EXIN Information Security Management ISO/IEC 27001

FOUNDATION

Certified by EXIN

Musterexamen

Ausgabe 201804

Inhalt

Einführung

Dies ist das Musterexamen Information Security Foundation based on ISO/IEC 27001. Es gelten die EXIN Examen Regeln und Vorschriften.

Dieses Musterexamen erfolgt im Multiple-Choice-Verfahren und umfasst 40 Fragen. Von den pro Frage gegebenen Antworten ist jeweils nur eine richtig.

Die maximal erreichbare Punktzahl beträgt 40 Punkte. Jede richtige Antwort zählt einen Punkt. Das Examen gilt als bestanden, wenn ein Kandidat 26 oder mehr Punkte erreicht hat.

Die Dauer des Examens ist 60 Minuten.

Viel Erfolg!

Musterexamen

1 / 40
Wie stehen Daten und Informationen zueinander in Beziehung?

A. Daten sind strukturierte Informationen.
B. Mit Informationen bezeichnet man die Bedeutung und den Wert einer Datensammlung.

2 / 40
Ein Verwaltungsamt möchte eine Brandversicherung abschließen und muss dazu den Wert der von ihm verwalteten Daten bestimmen.

Welcher der unten genannten Faktoren spielt dabei **keine** Rolle?

A. Der Dateninhalt
B. Das Maß, in dem fehlende, unvollständige oder falsche Daten wiederhergestellt werden können.
C. Die Unentbehrlichkeit der Daten für die Geschäftsprozesse
D. Die Bedeutung der Geschäftsprozesse, für die die Daten verwendet werden.

3 / 40
Ein Hacker verschafft sich Zugriff auf einen Webserver und erhält Einblick in eine auf dem Server befindliche Datei mit Kreditkartendaten.

Gegen welchen Grundsatz der Informationssicherheit der Kreditkarte wird hier verstoßen?

A. Verfügbarkeit
B. Vertraulichkeit
C. Integrität

4 / 40
Auf dem Flur des Unternehmens, in dem Sie arbeiten, steht ein Netzwerkdrucker. Viele Mitarbeiter holen ihre Ausdrucke nicht sofort ab, sondern lassen sie im Drucker liegen.

Welche Folgen hat dieses Verhalten für die Zuverlässigkeit von Informationen?

A. Die Integrität der Informationen ist nicht länger gewährleistet.
B. Die Verfügbarkeit der Informationen ist nicht länger gewährleistet.
C. Die Vertraulichkeit der Informationen ist nicht länger gewährleistet.

5 / 40
Eine gute Risikoanalyse bietet jede Menge nützliche Informationen und verfolgt vier primäre Ziele.

Was ist **kein** primäres Ziel der Risikoanalyse?

A. Die Identifizierung von organisationseigenen Werten (Assets) und ihrem Wert für die Organisation
B. Die Durchführung von Gegenmaßnahmen
C. Die Herstellung eines Gleichgewichts zwischen den Kosten eines Informationssicherheitsvorfalls und den Kosten der Sicherheitsmaßnahmen
D. Die Bestimmung der relevanten Schwachstellen und Bedrohungen im Bereich der Informationssicherheit

6 / 40
Ein Verwaltungsamt beabsichtigt, die Gefahren zu bestimmen, denen es ausgesetzt ist.

Wie nennt man ein mögliches Informationssicherheitsereignis, das sich negativ auf die Zuverlässigkeit von Informationen auswirken kann?

A. Abhängigkeit
B. Bedrohung
C. Schwachstellen
D. Risiko

7 / 40
Was ist die Aufgabe des Risikomanagements?

A. Das Risikomanagement bestimmt, mit welcher Wahrscheinlichkeit ein bestimmtes Risiko eintreten wird.
B. Das Risikomanagement bestimmt, welcher Schaden durch mögliche Informationssicherheitsvorfälle verursacht wird.
C. Das Risikomanagement beschreibt, welchen Bedrohungen die IT-Ressourcen ausgesetzt sind.
D. Das Risikomanagement wendet Sicherheitsmaßnahmen an, um die Risiken auf ein akzeptabeles Maß zu senken.

8 / 40
Sie haben vor ein paar Jahren ein Unternehmen gegründet, dessen Belegschaft inzwischen von einem auf 20 Mitarbeiter gewachsen ist. Die Informationen Ihres Unternehmens haben einen zunehmend größeren Wert und die Tage, als Sie alles alleine regeln konnten, gehören der Vergangenheit an. Ihnen ist klar, dass Sie Maßnahmen ergreifen müssen, es fragt sich nur, welche? Sie wenden sich an einen Berater. Dieser rät Ihnen, zuerst eine qualitative Risikoanalyse durchzuführen.

Was ist eine qualitative Risikoanalyse?

A. Die qualitative Risikoanalyse berechnet mit Hilfe einer präzisen statistischen Wahrscheinlichkeitsrechnung den exakten, durch einen Schaden verursachten Verlust.
B. Die qualitative Risikoanalyse basiert auf Szenarien und Situationen und bietet einen subjektiven Blick auf die möglichen Bedrohungen.

9 / 40
In einer Niederlassung des Unternehmens Midwest Insurance kam es zu einem Brand. Die Feuerwehr war schnell am Brandort und konnte das Feuer löschen, bevor es sich ausbreitete und auf das gesamte Firmengelände übergriff. Der Server wurde jedoch bei dem Brand zerstört. Bei dem Brand wurden auch die Backup-Bänder, die in einem anderen Raum aufbewahrt wurden, und viele Dokumente völlig zerstört.

Was ist ein Beispiel für einen indirekten Schaden, der von diesem Brand verursacht wurde?

A. Die zerstörten Backup-Bänder
B. Die verbrannten Computer-Systeme
C. Die verbrannten Dokumente
D. Die aufgrund der Löscharbeiten entstandenen Wasserschäden

10 / 40
Sie sind der Eigentümer des Kurierunternehmens SpeeDelivery. Sie haben eine Risikoanalyse durchgeführt und möchten jetzt Ihre Risikostrategie festlegen. Sie entschließen sich, Sicherheitsmaßnahmen auf große Risiken zu beschränken und bei kleinen Risiken keine Maßnahmen zu ergreifen.

Wie nennt man diese Risikostrategie?

A. Risikotragfähig
B. Risikovermeidung
C. Risikoneutral

11 / 40
Was ist ein Beispiel für eine Bedrohung, die vom Menschen ausgeht?

A. Das Netzwerk wird über einen USB-Stick mit einem Virus infiziert.
B. Der Server-Raum ist zu staubig.
C. Ein Leck hat einen Stromausfall zur Folge.

12 / 40
Was ist ein Beispiel für eine Bedrohung, die vom Menschen ausgeht?

A. Blitzschlag
B. Feuer
C. Phishing

13 / 40
Sie arbeiten im Büro eines großen Unternehmens. Sie erhalten einen Anruf. Der Anrufer gibt vor, ein Helpdesk-Mitarbeiter zu sein und fragt Sie nach Ihrem Passwort.

Wie nennt man diese Art von Bedrohung?

A. Natürliche Bedrohung
B. Organisatorische Bedrohung
C. Social Engineering

14 / 40
In einer Niederlassung einer Krankenversicherung bricht ein Feuer aus. Das Personal wird auf andere Niederlassungen in der Umgebung verteilt und soll dort weiter arbeiten.

Wo im Lebenszyklus eines Informationssicherheitsvorfalls sind solche Standby-Arrangements angesiedelt?

