Fragebogen

Name: _____

Matrikelnummer: _____

Unterschrift: _____

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

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

Sprache: Deutsch

Dauer: 75 Minuten

Format: 50 Multiple-Choice-Fragen; zwei bis sechs Antwortmöglichkeiten, von denen eine, mehrere oder auch alle Antwortmöglichkeiten korrekt sein können.

min. Punkte: 33 von 50
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 der folgenden Beschreibungen von Zielen gehören zu Maßnahmenzielen aus Anhang A.12 "Betriebssicherheit" der ISO/IEC 27001?

a) Die Ehrlichkeit von Anwendern und Mitarbeitern ist im Betrieb garantiert.
b) Der Schutz von Daten, die für das Testen verwendet werden, ist sichergestellt.
c) Information und informationsverarbeitende Einrichtungen sind vor Schadsoftware geschützt.
d) Audittätigkeiten während des Betriebs werden wirksam unterbunden.

2) Welche Aussagen sind im Zusammenhang von Audits zutreffend?

a) ISO 19011 beinhaltet einen Leitfaden zur Auditierung von Managementsystemen.
b) ISO/IEC 27007 beinhaltet einen Leifaden zur Auditierung von Informationssicherheitsmanagementsystemen und ergänzt ISO 19011.
c) Zertifizierungsaudits sind externe Audits.

3) Was ist nach der ISO/IEC 27001 Teil der Beurteilung von Informationssicherheitsrisiken bzw. der Planung für diesen Prozess?

a) Sicherstellung, dass wiederholte Informationssicherheitsrisikobeurteilungen zu konsistenten, gültigen und vergleichbaren Ergebnissen führen
b) Festlegung von Kriterien zur Durchführung von Informationssicherheitsrisikobeurteilungen
c) Abschätzung der möglichen Folgen bei Eintritt der identifizierten Risiken
d) Abschätzung der realistischen Eintrittswahrscheinlichkeiten der identifizierten Risiken

4) In ihrer Organisation sind verschiedene Richtlinien, Verfahren und Maßnahmen umgesetzt.

Welche hiervon lassen sich klar den Referenzmaßnahmen der ISO/IEC 27001 aus A.12 "Betriebssicherheit" oder A.14 "Anschaffung, Entwicklung und Instandhalten von Systemen" zuordnen?

a) Trennung von Entwicklungs-, Test- und Betriebsumgebungen
b) Zuteilung von Benutzerzugängen
c) Schutz der Transaktionen bei Anwendungsdiensten
d) Maßnahmen gegen Schadsoftware

5) Welche Maßnahmen (Controls) gehören zum Maßnahmenziel "Interne Organisation" (A.6.1)?

a) Beschäftigungs- und Vertragsbedingungen
b) Informationssicherheit im Projektmanagement
c) Kontakt mit speziellen Interessensgruppen

6) Im Rahmen eines Projektes zur Etablierung eines nach ISO/IEC 27001 konformen ISMS überprüfen Sie, welche Regelungen ihre Organisation in Hinblick die Auswahl und Einstellung von neuem Personal implementiert hat. Einige Regelungen empfinden Sie als nicht optimal. Welche Regelungen stellen eine **Abweichung** dar, die korrigiert werden muss?

a) Eine Sicherheitsüberprüfung von Bewerbern findet grundsätzlich statt, aber in unterschiedlicher Gründlichkeit. Dies ist von der Position, auf welche die Einstellung der neuen Mitarbeiters erfolgen, soll abhängig.
b) Einige Bewerber werden überprüft. Regelungen dafür welche, existieren aber nicht - es kommt hauptsächlich darauf an, welcher Mitarbeiter der Personalabteilung die Bewerbung bearbeitet.
c) In den vertraglichen Vereinbarungen mit Beschäftigten werden Verantwortlichkeiten in Bezug auf Informationssicherheit festgelegt. Diese sind aber in der Vereinbarung nicht explizit aufgeführt, es wird nur auf die Pflicht zur Einhaltung der relevanten Richtlinien verwiesen.
d) Die Sicherheitsüberprüfung von Bewerbern umfasst nicht die Überprüfung von Profilen in sozialen Medien.

