


# Musterprüfung

Ausgabe 202404

Copyright © EXIN Holding B.V. 2024. All rights reserved.
EXIN® is a registered trademark.

No part of this publication may be reproduced, stored, utilized or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written permission from EXIN.

# Inhalt


| | |
|---|---|
| Einführung | 4 |
| Musterprüfung | 5 |
| Antwortschlüssel | 15 |
| Beurteilung | 34 |

# Einführung

Dies ist die EXIN Information Security Foundation based on ISO/IEC 27001 (ISFS.DE) Musterprüfung. Es gilt die Prüfungsordnung von EXIN.

Die Musterprüfung besteht aus 40 Multiple-Choice-Fragen. Zu jeder Multiple-Choice-Frage werden mehrere Antwortmöglichkeiten angeboten. Es gibt jeweils eine richtige Antwort.

Sie können maximal 40 Punkte erreichen. Jede richtige Antwort zählt 1 Punkt. Um die Prüfung zu bestehen, müssen Sie mindestens 26 Punkte erzielen.

Die Bearbeitungszeit beträgt 60 Minuten.

Viel Erfolg!

# Musterprüfung

**1 / 40**
In einer Datenbank sind Millionen von Transaktionen eines Telefonunternehmens gespeichert. Für einen Kunden wurde eine Rechnung erstellt und verschickt.

Was enthält diese Rechnung für den Kunden?

**A)** Daten
**B)** Informationen
**C)** Daten und Informationen

**2 / 40**
Was ist der Unterschied zwischen Daten und Informationen?

**A)** Bei Daten kann es sich um alle erdenklichen Fakten oder Zahlen handeln. Informationen sind Daten, die eine Bedeutung haben.
**B)** Daten bestehen aus unstrukturierten Zahlen. Informationen bestehen aus strukturierten Zahlen.
**C)** Daten erfordern keine Sicherheit. Informationen erfordern Sicherheit.
**D)** Daten haben keinen Wert. Informationen dagegen sind verarbeitete Daten und haben einen Wert.

**3 / 40**
Was ist der Fokus des Informationsmanagements?

**A)** Die unterbrechungsfreie Fortführung von Business-Aktivitäten und -Prozessen zu ermöglichen
**B)** Die Identifizierung und Nutzung des Werts von Informationen sicherzustellen
**C)** Den Zugriff auf automatisierte Systeme durch Unbefugte zu verhindern
**D)** Die Informationsflüsse im Unternehmen zu verstehen

**4 / 40**
Eine Organisation muss wissen, mit welchen Risiken sie konfrontiert ist, bevor sie entsprechende Maßnahmen (Measures) ergreifen kann.

Was sollte die Organisation kennen, um das Risiko zu bestimmen?

**A)** Die Eintrittswahrscheinlichkeit eines Ereignisses und die Auswirkungen des Ereignisses auf die Organisation
**B)** Die häufigsten Risiken und wie diese gemäß den Festlegungen in Best Practices reduziert werden können
**C)** Die Bedrohungen, mit denen eine Organisation konfrontiert ist und wie anfällig die Organisation für diese Bedrohungen ist
**D)** Die ungeplanten Ereignisse, mit denen eine Organisation konfrontiert ist und was in einem solche Fall zu tun ist

**5 / 40**
Was ist neben Integrität und Vertraulichkeit der dritte Aspekt der Zuverlässigkeit von Informationen?

**A)** Genauigkeit
**B)** Verfügbarkeit
**C)** Vollständigkeit
**D)** Monetärer Wert

**6 / 40**
Eine Organisation verfügt über einen Netzwerkdrucker, der im Flur des Unternehmens steht. Viele Mitarbeiter holen ihre Ausdrucke nicht sofort, sondern lassen sie im Drucker liegen.

Wie wirkt sich dies auf die Zuverlässigkeit der Informationen aus?

**A)** Die Verfügbarkeit der Informationen ist nicht mehr gewährleistet.
**B)** Die Vertraulichkeit der Informationen ist nicht mehr gewährleistet.
**C)** Die Integrität der Informationen ist nicht mehr gewährleistet.

**7 / 40**
Was ist der Unterschied zwischen Verantwortlichkeit und Auditierbarkeit?

**A)** Verantwortlichkeit bedeutet, dass eine Organisation ihre Finanzkonten gut verwaltet. Auditierbarkeit bedeutet, dass eine Organisation ein Audit bestanden hat.
**B)** Verantwortlichkeit bedeutet, dass man für die Folgen der Aktivitäten einer Organisation haftet. Auditierbarkeit bezeichnet den Reifegrad einer Organisation, sich einer unabhängigen Bewertung zu unterziehen.
**C)** Verantwortlichkeit bedeutet die Verantwortung für die Handlungen einer Person zu übernehmen. Auditierbarkeit bedeutet die Verantwortung für die Handlungen einer Organisation zu haben.
**D)** Verantwortlichkeit bedeutet, dass eine Organisation den Sarbanes Oxley Act (SOX) einhält. Auditierbarkeit bedeutet, dass eine Organisation der Norm ISO/IEC 27001 entspricht.

**8 / 40**
Wie lässt sich der Zweck einer Informationssicherheitsrichtlinie **am besten** beschreiben?

**A)** Eine Informationssicherheitsrichtlinie dokumentiert die Analyse der Risiken und die Suche nach entsprechenden Sicherheitsmaßnahmen.
**B)** Eine Informationssicherheitsrichtlinie bietet der Organisation Orientierung und Unterstützung hinsichtlich der Informationssicherheit.
**C)** Eine Informationssicherheitsrichtlinie konkretisiert die Sicherheitsplanung mit den erforderlichen Details.
**D)** Eine Informationssicherheitsrichtlinie bieten Einblick in Bedrohungen und deren mögliche Folgen.

**9 / 40**
Sara soll sicherstellen, dass ihre Organisation die Gesetzgebung zum Schutz personenbezogener Daten einhält.

Was sollte Sara **zuerst** tun?

**A)** Einen Mitarbeiter benennen, der die Manager bei der Einhaltung der Richtlinie unterstützt
**B)** Die Erhebung und Speicherung personenbezogener Daten verbieten
**C)** Die Mitarbeitenden für die Übermittlung ihrer personenbezogenen Daten zuständig machen
**D)** Die Gesetzgebung zum Schutz personenbezogener Daten in einer Datenschutzrichtlinie umsetzen.

**10 / 40**
Eine Organisation beschließt, einen gewissen Teil ihrer IT auszulagern.

Wie lässt sich die Informationssicherheit **am besten** gewährleisten, wenn man mit einem Lieferanten arbeitet?

**A)** Indem man in der Organisation des Lieferanten einen neuen Information Security Officer (ISO) ernennt
**B)** Indem man die Informationssicherheitsanforderungen an den Lieferanten förmlich in einem Vertrag festlegt
**C)** Indem man die beiden Organisationen vollständig voneinander trennt, damit jede für ihre eigenen Daten verantwortlich ist
**D)** Indem man vom Lieferanten verlangt, dass er die Prozesse und Verfahren der Kundenorganisation befolgt

**11 / 40**
Wer ist dafür zuständig, aus der Unternehmensstrategie und den Unternehmenszielen eine Sicherheitsstrategie und Sicherheitsziele abzuleiten?

**A)** Chief Information Security Officer (CISO)
**B)** Geschäftsführung
**C)** Information Security Officer (ISO)
**D)** Information Security Policy Officer

**12 / 40**
Welches ist das **beste** Beispiel einer menschlichen Bedrohung?

**A)** Ein Leck verursacht einen Stromausfall.
**B)** Ein USB-Stick infiziert ein Netzwerk mit einem Virus.
**C)** Der Server-Raum ist zu staubig.

**13 / 40**
Ein Datenbanksystem verfügt nicht über die neuesten Sicherheitspatches und wurde gehackt. Die Hacker konnten auf die Daten zugreifen und diese löschen.

Welcher Begriff aus der Informationssicherheit beschreibt das Fehlen von Sicherheitspatches?

**A)** Auswirkung
**B)** Risiko
**C)** Bedrohung
**D)** Schwachstelle

**14 / 40**
In einem Unternehmen gab es einen Brand. Die Feuerwehr war schnell vor Ort und konnte den Brand löschen, bevor er sich ausbreitete und das gesamte Firmengelände abbrannte. Bei dem Brand wurde jedoch der Server zerstört. Die in einem anderen Raum aufbewahrten Backup-Bänder waren geschmolzen und viele weitere Dokumente gingen verloren.

Welchen **indirekten** Schaden hat der Brand verursacht?

**A)** Verbrannte Computer-Systeme
**B)** Verbrannte Dokumente
**C)** Geschmolzene Backup-Bänder
**D)** Wasserschaden

**15 / 40**
Die Risikostrategien von Unternehmen können sich je nach Art der Geschäftstätigkeit unterscheiden.

Welche Risikostrategie eignet sich für ein Krankenhaus **am besten**?