A. Zwischen Bedrohung und Vorfall
B. Zwischen Wiederherstellung und Bedrohung
C. Zwischen Schaden und Wiederherstellung
D. Zwischen Vorfall und Schaden

15 / 40
Informationen umfassen verschiedene Aspekte der Zuverlässigkeit. Die Zuverlässigkeit von Informationen ist konstant bedroht. Beispiele für mögliche Bedrohungen sind u.a.: Ein lockeres Kabel, die versehentliche Änderung von Informationen, die Nutzung von Daten für private Zwecke und die Fälschung von Daten.

Welches dieser Beispiele ist eine Bedrohung für die Integrität von Informationen?

A. Ein lockeres Kabel
B. Die versehentliche Änderung von Daten
C. Die Nutzung von Daten für private Zwecke

16 / 40
Ein Mitarbeiter streitet ab, eine bestimmte Nachricht versendet zu haben.

Welcher Aspekt der Zuverlässigkeit von Informationen ist hier in Gefahr?

A. Die Verfügbarkeit
B. Die Richtigkeit
C. Die Integrität
D. Die Vertraulichkeit

17 / 40
Wie lässt sich der Zweck von Weisungen und Richtlinien zur Informationssicherheit **am besten** beschreiben?

A. Die Weisungen und Richtlinien dokumentieren die Risikoanalyse und die Suche nach Gegenmaßnahmen.
B. Die Weisungen und Richtlinien bieten der Geschäftsführung Orientierung und Unterstützung im Bereich der Informationssicherheit.
C. Die Weisungen und Richtlinien konkretisieren die Planung der Informationssicherheit und enthalten die erforderlichen Einzelheiten.
D. Die Weisungen und Richtlinien bieten Einblicke in Bedrohungen und die möglichen Folgen.

18 / 40
Einem Mitarbeiter des Helpdesk wird ein Sicherheitsvorfall bezüglich eines Webservers gemeldet. Da seine Kollegin mehr Erfahrung mit Webservern hat, leitet er den Fall an sie weiter.

Wie nennt man diesen Vorgang?

A. Fachliche Eskalation
B. Hierarchische Eskalation

19 / 40
Eine Mitarbeiterin des Versicherungsunternehmens entdeckt, dass das Ablaufdatum einer Versicherungspolice ohne ihr Wissen geändert wurde. Sie ist als Einzige zur Vornahme dieser Änderung berechtigt. Sie meldet diesen Sicherheitsvorfall an den Helpdesk. Der Helpdesk-Mitarbeiter zeichnet diesbezüglich folgende Informationen auf:

•Datum und Zeit
•Beschreibung des Sicherheitsvorfalls
•Mögliche Folgen des Sicherheitsvorfalls

Welche **wichtigen** Informationen bezüglich des Sicherheitsvorfalls fehlen in den Aufzeichnungen?

A. Der Name der Person, die den Vorfall gemeldet hat
B. Der Name des Software-Pakets
C. Die PC-Nummer
D. Eine Liste der Personen, die über den Vorfall informiert wurden

20 / 40
Der Lebenszyklus eines Informationssicherheitsvorfalls besteht aus vier aufeinanderfolgenden Phasen.

Welche Phase folgt auf den Vorfall?

A. Bedrohung
B. Schaden
C. Wiederherstellung

21 / 40
Welche Informationssicherheitsmaßnahme ist eine vorbeugende Maßnahme?

A. Die Installation eines Erfassungssystems, das Änderungen am System erkennt.
B. Die Einstellung des gesamten Internetverkehrs, nachdem sich ein Hacker Zugang zu den Systemen des Unternehmens verschafft hat.
C. Die Aufbewahrung sensibler Informationen in einem Safe.

22 / 40
Was stellt im Falle eines Brandes eine unterdrückende Maßnahme dar?

A. Der Abschluss einer Brandversicherung
B. Das Löschen des Brandes, nachdem er durch einen Feuermelder entdeckt wurde
C. Die Reparatur der durch den Brand verursachten Schäden

23 / 40
Welches Ziel wird mit Klassifizierung von Informationen verfolgt?

A. Die Erarbeitung eines Handbuchs zum Umgang mit mobilen Geräten
B. Die leichtere Erkennbarkeit von Informationen durch Anbringen einer Kennzeichnung
C. Die Strukturierung der Informationen gemäß ihrer Vertraulichkeit

24 / 40
Wer ist autorisiert, die Klassifizierung eines Dokuments zu ändern?

A. Der Verfasser des Dokuments
B. Der Administrator des Dokuments
C. Der für das Dokument Verantwortliche
D. Der Vorgesetzte des für das Dokument Verantwortlichen

25 / 40
Der Zugang zu einem Computerraum ist mit Hilfe eines Karten-Lesegeräts geschützt. Nur die für das Systemmanagement zuständige Abteilung verfügt über eine Zugangskarte.

Um welche Art von Sicherheitsmaßnahme handelt es sich?

A. Eine korrigierende Sicherheitsmaßnahme
B. Eine physische Sicherheitsmaßnahme
C. Eine logische Sicherheitsmaßnahme
D. Eine unterdrückende Sicherheitsmaßnahme

26 / 40

Der Zugriff auf streng geschützte Bereiche erfordert eine starke Autorisierung. Bei einer starken Autorisierung wird die Identität einer Person mittels drei Faktoren identifiziert.

Was wird bei Eingabe der persönlichen Identifizierungsnummer (PIN) verifiziert?

A. Was man ist
B. Was man hat
C. Was man weiß

27 / 40
In der physischen Informationssicherheit können mehrere sogenannte Protection Rings angewendet werden, in denen verschiedene Maßnahmen ergriffen werden.

Was ist **kein** Protection Ring?

A. Gebäude
B. Mittlerer Ring
C. Objekt
D. Außenring

28 / 40
Welche Bedrohung kann sich bei Fehlen einer physischen Sicherheitsmaßnahme ergeben?

A. Ein Benutzer kann die Dateien eines anderen Nutzers einsehen.
B. Ein Server fährt aufgrund von Überhitzung herunter.
C. Ein vertrauliches Dokument bleibt im Drucker.
D Hacker können sich im Computernetz frei bewegen.

29 / 40
Welche Sicherheitsmaßnahme ist eine technische Maßnahme?

A. Die Zuweisung von Informationen an einen Verantwortlichen
B. Die Verschlüsselung von Dateien
C. Die Erstellung von Weisungen und Richtlinien, die festlegen, was in einer E-Mail erlaubt ist und was nicht
D. Die Aufbewahrung von Passwörtern für das Management des Systems in einem Safe

30 / 40
Die Backups des zentralen Servers werden im gleichen verschlossenen Raum aufbewahrt wie die Server selbst.

Welches Risiko ergibt sich daraus für die Organisation?

A. Bei einem Server-Ausfall dauert es lange, bis der Server wieder in Betrieb genommen werden kann.
B. Im Falle eines Brandes lässt sich der Zustand des Systems vor dem Brand nicht wiederherstellen.
C. Keiner ist für die Backups zuständig.
D. Unbefugte können leicht auf die Backups zugreifen.

31 / 40
Welche Art von Schadsoftware erstellt auf einem infizierten Computer ein Netzwerk?

A. Eine logische Bombe (Logic Bomb)
B. Ein Storm Worm oder Storm Botnet
C. Ein Trojaner
D. Spyware

32 / 40
In einer Organisation entdeckt der Informationssicherheits-Beauftragte, dass ein Computer eines Mitarbeiters mit Schadsoftware infiziert ist. Die Schadsoftware wurde bei einem gezielten Phishing-Angriff installiert.

Welche Maßnahme eignet sich am **besten,** um solche Vorfälle künftig zu vermeiden?