7) Welche der folgenden Maßnahmen sind unter anderem mit dem Maßnahmenziel einer konsistenten und wirksamen Herangehensweise für die Handhabung von Informationssicherheitsvorfällen (A.16.1) gemäß ISO/IEC 27001 (Anhang A) verbunden?

a) Sammeln von Beweismaterial
b) Reaktion auf Informationssicherheitsvorfälle
c) Meldung von Informationssicherheitsereignissen
d) Maßnahmen gegen Schadsoftware

8) Welche der folgenden Maßnahmen sind unter anderem mit dem Maßnahmenziel der Identifikation von Werten (Assets) sowie der Festlegung angemessener Verantwortlichkeiten zu ihrem Schutz (A.8.1) gemäß ISO/IEC 27001 (Anhang A) verbunden?

a) Sichere Anmeldeverfahren
b) Zulässiger Gebrauch von Werten
c) Physische Zutrittssteuerung
d) Zuständigkeit für Werte

9) Welche der folgenden Maßnahmen sind unter anderem mit dem Maßnahmenziel der Unterbindung der unerlaubten Offenlegung, Veränderung, Entfernung oder Zerstörung von Information, die auf Datenträgern gespeichert ist (A.8.3), gemäß ISO/IEC 27001 (Anhang A) verbunden?

a) Klassifizierung von Datenträgern
b) Inventarisierung von Datenträgern
c) Handhabung von Wechseldatenträgern

10) Was sollte im Zusammenhang mit Benutzerkennungen, Kennwörtern und weiterer Information zur Authentifizierung von Benutzern sichergestellt sein?

a) Kennwörter basieren nicht auf relativ einfach zu ermittelnden Sachverhalten (z.B. Geburtsdatum, Namen von Familienangehörigen usw.)
b) Kennwörter haben eine ausreichende Mindestlänge.
c) Benutzer sind verpflichtet, die Regeln der Organisation zur Verwendung geheimer Authentisierungsinformation zu befolgen.

11) Welche Tätigkeiten sind nach ISO/IEC 27001 im Rahmen der Lenkung von dokumentierter Information zu berücksichtigen?

a) Aufbewahrung und Verfügung über den weiteren Verbleib
b) Verteilung, Zugriff, Auffindung und Verwendung
c) Ablage/Speicherung und Erhaltung, einschließlich Erhaltung der Lesbarkeit

12) Welche Dokumentation ist nach der ISO/IEC 27001 gefordert?

a) Informationssicherheitsrichtlinie
b) Prozessdefinition Customer Relationship Management
c) Zugangssteuerungsrichtlinie

13) Welche der folgenden elementaren Grundsätze tragen nach ISO/IEC 27000 zur erfolgreichen Umsetzung eines ISMS bei?

a) Sicherstellung der Nicht-Nachweisbarkeit von Compliance-Verstößen
b) Redundante Verteilung von Verantwortlichkeiten für Informationssicherheit
c) Backend-Sicherheit vor Client-Sicherheit
d) Sicherstellung einer ganzheitlichen Herangehensweise an das Management von Informationssicherheit

14) In ihrer Organisation sollen in einigen Monaten die Controls zu Lieferantenbeziehungen (A.15) auditiert werden.

Welche Umstände würden auf alle Fälle eine Abweichung darstellen und sollten daher unbedingt vor dem Audit geändert werden?

a) Die Informationssicherheitsanforderungen im Zusammenhang mit dem Zugriff von Lieferanten auf Werte sind nicht dokumentiert.
b) Einige Dienste werden von mehreren Lieferanten erbracht (co-sourcing).
c) Informationssicherheitsanforderungen sind bezüglich der Kommunikation von Sicherheitsvorfällen mit den Hauptlieferanten nicht berücksichtigt.