**A)** Risikoakzeptanz
**B)** Risikovermeidung
**C)** Risikotragfähigkeit
**D)** Risikoneutralität

**16 / 40**
Eine professionell durchgeführte Risikoanalyse bietet viele nützliche Informationen. Eine Risikoanalyse verfolgt mehrere Hauptziele.

Was zählt **nicht** zu den Hauptzielen einer Risikoanalyse?

**A)** Die Kosten eines Incidents und die Kosten einer Sicherheitsmaßnahme gegeneinander abzuwägen
**B)** Die relevanten Schwachstellen und Bedrohungen zu bestimmen
**C)** Die Werte (Assets) und deren wirtschaftlichen Wert zu identifizieren
**D)** Die Maßnahmen (Measures) und Sicherheitsmaßnahmen zu implementieren

**17 / 40**
Was ist bei einem Brand eine unterdrückende Sicherheitsmaßnahme?

**A)** Den Brand zu löschen, nachdem er entdeckt wurde
**B)** Den durch den Brand verursachten Schaden zu reparieren
**C)** Eine Brandversicherung abzuschließen

**18 / 40**
Was ist das Ziel der Klassifizierung von Informationen?

**A)** Die Kennzeichnung von Informationen, um ihre Erkennbarkeit zu verbessern
**B)** Die Erstellung eines Handbuchs zum Umgang mit Mobilgeräten
**C)** Die Gliederung der Informationen nach dem Grad ihrer Vertraulichkeit

**19 / 40**
Was ist der **wichtigste** Grund für die Trennung der Verantwortlichkeit?

**A)** Sicherzustellen, dass Mitarbeiter nicht zur gleichen Zeit das Gleiche machen
**B)** Alle Mitarbeiter gemeinsam für die gemachten Fehler zuständig zu machen
**C)** Klarzustellen, wer für welche Aufgaben und Tätigkeiten zuständig ist
**D)** Die Wahrscheinlichkeit unbefugter oder unbeabsichtigter Änderungen auf ein Minimum zu beschränken

**20 / 40**
Wie lässt sich ein angemessener Zugriff auf Informationen **am besten** sicherstellen?

**A)** Durch die Automatisierung von Arbeitsabläufen
**B)** Durch die Festlegung von Verfahrensanweisungen
**C)** Durch die Entwicklung von Arbeitsanweisungen für alle Aufgaben
**D)** Durch die Bereitstellung von Schulungen

**21 / 40**
In der Geschäftsstelle einer Organisation bricht ein Brand aus. Die Mitarbeiter werden auf andere Geschäftsstellen in der Nähe verteilt und sollen dort weiter arbeiten.

Wo ist eine solche Stand-by-Regelung im Lebenszyklus der Incidents (Incident Cycle) angesiedelt?

**A)** Zwischen Schaden und Wiederherstellung
**B)** Zwischen Incident und Schaden
**C)** Zwischen Wiederherstellung und Bedrohung
**D)** Zwischen Bedrohung und Incident

**22 / 40**
Eine Mitarbeiterin entdeckt, dass das Fälligkeitsdatum einer Police ohne ihr Wissen geändert wurde. Da sie die Einzige ist, die dieses Datum ändern darf, meldet sie den Security Incident an den Helpdesk.

Der Helpdesk-Mitarbeiter zeichnet zu diesem Incident folgende Informationen auf:
- Datum und Zeit
- Beschreibung des Incidents
- Mögliche Folgen des Incidents

Welche wichtige Information über den Incident fehlt?

**A)** Der Name der Person, die den Incident gemeldet hat
**B)** Der Name des Software-Pakets
**C)** Die PC-Nummer

**23 / 40**
Warum ist es wichtig, das Informationssicherheitsmanagementsystem (ISMS) der Organisation regelmäßig zu auditieren?

**A)** Viele Kundenverträge fordern Audits zur Gewährleistung der Informationssicherheit.
**B)** Audits sind für die Einhaltung der gesetzlichen und regulatorischen Vorgaben (Compliance) obligatorisch.
**C)** Audits zeigen, ob eine Organisation Probleme hat, ihre finanziellen Ziele zu erreichen.
**D)** Audits decken Schwächen bei der Implementierung von Informationssicherheitsmaßnahmen auf.

**24 / 40**
Welches Dokument enthält die Vorschrift, die die Nutzung des geschäftlichen E-Mail-Accounts für private Zwecke verbietet?

**A)** Führungszeugnis
**B)** Verhaltenskodex
**C)** Datenschutz-Grundverordnung (DSGVO)
**D)** Vertraulichkeitsvereinbarung (NDA)

**25 / 40**
Ein Mitarbeiter entdeckt einen Incident.

An wen sollte er diesen **zuerst** melden?

**A)** An den Helpdesk
**B)** An den Information Security Manager (ISM)
**C)** An den Information Security Officer (ISO)
**D)** An den Vorgesetzten

**26 / 40**
Wie kann man bei Mitarbeitenden **am effektivsten** Bewusstsein für Informationssicherheit schaffen?

**A)** Durch gezielte Schulungen zur Bewusstseinsbildung für die Geschäftsführung
**B)** Durch Teilnahme aller Mitarbeitenden an externen Schulungen zum Thema Informationssicherheit
**C)** Durch Einrichtung eines speziell auf die Organisation ausgerichteten Programms zur Bewusstseinsbildung
**D)** Durch das Angebot einer allgemeinen Online-Schulung zum Thema Informationssicherheit

**27 / 40**
Welche physische Sicherheitsmaßnahme regelt den Zugriff auf die Informationen einer Organisation?

**A)** Installation einer Klimaanlage
**B)** Verbot der Nutzung von USB-Sticks
**C)** Erfordernis von Benutzernamen und Password
**D)** Verwendung von Sicherheitsglas

**28 / 40**
Ein Rechenzentrum nutzt Akkus, hat jedoch keinen Stromgenerator.

Welches Risiko besteht in diesem Fall für die Verfügbarkeit des Rechenzentrums?

**A)** Bei einer Wiederherstellung der Stromversorgung schaltet sich die Hauptstromversorgung möglicherweise nicht automatisch wieder ein, da dazu ein Generator benötigt wird.
**B)** Der Ausfall der Hauptstromversorgung kann länger als nur ein paar Minuten oder Stunden dauern und in diesem Fall wäre kein Strom verfügbar.
**C)** Die Lebensspanne der Akkus ist begrenzt, und nach ein paar Tagen haben die Akkus möglicherweise keinen Diesel mehr und würden dann auch nicht mehr funktionieren.
**D)** Die Akkus müssen nach ein paar Stunden vom Stromgenerator mit Strom versorgt werden und bieten daher nur eingeschränkt Schutz.

**29 / 40**
Warum wird im Server-Raum eine Klimaanlage installiert?

**A)** Die Backup-Bänder sind aus dünnem Plastik, das hohen Temperaturen nicht standhalten kann. Bei zu hohen Temperaturen im Server-Raum könnten sie beschädigt werden.
**B)** Die im Server-Raum tätigen Mitarbeitenden sollten nicht in der Hitze arbeiten müssen. Mit den Temperaturen steigt auch die Wahrscheinlichkeit, dass die Mitarbeitenden Fehler machen.
**C)** Die Luft im Server-Raum muss gekühlt und die von den Geräten produzierte Wärme abgeführt werden. Darüber hinaus filtert die Klimaanlage die Raumluft und entzieht ihr Feuchtigkeit.
**D)** Der Server-Raum bietet die beste Möglichkeit, um die Raumluft der Niederlassung zu kühlen. Installiert man die Klimaanlage dort, muss kein Büroraum für eine so große technische Anlage geopfert werden.

**30 / 40**
Im Rahmen der physischen Informationssicherheit können mehrere Sicherheitsringe (Protection Rings) zum Einsatz kommen, in denen dann verschiedene Maßnahmen (Measures) ergriffen werden können.

Was ist **kein** Sicherheitsring?

**A)** Building Ring (Gebäude Ring)
**B)** Middle Ring (Mittlerer Ring)
**C)** Secure Room Ring (Sicherheitsbereich Ring)
**D)** Outer Ring (Äußerer Ring)

**31 / 40**
Welche Sicherheitsmaßnahme für einen Wert (Asset) erforderlich ist, richtet sich nach dem jeweiligen Wert (Asset).

Wie lässt sich die Sicherheit eines Werts **am besten** gewährleisten?

**A)** Indem man ein Formular sichert durch ausfüllen und abzeichnen
**B)** Indem man einen Laptop sichert und diesen einem einzigen Benutzer zuweist
**C)** Indem man einen USB-Stick mittels Verschlüsselung sichert
**D)** Indem man eine Internetverbindung mittels Backup sichert

**32 / 40**
Welche Sicherheitsmaßnahme trägt dazu bei, Informationssicherheit bereits bei der Entwicklung von Systemen zu berücksichtigen?