A. Die Umsetzung der MAC-Technologie
B. Die Einführung eines Security Awareness Programms
C. Die Aktualisierung der Regeln der Firewall
D. Die Aktualisierung der Signaturen des Spam-Filters

33 / 40
Sie arbeiten in der IT-Abteilung eines mittelständischen Unternehmens. Es sind bereits mehrmals vertrauliche Informationen in die falschen Hände geraten. Dies hat dem Image des Unternehmens geschadet. Sie wurden gebeten, in Ihrem Unternehmen organisatorische Maßnahmen für die Laptops vorzuschlagen.

Welchen Schritt sollten Sie als **erstes** setzen?

A. Weisungen und Richtlinien zu mobilen Medien (PDAs, Laptops, Smartphones, USB-Sticks) formulieren.
B. Wachpersonal ernennen
C. Die Festplatten der Laptops und die USB-Sticks verschlüsseln
D. Weisungen und Richtlinien zur Zugangs- und Zugriffskontrolle einführen

34 / 40
Wie nennt man ein System, das in einer Organisation für eine einheitliche und logisch zusammenhängende Informationssicherheit sorgt?

A. Das Informationssicherheit-Management-System (ISMS)
B. Das Rootkit
C. Die Sicherheitsvorschriften für besondere Regierungsinformationen

35 / 40
Wie nennt man 'Identifizierung ob die Identität einer Person korrekt ist'?

A. Authentisierung
B. Autorisierung
C. Identifizierung

36 / 40
Warum muss ein Notfallwiederherstellungsplan ständig aktualisiert und in regelmäßigen Abständen getestet werden?

A. Um stets Zugriff auf die neuesten Backups zu haben, die sich außerhalb des Büros befinden.
B. Um mit den täglich auftretenden Fehlern fertig zu werden.
C. Weil anderenfalls die bei einer weitreichenden Störung ergriffenen Maßnahmen und die Verfahren zur Behebung von Sicherheitsvorfällen möglicherweise nicht ausreichend oder veraltet sind.
D. Weil dies laut Datenschutzgesetz notwendig ist.

37 / 40
Auf der Basis von welchem Gesetz kann eine Person verlangen, die über sie gespeicherten Daten einzusehen?

A. Auf der Basis des Bundesarchivgesetzes
B. Auf der Basis des Datenschutzgesetzes
C. Auf der Basis des Gesetzes zur Bekämpfung der Computerkriminalität
D. Auf der Basis des Gesetzes zur Regelung des Zugangs zu Informationen des Bundes (Informationsfreiheitsgesetz)

38 / 40
Welche der nachfolgenden Möglichkeiten ist eine gesetzliche oder behördliche Vorschrift der Informationssicherheit, die für alle Organisationen gilt?

A. Geistiges Urheberrecht
B. ISO/IEC 27001
C. ISO/IEC 27002
D. Datenschutzgesetz

39 / 40
Sie sind der Eigentümer des Kurierunternehmen SpeeDelivery. Sie beschäftigen ein paar Leute, die während sie auf ihre nächste Auslieferung warten, andere Aufgaben erfüllen können. Sie stellen jedoch fest, dass ihre Mitarbeiter die Zeit dazu nutzen, private Mails zu versenden und im Internet zu surfen.

Wie können Sie im Rahmen des Gesetzes die Verwendung des Internets und des E-Mail-Programms am besten regeln?

A. Durch die Installation einer Anwendung, die den Zugriff auf gewisse Webseiten verwehrt und Anhänge in E-Mails herausfiltert
B. Durch die Ausarbeitung eines Verhaltenskodex zur Nutzung von Internet und E-Mail-Verkehr, in dem die Rechte und Pflichten des Arbeitgebers und der Mitarbeiter festgelegt werden
C. Durch die Implementierung von Geheimhaltungsvorschriften
D. Durch die Installation eines Virenscanners

40 / 40
Unter welchen Bedingungen darf ein Arbeitgeber überprüfen, ob Internet und E-Mail am Arbeitsplatz für private Zwecke genutzt werden?

A. Der Arbeitgeber darf dies überprüfen, wenn er die Mitarbeiter nach der Überprüfung stets in Kenntnis setzt.
B. Der Arbeitgeber darf dies überprüfen, wenn die Mitarbeiter wissen, dass eine Überprüfung stattfinden könnte.
C. Der Arbeitgeber darf dies überprüfen, wenn auch eine Firewall installiert ist.

Antwortschlüssel

1 / 40
Wie stehen Daten und Informationen zueinander in Beziehung?

A. Daten sind strukturierte Informationen.
B. Mit Informationen bezeichnet man die Bedeutung und den Wert einer Datensammlung.

A. Falsch. Informationen sind strukturierte Daten
B. Richtig. Informationen sind Daten mit einer Bedeutung in einem bestimmten Kontext für ihre Empfänger. (Kapitel 3)

2 / 40
Ein Verwaltungsamt möchte eine Brandversicherung abschließen und muss dazu den Wert der von ihm verwalteten Daten bestimmen.

Welcher der unten genannten Faktoren spielt dabei **keine** Rolle?

A. Der Dateninhalt
B. Das Maß, in dem fehlende, unvollständige oder falsche Daten wiederhergestellt werden können.
C. Die Unentbehrlichkeit der Daten für die Geschäftsprozesse
D. Die Bedeutung der Geschäftsprozesse, für die die Daten verwendet werden.

A. Richtig. Der Dateninhalt ist nicht maßgeblich für den Wert der Daten. (Kapitel 4)
B. Falsch. Fehlende, unvollständige oder falsche Daten, die leicht wiederhergestellt werden können, haben einen geringeren Wert als Daten, die nur sehr schwer oder gar nicht wiederhergestellt werden können.
C. Falsch. Die Unentbehrlichkeit der Daten für Geschäftsprozesse ist teilweise maßgeblich für deren Wert.
D. Falsch. Daten, die für wichtige Geschäftsprozesse von entscheidender Bedeutung sind, haben aus diesem Grund auch einen hohen Wert.

3 / 40
Ein Hacker verschafft sich Zugriff auf einen Webserver und erhält Einblick in eine auf dem Server befindliche Datei mit Kreditkartendaten.

Gegen welchen Grundsatz der Informationssicherheit der Kreditkarte wird hier verstoßen?

A. Verfügbarkeit
B. Vertraulichkeit
C. Integrität

A. Falsch. Der Hacker hat die Datei nicht gelöscht oder den Zugang für autorisierte Personen in irgendeiner Weise verweigert, deswegen ist die Verfügbarkeit nicht geschädigt worden.
B. Richtig. Der Hacker war in der Lage, die Datei (Vertraulichkeit) zu lesen. (Kapitel 3)
C. Falsch. Es wurde keine Informationen in der Kreditkarten-Datei verändert; deswegen ist die Integrität der Datei nicht verletzt worden.

4 / 40
Auf dem Flur des Unternehmens, in dem Sie arbeiten, steht ein Netzwerkdrucker. Viele Mitarbeiter holen ihre Ausdrucke nicht sofort ab, sondern lassen sie im Drucker liegen.

Welche Folgen hat dieses Verhalten für die Zuverlässigkeit von Informationen?

A. Die Integrität der Informationen ist nicht länger gewährleistet.
B. Die Verfügbarkeit der Informationen ist nicht länger gewährleistet.
C. Die Vertraulichkeit der Informationen ist nicht länger gewährleistet.

A. Falsch. Die Integrität der Information ist immer noch gewährleistet, weil sie auf Papier ist.
B. Falsch. Die Information ist immer noch in dem System vorhanden, das verwendet wurde, um das Dokument zu erstellen und auszudrucken.
C. Richtig. Die Information könnte gelesen von Personen, die keinen Zugang zu den Informationen haben sollten, gelesen werden. (Kapitel 3)

5 / 40
Eine gute Risikoanalyse bietet jede Menge nützliche Informationen und verfolgt vier primäre Ziele.