15) Was muss nach der ISO/IEC 27001 in Bezug auf die Personalsicherheit während der Beschäftigung gewährleistet sein?

a) Die Leitung verlangt von allen Beschäftigten die Einhaltung der relevanten Richtlinien.
b) Der Maßregelungsprozess ist vetraulich und nur den leitenden Mitarbeitern bekannt.
c) Die Personalakten aller Mitarbeiter sind durch den Information Security Officer überprüft und genehmigt.
d) Durch Ausbildung, Schulung und ähnliche Maßnahmen wird bei alle Beschäftigten das Bewusstsein (Awareness) für Informationssicherheit gefördert.

16) Welche Aussagen sind im Zusammenhang mit Business Continuity Management richtig, wenn Konformität mit ISO/IEC 27001 angestrebt wird?

a) Continuity- bzw. Notfallpläne müssen in in regelmäßigen Abständen überprüft werden.
b) Die Anforderungen zum Business Continuity Management können ohne außreichende Begründung in der Erklärung zur Anwendbarkeit (statement of applicability) weggelassen werden.
c) Die Aufrechterhaltung eines angemessenen Maßes an Informationssicherheit in Krisen- und Katastrophenfällen muss geplant werden.
d) Zum Continuity-Management gehört auch die Planung ausreichender Redundanzen von informationsverarbeitenden Einrichtungen.

17) Zu welchen Themen definiert die ISO/IEC 27001 im Kapitel 7 "Unterstützung" (Support) Anforderungen?

a) 24h Support
b) Risikounterstützung
c) Dokumentierte Information
d) Service-Desk

18) Welchen Anforderungen muss die Informationssicherheitspolitik (allgemeine Informationssicherheitsrichtlinie) genügen?

a) Sie muss eine Verpflichtung zur fortlaufenden Verbesserung beinhalten.
b) Sie muss für den Zweck der Organisation angemessen sein.
c) Sie muss innerhalb der Organisation bekanntgemacht werden.
d) Sie muss Informationssicherheitsziele beinhalten.

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

a) Sicherung rechtlicher Ansprüche (Defense of legal claims) im Zusammenhang mit Informationssicherheitsvorfällen
b) Klassifizierungstypen für Informationswerte (Information Assets)
c) Personalsicherheit (Human resource security)

20) Für welche Begriffe aus der ISO/IEC 27000 trifft eine der folgenden Definitionen zu?

- Satz zusammenhängender und sich gegenseitig beeinflussender Tätigkeiten, der Eingaben in Ergebnisse umwandelt
- Absichten und Ausrichtung einer Organisation, wie von der obersten Leitung formell ausgedrückt
- Nichterfüllung einer Anforderung
- Satz zusammenhängender und sich gegenseitig beeinflussender Elemente einer Organisation, um Politiken (Richtlinien), Ziele und Prozesse zum Erreichen dieser Ziele festzulegen
- Person oder Personengruppe, die die rechtliche Verantwortung (accountability) für die Leistung und Konformität der Organisation trägt
- Eigenschaft der Richtigkeit und Vollständigkeit

a) Steuerungsgremium (governing body)
b) Prozess (process)
c) Politik / Richtlinie (policy)

21) Was ist bei der Festlegung des Anwendungsbereichs des Informationssicherheitsmanagementsystems (scope of the information security management system) zu beachten?

a) Der Anwendungsbereich des ISMS muss vor Offenlegung (Verlust der Vetraulichkeit) geschützt werden.
b) Der festgelegte Anwendungsbereich muss dokumentiert sein.
c) Der Anwendungsbereich des ISMS kann, zumindest grundsätzlich, danach eingeschränkt werden, welche Anforderungen der ISO/IEC 27001 erfüllt werden müssen.