**A)** Die Redundanz der Server sicherzustellen
**B)** Physische Zugangskontrollen zu implementieren
**C)** Background Checks bei Mitarbeitenden durchzuführen
**D)** Datenklassifizierung bei Informationswerten (Informationsassets) zu nutzen

**33 / 40**
Eine Organisation ändert ihre Richtlinie. Ab sofort haben die Mitarbeitenden auch die Möglichkeit zu Remote- oder Telearbeit.

Welche Sicherheitsmaßnahme sollte nun eingeführt werden?

**A)** Erstellen von V-Lans zur Segmentierung des Unternehmensnetzwerks
**B)** Verschlüsselung der Informationen im Unternehmensnetzwerk
**C)** Einrichtung von Firewalls im Unternehmensnetzwerk
**D)** Verbindung mit dem Unternehmensnetzwerk über virtuelles privates Netzwerk (VPN)

**34 / 40**
Die Mitarbeitenden einer Organisation arbeiten an Laptops, die mittels asymmetrischer Kryptographie geschützt sind. Um die Schlüsselverwaltung so wirtschaftlich wie möglich zu gestalten, nutzen alle Berater das selbe Schlüsselpaar.

Bei Gefährdung bestimmter Informationen sind neue Schlüssel bereitzustellen.

In welchem Fall sollten neue Schlüssel bereitgestellt werden?

**A)** Wenn der private Schlüssel bekannt wird
**B)** Wenn der öffentliche Schlüssel bekannt wird
**C)** Wenn die Infrastruktur mit öffentlichem Schlüssel (PKI) bekannt wird

**35 / 40**
Welche Art von Sicherheit bietet eine Infrastruktur mit öffentlichem Schlüssel (PKI)?

**A)** Eine PKI stellt regelmäßige Backups der Unternehmensdaten sicher.
**B)** Eine PKI weist gegenüber den Kunden nach, dass ein webbasiertes Geschäft sicher ist.
**C)** Eine PKI verifiziert, ob eine Person oder ein System zu einem bestimmten öffentlichen Schlüssel gehört.

**36 / 40**
Bei welcher Art von Schadsoftware handelt es sich um ein Programm, das neben seiner offensichtlichen Funktion auch bewusst weitere Aktivitäten ausführt?

**A)** Logikbombe (Logic Bomb)
**B)** Spyware
**C)** Trojaner
**D)** Wurm

**37 / 40**
Bei welcher Art von Schadsoftware handelt es sich um ein Programm, das ein Netzwerk infizierter Computer erstellt, indem es sich selbst repliziert?

**A)** Logikbombe (Logic Bomb)
**B)** Spyware
**C)** Trojaner
**D)** Wurm

**38 / 40**
Welche Gesetzgebung oder Rechtsvorschrift im Bereich der Informationssicherheit gilt für alle Organisationen?

**A)** Datenschutz-Grundverordnung (DSGVO)
**B)** Geistige Eigentumsrechte
**C)** ISO/IEC 27001
**D)** ISO/IEC 27002

**39 / 40**
Welche ISO-Norm konzentriert sich auf die Implementierung von Informationssicherheitsmaßnahmen?

**A)** ISO/IEC 27000
**B)** ISO/IEC 27001
**C)** ISO/IEC 27002
**D)** ISO/IEC 27005

**40 / 40**
Die Normen welcher Normenorganisation werden in Europa **am häufigsten** genutzt?

**A)** American National Standards Institute (ANSI)
**B)** International Organization for Standardization (ISO)
**C)** National Institute of Standards and Technology (NIST)

# Antwortschlüssel

**1 / 40**
In einer Datenbank sind Millionen von Transaktionen eines Telefonunternehmens gespeichert. Für einen Kunden wurde eine Rechnung erstellt und verschickt.

Was enthält diese Rechnung für den Kunden?

**A)** Daten
**B)** Informationen
**C)** Daten und Informationen

**A)** Falsch. Die Datenbank enthält Daten. Wird eine Rechnung erstellt und an einen Empfänger geschickt, werden diese Daten für den Empfänger zu Informationen.
**B)** Richtig. Der Wert von Informationen richtet sich nach dem Empfänger. Die Rechnung enthält Daten, die für den Empfänger wertvoll sind. Damit handelt es sich um Informationen. (Literatur A, Kapitel 4.8.5)
**C)** Falsch. Die Rechnung enthält für den Empfänger nur Informationen.

**2 / 40**
Was ist der Unterschied zwischen Daten und Informationen?

**A)** Bei Daten kann es sich um alle erdenklichen Fakten oder Zahlen handeln. Informationen sind Daten, die eine Bedeutung haben.
**B)** Daten bestehen aus unstrukturierten Zahlen. Informationen bestehen aus strukturierten Zahlen.
**C)** Daten erfordern keine Sicherheit. Informationen erfordern Sicherheit.
**D)** Daten haben keinen Wert. Informationen dagegen sind verarbeitete Daten und haben einen Wert.

**A)** Richtig. Informationen leiten sich von Daten ab, die in einem bestimmten Kontext eine Bedeutung erhalten. (Literatur: A, Kapitel 3.1)
**B)** Falsch. Daten können sowohl strukturiert als auch unstrukturiert sein. Informationen sind in der Regel strukturiert.
**C)** Falsch. Sowohl Daten als auch Informationen erfordern Sicherheit.
**D)** Falsch. Sowohl Daten als auch Informationen haben einen Wert.

**3 / 40**
Was ist der Fokus des Informationsmanagements?

**A)** Die unterbrechungsfreie Fortführung von Business-Aktivitäten und -Prozessen zu ermöglichen
**B)** Die Identifizierung und Nutzung des Werts von Informationen sicherzustellen
**C)** Den Zugriff auf automatisierte Systeme durch Unbefugte zu verhindern
**D)** Die Informationsflüsse im Unternehmen zu verstehen

**A)** Falsch. Das ist der Fokus des Business Continuity Management (BCM). Ziel des BCM ist, die Störung von Business-Aktivitäten zu vermeiden, wichtige Prozesse vor den Konsequenzen weitreichender Störungen in Informationssystemen zu schützen und eine schnelle Wiederherstellung zu ermöglichen.
**B)** Richtig. Das Informationsmanagement beschreibt, wie eine Organisation seine Informationen effizient plant, erhebt, organisiert, nutzt, kontrolliert, verbreitet und entsorgt und wie die Organisation dafür sorgt, dass der Wert von Informationen identifiziert und möglichst vollumfänglich genutzt wird. (Literatur: A, Kapitel 4.9)
**C)** Falsch. Dies ist der Fokus des Zugangs- und Zugriffsmanagements. Dieses stellt sicher, dass unbefugte Personen oder Prozesse nicht auf automatisierte Systeme, Datenbanken und Programme zugreifen können.
**D)** Falsch. Dies ist der Fokus der Informationsanalyse. Sie zeichnet ein klares Bild, wie die Organisation mit Informationen umgeht und wie die Informationsflüsse im Unternehmen verlaufen.

**4 / 40**
Eine Organisation muss wissen, mit welchen Risiken sie konfrontiert ist, bevor sie entsprechende Maßnahmen (Measures) ergreifen kann.

Was sollte die Organisation kennen, um das Risiko zu bestimmen?

**A)** Die Eintrittswahrscheinlichkeit eines Ereignisses und die Auswirkungen des Ereignisses auf die Organisation
**B)** Die häufigsten Risiken und wie diese gemäß den Festlegungen in Best Practices reduziert werden können
**C)** Die Bedrohungen, mit denen eine Organisation konfrontiert ist und wie anfällig die Organisation für diese Bedrohungen ist
**D)** Die ungeplanten Ereignisse, mit denen eine Organisation konfrontiert ist und was in einem solche Fall zu tun ist

**A)** Richtig. Das Risiko wird von zwei übergeordneten Faktoren bestimmt: der Eintrittswahrscheinlichkeit eines Ereignisses und den Auswirkungen des Ereignisses auf das Geschäft. (Literatur: A, Kapitel 3.1)
**B)** Falsch. Davon ausgehend das Risiko einer Organisation zu bestimmen ist nicht ratsam. Einfach dem Beispiel anderer Organisationen zu folgen, sorgt nicht für die Sicherheit dieser Organisation.
**C)** Falsch. Dies ist die Definition des Begriffs Eintrittswahrscheinlichkeit. Es ist zwar wichtig, die Eintrittswahrscheinlichkeit eines Ereignisses zu kennen, aber hier fehlt ein wichtiger Aspekt: nämlich, wie sich das Ereignis auf das Geschäft auswirkt.
**D)** Falsch. Letztendlich werden zwar Sicherheitsmaßnahmen benötigt, die auf die jeweiligen Risiken abgestimmt sind, aber hierbei handelt es sich eher um eine Maßnahme zur Risikobewältigung als um eine Maßnahme um das Risiko erst einmal zu bestimmen.