Was ist **kein** primäres Ziel der Risikoanalyse?

A. Die Identifizierung von organisationseigenen Werten (Assets) und ihrem Wert für die Organisation
B. Die Durchführung von Gegenmaßnahmen
C. Die Herstellung eines Gleichgewichts zwischen den Kosten eines Informationssicherheitsvorfalls und den Kosten der Sicherheitsmaßnahmen
D. Die Bestimmung der relevanten Schwachstellen und Bedrohungen im Bereich der Informationssicherheit

A. Falsch. Dies ist eines der Hauptziele einer Risikoanalyse.
B. Richtig. Dies ist kein Ziel einer Risikoanalyse. Maßnahmen können ausgewählt werden, wenn in einer Risikoanalyse bestimmt worden ist, welches Risiko eine Sicherheitsmaßnahme erfordert. (Kapitel 3)
C. Falsch. Dies ist eines der Hauptziele einer Risikoanalyse.
D. Falsch. Dies ist eines der Hauptziele einer Risikoanalyse.

6 / 40
Ein Verwaltungsamt beabsichtigt, die Gefahren zu bestimmen, denen es ausgesetzt ist.

Wie nennt man ein mögliches Informationssicherheitsereignis, das sich negativ auf die Zuverlässigkeit von Informationen auswirken kann?

A. Abhängigkeit
B. Bedrohung
C. Schwachstellen
D. Risiko

A. Falsch. Abhängigkeit ist kein Ereignis.
B. Richtig. Eine Bedrohung ist ein mögliches Informationssicherheitsereignis, das sich negativ auf die Zuverlässigkeit von Informationen auswirken kann. (Kapitel 3)
C. Falsch. Schwachstellen bezeichnen wie anfällig ein Objekt für eine Bedrohung ist.
D. Falsch. Das Risiko bezeichnet den Schaden über einen bestimmten Zeitraum, der normalerweise infolge einer oder mehrerer Bedrohungen, die zu Störungen führen, erwartet wird.

7 / 40
Was ist die Aufgabe des Risikomanagements?

A. Das Risikomanagement bestimmt, mit welcher Wahrscheinlichkeit ein bestimmtes Risiko eintreten wird.
B. Das Risikomanagement bestimmt, welcher Schaden durch mögliche Informationssicherheitsvorfälle verursacht wird.
C. Das Risikomanagement beschreibt, welchen Bedrohungen die IT-Ressourcen ausgesetzt sind.
D. Das Risikomanagement wendet Sicherheitsmaßnahmen an, um die Risiken auf ein akzeptabeles Maß zu senken.

A. Falsch. Das ist Aufgabe der Risikoanalyse.
B. Falsch. Das ist Aufgabe der Risikoanalyse.
C. Falsch. Das ist Aufgabe der Risikoanalyse.
D. Richtig. Die Aufgabe des Risikomanagements ist es, das Risiko auf ein akzeptables Maß zu senken. (Kapitel 3)

8 / 40
Sie haben vor ein paar Jahren ein Unternehmen gegründet, dessen Belegschaft inzwischen von einem auf 20 Mitarbeiter gewachsen ist. Die Informationen Ihres Unternehmens haben einen zunehmend größeren Wert und die Tage, als Sie alles alleine regeln konnten, gehören der Vergangenheit an. Ihnen ist klar, dass Sie Maßnahmen ergreifen müssen, es fragt sich nur, welche? Sie wenden sich an einen Berater. Dieser rät Ihnen, zuerst eine qualitative Risikoanalyse durchzuführen.

Was ist eine qualitative Risikoanalyse?

A. Die qualitative Risikoanalyse berechnet mit Hilfe einer präzisen statistischen Wahrscheinlichkeitsrechnung den exakten, durch einen Schaden verursachten Verlust.
B. Die qualitative Risikoanalyse basiert auf Szenarien und Situationen und bietet einen subjektiven Blick auf die möglichen Bedrohungen.

A. Falsch. In einer quantitativen Risikoanalyse wird versucht, numerisch die Wahrscheinlichkeiten der verschiedenen Vorkommnisse und das wahrscheinliche Ausmaß der Verluste zu bestimmen, falls ein bestimmtes Ereignis eintritt.
B. Richtig. Eine qualitative Risikoanalyse beinhaltet die Definition der verschiedenen Bedrohungen, die Festsetzung des Umfangs der Schwachstellen, sowie die entwickelten Gegenmaßnahmen im Falle eines Angriffs. (Kapitel 3).

9 / 40
In einer Niederlassung des Unternehmens Midwest Insurance kam es zu einem Brand. Die Feuerwehr war schnell am Brandort und konnte das Feuer löschen, bevor es sich ausbreitete und auf das gesamte Firmengelände übergriff. Der Server wurde jedoch bei dem Brand zerstört. Bei dem Brand wurden auch die Backup-Bänder, die in einem anderen Raum aufbewahrt wurden, und viele Dokumente völlig zerstört.

Was ist ein Beispiel für einen indirekten Schaden, der von diesem Brand verursacht wurde?

A. Die zerstörten Backup-Bänder
B. Die verbrannten Computer-Systeme
C. Die verbrannten Dokumente
D. Die aufgrund der Löscharbeiten entstandenen Wasserschäden

A. Falsch. Geschmolzene Backup-Bänder sind durch das Feuer direkt verursachte Schäden.
B. Falsch. Verbrannte Computer-Systeme sind durch das Feuer direkt verursachte Schäden.
C. Falsch. Der Verlust von Kundenvertrauen ist ein indirekter Schaden.
D. Richtig. Die Unfähigkeit des Unternehmens, gesetzliche Verpflichtungen zu erfüllen, ist ein indirekter Schaden. (Kapitel 3)

10 / 40
Sie sind der Eigentümer des Kurierunternehmens SpeeDelivery. Sie haben eine Risikoanalyse durchgeführt und möchten jetzt Ihre Risikostrategie festlegen. Sie entschließen sich, Sicherheitsmaßnahmen auf große Risiken zu beschränken und bei kleinen Risiken keine Maßnahmen zu ergreifen.

Wie nennt man diese Risikostrategie?

A. Risikotragfähig
B. Risikovermeidung
C. Risikoneutral

A. Richtig. Dies bedeutet, bestimmte Risiken werden akzeptiert. (Kapitel 3)
B. Falsch. Dies bedeutet, dass Maßnahmen ergriffen werden, die die Bedrohung auf ein solches Ausmaß reduzieren, dass es zu keinem Vorfall mehr kommt.
C. Falsch. Dies bedeutet, dass die Sicherheitsmaßnahmen so getroffen werden, dass die Bedrohungen entweder nicht mehr auftreten, oder, wenn sie es doch tun, der resultierende Schaden minimiert ist.

11 / 40
Was ist ein Beispiel für eine Bedrohung, die vom Menschen ausgeht?

A. Das Netzwerk wird über einen USB-Stick mit einem Virus infiziert.
B. Der Server-Raum ist zu staubig.
C. Ein Leck hat einen Stromausfall zur Folge.

A. Richtig. Ein USB-Stick wird stets von einem Menschen verwendet. Wird das Netzwerk dadurch mit einem Virus infiziert, so stellt dies eine Bedrohung dar, die vom Menschen ausgeht. (Kapitel 3)
B. Falsch. Staub ist keine Bedrohung, die vom Menschen ausgeht.
C. Falsch. Ein Leck ist keine Bedrohung, die vom Menschen ausgeht.

12 / 40
Was ist ein Beispiel für eine Bedrohung, die vom Menschen ausgeht?