22) Was umfasst ein (Informationssicherheits-)Managementsystem im Sinne der ISO/IEC 27000?

a) Richtlinien
b) Organisationsstrukturen
c) Zuständigkeiten (Verantwortlichkeiten)

23) Was kann erwartet werden, wenn alle Maßnahmen zur Verwaltung der Werte (A.8) sinnvoll umgesetzt wurden?

a) Verantwortlichkeiten bzw. Zuständigkeiten für die Werte sind dokumentiert.
b) Die Rückgabe von Werten ist geregelt.
c) Informationswerte der Organisation sind in einem Inventar der Werte (Asset-Inventar) erfasst.

24) Was sind grundsätzliche Methoden zur Bewertung der Leistung eines ISMS?

a) Umsetzung von Korrekturmaßnahmen
b) Kontinuierliche Leistungsbeurteilung der Mitarbeiter
c) Managementbewertungen

25) Ihre Aufgabe ist es, eine Organisation bei der Erreichung des Schutzziels "Die Informationssicherheit bei Telearbeit und der Nutzung von Mobilgeräten ist sichergestellt." (A.6.2) zu unterstützen.

Die Organisation erlaubt sowohl die Nutzung von Mobilgeräten wie auch Telearbeit.

Beides ist, inbesondere in Hinblick auf Informationssicherheit, aber noch weitestgehend ungeregelt.

Was **müssen** Sie umsetzen bzw. sicherstellen, um in diesem Bereich Konformität zur ISO/IEC 27001 herzustellen?

a) Erstellung einer Richtlinie zu Mobilgeräten
b) Beurteilung von Risiken im Zusammenhang mit der Nutzung von Mobilgeräten und Telearbeit
c) Maßnahmen zur Handhabung von Risiken bei der Nutzung von Laptops.
d) Sicherstellen, dass für Telearbeit und Arbeit auf Dienstreisen identische Regelungen existieren

26) Welche Aussagen zur Normenfamilie ISO/IEC 27000 sind korrekt?

a) Die Umsetzung von ISO/IEC 27002 ist eine zwingende Voraussetzung für eine Zertifizierung nach ISO/IEC 27003
b) ISO/IEC 27003 enthält Anforderungen an die Umsetzung von Maßnahmen.
c) ISO/IEC 27000 beschreibt die Grundlagen von Informationssicherheitsmanagementsystemen und definiert zugehörige Begriffe.
d) ISO/IEC 27001 enthält Anforderungen an ein ISMS.

27) Kryptographische Maßnahmen können zur Erreichung verschiedener Ziele der Informationsicherheit beitragen.

Welche Schutzziele lassen sich mittels Einsatz von Verschlüsselung und digitaler Signaturen unterstützen?

a) Vetraulichkeit
b) Authentizität
c) Integrität
d) Verlässlichkeit

28) Welche Anforderungen stellt die ISO/IEC 27001 in Bezug auf interne Audits?

a) Die Organisation muss für jedes Audit die Auditkriterien festlegen
b) Die Organisation muss ihre Kunden auditieren.
c) Die Organisation muss mindestens alle 6 Monate ein Audit durchführen.
d) Die Organisation muss ein Auditprogramm aufbauen

29) Ihre Aufgabe ist es, die in Ihrer Organisation umgesetzten Maßnahmen im Bereich "Physische und umgebungsbezogene Sicherheit" (A.11) auf Konformität zu ISO/IEC 27001 zu überprüfen. In der Erklärung zur Anwendbarkeit wurden keine Maßnahmen ausgeschlossen. Welche Umstände stellen (bereits für sich alleine genommen) eine Abweichung bzw. eine Nichtkonformität dar?

a) Es existieren auf dem Betriebsgelände mehrere Anlieferungs- und Ladebereiche.
b) Gegen die Auswirkungen von Erdbeben sind keinerlei vorbeugende Maßnahmen umgesetzt.
c) Es kommt regelmäßig vor, dass Administratoren und andere Mitarbeiter ohne vorherige Genehmigung PCs und Laptops z.B. über ein Wochenende mit nach Hause nehmen. Da bisher alle Geräte wiedergebracht wurden, wird dies von der Geschäftsleitung toleriert.
d) Es existiert kein elektronisches Schließsystem. Alle Türen sind nur mit mechanischen Schlössern gesichert.