**5 / 40**
Was ist neben Integrität und Vertraulichkeit der dritte Aspekt der Zuverlässigkeit von Informationen?

**A)** Genauigkeit
**B)** Verfügbarkeit
**C)** Vollständigkeit
**D)** Monetärer Wert

**A)** Falsch. Die drei Aspekte der Zuverlässigkeit von Informationen sind Verfügbarkeit, Integrität und Vertraulichkeit. Genauigkeit ist Teil der Integrität.
**B)** Richtig. Die drei Aspekte der Zuverlässigkeit von Informationen sind Verfügbarkeit, Integrität und Vertraulichkeit. (Literatur: A, Kapitel 3.4.3)
**C)** Falsch. Die drei Aspekte der Zuverlässigkeit von Informationen sind Verfügbarkeit, Integrität und Vertraulichkeit. Vollständigkeit ist Teil der Integrität.
**D)** Falsch. Die drei Aspekte der Zuverlässigkeit von Informationen sind Verfügbarkeit, Integrität und Vertraulichkeit.

**6 / 40**
Eine Organisation verfügt über einen Netzwerkdrucker, der im Flur des Unternehmens steht. Viele Mitarbeiter holen ihre Ausdrucke nicht sofort, sondern lassen sie im Drucker liegen.

Wie wirkt sich dies auf die Zuverlässigkeit der Informationen aus?

**A)** Die Verfügbarkeit der Informationen ist nicht mehr gewährleistet.
**B)** Die Vertraulichkeit der Informationen ist nicht mehr gewährleistet.
**C)** Die Integrität der Informationen ist nicht mehr gewährleistet.

**A)** Falsch. Die Informationen sind in dem System, in dem sie erstellt und gedruckt wurden, nach wie vor verfügbar.
**B)** Richtig. Die Informationen können in die Hände von Personen fallen oder von Personen gelesen werden, die keinen Zugriff auf diese Informationen haben sollten. (Literatur: A, Kapitel 3.4.1)
**C)** Falsch. Die Informationen sind auf Papier gedruckt, sodass ihre Integrität nach wie vor gewährleistet ist.

**7 / 40**
Was ist der Unterschied zwischen Verantwortlichkeit und Auditierbarkeit?

**A)** Verantwortlichkeit bedeutet, dass eine Organisation ihre Finanzkonten gut verwaltet. Auditierbarkeit bedeutet, dass eine Organisation ein Audit bestanden hat.
**B)** Verantwortlichkeit bedeutet, dass man für die Folgen der Aktivitäten einer Organisation haftet. Auditierbarkeit bezeichnet den Reifegrad einer Organisation, sich einer unabhängigen Bewertung zu unterziehen.
**C)** Verantwortlichkeit bedeutet die Verantwortung für die Handlungen einer Person zu übernehmen. Auditierbarkeit bedeutet die Verantwortung für die Handlungen einer Organisation zu haben.
**D)** Verantwortlichkeit bedeutet, dass eine Organisation den Sarbanes Oxley Act (SOX) einhält. Auditierbarkeit bedeutet, dass eine Organisation der Norm ISO/IEC 27001 entspricht.

**A)** Falsch. Verantwortlichkeit hat nicht direkt etwas mit Finanzbuchhaltung und Auditierbarkeit hat nichts mit dem Bestehen eines Audits zu tun.
**B)** Richtig. So lauten die korrekten Definitionen von Verantwortlichkeit und Auditierbarkeit. (Literatur: A, Kapitel 3.4.4)
**C)** Falsch. Die Definition von Verantwortlichkeit ist zwar korrekt, nicht aber die Definition von Auditierbarkeit. Auditierbarkeit hat nichts mit der Verantwortung für die Handlungen einer Organisation zu tun.
**D)** Falsch. Weder Verantwortlichkeit noch Auditierbarkeit beziehen sich auf die Einhaltung der Vorgaben (Compliance) von SOX oder ISO/IEC-Normen.

**8 / 40**
Wie lässt sich der Zweck einer Informationssicherheitsrichtlinie **am besten** beschreiben?

**A)** Eine Informationssicherheitsrichtlinie dokumentiert die Analyse der Risiken und die Suche nach entsprechenden Sicherheitsmaßnahmen.
**B)** Eine Informationssicherheitsrichtlinie bietet der Organisation Orientierung und Unterstützung hinsichtlich der Informationssicherheit.
**C)** Eine Informationssicherheitsrichtlinie konkretisiert die Sicherheitsplanung mit den erforderlichen Details.
**D)** Eine Informationssicherheitsrichtlinie bieten Einblick in Bedrohungen und deren mögliche Folgen.

**A)** Falsch. Die Analyse der Risiken und die Suche nach Sicherheitsmaßnahmen sind der Zweck der Risikoanalyse und des Risikomanagements.
**B)** Richtig. Die Geschäftsführung bietet durch ihre Sicherheitsrichtlinie Orientierung und Unterstützung hinsichtlich der Informationssicherheit. (Literatur: A, Kapitel 4.2.1)
**C)** Falsch. Die Sicherheitsplanung konkretisiert die Informationssicherheitsrichtlinie. Die Planung enthält die gewählten Sicherheitsmaßnahmen, wer für was zuständig ist sowie die Leitlinien zur Umsetzung der Sicherheitsmaßnahmen etc.
**D)** Falsch. Einblick in Bedrohungen und deren mögliche Folgen ist der Zweck der Bedrohungsanalyse.

**9 / 40**
Sara soll sicherstellen, dass ihre Organisation die Gesetzgebung zum Schutz personenbezogener Daten einhält.

Was sollte Sara **zuerst** tun?

**A)** Einen Mitarbeiter benennen, der die Manager bei der Einhaltung der Richtlinie unterstützt
**B)** Die Erhebung und Speicherung personenbezogener Daten verbieten
**C)** Die Mitarbeitenden für die Übermittlung ihrer personenbezogenen Daten zuständig machen
**D)** Die Gesetzgebung zum Schutz personenbezogener Daten in einer Datenschutzrichtlinie umsetzen.

**A)** Falsch. Ein Mitarbeiter, der die Manager unterstützt, ist für die Einhaltung der Gesetzgebung zum Schutz personenbezogener Daten nicht gefordert. Darüber hinaus sollte die Richtlinie zuerst an die Gesetzgebung angepasst werden.
**B)** Falsch. Dies ist nicht der beste Weg, um die Gesetzgebung zum Schutz personenbezogener Daten einzuhalten.
**C)** Falsch. So sorgt man nicht für die Einhaltung der Gesetzgebung zum Schutz personenbezogener Daten.
**D)** Richtig. Der erste Schritt zur Einhaltung der Gesetzgebung ist die Erstellung einer internen Richtlinie für die Organisation. (Literatur: A, Kapitel 5.1)

**10 / 40**
Eine Organisation beschließt, einen gewissen Teil ihrer IT auszulagern.

Wie lässt sich die Informationssicherheit **am besten** gewährleisten, wenn man mit einem Lieferanten arbeitet?

**A)** Indem man in der Organisation des Lieferanten einen neuen Information Security Officer (ISO) ernennt
**B)** Indem man die Informationssicherheitsanforderungen an den Lieferanten förmlich in einem Vertrag festlegt
**C)** Indem man die beiden Organisationen vollständig voneinander trennt, damit jede für ihre eigenen Daten verantwortlich ist
**D)** Indem man vom Lieferanten verlangt, dass er die Prozesse und Verfahren der Kundenorganisation befolgt

**A)** Falsch. Verfügt die Organisation des Lieferanten bereits über einen ISO, so muss kein neuer ISO benannt werden.
**B)** Richtig. Auch der Abschluss eines Vertrags bietet zwar keine hundertprozentige Sicherheit bezüglich des mit dem Lieferanten verbundenen Risikos, aber ein Vertrag ist die effektivste Lösung. (Literatur: A, Kapitel 5.20)
**C)** Falsch. Die Verantwortlichkeit für alle Informationen bleibt bei der Kundenorganisation. Die vollständige Trennung der Organisationen impliziert häufig, dass die Kundenorganisation die Informationssicherheit in der Organisation des Lieferanten weder sicherstellen noch beeinflussen kann.
**D)** Falsch. Dies ist nicht die beste Lösung, denn Lieferanten sollten einen eigenen Informationssicherheitsprozess haben dürfen.

**11 / 40**
Wer ist dafür zuständig, aus der Unternehmensstrategie und den Unternehmenszielen eine Sicherheitsstrategie und Sicherheitsziele abzuleiten?