A. Blitzschlag
B. Feuer
C. Phishing

A. Falsch. Ein Blitzschlag ist ein Beispiel für eine Bedrohung, die nicht vom Menschen ausgeht.
B. Falsch. Feuer ist ein Beispiel für eine Bedrohung, die nicht vom Menschen ausgeht.
C. Richtig. Phishing (bei dem Anwender auf falsche Webseiten gelockt werden) ist eine Form der Bedrohung, die vom Menschen ausgeht (Kapitel 3)

13 / 40
Sie arbeiten im Büro eines großen Unternehmens. Sie erhalten einen Anruf. Der Anrufer gibt vor, ein Helpdesk-Mitarbeiter zu sein und fragt Sie nach Ihrem Passwort.

Wie nennt man diese Art von Bedrohung?

A. Natürliche Bedrohung
B. Organisatorische Bedrohung
C. Social Engineering

A. Falsch. Ein Anruf ist ein menschliches Handeln, keine natürliche Bedrohung.
B. Falsch. Der Begriff "Organisations Bedrohung" ist keine gemeinsame Bezeichnung für eine Art von Bedrohung.
C. Richtig. Das Verwenden der richtigen Ausdrücke oder Namen von bekannten Menschen und ihren Abteilungen, vermittelt den Eindruck, ein Kollege versucht Unternehmens- und Geschäftsgeheimnisse zu erhalten. Sie sollten überprüfen, ob Sie tatsächlich mit dem Helpdesk sprechen. Ein Helpdesk-Mitarbeiter wird nie nach Ihrem Passwort fragen. (Kapitel 3)

14 / 40
In einer Niederlassung einer Krankenversicherung bricht ein Feuer aus. Das Personal wird auf andere Niederlassungen in der Umgebung verteilt und soll dort weiter arbeiten.

Wo im Lebenszyklus eines Informationssicherheitsvorfalls sind solche Standby-Arrangements angesiedelt?

A. Zwischen Bedrohung und Vorfall
B. Zwischen Wiederherstellung und Bedrohung
C. Zwischen Schaden und Wiederherstellung
D. Zwischen Vorfall und Schaden

A. Falsch. Die Durchführung eines Standby-Arrangements ohne vorhergehenden Vorfall ist äußerst kostspielig.
B. Falsch. Die Wiederherstellung erfolgt erst nach Inkrafttreten eines Standby-Arrangements.
C. Falsch. Ein Standby-Arrangement hält Schaden und Wiederherstellung in Grenzen.
D. Richtig. Ein Standby-Arrangement ist eine unterdrückende Maßnahme, die zur Schadensbegrenzung ergriffen wird. (Kapitel 3)

15 / 40
Informationen umfassen verschiedene Aspekte der Zuverlässigkeit. Die Zuverlässigkeit von Informationen ist konstant bedroht. Beispiele für mögliche Bedrohungen sind u.a.: Ein lockeres Kabel, die versehentliche Änderung von Informationen, die Nutzung von Daten für private Zwecke und die Fälschung von Daten.

Welches dieser Beispiele ist eine Bedrohung für die Integrität von Informationen?

A. Ein lockeres Kabel
B. Die versehentliche Änderung von Daten
C. Die Nutzung von Daten für private Zwecke

A. Falsch. Ein lockeres Kabel ist eine Bedrohung der Verfügbarkeit von Informationen.
B. Richtig. Das versehentliche Ändern von Daten ist eine Bedrohung der Datenintegrität.(Kapitel 3)
C. Falsch. Die Nutzung der Daten für private Zwecke ist eine Form des Missbrauchs und eine Bedrohung der Vertraulichkeit von Informationen.

16 / 40
Ein Mitarbeiter streitet ab, eine bestimmte Nachricht versendet zu haben.

Welcher Aspekt der Zuverlässigkeit von Informationen ist hier in Gefahr?

A. Die Verfügbarkeit
B. Die Richtigkeit
C. Die Integrität
D. Die Vertraulichkeit

A. Falsch. Ein Beispiel für eine Bedrohung der Verfügbarkeit wäre eine Überlastung der Infrastruktur.
B. Falsch. Die Richtigkeit der Daten ist kein Aspekt der Zuverlässigkeit, sondern ein Merkmal der Integrität.
C. Richtig. Das Abstreiten, eine Nachricht gesendet zu haben, hängt mit der Nichtabstreitbarkeit zusammen und stellt damit eine Bedrohung der Integrität dar, die ein Aspekt der Zuverlässigkeit ist. (Kapitel 3)
D. Falsch. Der Missbrauch bzw. die Enthüllung von Daten ist eine Bedrohung der Vertraulichkeit.

17 / 40
Wie lässt sich der Zweck von Weisungen und Richtlinien zur Informationssicherheit am besten beschreiben?

A. Die Weisungen und Richtlinien dokumentieren die Risikoanalyse und die Suche nach Gegenmaßnahmen.
B. Die Weisungen und Richtlinien bieten der Geschäftsführung Orientierung und Unterstützung im Bereich der Informationssicherheit.
C. Die Weisungen und Richtlinien konkretisieren die Planung der Informationssicherheit und enthalten die erforderlichen Einzelheiten.
D. Die Weisungen und Richtlinien bieten Einblicke in Bedrohungen und die möglichen Folgen.

A. Falsch. Diesen Zweck verfolgen die Risikoanalyse und das Risikomanagement.
B. Richtig. Die Weisungen und Richtlinien der Informationssicherheit bieten der Geschäftsführung Orientierung und Unterstützung im Bereich der Informationssicherheit. (Kapitel 5)
C. Falsch. Der Sicherheitsplan konkretisiert die Weisungen und Richtlinien zur Informationssicherheit. Der Plan enthält die gewählten Maßnahmen, die Verantwortlichkeiten und Zuständigkeiten, die Richtlinien für die Umsetzung der Maßnahmen etc.
D. Falsch. Diesen Zweck verfolgt die Bedrohungsanalyse.

18 / 40
Einem Mitarbeiter des Helpdesk wird ein Sicherheitsvorfall bezüglich eines Webservers gemeldet. Da seine Kollegin mehr Erfahrung mit Webservern hat, leitet er den Fall an sie weiter.

Wie nennt man diesen Vorgang?

A. Fachliche Eskalation
B. Hierarchische Eskalation

A. Richtig. Wenn der Helpdesk-Mitarbeiter nicht in der Lage ist, sich persönlich mit dem Vorfall zu beschäftigen, kann der Vorfall einer Person mit mehr Know-how gemeldet werden, die in der Lage ist, das Problem zu lösen. Dies ist eine funktionelle (horizontale) Eskalation. (Kapitel 16)
B. Falsch. Dies ist eine funktionelle (horizontale) Eskalation. Hierarchische Eskalation ist, wenn eine Aufgabe jemandem mit mehr Autorität übertragen wird.

19 / 40
Eine Mitarbeiterin des Versicherungsunternehmens entdeckt, dass das Ablaufdatum einer Versicherungspolice ohne ihr Wissen geändert wurde. Sie ist als Einzige zur Vornahme dieser Änderung berechtigt. Sie meldet diesen Sicherheitsvorfall an den Helpdesk. Der Helpdesk-Mitarbeiter zeichnet diesbezüglich folgende Informationen auf:

•Datum und Zeit
•Beschreibung des Sicherheitsvorfalls
•Mögliche Folgen des Sicherheitsvorfalls

Welche **wichtigen** Informationen bezüglich des Sicherheitsvorfalls fehlen in den Aufzeichnungen?