30) Was trifft auf interne Audits im Kontext eines ISMS zu?

a) Ihre Ergebnisse sind Basis für die Erklärung zur Anwendbarkeit.
b) Sie dienen dazu, die Konformität des ISMS mit den Anforderungen aus ISO/IEC 27001 zu überprüfen
c) Sie dienen dazu, die Konformität des ISMS mit den Anforderungen der Organisation an ihr ISMS zu überprüfen

31) Sie beraten eine Organisation, die eine Zertfizierung nach ISO/IEC 27001 anstrebt, in Bezug auf ihren Umgang mit Informationssicherheitsrichtlinien.

Welche Aussagen sind in diesem Zusammenhang richtig?

a) Informationssicherheitsrichtlinien müssen an die Verfahren zum Umgang mit Informationssicherheitsvorfällen angeglichen werden.
b) Informationssicherheitsrichtlinien müssen vom Information Security Officer genehmigt werden.
c) Informationssicherheitsrichtlinien müssen in geplanten Abständen überprüft werden

32) Welche der folgenden Aussagen ist in Bezug auf das Risikomanagement und seine Teilprozesse nach ISO/IEC 27000 und ISO/IEC 27001 korrekt?

a) Risikoanalyse ist Teil der Risikobeurteilung
b) Im Rahmen der Risikobewertung werden Ergebnisse der Risikoanalyse mit Risikokriterien verglichen.
c) Risikobewertung ist Teil der Risikobeurteilung
d) Im Rahmen der Risikoanalyse wird das Risikoniveau bestimmt

33) Ein Verfahren für das Risikomanagement sieht vor, dass jedes Risiko in Hinblick auf zwei Faktoren analysiert wird: Schadensauswirkung (in Tausenden von Euro) und Eintrittswahrscheinlichkeit innerhalb eines Jahres (in Prozent). Als Risikoniveau ist der Erwartungswert des Schadens pro Jahr, also die Eintrittswahrscheinlichkeit multipliziert mit der Schadensauswirkung, definiert.

Beispiel: Für das Risiko A wird geschätzt, dass es mit 10% Wahrscheinlichkeit pro Jahr auftritt und einen Schaden von 50.000 Euro verursacht. Entsprechend wird sein Risikoniveau mit 5.000 Euro/Jahr berechnet. In den Akzeptanzkriterien wurde (im Rahmen eines anderen Verfahrens) definiert, dass nur Risiken mit einem Niveau von unter 10.000 Euro / Jahr zu akzeptieren sind.

Welche Aussagen treffen zu?

a) Im beschriebenen Verfahren fehlt ein wichtiger dritter Risikofaktor
b) Es handelt sich hier um ein Verfahren zur Risikoidentifikation
c) Das Risiko A entspricht dem genannten Risikoakzeptanzkriterium

34) Bei einer Managementbewertung sind Rückmeldungen über die Informationssicherheitsleistung zu behandeln.

Zu welchen Aspekten bzw. Themen sind hierbei die Entwicklungen zu berücksichtigen?

a) Ergebnisse von Überwachungen und Messungen
b) Gesamtkosten für das ISMS
c) Nichtkonformitäten und Korrekturmaßnahmen

35) Welche Controls sind Teil von A.14 "Anschaffung, Entwicklung und Instandhalten von Systemen" in der ISO/IEC 27001?

a) Richtlinie für Entwicklung von Prototypen
b) Schutz von Testdaten
c) Richtlinie für sichere Entwicklung

36) Was sind Schutzziele für Informationen (Eigenschaften, die im Rahmen der Informationssicherheit erhalten werden sollen)?

a) Fachliche Korrektheit
b) Anonymität
c) Nicht-Abstreitbarkeit (non-repudiation)

37) Man kann die Handhabung von Informationssicherheitsvorfällen und Verbesserungen, so wie sie in ISO/IEC 27001 A.16.1 beschrieben ist, als Prozess verstehen.

