermeidbar gewesen wären

**17)** Eine Organisation muss nach ISO/IEC 27001 zur Unterstützung alle erforderlichen Ressourcen für ein Informationssicherheitsmanagementsystem bestimmen und bereitstellen. Die Organisation muss dafür Sorge tragen, dass'

a) ... jede beteiligte Person auf Grundlage angemessener Ausbildung, Schulung oder Erfahrung kompetent ist.
b) ... der Security Officer die Security Policy erstellt, veröffentlicht und freigegeben hat.
c) ... die von der Norm geforderten Infomationen dokumentiert und vorhanden sind.

**18)** Welche der folgenden Aussagen im Zusammenhang mit Vertraulichkeit und Integrität von Informationen sind korrekt?

a) Vertraulichkeit bedeutet Schutz vor Offenlegung von Informationen gegenüber unbefugten Personen
b) Informationen, deren Vertraulichkeit nicht gegeben ist, können auch nicht in ihrer Integrität geschützt werden
c) Ein angemessenes Niveau an Vertraulichkeit und Integrität lässt sich nur durch den Einsatz von Verschlüsselung und durch digitale Signaturen erreichen

**19)** Bei welchem der folgenden Standards handelt es sich einen allgemeinen Leitfaden aus der ISO/IEC 27000 Familie?

a) 17021
b) 27006
c) 27002

**20)** Welche der folgenden Aussagen zum Anhang A aus ISO/IEC 27001 sind insbesondere vor dem Hintergrund der Behandlung von Informationssicherheitsrisiken korrekt?

a) Anhang A enthält eine Erklärung zum Geltungsbereich, die von allen Organisationen, die Konformität mit ISO/IEC 27001 beanspruchen, übernommen werden muss.
b) Anhang A enthält eine Übersicht der wesentlichen Bedrohungen auf die Informationssicherheit, die im Rahmen der Beurteilung von Informationssicherheitsrisiken berücksichtigt werden müssen
c) Anhang A enthält eine umfassende Liste von Maßnahmenzielen und Maßnahmen.

**21)** Auch in der Phase Betrieb (Operation) eines ISMS nach ISO/IEC 27001 gibt es im Zusammenhang mit dem Risikomanagement Tätigkeiten zu erledigen. Welche der folgenden gehören dazu?

a) In regelmäßigen Abständen muss eine Risikobeurteilung vorgenommen werden.
b) Die Risikobehandlung muss nicht dokumentiert werden.
c) Nach erheblichen Änderungen muss eine Risikobeurteilung vorgenommen werden.

**22)** Zu welchen Themen definiert ISO/IEC 27001 im Anhang A Maßnahmenziele und Maßnahmen?

a) Organisation der Informationssicherheit
b) Compliance
c) Energieeffizienz

**23)** Welche der folgenden Schritte muss eine Organisation zur Einführung, Pflege und / oder Verbesserung eines ISMS unter anderem durchführen?

a) Melden von schwerwiegenden Sicherheitsvorfällen an das BSI (Bundesamt für Sicherheit in der Informationstechnik) oder an andere Aufsichtsbehörden
b) Offenlegung des Risikobehandlungsplans gegenüber allen interessierten Parteien
c) Identifikation von Informationswerten und der mit ihnen verbundenen Informationssicherheitsanforderungen (Schutzbedarf)

**24)** Im Kapitel Führung (Leadership) der ISO/IEC 27001 sind Führungsaktivitäten und Verpflichtung der obersten Leitung definiert. Welche Aufgaben gehören dazu?

a) Regelmäßige Teilnahme an den Sitzungen des organisationsinternen Computer Emergency Response Teams (CERT).
b) Gewährleistung, dass die Informationssicherheitspolitik und die Informationssicherheitsziele festgelegt und mit der strategischen Ausrichtung der Organisation vereinbar sind.
c) Bereitstellen der für das ISMS erforderlichen Ressourcen.

**25)** Was trifft auf den PDCA-Zyklus zu?

a) Die Struktur der ISO/IEC 27001 ist, zumindest in Teilen, an dem PDCA-Ansatz ausgerichtet
b) P steht für "Plan", D für "Do", C für "Check" und A für "Act"
c) PDCA beschreibt die Eigenschaften von Information, die im Rahmen der Informationssicherheit aufrechterhalten werden sollen

**26)** Welche Aktivitäten sind für eine Organisation hinsichtlich des Kapitels "Kontext der Organisation" in der Norm ISO/IEC 27001 vorgeschrieben?

a) Bestimmen der interessierten Parteien, die für das Informationssicherheitsmanagementsystem relevant sind.
b) Bestimmen der Anforderungen von interessierten Parteien im Bezug auf die Informationssicherheit.
c) Festlegen der organisatorischen Verantwortichkeiten für Lieferanten in Zusammnarbeit mit der zuständigen Stabsstelle.

**27)** Welche der folgenden Rahmenwerke, Standards oder Standardfamilen befassen sich schwerpunktmäßig mit IT- oder Informationssicherheit (oder werden als Standard für IT- oder Informationssicherheit bezeichnet)?

a) BSI Grundschutz
b) FitSM
c) ISO/IEC 27000

**28)** Was sind Schritte, die im Rahmen des Prozesses zur Beurteilung von Informationssicherheitsrisiken festgelegt und angewendet (durchgeführt) werden müssen?

a) Informationssicherheitsrisiken identifizieren
b) Informationssicherheitsrisiken behandeln
c) Informationssicherheitsrisiken umgehen

**29)** Zu welchen Themen definiert ISO/IEC 27001 (Anhang A) Maßnahmenziele und Maßnahmen im Zusammenhang mit dem Abschnitt "Betriebssicherheit" (A.12)?

a) Protokollierung und Überwachung
b) Schutz vor Schadsoftware
c) Informationsklassifizierung

**30)** Welche der folgenden Aussagen zu Maßnahmen (Controls) sind korrekt?

a) Alle Maßnahmen, die die Norm ISO/IEC 27001 im Anhang A formuliert, sind rein technischer Natur
b) Alle Maßnahmen, die die Norm ISO/IEC 27001 im Anhang A formuliert, sind rein organisatorischer Natur
c) Maßnahmen können Prozesse und Richtlinien umfassen