A. Der Name der Person, die den Vorfall gemeldet hat
B. Der Name des Software-Pakets
C. Die PC-Nummer
D. Eine Liste der Personen, die über den Vorfall informiert wurden

A. Richtig. Bei der Meldung eines Sicherheitsvorfalls muss mindestens der Name der Person, die den Vorfall meldet, aufgezeichnet werden (Kapitel 16)
B. Falsch. Hierbei handelt es sich um eine zusätzliche Information, die zu einem späteren Zeitpunkt hinzugefügt werden kann.
C. Falsch. Hierbei handelt es sich um eine zusätzliche Information, die zu einem späteren Zeitpunkt hinzugefügt werden kann.
D. Falsch. Hierbei handelt es sich um eine zusätzliche Information, die zu einem späteren Zeitpunkt hinzugefügt werden kann.

20 / 40
Der Lebenszyklus eines Informationssicherheitsvorfalls besteht aus vier aufeinanderfolgenden Phasen.

Welche Phase folgt auf den Vorfall?

A. Bedrohung
B. Schaden
C. Wiederherstellung

A. Falsch. Der Schaden tritt erst nach dem Vorfall ein.
B. Richtig. Die Phasen im Lebenszyklus eines Informationssicherheitsvorfalls erfolgen in folgender Reihenfolge: Bedrohung, Vorfall, Schaden, Wiederherstellung. (Kapitel 16)
C. Falsch. Der Vorfall folgt auf die Bedrohung.

21 / 40
Welche Informationssicherheitsmaßnahme ist eine vorbeugende Maßnahme?

A. Die Installation eines Erfassungssystems, das Änderungen am System erkennt.
B. Die Einstellung des gesamten Internetverkehrs, nachdem sich ein Hacker Zugang zu den Systemen des Unternehmens verschafft hat.
C. Die Aufbewahrung sensibler Informationen in einem Safe.

A. Falsch. Über ein Logging-System kann erst nach dem Vorfall untersucht werden, was passiert ist. Dies ist eine erkennende Maßnahme, die auf die Entdeckung von Vorfällen abzielt.
B. Falsch. Das Herunterfahren des gesamten Internet-Verkehrs ist eine repressive Maßnahme zur Begrenzung eines Vorfalls.
C. Richtig. Ein Safe ist eine vorbeugende Maßnahme die vermeidet, dass Schäden an den sensiblen Informationen in Sicherheitskassetten entstehen können. (Kapitel 3).

22 / 40
Was stellt im Falle eines Brandes eine unterdrückende Maßnahme dar?

A. Der Abschluss einer Brandversicherung
B. Das Löschen des Brandes, nachdem er durch einen Feuermelder entdeckt wurde
C. Die Reparatur der durch den Brand verursachten Schäden

A. Falsch. Abschluss einer Versicherung schützt vor den finanziellen Folgen eines Brandes.
B. Richtig. Diese repressive Maßnahme minimiert den durch das Feuer verursachten Schaden. (Kapitel 3)
C. Falsch. Dies ist keine repressive Maßnahme. Sie minimiert den durch das Feuer verursachten Schaden nicht.

23 / 40
Welches Ziel wird mit Klassifizierung von Informationen verfolgt?

A. Die Erarbeitung eines Handbuchs zum Umgang mit mobilen Geräten
B. Die leichtere Erkennbarkeit von Informationen durch Anbringen einer Kennzeichnung
C. Die Strukturierung der Informationen gemäß ihrer Vertraulichkeit

A. Falsch. Das Erstellen eines Handbuchs hat mit Benutzerrichtlinien zu tun und ist keine Einstufung der Informationen.
B. Falsch. Anbringen von Etiketten auf Informationen ist Bezeichnung und eine besondere Form der Kategorisierung, die auf Klassifizierung folgt.
C. Richtig. Klassifizierung der Informationen wird verwendet, um die verschiedenen Empfindlichkeitsniveaus in die Informationen strukturiert werden kann, zu definieren. (Kapitel 3 und 8)

24 / 40

Wer ist autorisiert, die Klassifizierung eines Dokuments zu ändern?

A. Der Verfasser des Dokuments
B. Der Administrator des Dokuments
C. Der für das Dokument Verantwortliche
D. Der Vorgesetzte des für das Dokument Verantwortlichen

A. Falsch. Der Verfasser darf den Inhalt ändern, aber die Klassifizierung eines Dokuments nicht.
B. Falsch. Der Administrator darf die Klassifizierung eines Dokuments nicht ändern.
C. Richtig. Der Inhaber muss den Vermögenswert klassifizieren oder falls notwendig re-klassifizieren, und ist somit befugt, die Klassifizierung eines Dokuments zu ändern. (Kapitel 3 und 8)
D. Falsch. Der Manager des Inhabers hat keine Autorität dazu.

25 / 40
Der Zugang zu einem Computerraum ist mit Hilfe eines Karten-Lesegeräts geschützt. Nur die für das Systemmanagement zuständige Abteilung verfügt über eine Zugangskarte.

Um welche Art von Sicherheitsmaßnahme handelt es sich?

A. Eine korrigierende Sicherheitsmaßnahme
B. Eine physische Sicherheitsmaßnahme
C. Eine logische Sicherheitsmaßnahme
D. Eine unterdrückende Sicherheitsmaßnahme

A. Falsch. Eine korrigierende Sicherheitsmaßnahme ist eine Maßnahme zur Wiederherstellung.
B. Richtig. Hierbei handelt es sich um eine physische Sicherheitsmaßnahme. (Kapitel 3 und 11)
C. Falsch. Eine logische Sicherheitsmaßnahme kontrolliert den Zugriff auf die Software und die Informationen, nicht den physischen Zugang zu einem Raum.
D. Falsch. Eine unterdrückende Sicherheitsmaßnahme ist darauf ausgerichtet, die Folgen einer Betriebsunterbrechung auf ein Minimum zu beschränken.

26 / 40
Der Zugriff auf streng geschützte Bereiche erfordert eine starke Autorisierung. Bei einer starken Autorisierung wird die Identität einer Person mittels drei Faktoren identifiziert.

Was wird bei Eingabe der persönlichen Identifizierungsnummer (PIN) verifiziert?

A. Was man ist
B. Was man hat
C. Was man weiß

A. Falsch. Ein PIN-Code ist kein Beispiel für etwas, was man ist.
B. Falsch. Ein PIN-Code ist kein Beispiel für etwas, was man hat.
C. Richtig. Ein PIN-Code ist etwas, das man weiß. (Kapitel 11)

27 / 40
In der physischen Informationssicherheit können mehrere sogenannte Protection Rings angewendet werden, in denen verschiedene Maßnahmen ergriffen werden.

Was ist **kein** Protection Ring?

A. Gebäude
B. Mittlerer Ring
C. Objekt
D. Außenring

A. Falsch. Ein Gebäude ist ein gültiger Bereich und beschäftigt sich mit dem Zugang zu den Stellen.
B. Richtig. Protection Rings: Außenring (Gebiet um die Stellen), Gebäude (Zugang zu den Stellen), Arbeitsraum (die Zimmer in den Stellen, die auch als "Inner Ring" bezeichnet werden), Objekt (der zu schützende Vermögenswert). So etwas wie einen mittleren Ring gibt es nicht. (Kapitel 11)
C. Falsch. Ein Objekt ist eine gültige Zone und befasst sich mit dem Gut, das geschützt werden soll.
D. Falsch. Ein Außenring ist eine gültige Zone und befasst sich mit dem Bereich um die Stellen.

28 / 40
Welche Bedrohung kann sich bei Fehlen einer physischen Sicherheitsmaßnahme ergeben?

A. Ein Benutzer kann die Dateien eines anderen Nutzers einsehen.
B. Ein Server fährt aufgrund von Überhitzung herunter.
C. Ein vertrauliches Dokument bleibt im Drucker.
D Hacker können sich im Computernetz frei bewegen.