Was wären für Konformität zu ISO/IEC 27001 notwendige Aktivitäten dieses Prozesses?

a) Veränderungen an der Infrastruktur vornehmen um zukünftige Informationssicherheitsereignisse zu vermeiden.
b) Informationssicherheitsereignisse melden
c) Informationssicherheitsereignisse beurteilen und klassifzieren (inbesondere in Hinblick darauf, ob ein Informationssicherheitsvorfall vorliegt oder nicht)

38) Welche Aussagen zu Informationssicherheitsvorfällen (information security incidents) sind zutreffend?

a) Jedes Informationssicherheitsereignis ist auch ein Informationssicherheitsvorfall.
b) Ein Informationssicherheitsvorfall kann z.B. dann entstehen, wenn eine Schwachstelle (vulnerability) durch einen Angreifer ausgenutzt wird.
c) Ein Informationssicherheitsvorfall ist ein einzelnes oder eine Reihe von Informationssicherheitsereignissen.
d) Eine Häufung von mehreren auch kleinen Informationsicherheitsereignissen ist als Informationsicherheitsproblem zu definieren

39) Welche Apekte muss eine Managementbewertung nach ISO/IEC 27001 behandeln?

a) Status von Maßnahmen vorheriger Managementbewertungen
b) Veränderungen bei externen und internen Themen
c) Status der aktuell in Bearbeitung befindlichen Sicherheitsereignisse

40) Was sind Anforderungen an den Betrieb eines ISMS (ISO/IEC 27001, Kapitel 8)?

a) Die Organisation muss dokumentierte Information im notwendigen Umfang aufbewahren, so dass darauf vertraut werden kann, dass die Prozesse wie geplant umgesetzt wurden.
b) Die Organisation muss die Prozesse zur Erfüllung der Informationssicherheitsanforderungen planen, verwirklichen und steuern.
c) Die Organisation muss dokumentierte Information über die Ergebnisse der Beurteilung von Informationssicherheitsrisiken aufbewahren.
d) Die Organisation muss sicherstellen, dass ausgegliederte Prozesse bestimmt und gesteuert werden.

41) Was ist im Kontext eines ISMS in Bezug auf die Informationsklassifizierung (Maßnahmenziel A.8.2) zu beachten?

a) Bei der Klassifikation von Information ist ihr Wert zu berücksichtigen.
b) Bei der Klassifikation von Information ist ihre Kritikalität zu berücksichtigen.
c) Bei der Klassifikation von Information sind gesetzliche Anforderungen zu berücksichtigen.

42) In ihrer Organisation sollen in einigen Monaten die Controls zur Kommunikationssicherheit (A.13) auditiert werden.

Sie haben ein erstes Self-Assessment durchgeführt und dabei einige Feststellungen gemacht.

Welche der festgestellten Umstände würden auf alle Fälle im Audit eine Abweichung darstellen und sollten daher unbedingt vor dem Audit behandelt werden?

a) Nicht der gesamte Datenverkehr über die Kommunikationssnetze ist verschlüsselt.
b) Zum Thema Informationsübertragung existiert keine Richtlinie.
c) Die Trennung von Netzwerken erfolgt nur über VPNs.
d) Zur Sicherung von Anwendungsdiensten in öffentlichen Netzwerken existieren keine Vorgaben und keine Dokumentation.