**A)** Chief Information Security Officer (CISO)
**B)** Geschäftsführung
**C)** Information Security Officer (ISO)
**D)** Information Security Policy Officer

**A)** Richtig. Der CISO berichtet an die oberste Geschäftsführung und erarbeitet die allgemeine Sicherheitsstrategie für das gesamte Unternehmen. (Literatur: A, Kapitel 5.2)
**B)** Falsch. Die Geschäftsführung legt die Unternehmensstrategie fest, auf deren Grundlage der CISO dann die allgemeine Sicherheitsstrategie festlegt.
**C)** Falsch. Der ISO erarbeitet ausgehend von der Unternehmensrichtlinie die Informationssicherheitsrichtlinie einer Geschäftseinheit und stellt sicher, dass diese eingehalten wird.
**D)** Falsch. Der Information Security Policy Officer ist für die Pflege der von der Sicherheitsstrategie abgeleiteten Informationssicherheitsrichtlinie zuständig.

**12 / 40**
Welches ist das **beste** Beispiel einer menschlichen Bedrohung?

**A)** Ein Leck verursacht einen Stromausfall.
**B)** Ein USB-Stick infiziert ein Netzwerk mit einem Virus.
**C)** Der Server-Raum ist zu staubig.

**A)** Falsch. Ein Leck ist keine menschliche, sondern eine nicht-menschliche Bedrohung.
**B)** Richtig. Ein USB-Stick wird immer von einem Menschen eingesteckt. Infiziert der USB-Stick das Netzwerk mit einem Virus, handelt es sich um eine menschliche Bedrohung. (Literatur: A, Kapitel 3.9.1)
**C)** Falsch. Staub ist keine menschliche, sondern eine nicht-menschliche Bedrohung.

**13 / 40**
Ein Datenbanksystem verfügt nicht über die neuesten Sicherheitspatches und wurde gehackt. Die Hacker konnten auf die Daten zugreifen und diese löschen.

Welcher Begriff aus der Informationssicherheit beschreibt das Fehlen von Sicherheitspatches?

**A)** Auswirkung
**B)** Risiko
**C)** Bedrohung
**D)** Schwachstelle

**A)** Falsch. Der Begriff Auswirkung beschreibt die Folgen, die ein Ereignis für die Organisation oder die Informationen der Organisation hat.
**B)** Falsch. Der Begriff Risiko beschreibt die Kombination aus der Eintrittswahrscheinlichkeit und den Auswirkungen eines Ereignisses.
**C)** Falsch. Ein Beispiel für eine Bedrohung ist eine externe Instanz, die versucht, eine Schwachstelle auszunutzen. In dem hier beschriebenen Beispiel sind die Hacker die Bedrohung.
**D)** Richtig. Mangelnder Schutz ist ein Beispiel für eine Schwachstelle. (Literatur: A, Kapitel 3.5.3)

**14 / 40**
In einem Unternehmen gab es einen Brand. Die Feuerwehr war schnell vor Ort und konnte den Brand löschen, bevor er sich ausbreitete und das gesamte Firmengelände abbrannte. Bei dem Brand wurde jedoch der Server zerstört. Die in einem anderen Raum aufbewahrten Backup-Bänder waren geschmolzen und viele weitere Dokumente gingen verloren.

Welchen **indirekten** Schaden hat der Brand verursacht?

**A)** Verbrannte Computer-Systeme
**B)** Verbrannte Dokumente
**C)** Geschmolzene Backup-Bänder
**D)** Wasserschaden

**A)** Falsch. Verbrannte Computer-Systeme sind ein direkter Schaden des Brands.
**B)** Falsch. Verbrannte Dokumente sind ein direkter Schaden des Brands.
**C)** Falsch. Geschmolzene Backup-Bänder sind ein direkter Schaden des Brands.
**D)** Richtig. Der durch die Brandlöschung verursachte Wasserschaden ist ein indirekter Schaden des Brands. Er ist eine Nebenwirkung der Löschmaßnahmen, die darauf ausgerichtet waren, die Brandschäden zu minimieren. (Literatur: A, Kapitel 3.10)

**15 / 40**
Die Risikostrategien von Unternehmen können sich je nach Art der Geschäftstätigkeit unterscheiden.

Welche Risikostrategie eignet sich für ein Krankenhaus **am besten**?

**A)** Risikoakzeptanz
**B)** Risikovermeidung
**C)** Risikotragfähigkeit
**D)** Risikoneutralität

**A)** Falsch. Ein Krankenhaus kann Risiken in Form von finanziellen Verlusten oder sterbenden Patienten nicht einfach akzeptieren.
**B)** Richtig. Krankenhäuser sollten versuchen, Risiken zu vermeiden. (Literatur: A, Kapitel 3.11)
**C)** Falsch. Risikotragfähigkeit bedeutet, dass bestimmte Risiken akzeptiert werden, beispielsweise wenn die Kosten für Sicherheitsmaßnahmen die Kosten möglicher Schäden übersteigen. Für ein Krankenhaus ist dies nicht die beste Art und Weise, um mit Risiken umzugehen.
**D)** Falsch. Risikoneutralität bedeutet, dass Maßnahmen (Measures) ergriffen werden, damit sich die Bedrohungen entweder nicht mehr manifestieren oder, falls sie es doch tun, der daraus resultierende Schaden auf ein Minimum begrenzt wird. Da Schaden bei Patienten immer schlecht ist, sollten Krankenhäuser sich für die Risikovermeidung entscheiden.

**16 / 40**
Eine professionell durchgeführte Risikoanalyse bietet viele nützliche Informationen. Eine Risikoanalyse verfolgt mehrere Hauptziele.

Was zählt **nicht** zu den Hauptzielen einer Risikoanalyse?

**A)** Die Kosten eines Incidents und die Kosten einer Sicherheitsmaßnahme gegeneinander abzuwägen
**B)** Die relevanten Schwachstellen und Bedrohungen zu bestimmen
**C)** Die Werte (Assets) und deren wirtschaftlichen Wert zu identifizieren
**D)** Die Maßnahmen (Measures) und Sicherheitsmaßnahmen zu implementieren

**A)** Falsch. Das ist durchaus eines der Hauptziele der Risikoanalyse.
**B)** Falsch. Das ist durchaus eines der Hauptziele der Risikoanalyse.
**C)** Falsch. Das ist durchaus eines der Hauptziele der Risikoanalyse.
**D)** Richtig. Das ist kein Ziel der Risikoanalyse. (Literatur: A, Kapitel 3.7)

**17 / 40**
Was ist bei einem Brand eine unterdrückende Sicherheitsmaßnahme?

**A)** Den Brand zu löschen, nachdem er entdeckt wurde
**B)** Den durch den Brand verursachten Schaden zu reparieren
**C)** Eine Brandversicherung abzuschließen

**A)** Richtig. Dies ist eine unterdrückende Sicherheitsmaßnahme. Sie begrenzt den durch den Brand verursachten Schaden auf ein Minimum. (Literatur: A, Kapitel 3.8)
**B)** Falsch. Dies ist keine unterdrückende Sicherheitsmaßnahme. Sie begrenzt den durch den Brand verursachten Schaden nicht auf ein Minimum.
**C)** Falsch. Der Abschluss einer Versicherung bietet Schutz vor den finanziellen Auswirkungen eines Brands und dient als Risikoversicherung.

**18 / 40**
Was ist das Ziel der Klassifizierung von Informationen?

**A)** Die Kennzeichnung von Informationen, um ihre Erkennbarkeit zu verbessern
**B)** Die Erstellung eines Handbuchs zum Umgang mit Mobilgeräten
**C)** Die Gliederung der Informationen nach dem Grad ihrer Vertraulichkeit

**A)** Falsch. Die Kennzeichnung von Informationen ist eine besondere Form der Kategorisierung von Informationen, die nach deren Klassifizierung erfolgt.
**B)** Falsch. Die Erstellung eines Handbuchs bezieht sich auf die Benutzerrichtlinien. Hierbei handelt es sich nicht um die Klassifizierung von Informationen.
**C)** Richtig. Bei der Klassifizierung von Informationen werden verschiedene Vertraulichkeitsstufen festgelegt, sodass die Informationen dann entsprechend eingeteilt werden können. (Literatur: A, Kapitel 5.12)

**19 / 40**
Was ist der **wichtigste** Grund für die Trennung der Verantwortlichkeit?

**A)** Sicherzustellen, dass Mitarbeiter nicht zur gleichen Zeit das Gleiche machen
**B)** Alle Mitarbeiter gemeinsam für die gemachten Fehler zuständig zu machen
**C)** Klarzustellen, wer für welche Aufgaben und Tätigkeiten zuständig ist
**D)** Die Wahrscheinlichkeit unbefugter oder unbeabsichtigter Änderungen auf ein Minimum zu beschränken