A. Falsch. Logische Zugangskontrolle ist eine technische Maßnahme, die den unbefugten Zugriff auf Dokumente eines anderen Benutzers verhindert.
B. Richtig. Physische Sicherheit umfasst den Schutz der Ausrüstung durch Klimatisierung (Klimaanlage, Luftfeuchte). (Kapitel 11)
C. Falsch. Eine Sicherheitsrichtlinie sollte Regeln beinhalten, wie vertrauliche Dokumente zu behandeln sind. Alle Mitarbeiter sollten sich diese Politik merken und die Regeln befolgen. Es ist eine organisatorische Maßnahme.
D. Falsch. Den Computer oder das Netzwerk vor dem Zugriff von Hackern zu schützen ist eine technische Maßnahme.

29 / 40
Welche Sicherheitsmaßnahme ist eine technische Maßnahme?

A. Die Zuweisung von Informationen an einen Verantwortlichen
B. Die Verschlüsselung von Dateien
C. Die Erstellung von Weisungen und Richtlinien, die festlegen, was in einer E-Mail erlaubt ist und was nicht
D. Die Aufbewahrung von Passwörtern für das Management des Systems in einem Safe

A. Falsch. Bei der Zuweisung von Informationen an einen Verantwortlichen handelt es sich um eine Klassifizierung und damit um eine organisatorische Maßnahme.
B. Richtig. Hierbei handelt es sich um eine technische Maßnahme, mit der verhindert wird, dass Informationen von Unbefugten gelesen werden können. (Kapitel 6)
C. Falsch. Hierbei handelt es sich um eine organisatorische Maßnahme, einen Verhaltenskodex, der Teil des Arbeitsvertrages ist.
D. Falsch. Hierbei handelt es sich um eine organisatorische Maßnahme.

30 / 40
Die Backups des zentralen Servers werden im gleichen verschlossenen Raum aufbewahrt wie die Server selbst.

Welches Risiko ergibt sich daraus für die Organisation?

A. Bei einem Server-Ausfall dauert es lange, bis der Server wieder in Betrieb genommen werden kann.
B. Im Falle eines Brandes lässt sich der Zustand des Systems vor dem Brand nicht wiederherstellen.
C. Keiner ist für die Backups zuständig.
D. Unbefugte können leicht auf die Backups zugreifen.

A. Falsch. Dies würde im Gegenteil sogar dazu beitragen, dass der Serverbetrieb schneller wieder aufgenommen werden kann.
B. Richtig. Es ist sehr wahrscheinlich, dass bei einem Brand auch die Backups zerstört würden. (Kapitel 11)
C. Falsch. Die Verantwortlichkeit hat nichts mit dem Ort der Aufbewahrung zu tun.
D. Falsch. Der Computerraum ist verschlossen.

31 / 40
Welche Art von Schadsoftware erstellt auf einem infizierten Computer ein Netzwerk?

A. Eine logische Bombe (Logic Bomb)
B. Ein Storm Worm oder Storm Botnet
C. Ein Trojaner
D. Spyware

A. Falsch. Eine logische Bombe ist nicht immer Malware. Es ist ein Stück Code, der in einem Softwaresystem eingebaut worden ist.
B. Richtig. Ein Storm Worm ist ein kleines Computerprogramm, das sich absichtlich selbst repliziert und Kopien des Originals durch Nutzung der Netzwerkeinrichtungen seines Hosts verbreitet. (Kapitel 12)
C. Falsch. Ein Trojaner ist ein Programm, das, zusätzlich zu der Funktion, dass es durchzuführen scheint, absichtlich Nebentätigkeiten leitet, vom Benutzer unbemerkt.
D. Falsch. Spyware ist ein Computerprogramm, das Daten auf dem Computer des Benutzers speichert und diese Informationen an eine andere Partei sendet.

32 / 40
In einer Organisation entdeckt der Informationssicherheits-Beauftragte, dass ein Computer eines Mitarbeiters mit Schadsoftware infiziert ist. Die Schadsoftware wurde bei einem gezielten Phishing-Angriff installiert.

Welche Maßnahme eignet sich am **besten,** um solche Vorfälle künftig zu vermeiden?

A. Die Umsetzung der MAC-Technologie
B. Die Einführung eines Security Awareness Programms
C. Die Aktualisierung der Regeln der Firewall
D. Die Aktualisierung der Signaturen des Spam-Filters

A. Falsch. MAC betrifft die Zugangskontrolle; Dies verhindert nicht, dass ein Benutzer überzeugt wird, einige Aktionen als Folge der gezielten Angriffe auszuführen.
B. Richtig. Die zugrunde liegende Sicherheitsanfälligkeit dieser Bedrohung ist die Unkenntnis des Benutzers. Die Benutzer werden in dieser Art von Angriffen überzeugt einige Codes auszuführen (zB Installation verdächtiger Software), die gegen die Sicherheitsrichtlinien verstoßen. Diese Art von Angriffen in einem Security-Awareness-Programm anzusprechen wird die Wahrscheinlichkeit des Wiederauftretens in der Zukunft reduzieren. (Kapitel 12)
C. Falsch. Die Firewall kann zwar beispielsweise Datenverkehr, der von der installierten Schadsoftware geführt wird blockieren. Um Wiederholung zu verhindern wird die Firewall nicht helfen.
D. Falsch. Der gezielte Angriff muss nicht unbedingt via E-Mail erfolgen. Der Angreifer kann beispielsweise auch soziale Medien nutzen, oder sogar das Telefon, um Kontakt mit dem Opfer aufzunehmen.

33 / 40
Sie arbeiten in der IT-Abteilung eines mittelständischen Unternehmens. Es sind bereits mehrmals vertrauliche Informationen in die falschen Hände geraten. Dies hat dem Image des Unternehmens geschadet. Sie wurden gebeten, in Ihrem Unternehmen organisatorische Maßnahmen für die Laptops vorzuschlagen.

Welchen Schritt sollten Sie als **erstes** setzen?

A. Weisungen und Richtlinien zu mobilen Medien (PDAs, Laptops, Smartphones, USB-Sticks) formulieren.
B. Wachpersonal ernennen
C. Die Festplatten der Laptops und die USB-Sticks verschlüsseln
D. Weisungen und Richtlinien zur Zugangs- und Zugriffskontrolle einführen

A. Richtig. Die Politik, wie mobile Medien zu verwenden sind, ist eine organisatorische Maßnahme und Sicherheitsmaßnahmen für Laptops können eine Verpflichtung sein. (Kapitel 6)
B. Falsch. Die Ernennung von Sicherheitspersonal ist eine technische Maßnahme. Wenn jemand einen Laptop aus dem Büro nimmt, bleibt die Gefahr des Informationsaustritts gegeben.
C. Falsch. Das Verschlüsseln von Festplatten der Laptops und von USB Sticks ist eine technische Maßnahme. Dies kann getan werden auf Grund organisationeller Maßnahmen.
D. Falsch. Weisungen und Richtlinien zur Zugangs- und Zugriffskontrolle sind organisationelle Maßnahmen, die nur den Zugang zu Gebäuden oder IT-Systemen umfassen.

34 / 40
Wie nennt man ein System, das in einer Organisation für eine einheitliche und logisch zusammenhängende Informationssicherheit sorgt?

A. Das Informationssicherheit-Management-System (ISMS)
B. Das Rootkit
C. Die Sicherheitsvorschriften für besondere Regierungsinformationen

A. Richtig. Das ISMS ist in ISO / IEC 27001 beschrieben worden. (Kapitel 3)
B. Falsch. Ein Rootkit ist eine Menge bösartige Software-Tools, oft von einer dritten Partei (in der Regel einem Hacker) verwendet.
C. Falsch. Dies ist eine von staatlichen Behörden verfasste Anzahl von Regeln, wie man spezielle Informationen behandelt.