43) Was trifft auf ISMS-Zertifizierungen nach ISO/IEC 27001 (in Europa) grundsätzlich zu?

a) Im Rahmen der Zertifizierung lässt die Zertifizierungsstelle die Konformität des ISMS zu den Anforderungen der Norm ISO/IEC 27001 durch ein sogenanntes Zertifzierungsaudit überprüfen
b) Die Zertifizierungsstelle erfüllt die Anforderungen der ISO/IEC 27021.
c) Die Zertifizierungsstelle muss bei einer nationalen Akkredierungsstelle (z.B. in Deutschland die DAkkS) akkreditiert sein

44) Was muss die Organisation nach ISO/IEC 27001 (u.a.) für die interne und externe Kommunikation in Bezug auf das Informationssicherheitsmanagementsystem bestimmen?

a) Welche Kommunikation als unerwünscht zu klassifizieren ist
b) Worüber kommuniziert wird
c) Mit wem kommuniziert wird
d) Obergrenze für die Kommunikationskosten

45) Welche Maßnahmen sind in der ISO/IEC 27001 dem Maßnahmenziel A.12.1 "Betriebsabläufe und -verantwortlichkeiten" zugeordnet?

a) Kapazitätssteuerung
b) Dokumentierte Bedienabläufe
c) Änderungssteuerung
d) Uhrensynchronisation

46) Welche der genannten Maßnahmen (controls) gehören zum Maßnahmenziel "Benutzerzugangsverwaltung" (A.9.2)?

a) Registrierung und Deregistrierung von Benutzern
b) Physische Zutrittssteuerung
c) Entzug oder Anpassung von Zugangsrechten

47) In der Norm ISO/IEC 27001 werden unter A.18.1 Maßnahmen zur "Einhaltung gesetzlicher und vertraglicher Anforderungen" definiert.

Welche Aspekte bzw. Bereiche müssen Sie **im Kontext eines ISMS** notwendigerweise berücksichtigen, wenn Konformität zu ISO/IEC 27001 erreicht werden soll?

a) Einhaltung physikalischer Gesetze
b) Datenschutz bzw. Schutz personenbezogener Information
c) Wahrung geistige Eigentumsrechte bzw. des Urheberrechts

48) Ihre Organisation plant, die Langzeitarchivierung von Geschäftsdaten auszulagern (zu outsourcen). Unter anderem bewirbt sich die Firma ACME IT um diesen Auftrag. ACME IT wirbt damit, dass sie "nach ISO/IEC 27001 zertifziert sind". Sie wissen, dass das Zertifikat aktuell und gültig ist, nähere Informationen haben Sie aber nicht. Was bedeutet das grundlegende Vorliegen des Zertifikats bzw. welche folgenden Aussagen sind auf jeden Fall richtig?

a) ACME IT betreibt ein ISMS.
b) Alle von ACME IT erbrachten IT-Dienste unterliegen der Lenkung des ISMS.
c) Eine akkreditierte Zertifzierungsstelle hat bestätigt, dass das ISMS der ACME IT die Anforderungen der ISO/IEC 27001 erfüllt.

49) Welche Controls sind in Anhang A der ISO/IEC 27001 dem Maßnahmenziel "Geräte und Betriebsmittel" (A.11.2) zugeordnet?

a) Entfernen von Werten
b) Zuteilung von Benutzerzugängen
c) Unbeaufsichtigte Benutzergeräte
d) Richtlinie für eine aufgeräumte Arbeitsumgebung und Bildschirmsperren

50) Welche Regelungen zur Handhabung von Datenträgern können dazu beitragen, die Vetraulichkeit der gespeicherten Information zu schützen?

a) Die Verwendung von Wechseldatenträgern ist nur zulässig, wenn es dafür geschäftliche Gründe gibt.
b) Nicht mehr benötigte Inhalte auf Wechseldatenträgern sind so zu löschen, dass sie nicht (ohne erheblichen Aufwand) wiederhergestellt werden können.
c) Datenträger, die vertrauliche Daten enthalten, dürfen nur unter Einhaltung sicherer Verfahren entsorgt werden (z.B. mehrfaches Überschreiben vor der Entsorgung, schreddern ...).
d) Als vertraulich klassifizierte Daten sind bei Speicherung auf Wechseldatenträgern grundsätzlich zu verschlüsseln.