**A)** Falsch. Die Trennung der Verantwortlichkeit soll unbefugte oder unbeabsichtigte Änderungen und den Missbrauch von Werten (Assets) der Organisation verhindern. Sie legt nicht fest, wann diese Tätigkeiten durchzuführen sind.
**B)** Falsch. Die Trennung der Verantwortlichkeit trennt Aufgaben und Zuständigkeiten. Sie sorgt nicht für die gemeinsame Verantwortung einer Gruppe von Menschen.
**C)** Falsch. Die Trennung der Verantwortlichkeiten soll unbefugte oder unbeabsichtigte Änderungen und den Missbrauch von Werten (Assets) der Organisation verhindern. Sie soll nicht klarstellen, wer für was zuständig ist.
**D)** Richtig. Verantwortlichkeiten müssen getrennt werden, um unbefugte oder unbeabsichtigte Änderungen und den Missbrauch von Werten (Assets) der Organisation zu verhindern. (Literatur: A, Kapitel 5.3)

**20 / 40**
Wie lässt sich ein angemessener Zugriff auf Informationen **am besten** sicherstellen?

**A)** Durch die Automatisierung von Arbeitsabläufen
**B)** Durch die Festlegung von Verfahrensanweisungen
**C)** Durch die Entwicklung von Arbeitsanweisungen für alle Aufgaben
**D)** Durch die Bereitstellung von Schulungen

**A)** Falsch. Die Automatisierung von Arbeitsabläufen trägt zwar sicherlich zur Informationssicherheit bei, sorgt aber nicht für einen entsprechenden Zugriff auf Informationen.
**B)** Richtig. Verfahrensanweisungen bieten Orientierung, wie Arbeit korrekt, sicher und verantwortungsvoll ausgeführt wird, und sind die beste Möglichkeit, um eine wirksame Informationssicherheit zu erzielen. (Literatur: A, Kapitel 5.36.1)
**C)** Falsch. Dies geht zu sehr ins Detail und ist zu präskriptiv. Daher ist dies nicht die beste Lösung.
**D)** Falsch. Schulungen sind zwar wichtig, sorgen aber nicht für einen entsprechenden Zugriff auf Informationen.

**21 / 40**
In der Geschäftsstelle einer Organisation bricht ein Brand aus. Die Mitarbeiter werden auf andere Geschäftsstellen in der Nähe verteilt und sollen dort weiter arbeiten.

Wo ist eine solche Stand-by-Regelung im Lebenszyklus der Incidents (Incident Cycle) angesiedelt?

**A)** Zwischen Schaden und Wiederherstellung
**B)** Zwischen Incident und Schaden
**C)** Zwischen Wiederherstellung und Bedrohung
**D)** Zwischen Bedrohung und Incident

**A)** Falsch. Schaden und Wiederherstellung werden durch die Stand-by-Regelung begrenzt.
**B)** Richtig. Die Stand-by-Regelung ist eine unterdrückende Maßnahme (Measure), um den Schaden zu begrenzen. (Literatur: A., Kapitel 3.8.4)
**C)** Falsch. Die Wiederherstellung erfolgt erst nachdem die Stand-by-Regelung in die Tat umgesetzt wurde.
**D)** Falsch. Eine Stand-by-Regelung zu realisieren, ohne dass ein Incident vorliegt, wäre sehr kostspielig.

**22 / 40**
Eine Mitarbeiterin entdeckt, dass das Fälligkeitsdatum einer Police ohne ihr Wissen geändert wurde. Da sie die Einzige ist, die dieses Datum ändern darf, meldet sie den Security Incident an den Helpdesk.

Der Helpdesk-Mitarbeiter zeichnet zu diesem Incident folgende Informationen auf:
- Datum und Zeit
- Beschreibung des Incidents
- Mögliche Folgen des Incidents

Welche wichtige Information über den Incident fehlt?

**A)** Der Name der Person, die den Incident gemeldet hat
**B)** Der Name des Software-Pakets
**C)** Die PC-Nummer

**A)** Richtig. Wird ein Incident gemeldet, so muss mindestens der Name der Person aufgezeichnet werden, die den Security Incident meldet. (Literatur: A, Kapitel 5.25)
**B)** Falsch. Hierbei handelt es sich um zusätzliche Informationen, die später ergänzt werden können.
**C)** Falsch. Hierbei handelt es sich um zusätzliche Informationen, die später ergänzt werden können.

**23 / 40**
Warum ist es wichtig, das Informationssicherheitsmanagementsystem (ISMS) der Organisation regelmäßig zu auditieren?

**A)** Viele Kundenverträge fordern Audits zur Gewährleistung der Informationssicherheit.
**B)** Audits sind für die Einhaltung der gesetzlichen und regulatorischen Vorgaben (Compliance) obligatorisch.
**C)** Audits zeigen, ob eine Organisation Probleme hat, ihre finanziellen Ziele zu erreichen.
**D)** Audits decken Schwächen bei der Implementierung von Informationssicherheitsmaßnahmen auf.

**A)** Falsch. Kundenverträge enthalten nur selten Forderungen nach Audits.
**B)** Falsch. Gesetzliche oder regulatorische Vorgaben fordern in der Regel keine Durchführung von Audits.
**C)** Falsch. Audits dienen in der Regel nicht zur Verifizierung der Finanzleistung.
**D)** Richtig. Audits verfolgen den Zweck, Schwächen in den implementierten Sicherheitsmaßnahmen aufzudecken. (Literatur: A, Kapitel 5.35)

**24 / 40**
Welches Dokument enthält die Vorschrift, die die Nutzung des geschäftlichen E-Mail-Accounts für private Zwecke verbietet?

**A)** Führungszeugnis
**B)** Verhaltenskodex
**C)** Datenschutz-Grundverordnung (DSGVO)
**D)** Vertraulichkeitsvereinbarung (NDA)

**A)** Falsch. Ein Führungszeugnis wird von einer Organisation wie dem Bundesamt für Justiz ausgestellt und dient als Nachweis, dass eine Person keine strafbaren Handlungen begangen hat.
**B)** Richtig. Der Verhaltenskodex ist ein Dokument (häufig Teil des Mitarbeiterhandbuchs), das die Richtlinien beschreibt, die für die Mitarbeitenden des Unternehmens gelten. (Literatur: A, Kapitel 6.2)
**C)** Falsch. Bei der DSGVO geht es um den Schutz personenbezogener Informationen.
**D)** Falsch. Eine NDA ist ein Vertrag, der die Offenlegung bestimmter Informationen verbietet. Die Nutzung des geschäftlichen E-Mail-Accounts für private Zwecke regelt ein solches Dokument nicht.

**25 / 40**
Ein Mitarbeiter entdeckt einen Incident.

An wen sollte er diesen **zuerst** melden?

**A)** An den Helpdesk
**B)** An den Information Security Manager (ISM)
**C)** An den Information Security Officer (ISO)
**D)** An den Vorgesetzten

**A)** Richtig. Normalerweise sollten Incidents zur Bewertung, Einleitung von Sofortmaßnahmen und gegebenenfalls Eskalation zuerst an den Helpdesk gemeldet werden. Incidents sollten nicht sofort vertikal eskaliert werden. (Literatur: A, Kapitel 6.8)
**B)** Falsch. Incidents sollten nicht sofort vertikal eskaliert werden. Außerdem ist nicht jeder Incident ein Security Incident. Daher sollte der Incident zuerst vom Helpdesk geprüft werden, um festzustellen, ob es sich um einen Security Incident handelt.
**C)** Falsch. Incidents sollten nicht sofort vertikal eskaliert werden. Außerdem ist nicht jeder Incident ein Security Incident. Daher sollte der Incident zuerst vom Helpdesk geprüft werden, um festzustellen, ob es sich um einen Security Incident handelt.
**D)** Falsch. Incidents sollten nicht sofort vertikal eskaliert werden.

**26 / 40**
Wie kann man bei Mitarbeitenden **am effektivsten** Bewusstsein für Informationssicherheit schaffen?

**A)** Durch gezielte Schulungen zur Bewusstseinsbildung für die Geschäftsführung
**B)** Durch Teilnahme aller Mitarbeitenden an externen Schulungen zum Thema Informationssicherheit
**C)** Durch Einrichtung eines speziell auf die Organisation ausgerichteten Programms zur Bewusstseinsbildung
**D)** Durch das Angebot einer allgemeinen Online-Schulung zum Thema Informationssicherheit

**A)** Falsch. Bewusstsein für Informationssicherheit ist für alle Mitarbeitenden wichtig, nicht nur für die Geschäftsführung.
**B)** Falsch. Externe Schulungen erfüllen möglicherweise die Bedürfnisse einer bestimmten Organisation nicht vollumfänglich.
**C)** Richtig. Am effektivsten ist es, wenn das Programm zur Bewusstseinsbildung für Informationssicherheit auf die spezifischen Bedürfnisse der Organisation ausgerichtet ist. (Literatur: A, Kapitel 6.3)
**D)** Falsch. Allgemeine Schulungen zum Thema Informationssicherheit erfüllen die Bedürfnisse einer bestimmten Organisation möglicherweise nicht vollumfänglich.

**27 / 40**
Welche physische Sicherheitsmaßnahme regelt den Zugriff auf die Informationen einer Organisation?

**A)** Installation einer Klimaanlage
**B)** Verbot der Nutzung von USB-Sticks
**C)** Erfordernis von Benutzernamen und Password
**D)** Verwendung von Sicherheitsglas

**A)** Falsch. Klimaanlagen haben nichts mit der Regelung des Zugriffs auf die Informationen einer Organisation zu tun.
**B)** Falsch. Dies ist eine organisatorische Sicherheitsmaßnahme.
**C)** Falsch. Dies ist eine technische Sicherheitsmaßnahme.
**D)** Richtig. Die Verwendung von Sicherheitsglas ist ein Beispiel für eine physische Sicherheitsmaßnahme, um Unbefugten den Zutritt zu einem Gebäude zu verwehren. (Literatur: A, Kapitel 7.4)

**28 / 40**
Ein Rechenzentrum nutzt Akkus, hat jedoch keinen Stromgenerator.

Welches Risiko besteht in diesem Fall für die Verfügbarkeit des Rechenzentrums?

**A)** Bei einer Wiederherstellung der Stromversorgung schaltet sich die Hauptstromversorgung möglicherweise nicht automatisch wieder ein, da dazu ein Generator benötigt wird.
**B)** Der Ausfall der Hauptstromversorgung kann länger als nur ein paar Minuten oder Stunden dauern und in diesem Fall wäre kein Strom verfügbar.
**C)** Die Lebensspanne der Akkus ist begrenzt, und nach ein paar Tagen haben die Akkus möglicherweise keinen Diesel mehr und würden dann auch nicht mehr funktionieren.
**D)** Die Akkus müssen nach ein paar Stunden vom Stromgenerator mit Strom versorgt werden und bieten daher nur eingeschränkt Schutz.

**A)** Falsch. Ein Stromgenerator dient nicht dazu, die Hauptstromversorgung einzuschalten.
**B)** Richtig. Akkus schützen nur bei vorübergehenden Stromausfällen oder Überlastungen. Ein Stromgenerator dagegen bietet auch Schutz bei längeren Stromausfällen. (Literatur: A, Kapitel 7.11.1)
**C)** Falsch. Diesel dient als Treibstoff für den Generator. Akkus werden mit Hilfe von Batterien betrieben.
**D)** Falsch. Es ist zwar richtig, dass Akkus nur über einen kurzen Zeitraum funktionieren, sie werden aber nicht vom Generator mit Strom versorgt. Der Generator übernimmt ganz einfach die Stromversorgung anstelle der Akkus.

**29 / 40**
Warum wird im Server-Raum eine Klimaanlage installiert?

**A)** Die Backup-Bänder sind aus dünnem Plastik, das hohen Temperaturen nicht standhalten kann. Bei zu hohen Temperaturen im Server-Raum könnten sie beschädigt werden.
**B)** Die im Server-Raum tätigen Mitarbeitenden sollten nicht in der Hitze arbeiten müssen. Mit den Temperaturen steigt auch die Wahrscheinlichkeit, dass die Mitarbeitenden Fehler machen.
**C)** Die Luft im Server-Raum muss gekühlt und die von den Geräten produzierte Wärme abgeführt werden. Darüber hinaus filtert die Klimaanlage die Raumluft und entzieht ihr Feuchtigkeit.
**D)** Der Server-Raum bietet die beste Möglichkeit, um die Raumluft der Niederlassung zu kühlen. Installiert man die Klimaanlage dort, muss kein Büroraum für eine so große technische Anlage geopfert werden.

**A)** Falsch. Backup-Bänder sollten nicht im Server-Raum gelagert werden. Bei einem Brand würden sonst sowohl die aktuell genutzten Informationen als auch das Backup zerstört.
**B)** Falsch. Dies ist nicht der Grund, warum im Server-Raum eine Klimaanlage installiert werden sollte.
**C)** Richtig. Server-Räume sind hinsichtlich der physischen Sicherheit gesondert zu betrachten. Server-Räume beherbergen sensible Geräte, die feuchtigkeits- und hitzeempfindlich sind und selbst Wärme produzieren. (Literatur: A, Kapitel 7.11.2)
**D)** Falsch. Im Server-Raum wird nicht die Raumluft für die gesamte Niederlassung gekühlt.

**30 / 40**
Im Rahmen der physischen Informationssicherheit können mehrere Sicherheitsringe (Protection Rings) zum Einsatz kommen, in denen dann verschiedene Maßnahmen (Measures) ergriffen werden können.

Was ist **kein** Sicherheitsring?

**A)** Building Ring (Gebäude Ring)
**B)** Middle Ring (Mittlerer Ring)
**C)** Secure Room Ring (Sicherheitsbereich Ring)
**D)** Outer Ring (Äußerer Ring)

**A)** Falsch. Das Gebäude ist ein Sicherheitsring mit Zugang zum Betriebsgelände.
**B)** Richtig. Man unterscheidet zwischen den folgenden vier Sicherheitsringen: Outer Ring, Building, Workspaces, und Secure Room. (Literatur: A, Kapitel 7.0.1)
**C)** Falsch. Der Secure Room Ring ist ein gültiger Bereich, in dem sich der zu schützende Wert (Asset) befindet.
**D)** Falsch. Der Outer Ring ist ein gültiger Bereich und bezeichnet das Gebiet rund um das Betriebsgelände.

**31 / 40**
Welche Sicherheitsmaßnahme für einen Wert (Asset) erforderlich ist, richtet sich nach dem jeweiligen Wert (Asset).

Wie lässt sich die Sicherheit eines Werts **am besten** gewährleisten?

**A)** Indem man ein Formular sichert durch ausfüllen und abzeichnen
**B)** Indem man einen Laptop sichert und diesen einem einzigen Benutzer zuweist
**C)** Indem man einen USB-Stick mittels Verschlüsselung sichert
**D)** Indem man eine Internetverbindung mittels Backup sichert

**A)** Falsch. Ein Stück Papier mit Informationen abzulegen ist keine angemessene Sicherheitsmaßnahme.
**B)** Falsch. Zwar ist es eindeutig besser, wenn ein Laptop nur von einer einzigen Person benutzt wird, aber das ist nicht die beste Lösung. Die Verwaltung von Benutzerkonten und Password-Kontrollen sind bessere Sicherheitsmaßnahmen.
**C)** Richtig. Verschlüsselung stellt für einen USB-Stick eine valide Sicherheitsmaßnahme dar. Viele Organisationen nutzen diese Sicherheitsmaßnahme unabhängig von der Klassifizierung der auf dem USB-Stick gespeicherten Informationen. (Literatur: A, Kapitel 8.12)
**D)** Falsch. Ein Backup zu nutzen ist nicht die beste direkte Lösung, um eine Internetverbindung zu sichern.

**32 / 40**
Welche Sicherheitsmaßnahme trägt dazu bei, Informationssicherheit bereits bei der Entwicklung von Systemen zu berücksichtigen?

**A)** Die Redundanz der Server sicherzustellen
**B)** Physische Zugangskontrollen zu implementieren
**C)** Background Checks bei Mitarbeitenden durchzuführen
**D)** Datenklassifizierung bei Informationswerten (Informationsassets) zu nutzen

**A)** Richtig. Die Redundanz von Servern ist eine Sicherheitsmaßnahme, die bereits bei der Entwicklung des Systems in Betracht gezogen werden sollte. (Literatur: A, Kapitel 8.14)
**B)** Falsch. Dies ist zwar eine valide Sicherheitsmaßnahme zur Verbesserung der Informationssicherheit, hat aber nichts mit der Systementwicklung zu tun.
**C)** Falsch. Dies ist zwar eine valide Sicherheitsmaßnahme zur Verbesserung der Informationssicherheit, hat aber nichts mit der Systementwicklung zu tun.
**D)** Falsch. Dies ist zwar eine valide Sicherheitsmaßnahme zur Verbesserung der Informationssicherheit, hat aber nichts mit der Systementwicklung zu tun.

**33 / 40**
Eine Organisation ändert ihre Richtlinie. Ab sofort haben die Mitarbeitenden auch die Möglichkeit zu Remote- oder Telearbeit.

Welche Sicherheitsmaßnahme sollte nun eingeführt werden?

**A)** Erstellen von V-Lans zur Segmentierung des Unternehmensnetzwerks
**B)** Verschlüsselung der Informationen im Unternehmensnetzwerk
**C)** Einrichtung von Firewalls im Unternehmensnetzwerk
**D)** Verbindung mit dem Unternehmensnetzwerk über virtuelles privates Netzwerk (VPN)

**A)** Falsch. Die Segmentierung der Netzwerke zur Gewährleistung der Vertraulichkeit und die Trennung der Verantwortlichkeit sollten bereits eingeführt worden sein. Diese beiden Sicherheitsmaßnahmen gelten nicht speziell für die Umstellung der Richtlinie auf Remote- oder Telearbeit.
**B)** Falsch. Zwar ist Verschlüsselung zum Schutz von Informationen unabdingbar, sie gilt aber nicht speziell dafür, Mitarbeitenden Remote- oder Telearbeit zu ermöglichen.
**C)** Falsch. Firewalls zwischen dem Unternehmensnetzwerk und der Außenwelt sind zwar wichtig, sollten aber bereits bestehen. Außerdem dienen Firewalls nicht direkt der Sicherung von Remote- oder Televerbindungen.
**D)** Richtig. Die Nutzung von VPN ist eine Sicherheitsmaßnahme, die ergriffen werden sollte, um Mitarbeitenden Remote- oder Telearbeit zu ermöglichen. (Literatur: A, Kapitel 8.2)

**34 / 40**
Die Mitarbeitenden einer Organisation arbeiten an Laptops, die mittels asymmetrischer Kryptographie geschützt sind. Um die Schlüsselverwaltung so wirtschaftlich wie möglich zu gestalten, nutzen alle Berater das selbe Schlüsselpaar.

Bei Gefährdung bestimmter Informationen sind neue Schlüssel bereitzustellen.

In welchem Fall sollten neue Schlüssel bereitgestellt werden?

**A)** Wenn der private Schlüssel bekannt wird
**B)** Wenn der öffentliche Schlüssel bekannt wird
**C)** Wenn die Infrastruktur mit öffentlichem Schlüssel (PKI) bekannt wird

**A)** Richtig. Bei der asymmetrischen Kryptographie ist es wichtig, den privaten Schlüssel geheim zuhalten. Der öffentliche Schlüssel darf bekannt werden. (Literatur: A, Kapitel 8.24.5)
**B)** Falsch. Der öffentliche Schlüssel darf auf der ganzen Welt bekannt sein. Der private Schlüssel muss geheim gehalten werden, um Integrität und Verfügbarkeit sicherzustellen.
**C)** Falsch. Die PKI wird genutzt, um die Schlüssel für asymmetrische Verschlüsselungssysteme auszutauschen.

**35 / 40**
Welche Art von Sicherheit bietet eine Infrastruktur mit öffentlichem Schlüssel (PKI)?

**A)** Eine PKI stellt regelmäßige Backups der Unternehmensdaten sicher.
**B)** Eine PKI weist gegenüber den Kunden nach, dass ein webbasiertes Geschäft sicher ist.
**C)** Eine PKI verifiziert, ob eine Person oder ein System zu einem bestimmten öffentlichen Schlüssel gehört.

**A)** Falsch. Eine PKI stellt nicht sicher, dass Backups erstellt werden.
**B)** Falsch. Eine PKI garantiert, dass eine bestimmte Person oder ein bestimmtes System zu einem öffentlichen Schlüssel gehören.
**C)** Richtig. Eine PKI gewährleistet über Vereinbarungen, Verfahren und eine Organisationsstruktur, dass eine bestimmte Person oder ein bestimmtes System zu einem bestimmten öffentlichen Schlüssel gehören. (Literatur: A, Kapitel 8.24.6)

**36 / 40**
Bei welcher Art von Schadsoftware handelt es sich um ein Programm, das neben seiner offensichtlichen Funktion auch bewusst weitere Aktivitäten ausführt?

**A)** Logikbombe (Logic Bomb)
**B)** Spyware
**C)** Trojaner
**D)** Wurm

**A)** Falsch. Eine Logikbombe ist ein Stück Code, das in ein Softwaresystem eingeschleust wird. Treten bestimmte Bedingungen ein, führt der Code eine Funktion aus. Dabei werden nicht immer bösartige Absichten verfolgt. Eine Logikbombe führt nicht immer sekundäre Aktivitäten aus.
**B)** Falsch. Spyware ist ein Computer-Programm, das Informationen über den Benutzer des Computers sammelt und diese an eine andere Partei schickt.
**C)** Richtig. Ein Trojaner ist ein Programm, das neben seiner eigentlichen Funktion, absichtlich und vom Computer-Benutzer unbemerkt, weitere Aktivitäten ausführt, die der Integrität des infizierten Systems schaden können. (Literatur: A, Kapitel 8.7.2)
**D)** Falsch. Ein Wurm erstellt ein Netzwerk aus infizierten Computern, indem sie sich selbst repliziert.

**37 / 40**
Bei welcher Art von Schadsoftware handelt es sich um ein Programm, das ein Netzwerk infizierter Computer erstellt, indem es sich selbst repliziert?

**A)** Logikbombe (Logic Bomb)
**B)** Spyware
**C)** Trojaner
**D)** Wurm

**A)** Falsch. Eine Logikbombe ist ein Stück Code, das in ein Softwaresystem eingeschleust wird. Treten bestimmte Bedingungen ein, führt der Code eine Funktion aus. Dabei werden nicht immer bösartige Absichten verfolgt.
**B)** Falsch. Spyware ist ein Computer-Programm, das Informationen über den Benutzer des Computers sammelt und diese an eine andere Partei schickt.
**C)** Falsch. Ein Trojaner ist ein Programm, das neben seiner eigentlichen Funktion, absichtlich und vom Computer-Benutzer unbemerkt, weitere Aktivitäten ausführt, die der Integrität des infizierten Systems schaden können.
**D)** Richtig. Genau das macht ein Wurm. (Literatur: A, Kapitel 8.7)

**38 / 40**
Welche Gesetzgebung oder Rechtsvorschrift im Bereich der Informationssicherheit gilt für alle Organisationen?

**A)** Datenschutz-Grundverordnung (DSGVO)
**B)** Geistige Eigentumsrechte
**C)** ISO/IEC 27001
**D)** ISO/IEC 27002

**A)** Richtig. Alle Organisationen sollten über eine Richtlinie und über Verfahren zum Schutz personenbezogener Daten verfügen. Alle Mitarbeiter, die personenbezogene Daten verarbeiten, sollten diese Richtlinie und die Verfahren kennen. (Literatur: A, Kapitel 5.33)
**B)** Falsch. Diese Vorschrift hat nichts mit der Informationssicherheit von Organisationen zu tun.
**C)** Falsch. Hierbei handelt es sich um eine Norm, die Organisationen einen Leitfaden für die Einführung von Informationssicherheitsprozessen an die Hand gibt.
**D)** Falsch. Diese Norm mit dem Titel ‚Informationssicherheit, Cybersicherheit und Datenschutz – Informationssicherheitsmaßnahmen' enthält Leitlinien zur Informationssicherheitsrichtlinie und zu Sicherheitsmaßnahmen.

**39 / 40**
Welche ISO-Norm konzentriert sich auf die Implementierung von Informationssicherheitsmaßnahmen?

**A)** ISO/IEC 27000
**B)** ISO/IEC 27001
**C)** ISO/IEC 27002
**D)** ISO/IEC 27005

**A)** Falsch. Dies ist die Norm zur allgemeinen Einführung der Normenreihe ISO/IEC 27000.
**B)** Falsch. Diese Norm enthält die Anforderungen an ein Informationssicherheitsmanagementsystem (ISMS).
**C)** Richtig. Diese Norm spezifiziert die Informationssicherheitsmaßnahmen und bietet Orientierung bezüglich deren Implementierung. (Literatur: A, Kapitel 4.12)
**D)** Falsch. Die Norm ISO/IEC 27005 befasst sich hauptsächlich mit dem Risikomanagement im Bereich der Informationssicherheit.

**40 / 40**
Die Normen welcher Normenorganisation werden in Europa **am häufigsten** genutzt?

**A)** American National Standards Institute (ANSI)
**B)** International Organization for Standardization (ISO)
**C)** National Institute of Standards and Technology (NIST)

**A)** Falsch. ANSI-Normen werden eher in den Vereinigten Staaten von Amerika genutzt.
**B)** Richtig. ISO-Normen werden in Europa am häufigsten genutzt. (Literatur: A, Kapitel 5.36)
**C)** Falsch. NIST-Normen werden eher in den Vereinigten Staaten von Amerika genutzt.

# Beurteilung

Die richtigen Antworten auf die Fragen in dieser Musterprüfung finden Sie in nachstehender Tabelle.

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




## Kontakt EXIN

www.exin.com