35 / 40
Wie nennt man 'Identifizierung ob die Identität einer Person korrekt ist'?

A. Authentisierung
B. Autorisierung
C. Identifizierung

A. Richtig. Bei der Authentisierung handelt es sich um den Prozess, seine Identität bekanntzugeben.
B. Falsch. Die Feststellung, ob die Identität einer Person korrekt ist, nennt man Authentisierung.
C. Falsch. Die Feststellung, ob die Identität einer Person korrekt ist, nennt man Authentisierung.

36 / 40

Warum muss ein Notfallwiederherstellungsplan ständig aktualisiert und in regelmäßigen Abständen getestet werden?

A. Um stets Zugriff auf die neuesten Backups zu haben, die sich außerhalb des Büros befinden.
B. Um mit den täglich auftretenden Fehlern fertig zu werden.
C. Weil anderenfalls die bei einer weitreichenden Störung ergriffenen Maßnahmen und die Verfahren zur Behebung von Sicherheitsvorfällen möglicherweise nicht ausreichend oder veraltet sind.
D. Weil dies laut Datenschutzgesetz notwendig ist.

A. Falsch. Die Wiederherstellung des Systems ist eine technische Maßnahme.
B. Falsch. Bei normalen Störungen sind die normalerweise ergriffenen Maßnahmen und die Verfahren zur Behebung von Informationssicherheitsvorfällen ausreichend.
C. Richtig. Bei einer weitreichenden Störung ist ein aktualisierter und getesteter Notfallwiederherstellungsplan erforderlich. (Kapitel 17)
D. Falsch. Beim Datenschutzgesetz geht es um die Vertraulichkeit persönlicher Daten.

37 / 40
Auf der Basis von welchem Gesetz kann eine Person verlangen, die über sie gespeicherten Daten einzusehen?

A. Auf der Basis des Bundesarchivgesetzes
B. Auf der Basis des Datenschutzgesetzes
C. Auf der Basis des Gesetzes zur Bekämpfung der Computerkriminalität
D. Auf der Basis des Gesetzes zur Regelung des Zugangs zu Informationen des Bundes (Informationsfreiheitsgesetz)

A. Falsch. Das Bundesarchivgesetz regelt die Sicherung und die Vernichtung von Archivdokumenten.
B. Richtig. Das Recht auf Einsichtnahme ist im Datenschutzgesetz geregelt. (Kapitel 18)
C. Falsch. Das Gesetz zur Bekämpfung der Computerkriminalität ist eine Ergänzung des Strafgesetzes und des Strafgesetzbuches und erleichtert die strafrechtliche Verfolgung von Vergehen, die mit Hilfe der modernen Informationstechnik begangen werden. Ein Beispiel für ein solches Vergehen ist das Hacken von Computern.
D. Falsch. Das Gesetz zur Regelung des Zugangs zu Informationen des Bundes (Informationsfreiheitgesetz) regelt die Einsichtnahme in schriftliche Regierungsunterlagen. Persönliche Daten sind keine Regierungsdokumente.

38 / 40
Welche der nachfolgenden Möglichkeiten ist eine gesetzliche oder behördliche Vorschrift der Informationssicherheit, die für alle Organisationen gilt?

A. Geistiges Urheberrecht
B. ISO/IEC 27001
C. ISO/IEC 27002
D. Datenschutzgesetz

A. Falsch. Dieses Gesetz bezieht sich nicht auf Informationssicherheit für Organisationen.
B. Falsch. Dies ist ein Standard mit Richtlinien für Organisationen, wie man mit dem Aufbau eines Informationssicherheitsprozesses umgeht.
C. Falsch. Diese Norm, die auch als 'Code of practice for Information Security' bekannt ist, enthält Leitlinien für die Informationssicherheitspolitik und -Maßnahmen.
D. Richtig. Alle Organisationen sollten eine Politik und ein Verfahren für den Datenschutz haben, die bei jedem, der personenbezogenen Daten verarbeitet, bekannt sein sollten. (Kapitel 18)

39 / 40
Sie sind der Eigentümer des Kurierunternehmen SpeeDelivery. Sie beschäftigen ein paar Leute, die während sie auf ihre nächste Auslieferung warten, andere Aufgaben erfüllen können. Sie stellen jedoch fest, dass ihre Mitarbeiter die Zeit dazu nutzen, private Mails zu versenden und im Internet zu surfen.

Wie können Sie im Rahmen des Gesetzes die Verwendung des Internets und des E-Mail-Programms am besten regeln?

A. Durch die Installation einer Anwendung, die den Zugriff auf gewisse Webseiten verwehrt und Anhänge in E-Mails herausfiltert
B. Durch die Ausarbeitung eines Verhaltenskodex zur Nutzung von Internet und E-Mail-Verkehr, in dem die Rechte und Pflichten des Arbeitgebers und der Mitarbeiter festgelegt werden
C. Durch die Implementierung von Geheimhaltungsvorschriften
D. Durch die Installation eines Virenscanners

A. Falsch. Die Installation dieser Art von Software regelt die Nutzung von Internet und E-Mail teilweise. Es kann nicht die Zeit, die für private Nutzung verwandt wurde, regulieren. Dies ist eine technische Maßnahme.
B. Richtig. In einem Verhaltenskodex kann die Nutzung von Internet und E-Mail dokumentiert werden, welche Websites besucht oder nicht besucht werden können und in welchem Ausmaß private Nutzung zulässig ist. Dies sind interne Regelungen. (Kapitel 18)
C. Falsch. Datenschutzbestimmungen regeln lediglich die Verwendung personenbezogener Daten von Mitarbeitern und Kunden, nicht die Nutzung von Internet und E-Mail.
D. Falsch. Ein Virenscanner überprüft eingehende E-Mail und Internet-Verbindungen auf bösartige Software. Es reguliert nicht die Nutzung von Internet und E-Mail. Es ist eine technische Maßnahme.

40 / 40

Unter welchen Bedingungen darf ein Arbeitgeber überprüfen, ob Internet und E-Mail am Arbeitsplatz für private Zwecke genutzt werden?

A. Der Arbeitgeber darf dies überprüfen, wenn er die Mitarbeiter nach der Überprüfung stets in Kenntnis setzt.
B. Der Arbeitgeber darf dies überprüfen, wenn die Mitarbeiter wissen, dass eine Überprüfung stattfinden könnte.
C. Der Arbeitgeber darf dies überprüfen, wenn auch eine Firewall installiert ist.

A. Falsch. Der Arbeitnehmer muss nicht nach jeder Kontrolle informiert werden.
B. Richtig. Die Mitarbeiter müssen wissen, dass der Arbeitgeber das Recht hat, die Nutzung von IT-Services zu überwachen. (Kapitel 3 und 18)
C. Falsch. Eine Firewall schützt gegen äußere Eindringlinge. Dies wird das Recht des Arbeitgebers, den Einsatz von IT-Services zu überwachen, nicht beeinflussen.

Beurteilung

Die richtigen Antworten auf die Fragen in diesem Musterexamen finden Sie in nachstehender Tabelle.

Nummer	Antwort	Nummer	Antwort
1	B	21	C
2	A	22	B
3	B	23	C
4	C	24	C
5	B	25	B
6	B	26	C
7	D	27	B
8	B	28	B
9	D	29	B
10	A	30	B
11	A	31	B
12	C	32	B
13	C	33	A
14	D	34	A
15	B	35	A
16	C	36	C
17	B	37	B
18	A	38	D
19	A	39	B
20	B	40	B

Kontakt EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER