Musterprüfung

Ausgabe 202507

Inhalt

Einführung

Dies ist die EXIN Information Security Foundation based on ISO/IEC 27001 (ISFS.DE-EN) 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 database contains a few million transactions of a phone company. An invoice for a customer has been generated and sent.

What does this invoice contain for the customer?

A) Daten
Data
B) Informationen
Information
C) Daten und Informationen
Data and information

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

What is the difference between data and information?

A) Bei Daten kann es sich um alle erdenklichen Fakten oder Zahlen handeln. Informationen sind Daten, die eine Bedeutung haben.
Data can be any facts or figures. Information is data that has meaning.
B) Daten bestehen aus unstrukturierten Zahlen. Informationen bestehen aus strukturierten Zahlen.
Data consists of unstructured figures. Information consists of structured figures.
C) Daten erfordern keine Sicherheit. Informationen erfordern Sicherheit.
Data does not require security. Information requires security.
D) Daten haben keinen Wert. Informationen dagegen sind verarbeitete Daten und haben einen Wert.
Data has no value. Information, which is processed data, has value.

3 / 40
Was ist der Fokus des Informationsmanagements?

What is the focus of information management?

A) Die unterbrechungsfreie Fortführung von Business-Aktivitäten und -Prozessen zu ermöglichen
Allowing business activities and processes to continue without interruption
B) Die Identifizierung und Nutzung des Werts von Informationen sicherzustellen
Ensuring that the value of information is identified and exploited
C) Den Zugriff auf automatisierte Systeme durch Unbefugte zu verhindern
Preventing unauthorized persons from having access to automated systems
D) Die Informationsflüsse im Unternehmen zu verstehen
Understanding how information flows through an organization

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?

An organization must understand the risks it is facing before it can take appropriate measures.

What should be understood to determine risk?

A) Die Eintrittswahrscheinlichkeit eines Ereignisses und die Auswirkungen des Ereignisses auf die Organisation
The likelihood of something happening and its consequences to the organization
B) Die häufigsten Risiken und wie diese gemäß den Festlegungen in Best Practices reduziert werden können
The most common dangers and how to mitigate these as defined in best practices
C) Die Bedrohungen, mit denen eine Organisation konfrontiert ist und wie anfällig die Organisation für diese Bedrohungen ist
The threats an organization faces and how vulnerable the organization is to them
D) Die ungeplanten Ereignisse, mit denen eine Organisation konfrontiert ist und was in einem solche Fall zu tun ist
The unplanned events an organization faces and what to do in case of such an event

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

Besides integrity and confidentiality, what is the third reliability aspect of information?

A) Genauigkeit
Accuracy
B) Verfügbarkeit
Availability
C) Vollständigkeit
Completeness
D) Monetärer Wert
Value

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?

An organization has a network printer in the hallway of the company. Many employees do not pick up their printouts immediately and leave them on the printer.

What is the consequence of this to the reliability of the information?

A) Die Verfügbarkeit der Informationen ist nicht mehr gewährleistet.
The availability of the information is no longer guaranteed.
B) Die Vertraulichkeit der Informationen ist nicht mehr gewährleistet.
The confidentiality of the information is no longer guaranteed.
C) Die Integrität der Informationen ist nicht mehr gewährleistet.
The integrity of the information is no longer guaranteed.

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

What is the difference between accountability and auditability?

A) Verantwortlichkeit bedeutet, dass eine Organisation ihre Finanzkonten gut verwaltet. Auditierbarkeit bedeutet, dass eine Organisation ein Audit bestanden hat.
Accountability means an organization has their financial accounts well-administered. Auditability means an organization passed an audit.

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.
Accountability means being liable for the results of an organization's activities. Auditability refers to an organization's readiness for being independently reviewed.

C) Verantwortlichkeit bedeutet die Verantwortung für die Handlungen einer Person zu übernehmen. Auditierbarkeit bedeutet die Verantwortung für die Handlungen einer Organisation zu haben.
Accountability means having responsibility for an individual's actions. Auditability means having responsibility for an organization's actions.

D) Verantwortlichkeit bedeutet, dass eine Organisation den Sarbanes Oxley Act (SOX) einhält. Auditierbarkeit bedeutet, dass eine Organisation der Norm ISO/IEC 27001 entspricht.
Accountability means that an organization complies with Sarbanes-Oxley (SOX). Auditability refers to an organization complying with ISO/IEC 27001.

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

---
*How is the purpose of an information security policy **best** described?*

A) Eine Informationssicherheitsrichtlinie dokumentiert die Analyse der Risiken und die Suche nach entsprechenden Sicherheitsmaßnahmen.
An information security policy documents the analysis of risks and the search for appropriate controls.

B) Eine Informationssicherheitsrichtlinie bietet der Organisation Orientierung und Unterstützung hinsichtlich der Informationssicherheit.
An information security policy gives direction and support to the organization regarding information security.

C) Eine Informationssicherheitsrichtlinie konkretisiert die Sicherheitsplanung mit den erforderlichen Details.
An information security policy makes the security plan concrete by providing it with the necessary details.

D) Eine Informationssicherheitsrichtlinie bieten Einblick in Bedrohungen und deren mögliche Folgen.
An information security policy provides insight into threats and the possible consequences.

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

Was sollte Sara **zuerst** tun?

Sara has been tasked with ensuring that the organization complies with personal data protection legislation.

*What is the **first** thing she should do?*

A) Einen Mitarbeiter benennen, der die Manager bei der Einhaltung der Richtlinie unterstützt
Appoint a person responsible for supporting managers in adhering to the policy
B) Die Erhebung und Speicherung personenbezogener Daten verbieten
Issue a ban on collecting and storing personal information
C) Die Mitarbeitenden für die Übermittlung ihrer personenbezogenen Daten zuständig machen
Make employees responsible for submitting their personal data
D) Die Gesetzgebung zum Schutz personenbezogener Daten in einer Datenschutzrichtlinie umsetzen.
Translate the personal data protection legislation into a privacy policy

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?

An organization decides to outsource some of its IT.

*How can information security **best** be ensured when working with a supplier?*

A) Indem man in der Organisation des Lieferanten einen neuen Information Security Officer (ISO) ernennt
Appoint a new information security officer (ISO) in the supplier's organization
B) Indem man die Informationssicherheitsanforderungen an den Lieferanten förmlich in einem Vertrag festlegt
Formalize the information security requirements for the supplier in an agreement
C) Indem man die beiden Organisationen vollständig voneinander trennt, damit jede für ihre eigenen Daten verantwortlich ist
Keep both organizations fully separated to make everyone accountable for their data
D) Indem man vom Lieferanten verlangt, dass er die Prozesse und Verfahren der Kundenorganisation befolgt
Require the supplier to follow the customer organization's processes and procedures

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

Who is responsible for the translation of the business strategy and objectives to security strategy and objectives?

A) Chief Information Security Officer (CISO)
Chief information security officer (CISO)
B) Geschäftsführung
General management
C) Information Security Officer (ISO)
Information security officer (ISO)
D) Information Security Policy Officer
Information security policy officer

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

---
*Which is the **best** example of a human threat?*

A) Ein Leck verursacht einen Stromausfall.
A leak causes a failure of the electricity supply.
B) Ein USB-Stick infiziert ein Netzwerk mit einem Virus.
A USB-stick passes on a virus to a network.
C) Der Server-Raum ist zu staubig.
There is too much dust in the server room.

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 database system does not have the latest security patches applied to it and was hacked. The hackers were able to access the data and delete it.

What information security concept describes the lack of security patches?

A) Auswirkung
Impact
B) Risiko
Risk
C) Bedrohung
Threat
D) Schwachstelle
Vulnerability

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?

There was a fire in a company. The fire department quickly arrived at the scene and could extinguish the fire before it spread and burned down the entire premises. The server, however, was destroyed in the fire. The backup tapes kept in another room had melted and many other documents were lost.

*What **indirect** damage is caused by this fire?*

A) Verbrannte Computer-Systeme
Burned computer systems
B) Verbrannte Dokumente
Burned documents
C) Geschmolzene Backup-Bänder
Melted backup tapes
D) Wasserschaden
Water damage

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

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

Companies can have different risk strategies depending on the type of business.

*Which risk strategy is **most** suitable for a hospital?*

A) Risikoakzeptanz
Risk accepting
B) Risikovermeidung
Risk avoiding
C) Risikotragfähigkeit
Risk bearing
D) Risikoneutralität
Risk neutral

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

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

A well-executed risk analysis provides a great deal of useful information. A risk analysis has different main objectives.

*What is **not** a main objective of a risk analysis?*

A) Die Kosten eines Incidents und die Kosten einer Sicherheitsmaßnahme gegeneinander abzuwägen
Balance the costs of an incident and the costs of a control
B) Die relevanten Schwachstellen und Bedrohungen zu bestimmen
Determine relevant vulnerabilities and threats
C) Die Werte (Assets) und deren wirtschaftlichen Wert zu identifizieren
Identify assets and their value
D) Die Maßnahmen (Measures) und Sicherheitsmaßnahmen zu implementieren
Implement measures and controls

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

What is a repressive control in case of a fire?

A) Den Brand zu löschen, nachdem er entdeckt wurde
Putting out a fire after it has been detected
B) Den durch den Brand verursachten Schaden zu reparieren
Repairing damage caused by the fire
C) Eine Brandversicherung abzuschließen
Taking out a fire insurance

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

What is the goal of classification of information?

A) Die Kennzeichnung von Informationen, um ihre Erkennbarkeit zu verbessern
Applying labels to make the information easier to recognize
B) Die Erstellung eines Handbuchs zum Umgang mit Mobilgeräten
Creating a manual on how to handle mobile devices
C) Die Gliederung der Informationen nach dem Grad ihrer Vertraulichkeit
Structuring information according to its sensitivity

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

---
*What is the **most** important reason to apply segregation of duties?*

A) Sicherzustellen, dass Mitarbeiter nicht zur gleichen Zeit das Gleiche machen
Ensuring that employees do not do the same work at the same time
B) Alle Mitarbeiter gemeinsam für die gemachten Fehler zuständig zu machen
Holding all employees jointly responsible for the mistakes they make
C) Klarzustellen, wer für welche Aufgaben und Tätigkeiten zuständig ist
Making clear who is responsible for what tasks and activities
D) Die Wahrscheinlichkeit unbefugter oder unbeabsichtigter Änderungen auf ein Minimum zu beschränken
Minimizing the chance of unauthorized or unintended changes

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

---
*What is the **best** way to ensure appropriate access to information?*

A) Durch die Automatisierung von Arbeitsabläufen
Automate workflows
B) Durch die Festlegung von Verfahrensanweisungen
Define operating procedures
C) Durch die Entwicklung von Arbeitsanweisungen für alle Aufgaben
Develop work instructions for all tasks
D) Durch die Bereitstellung von Schulungen
Provide training

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 fire breaks out in an office of an organization. The employees are transferred to neighboring offices of the organization to continue their work.

Where in the incident cycle is moving to a stand-by arrangement found?

A) Zwischen Schaden und Wiederherstellung
Between the damage and recovery stages
B) Zwischen Incident und Schaden
Between the incident and damage stages
C) Zwischen Wiederherstellung und Bedrohung
Between the recovery and threat stages
D) Zwischen Bedrohung und Incident
Between the threat and incident stages

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?

An employee discovers that the expiration date of a policy has been changed without her knowledge. She is the only person authorized to do this and reports this security incident to the helpdesk.
The helpdesk worker records the following information regarding this incident:
- date and time
- description of the incident
- possible consequences of the incident

What important information about the incident is missing here?

A) Der Name der Person, die den Incident gemeldet hat
The name of the person reporting the incident
B) Der Name des Software-Pakets
The name of the software package
C) Die PC-Nummer
The PC number

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

Why is it important to regularly audit the organization's information security management system (ISMS)?

A) Viele Kundenverträge fordern Audits zur Gewährleistung der Informationssicherheit.
Audits are a common requirement in customer contracts to ensure information security.
B) Audits sind für die Einhaltung der gesetzlichen und regulatorischen Vorgaben (Compliance) obligatorisch.
Audits are a required element in order to comply with legal or regulatory requirements.
C) Audits zeigen, ob eine Organisation Probleme hat, ihre finanziellen Ziele zu erreichen.
Audits uncover issues with the ability to meet an organization's financial targets.
D) Audits decken Schwächen bei der Implementierung von Informationssicherheitsmaßnahmen auf.
Audits uncover weaknesses in the implementation of information security controls.

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

Which document would include a rule that forbids the use of company e-mail for private purposes?

A) Führungszeugnis
Certificate of good character
B) Verhaltenskodex
Code of conduct
C) Datenschutz-Grundverordnung (DSGVO)
General Data Protection Regulation (GDPR)
D) Vertraulichkeitsvereinbarung (NDA)
Non-disclosure agreement (NDA)

25 / 40
Ein Mitarbeiter entdeckt einen Incident.

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

---
*When an employee detects an incident, to whom should it typically be reported **first**?*

A) An den Helpdesk
The helpdesk
B) An den Information Security Manager (ISM)
The information security manager (ISM)
C) An den Information Security Officer (ISO)
The information security officer (ISO)
D) An den Vorgesetzten
The manager

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

---
*What is the **most** effective way to create information security awareness among employees?*

A) Durch gezielte Schulungen zur Bewusstseinsbildung für die Geschäftsführung
Focus awareness training on the management team
B) Durch Teilnahme aller Mitarbeitenden an externen Schulungen zum Thema Informationssicherheit
Send all employees to an external information security training
C) Durch Einrichtung eines speziell auf die Organisation ausgerichteten Programms zur Bewusstseinsbildung
Set up an organization-specific awareness program
D) Durch das Angebot einer allgemeinen Online-Schulung zum Thema Informationssicherheit
Use a generic, online information security training course

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

What physical control manages access to an organization's information?

A) Installation einer Klimaanlage
Installing air conditioning
B) Verbot der Nutzung von USB-Sticks
Prohibiting the use of USB sticks
C) Erfordernis von Benutzernamen und Password
Requiring username and password
D) Verwendung von Sicherheitsglas
Using unbreakable glass

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

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

A data center uses battery packs but has no power generator.

What is the risk associated with this setup for the availability of the data center?

A) Bei einer Wiederherstellung der Stromversorgung schaltet sich die Hauptstromversorgung möglicherweise nicht automatisch wieder ein, da dazu ein Generator benötigt wird.
The main power may not come up again automatically when restored, because this needs a power generator.
B) Der Ausfall der Hauptstromversorgung kann länger als nur ein paar Minuten oder Stunden dauern und in diesem Fall wäre kein Strom verfügbar.
The main power outage may last for longer than a few minutes or hours, which will cause unavailability of power.
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.
The battery packs' lifespan is limited, so they may run out of diesel and stop functioning after a couple of days.
D) Die Akkus müssen nach ein paar Stunden vom Stromgenerator mit Strom versorgt werden und bieten daher nur eingeschränkt Schutz.
The battery packs must be powered by the power generator after a few hours, so they only provide limited protection.

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

Why is air conditioning placed in the server room?

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.
Backup tapes are made from thin plastic that cannot withstand high temperatures. Therefore, if it gets too hot in the server room, they may get damaged.

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.
Employees that work in the server room should not work in the heat. The heat increases the chance that they make errors.

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.
In the server room the air must be cooled, and the heat produced by the equipment must be extracted. It also dehumidifies and filters the air in the room.

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.
The server room is the best way to cool the air in the office. No office space must be sacrificed for such a large piece of equipment.

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?

In physical security, multiple protection rings can be applied in which different measures can be taken.

*What is **not** a protection ring?*

A) Building Ring (Gebäude Ring)
Building ring

B) Middle Ring (Mittlerer Ring)
Middle ring

C) Secure Room Ring (Sicherheitsbereich Ring)
Secure room ring

D) Outer Ring (Äußerer Ring)
Outer 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?

The control to secure an asset depends on the asset.

*What is the **most** appropriate way to secure the asset?*

A) Indem man ein Formular sichert durch ausfüllen und abzeichnen
Secure a form by having it filled out and signed off
B) Indem man einen Laptop sichert und diesen einem einzigen Benutzer zuweist
Secure a laptop by assigning it to a single user
C) Indem man einen USB-Stick mittels Verschlüsselung sichert
Secure a USB-stick with encryption
D) Indem man eine Internetverbindung mittels Backup sichert
Secure an internet connection with a backup

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

What information security control helps to develop systems with information security in mind?

A) Die Redundanz der Server sicherzustellen
Ensuring redundancy of the servers
B) Physische Zugangskontrollen zu implementieren
Implementing physical entry controls
C) Background Checks bei Mitarbeitenden durchzuführen
Performing background checks on employees
D) Datenklassifizierung bei Informationswerten (Informationsassets) zu nutzen
Using data classification on information assets

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?

An organization changes its policy. Employees are now allowed to work remotely.

What control should now be put in place?

A) Erstellen von V-Lans zur Segmentierung des Unternehmensnetzwerks
Create V-LANs to segment the corporate network
B) Verschlüsselung der Informationen im Unternehmensnetzwerk
Encrypt the information on the corporate network
C) Einrichtung von Firewalls im Unternehmensnetzwerk
Install firewalls on the corporate network
D) Verbindung mit dem Unternehmensnetzwerk über virtuelles privates Netzwerk (VPN)
Use a VPN to connect to the corporate network

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?

The employees of an organization work on laptops that are protected by asymmetrical cryptography. To keep the management of the keys cheap, all consultants use the same key pair.
If certain information is compromised, new keys should be supplied.

In what case should new keys be supplied?

A) Wenn der private Schlüssel bekannt wird
When the private key becomes known
B) Wenn der öffentliche Schlüssel bekannt wird
When the public key becomes known
C) Wenn die Infrastruktur mit öffentlichem Schlüssel (PKI) bekannt wird
When the public key infrastructure (PKI) becomes known

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

What sort of security does a public key infrastructure (PKI) offer?

A) Eine PKI stellt regelmäßige Backups der Unternehmensdaten sicher.
A PKI ensures that backups of company data are made on a regular basis.
B) Eine PKI weist gegenüber den Kunden nach, dass ein webbasiertes Geschäft sicher ist.
A PKI shows customers that a web-based business is secure.
C) Eine PKI verifiziert, ob eine Person oder ein System zu einem bestimmten öffentlichen Schlüssel gehört.
A PKI verifies which person or system belongs to a specific public key.

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

Which type of malware is a program which, in addition to the function that it appears to perform, purposely conducts secondary activities?

A) Logikbombe (Logic Bomb)
Logic bomb
B) Spyware
Spyware
C) Trojaner
Trojan
D) Wurm
Worm

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

Which type of malware builds a network of contaminated computers by replicating itself?

A) Logikbombe (Logic Bomb)
Logic bomb
B) Spyware
Spyware
C) Trojaner
Trojan
D) Wurm
Worm

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

Which is a legislative or regulatory act related to information security that can be imposed upon all organizations?

A) Datenschutz-Grundverordnung (DSGVO)
General Data Protection Regulation (GDPR)
B) Geistige Eigentumsrechte
Intellectual property (IP) rights
C) ISO/IEC 27001
ISO/IEC 27001
D) ISO/IEC 27002
ISO/IEC 27002

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

Which ISO standard is focused on the implementation of information security controls?

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

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

---
*The standards of which organization is **most** commonly used in Europe?*

A) American National Standards Institute (ANSI)
American National Standards Institute (ANSI)
B) International Organization for Standardization (ISO)
International Organization for Standardization (ISO)
C) National Institute of Standards and Technology (NIST)
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 database contains a few million transactions of a phone company. An invoice for a customer has been generated and sent.

What does this invoice contain for the customer?

A) Daten
Data

B) Informationen
Information

C) Daten und Informationen
Data and information

A) Falsch. Die Datenbank enthält Daten. Wird eine Rechnung erstellt und an einen Empfänger geschickt, werden diese Daten für den Empfänger zu Informationen.
Incorrect. The database contains data. However, when an invoice is generated and sent to a recipient, it is information for the recipient.

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)
Correct. The value of information is determined by the recipient. The invoice contains valuable data for the recipient, and therefore it is information. (Literature: A, Chapter 4.8.5)

C) Falsch. Die Rechnung enthält für den Empfänger nur Informationen.
Incorrect. The invoice contains only information for the recipient.

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

What is the difference between data and information?

A) Bei Daten kann es sich um alle erdenklichen Fakten oder Zahlen handeln. Informationen sind Daten, die eine Bedeutung haben.
Data can be any facts or figures. Information is data that has meaning.

B) Daten bestehen aus unstrukturierten Zahlen. Informationen bestehen aus strukturierten Zahlen.
Data consists of unstructured figures. Information consists of structured figures.

C) Daten erfordern keine Sicherheit. Informationen erfordern Sicherheit.
Data does not require security. Information requires security.

D) Daten haben keinen Wert. Informationen dagegen sind verarbeitete Daten und haben einen Wert.
Data has no value. Information, which is processed data, has value.

A) Richtig. Informationen leiten sich von Daten ab, die in einem bestimmten Kontext eine Bedeutung erhalten. (Literatur: A, Kapitel 3.1)
Correct. Information is derived from data by giving it meaning in a certain context. (Literature: A, Chapter 3.1)

B) Falsch. Daten können sowohl strukturiert als auch unstrukturiert sein. Informationen sind in der Regel strukturiert.
Incorrect. Data can be either structured or unstructured. Information is usually structured.

C) Falsch. Sowohl Daten als auch Informationen erfordern Sicherheit.
Incorrect. Both data and information require security.

D) Falsch. Sowohl Daten als auch Informationen haben einen Wert.
Incorrect. Both data and information have value.

3 / 40
Was ist der Fokus des Informationsmanagements?

What is the focus of information management?

A) Die unterbrechungsfreie Fortführung von Business-Aktivitäten und -Prozessen zu ermöglichen
Allowing business activities and processes to continue without interruption

B) Die Identifizierung und Nutzung des Werts von Informationen sicherzustellen
Ensuring that the value of information is identified and exploited

C) Den Zugriff auf automatisierte Systeme durch Unbefugte zu verhindern
Preventing unauthorized persons from having access to automated systems

D) Die Informationsflüsse im Unternehmen zu verstehen
Understanding how information flows through an organization

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.
Incorrect. This is the focus of business continuity management (BCM). The purpose of BCM is to prevent business activities from being disrupted, to protect critical processes against the consequences of far-reaching disruptions in information systems, and to allow for speedy recovery.

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)
Correct. Information management describes how an organization efficiently plans, collects, organizes, uses, controls, disseminates, and disposes of its information, and through which it ensures that the value of that information is identified and exploited to the fullest extent. (Literature: A, Chapter 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.
Incorrect. This is the focus of access management. It ensures that unauthorized persons or processes do not have access to automated systems, databases, and programs.

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.
Incorrect. This is the focus of information analysis. It provides a clear picture of how an organization handles information, and how the information flows through the organization.

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?

An organization must understand the risks it is facing before it can take appropriate measures.

What should be understood to determine risk?

A) Die Eintrittswahrscheinlichkeit eines Ereignisses und die Auswirkungen des Ereignisses auf die Organisation
The likelihood of something happening and its consequences to the organization

B) Die häufigsten Risiken und wie diese gemäß den Festlegungen in Best Practices reduziert werden können
The most common dangers and how to mitigate these as defined in best practices

C) Die Bedrohungen, mit denen eine Organisation konfrontiert ist und wie anfällig die Organisation für diese Bedrohungen ist
The threats an organization faces and how vulnerable the organization is to them

D) Die ungeplanten Ereignisse, mit denen eine Organisation konfrontiert ist und was in einem solche Fall zu tun ist
The unplanned events an organization faces and what to do in case of such an event

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)
Correct. Two high-level factors determine risk: the likelihood of something happening and its impact on the business. (Literature: A, Chapter 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.
Incorrect. It is unwise to have this as a starting point when an organization defines their risks. Doing what other organizations do does not make this organization safe.

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.
Incorrect. This is a description of the term likelihood. Although it is important to understand likelihood, an important aspect is missing: how it will affect the business.

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.
Incorrect. Eventually, matching risks and controls are needed, but this is rather a response to risk than a way to understand risk in the first place.

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

Besides integrity and confidentiality, what is the third reliability aspect of information?

A) Genauigkeit
Accuracy
B) Verfügbarkeit
Availability
C) Vollständigkeit
Completeness
D) Monetärer Wert
Value

A) Falsch. Die drei Aspekte der Zuverlässigkeit von Informationen sind Verfügbarkeit, Integrität und Vertraulichkeit. Genauigkeit ist Teil der Integrität.
Incorrect. The three reliability aspects of information are availability, integrity, and confidentiality. Accuracy is a part of integrity.
B) Richtig. Die drei Aspekte der Zuverlässigkeit von Informationen sind Verfügbarkeit, Integrität und Vertraulichkeit. (Literatur: A, Kapitel 3.4.3)
Correct. The three reliability aspects of information are availability, integrity, and confidentiality. (Literature: A, Chapter 3.4.3)
C) Falsch. Die drei Aspekte der Zuverlässigkeit von Informationen sind Verfügbarkeit, Integrität und Vertraulichkeit. Vollständigkeit ist Teil der Integrität.
Incorrect. The three reliability aspects of information are availability, integrity, and confidentiality. Completeness is a part of integrity.
D) Falsch. Die drei Aspekte der Zuverlässigkeit von Informationen sind Verfügbarkeit, Integrität und Vertraulichkeit.
Incorrect. The three reliability aspects of information are availability, integrity, and confidentiality.

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?

An organization has a network printer in the hallway of the company. Many employees do not pick up their printouts immediately and leave them on the printer.

What is the consequence of this to the reliability of the information?

A) Die Verfügbarkeit der Informationen ist nicht mehr gewährleistet.
The availability of the information is no longer guaranteed.
B) Die Vertraulichkeit der Informationen ist nicht mehr gewährleistet.
The confidentiality of the information is no longer guaranteed.
C) Die Integrität der Informationen ist nicht mehr gewährleistet.
The integrity of the information is no longer guaranteed.

A) Falsch. Die Informationen sind in dem System, in dem sie erstellt und gedruckt wurden, nach wie vor verfügbar.
Incorrect. The information is still available in the system that was used to create and print it.
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)
Correct. The information can end up with, or be read by, persons who should not have access to this information. (Literature: A, Chapter 3.4.1)
C) Falsch. Die Informationen sind auf Papier gedruckt, sodass ihre Integrität nach wie vor gewährleistet ist.
Incorrect. The integrity of the information on the prints is still guaranteed since it is on paper.

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

What is the difference between accountability and auditability?

A) Verantwortlichkeit bedeutet, dass eine Organisation ihre Finanzkonten gut verwaltet. Auditierbarkeit bedeutet, dass eine Organisation ein Audit bestanden hat.
Accountability means an organization has their financial accounts well-administered. Auditability means an organization passed an audit.

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.
Accountability means being liable for the results of an organization's activities. Auditability refers to an organization's readiness for being independently reviewed.

C) Verantwortlichkeit bedeutet die Verantwortung für die Handlungen einer Person zu übernehmen. Auditierbarkeit bedeutet die Verantwortung für die Handlungen einer Organisation zu haben.
Accountability means having responsibility for an individual's actions. Auditability means having responsibility for an organization's actions.

D) Verantwortlichkeit bedeutet, dass eine Organisation den Sarbanes Oxley Act (SOX) einhält. Auditierbarkeit bedeutet, dass eine Organisation der Norm ISO/IEC 27001 entspricht.
Accountability means that an organization complies with Sarbanes-Oxley (SOX). Auditability refers to an organization complying with ISO/IEC 27001.

A) Falsch. Verantwortlichkeit hat nicht direkt etwas mit Finanzbuchhaltung und Auditierbarkeit hat nichts mit dem Bestehen eines Audits zu tun.
Incorrect. Accountability has no direct relationship with financial accounting. Auditability has no relationship with having passed an audit.

B) Richtig. So lauten die korrekten Definitionen von Verantwortlichkeit und Auditierbarkeit. (Literatur: A, Kapitel 3.4.4)
Correct. These are the correct definitions of accountability and auditability. (Literature: A, Chapter 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.
Incorrect. The definition of accountability is correct, but the definition of auditability is not. Auditability has nothing to do with responsibility for the organization's actions.

D) Falsch. Weder Verantwortlichkeit noch Auditierbarkeit beziehen sich auf die Einhaltung der Vorgaben (Compliance) von SOX oder ISO/IEC-Normen.
Incorrect. Neither accountability nor auditability refer to compliance with SOX or ISO/IEC standards.

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

---
*How is the purpose of an information security policy **best** described?*

A) Eine Informationssicherheitsrichtlinie dokumentiert die Analyse der Risiken und die Suche nach entsprechenden Sicherheitsmaßnahmen.
An information security policy documents the analysis of risks and the search for appropriate controls.

B) Eine Informationssicherheitsrichtlinie bietet der Organisation Orientierung und Unterstützung hinsichtlich der Informationssicherheit.
An information security policy gives direction and support to the organization regarding information security.

C) Eine Informationssicherheitsrichtlinie konkretisiert die Sicherheitsplanung mit den erforderlichen Details.
An information security policy makes the security plan concrete by providing it with the necessary details.

D) Eine Informationssicherheitsrichtlinie bieten Einblick in Bedrohungen und deren mögliche Folgen.
An information security policy provides insight into threats and the possible consequences.

A) Falsch. Die Analyse der Risiken und die Suche nach Sicherheitsmaßnahmen sind der Zweck der Risikoanalyse und des Risikomanagements.
Incorrect. The analysis of risks and the search for controls are the purpose of risk analysis and risk management.

B) Richtig. Die Geschäftsführung bietet durch ihre Sicherheitsrichtlinie Orientierung und Unterstützung hinsichtlich der Informationssicherheit. (Literatur: A, Kapitel 4.2.1)
Correct. With the security policy, management provides direction and support regarding information security. (Literature: A, Chapter 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.
Incorrect. The security plan makes the information security policy concrete. The plan includes which controls have been chosen, who is responsible for what, the guidelines for the implementation of controls, etc.

D) Falsch. Einblick in Bedrohungen und deren mögliche Folgen ist der Zweck der Bedrohungsanalyse.
Incorrect. The purpose of a threat analysis is to provide insight into threats and the possible consequences.

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

Was sollte Sara **zuerst** tun?

Sara has been tasked with ensuring that the organization complies with personal data protection legislation.

*What is the **first** thing she should do?*

A) Einen Mitarbeiter benennen, der die Manager bei der Einhaltung der Richtlinie unterstützt
Appoint a person responsible for supporting managers in adhering to the policy
B) Die Erhebung und Speicherung personenbezogener Daten verbieten
Issue a ban on collecting and storing personal information
C) Die Mitarbeitenden für die Übermittlung ihrer personenbezogenen Daten zuständig machen
Make employees responsible for submitting their personal data
D) Die Gesetzgebung zum Schutz personenbezogener Daten in einer Datenschutzrichtlinie umsetzen.
Translate the personal data protection legislation into a privacy policy

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.
Incorrect. A person to support managers is not a requirement to become compliant with personal data protection legislation. In addition, the policy should first align with the legislation.
B) Falsch. Dies ist nicht der beste Weg, um die Gesetzgebung zum Schutz personenbezogener Daten einzuhalten.
Incorrect. This is not the best way to comply with personal data protection legislation.
C) Falsch. So sorgt man nicht für die Einhaltung der Gesetzgebung zum Schutz personenbezogener Daten.
Incorrect. This is not a way to become compliant with personal data protection legislation.
D) Richtig. Der erste Schritt zur Einhaltung der Gesetzgebung ist die Erstellung einer internen Richtlinie für die Organisation. (Literatur: A, Kapitel 5.1)
Correct. The first step to becoming compliant is to create an internal policy for the organization. (Literature: A, Chapter 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?

An organization decides to outsource some of its IT.

*How can information security **best** be ensured when working with a supplier?*

A) Indem man in der Organisation des Lieferanten einen neuen Information Security Officer (ISO) ernennt
Appoint a new information security officer (ISO) in the supplier's organization
B) Indem man die Informationssicherheitsanforderungen an den Lieferanten förmlich in einem Vertrag festlegt
Formalize the information security requirements for the supplier in an agreement
C) Indem man die beiden Organisationen vollständig voneinander trennt, damit jede für ihre eigenen Daten verantwortlich ist
Keep both organizations fully separated to make everyone accountable for their data
D) Indem man vom Lieferanten verlangt, dass er die Prozesse und Verfahren der Kundenorganisation befolgt
Require the supplier to follow the customer organization's processes and procedures

A) Falsch. Verfügt die Organisation des Lieferanten bereits über einen ISO, so muss kein neuer ISO benannt werden.
Incorrect. It is not necessary to appoint a new ISO in the supplier's organization if the organization already has one.
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)
Correct. Although entering into an agreement is not a fail-safe mechanism to manage supplier risk, it is the most effective way of doing so. (Literature: A, Chapter 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.
Incorrect. The customer organization remains accountable for all information. Keeping the organizations fully separated often implies the customer organization does not know how to ensure or influence information security in the supplier's organization.
D) Falsch. Dies ist nicht die beste Lösung, denn Lieferanten sollten einen eigenen Informationssicherheitsprozess haben dürfen.
Incorrect. This is not the best way because a supplier should be allowed to have their own information security process in place.

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

Who is responsible for the translation of the business strategy and objectives to security strategy and objectives?

A) Chief Information Security Officer (CISO)
Chief information security officer (CISO)
B) Geschäftsführung
General management
C) Information Security Officer (ISO)
Information security officer (ISO)
D) Information Security Policy Officer
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)
Correct. The CISO is at the highest management level of the organization and develops the general security strategy for the entire business. (Literature: A, Chapter 5.2)
B) Falsch. Die Geschäftsführung legt die Unternehmensstrategie fest, auf deren Grundlage der CISO dann die allgemeine Sicherheitsstrategie festlegt.
Incorrect. General management defines the strategy that is input for the CISO to define the general security strategy.
C) Falsch. Der ISO erarbeitet ausgehend von der Unternehmensrichtlinie die Informationssicherheitsrichtlinie einer Geschäftseinheit und stellt sicher, dass diese eingehalten wird.
Incorrect. The ISO develops the information security policy of a business unit based on the company policy and ensures that it is observed.
D) Falsch. Der Information Security Policy Officer ist für die Pflege der von der Sicherheitsstrategie abgeleiteten Informationssicherheitsrichtlinie zuständig.
Incorrect. The information security policy officer is responsible for maintaining the policy that is derived from the security strategy.

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

---
*Which is the **best** example of a human threat?*

A) Ein Leck verursacht einen Stromausfall.
A leak causes a failure of the electricity supply.
B) Ein USB-Stick infiziert ein Netzwerk mit einem Virus.
A USB-stick passes on a virus to a network.
C) Der Server-Raum ist zu staubig.
There is too much dust in the server room.

A) Falsch. Ein Leck ist keine menschliche, sondern eine nicht-menschliche Bedrohung.
Incorrect. A leak is not a human threat, but a non-human threat.
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)
Correct. A USB-stick is always inserted by a person. If this causes a virus entering the network, it is a human threat. (Literature: A, Chapter 3.9.1)
C) Falsch. Staub ist keine menschliche, sondern eine nicht-menschliche Bedrohung.
Incorrect. Dust is not a human threat, but a non-human threat.

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 database system does not have the latest security patches applied to it and was hacked. The hackers were able to access the data and delete it.

What information security concept describes the lack of security patches?

A) Auswirkung
Impact
B) Risiko
Risk
C) Bedrohung
Threat
D) Schwachstelle
Vulnerability

A) Falsch. Der Begriff Auswirkung beschreibt die Folgen, die ein Ereignis für die Organisation oder die Informationen der Organisation hat.
Incorrect. Impact is the effect an event has on the organization or its information.
B) Falsch. Der Begriff Risiko beschreibt die Kombination aus der Eintrittswahrscheinlichkeit und den Auswirkungen eines Ereignisses.
Incorrect. A risk is the combination of the likelihood and impact of an event happening.
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.
Incorrect. An example of a threat is an external entity trying to exploit a vulnerability. In this case, the hackers form the threat.
D) Richtig. Mangelnder Schutz ist ein Beispiel für eine Schwachstelle. (Literatur: A, Kapitel 3.5.3)
Correct. An example of a vulnerability is a lack of protection. (Literature: A, Chapter 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?

There was a fire in a company. The fire department quickly arrived at the scene and could extinguish the fire before it spread and burned down the entire premises. The server, however, was destroyed in the fire. The backup tapes kept in another room had melted and many other documents were lost.

*What **indirect** damage is caused by this fire?*

A) Verbrannte Computer-Systeme
Burned computer systems
B) Verbrannte Dokumente
Burned documents
C) Geschmolzene Backup-Bänder
Melted backup tapes
D) Wasserschaden
Water damage

A) Falsch. Verbrannte Computer-Systeme sind ein direkter Schaden des Brands.
Incorrect. Burned computer systems are direct damage caused by the fire.
B) Falsch. Verbrannte Dokumente sind ein direkter Schaden des Brands.
Incorrect. Burned documents are direct damage caused by the fire.
C) Falsch. Geschmolzene Backup-Bänder sind ein direkter Schaden des Brands.
Incorrect. Melted backup tapes are direct damage caused by the fire.
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)
Correct. Water damage due to the fire extinguishers is indirect damage caused by the fire. This is a side effect of putting out the fire, which is aimed at minimizing the damage caused by the fire. (Literature: A, Chapter 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**?

Companies can have different risk strategies depending on the type of business.

*Which risk strategy is **most** suitable for a hospital?*

A) Risikoakzeptanz
Risk accepting
B) Risikovermeidung
Risk avoiding
C) Risikotragfähigkeit
Risk bearing
D) Risikoneutralität
Risk neutral

A) Falsch. Ein Krankenhaus kann Risiken in Form von finanziellen Verlusten oder sterbenden Patienten nicht einfach akzeptieren.
Incorrect. A hospital cannot easily accept risks due to financial losses or dying patients.
B) Richtig. Krankenhäuser sollten versuchen, Risiken zu vermeiden. (Literatur: A, Kapitel 3.11)
Correct. Hospitals should try to avoid any risk. (Literature: A, Chapter 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.
Incorrect. Risk bearing means that certain risks are accepted. This could be because the costs of controls exceed the possible damage. In a hospital, this is not the best way to handle risks.
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.
Incorrect. Risk neutral means that security measures are taken such that the threats either no longer manifest themselves or, if they do, the resulting damage is minimized. Damage to clients is never a good idea, so hospitals should be risk avoiding.

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

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

A well-executed risk analysis provides a great deal of useful information. A risk analysis has different main objectives.

*What is **not** a main objective of a risk analysis?*

A) Die Kosten eines Incidents und die Kosten einer Sicherheitsmaßnahme gegeneinander abzuwägen
Balance the costs of an incident and the costs of a control
B) Die relevanten Schwachstellen und Bedrohungen zu bestimmen
Determine relevant vulnerabilities and threats
C) Die Werte (Assets) und deren wirtschaftlichen Wert zu identifizieren
Identify assets and their value
D) Die Maßnahmen (Measures) und Sicherheitsmaßnahmen zu implementieren
Implement measures and controls

A) Falsch. Das ist durchaus eines der Hauptziele der Risikoanalyse.
Incorrect. This is one of the main objectives of a risk analysis.
B) Falsch. Das ist durchaus eines der Hauptziele der Risikoanalyse.
Incorrect. This is one of the main objectives of a risk analysis.
C) Falsch. Das ist durchaus eines der Hauptziele der Risikoanalyse.
Incorrect. This is one of the main objectives of a risk analysis.
D) Richtig. Das ist kein Ziel der Risikoanalyse. (Literatur: A, Kapitel 3.7)
Correct. This is not an objective of a risk analysis. (Literature: A, Chapter 3.7)

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

What is a repressive control in case of a fire?

A) Den Brand zu löschen, nachdem er entdeckt wurde
Putting out a fire after it has been detected
B) Den durch den Brand verursachten Schaden zu reparieren
Repairing damage caused by the fire
C) Eine Brandversicherung abzuschließen
Taking out a fire insurance

A) Richtig. Dies ist eine unterdrückende Sicherheitsmaßnahme. Sie begrenzt den durch den Brand verursachten Schaden auf ein Minimum. (Literatur: A, Kapitel 3.8)
Correct. This repressive control minimizes the damage caused by a fire. (Literature: A, Chapter 3.8)
B) Falsch. Dies ist keine unterdrückende Sicherheitsmaßnahme. Sie begrenzt den durch den Brand verursachten Schaden nicht auf ein Minimum.
Incorrect. This is not a repressive control. It does not minimize the damage caused by the fire.
C) Falsch. Der Abschluss einer Versicherung bietet Schutz vor den finanziellen Auswirkungen eines Brands und dient als Risikoversicherung.
Incorrect. Taking out an insurance protects against the financial consequences of a fire and is risk insurance.

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

What is the goal of classification of information?

A) Die Kennzeichnung von Informationen, um ihre Erkennbarkeit zu verbessern
Applying labels to make the information easier to recognize
B) Die Erstellung eines Handbuchs zum Umgang mit Mobilgeräten
Creating a manual on how to handle mobile devices
C) Die Gliederung der Informationen nach dem Grad ihrer Vertraulichkeit
Structuring information according to its sensitivity

A) Falsch. Die Kennzeichnung von Informationen ist eine besondere Form der Kategorisierung von Informationen, die nach deren Klassifizierung erfolgt.
Incorrect. Applying labels to information is designation, which is a special form of categorizing information that follows on the classification of information.
B) Falsch. Die Erstellung eines Handbuchs bezieht sich auf die Benutzerrichtlinien. Hierbei handelt es sich nicht um die Klassifizierung von Informationen.
Incorrect. Creating a manual relates to user guidelines and is not classification of information.
C) Richtig. Bei der Klassifizierung von Informationen werden verschiedene Vertraulichkeitsstufen festgelegt, sodass die Informationen dann entsprechend eingeteilt werden können. (Literatur: A, Kapitel 5.12)
Correct. Classification of information is used to define the different levels of sensitivity into which information can be structured. (Literature: A, Chapter 5.12)

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

---
*What is the **most** important reason to apply segregation of duties?*

A) Sicherzustellen, dass Mitarbeiter nicht zur gleichen Zeit das Gleiche machen
Ensuring that employees do not do the same work at the same time

B) Alle Mitarbeiter gemeinsam für die gemachten Fehler zuständig zu machen
Holding all employees jointly responsible for the mistakes they make

C) Klarzustellen, wer für welche Aufgaben und Tätigkeiten zuständig ist
Making clear who is responsible for what tasks and activities

D) Die Wahrscheinlichkeit unbefugter oder unbeabsichtigter Änderungen auf ein Minimum zu beschränken
Minimizing the chance of unauthorized or unintended changes

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.
Incorrect. Segregation of duties is used to avoid the chance of unauthorized or unintended changes, or the misuse of the organization's assets. It does not define when activities should be performed.

B) Falsch. Die Trennung der Verantwortlichkeit trennt Aufgaben und Zuständigkeiten. Sie sorgt nicht für die gemeinsame Verantwortung einer Gruppe von Menschen.
Incorrect. Segregation of duties separates tasks and responsibilities. It does not make a group of people jointly responsible.

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.
Incorrect. The segregation of duties is used to avoid the chance of unauthorized or unintended changes, or the misuse of the organization's assets. Its objective is not to make clear who is responsible for what.

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)
Correct. Duties must be segregated to avoid the chance of unauthorized or unintended changes, or the misuse of the organization's assets. (Literature: A, Chapter 5.3)

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

---
*What is the **best** way to ensure appropriate access to information?*

A) Durch die Automatisierung von Arbeitsabläufen
Automate workflows
B) Durch die Festlegung von Verfahrensanweisungen
Define operating procedures
C) Durch die Entwicklung von Arbeitsanweisungen für alle Aufgaben
Develop work instructions for all tasks
D) Durch die Bereitstellung von Schulungen
Provide training

A) Falsch. Die Automatisierung von Arbeitsabläufen trägt zwar sicherlich zur Informationssicherheit bei, sorgt aber nicht für einen entsprechenden Zugriff auf Informationen.
Incorrect. Automating workflows will certainly contribute to information security, but it does not help appropriate access.
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)
Correct. The use of procedures to guide how work is done in an appropriate, safe, and responsible manner is an effective way to achieve effective information security. (Literature: A, Chapter 5.36.1)
C) Falsch. Dies geht zu sehr ins Detail und ist zu präskriptiv. Daher ist dies nicht die beste Lösung.
Incorrect. This is too detailed and prescriptive, and therefore not the best way.
D) Falsch. Schulungen sind zwar wichtig, sorgen aber nicht für einen entsprechenden Zugriff auf Informationen.
Incorrect. Training is important but it does not ensure appropriate access to information.

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 fire breaks out in an office of an organization. The employees are transferred to neighboring offices of the organization to continue their work.

Where in the incident cycle is moving to a stand-by arrangement found?

A) Zwischen Schaden und Wiederherstellung
Between the damage and recovery stages
B) Zwischen Incident und Schaden
Between the incident and damage stages
C) Zwischen Wiederherstellung und Bedrohung
Between the recovery and threat stages
D) Zwischen Bedrohung und Incident
Between the threat and incident stages

A) Falsch. Schaden und Wiederherstellung werden durch die Stand-by-Regelung begrenzt.
Incorrect. Damage and recovery are limited by the stand-by arrangement.
B) Richtig. Die Stand-by-Regelung ist eine unterdrückende Maßnahme (Measure), um den Schaden zu begrenzen. (Literatur: A., Kapitel 3.8.4)
Correct. A stand-by arrangement is a repressive measure that is initiated to limit the damage. (Literature: A, Chapter 3.8.4)
C) Falsch. Die Wiederherstellung erfolgt erst nachdem die Stand-by-Regelung in die Tat umgesetzt wurde.
Incorrect. The recovery stage takes place after putting a stand-by arrangement into operation.
D) Falsch. Eine Stand-by-Regelung zu realisieren, ohne dass ein Incident vorliegt, wäre sehr kostspielig.
Incorrect. Carrying out a stand-by arrangement without an incident is very expensive.

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?

An employee discovers that the expiration date of a policy has been changed without her knowledge. She is the only person authorized to do this and reports this security incident to the helpdesk.
The helpdesk worker records the following information regarding this incident:
- date and time
- description of the incident
- possible consequences of the incident

What important information about the incident is missing here?

A) Der Name der Person, die den Incident gemeldet hat
The name of the person reporting the incident
B) Der Name des Software-Pakets
The name of the software package
C) Die PC-Nummer
The PC number

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)
Correct. When reporting an incident, the name of the reporter must be recorded at a minimum. (Literature: A, Chapter 5.25)
B) Falsch. Hierbei handelt es sich um zusätzliche Informationen, die später ergänzt werden können.
Incorrect. This is additional information that may be added later.
C) Falsch. Hierbei handelt es sich um zusätzliche Informationen, die später ergänzt werden können.
Incorrect. This is additional information that may be added later.

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

Why is it important to regularly audit the organization's information security management system (ISMS)?

A) Viele Kundenverträge fordern Audits zur Gewährleistung der Informationssicherheit.
Audits are a common requirement in customer contracts to ensure information security.

B) Audits sind für die Einhaltung der gesetzlichen und regulatorischen Vorgaben (Compliance) obligatorisch.
Audits are a required element in order to comply with legal or regulatory requirements.

C) Audits zeigen, ob eine Organisation Probleme hat, ihre finanziellen Ziele zu erreichen.
Audits uncover issues with the ability to meet an organization's financial targets.

D) Audits decken Schwächen bei der Implementierung von Informationssicherheitsmaßnahmen auf.
Audits uncover weaknesses in the implementation of information security controls.

A) Falsch. Kundenverträge enthalten nur selten Forderungen nach Audits.
Incorrect. Customer contracts rarely contain audit requirements.

B) Falsch. Gesetzliche oder regulatorische Vorgaben fordern in der Regel keine Durchführung von Audits.
Incorrect. Legal or regulatory requirements usually do not require audits to be done.

C) Falsch. Audits dienen in der Regel nicht zur Verifizierung der Finanzleistung.
Incorrect. Audits are not commonly used to verify financial performance.

D) Richtig. Audits verfolgen den Zweck, Schwächen in den implementierten Sicherheitsmaßnahmen aufzudecken. (Literatur: A, Kapitel 5.35)
Correct. The purpose of audits is to find weaknesses in implemented controls. (Literature: A, Chapter 5.35)

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

Which document would include a rule that forbids the use of company e-mail for private purposes?

A) Führungszeugnis
Certificate of good character
B) Verhaltenskodex
Code of conduct
C) Datenschutz-Grundverordnung (DSGVO)
General Data Protection Regulation (GDPR)
D) Vertraulichkeitsvereinbarung (NDA)
Non-disclosure agreement (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.
Incorrect. A certificate of good character is issued by an organization such as the Department of Justice and indicates that no criminal offences were committed by the individual.
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)
Correct. The code of conduct is a document (often part of the employee manual) that describes the company policies that are applicable to personnel. (Literature: A, Chapter 6.2)
C) Falsch. Bei der DSGVO geht es um den Schutz personenbezogener Informationen.
Incorrect. The GDPR is about the protection of personal information.
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.
Incorrect. An NDA is a contract that forbids the disclosure of certain information. The use of company e-mail for private purposes is not controlled by such a document.

25 / 40
Ein Mitarbeiter entdeckt einen Incident.

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

---
*When an employee detects an incident, to whom should it typically be reported **first**?*

A) An den Helpdesk
The helpdesk
B) An den Information Security Manager (ISM)
The information security manager (ISM)
C) An den Information Security Officer (ISO)
The information security officer (ISO)
D) An den Vorgesetzten
The manager

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)
Correct. Typically, incidents should be reported to the helpdesk for evaluation, application of initial procedures and escalation if required. They should not be escalated vertically immediately. (Literature: A, Chapter 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.
Incorrect. Incidents should not be escalated vertically immediately. Also, not every incident is a security incident, so the incident should be assessed by the help desk first to determine if there is a security incident.
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.
Incorrect. Incidents should not be escalated vertically immediately. Also, not every incident is a security incident, so the incident should be assessed by the help desk first to determine if there is a security incident.
D) Falsch. Incidents sollten nicht sofort vertikal eskaliert werden.
Incorrect. Incidents should not be escalated vertically immediately.

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

---
*What is the **most** effective way to create information security awareness among employees?*

A) Durch gezielte Schulungen zur Bewusstseinsbildung für die Geschäftsführung
Focus awareness training on the management team

B) Durch Teilnahme aller Mitarbeitenden an externen Schulungen zum Thema Informationssicherheit
Send all employees to an external information security training

C) Durch Einrichtung eines speziell auf die Organisation ausgerichteten Programms zur Bewusstseinsbildung
Set up an organization-specific awareness program

D) Durch das Angebot einer allgemeinen Online-Schulung zum Thema Informationssicherheit
Use a generic, online information security training course

A) Falsch. Bewusstsein für Informationssicherheit ist für alle Mitarbeitenden wichtig, nicht nur für die Geschäftsführung.
Incorrect. All employees need awareness of information security, not only managers.

B) Falsch. Externe Schulungen erfüllen möglicherweise die Bedürfnisse einer bestimmten Organisation nicht vollumfänglich.
Incorrect. External training may not be fully applicable to a specific organization's needs.

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)
Correct. Adapting a security awareness program to the specific organizational needs is most effective. (Literature: A, Chapter 6.3)

D) Falsch. Allgemeine Schulungen zum Thema Informationssicherheit erfüllen die Bedürfnisse einer bestimmten Organisation möglicherweise nicht vollumfänglich.
Incorrect. Generic information security training may not be fully applicable to a specific organization's needs.

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

What physical control manages access to an organization's information?

A) Installation einer Klimaanlage
Installing air conditioning
B) Verbot der Nutzung von USB-Sticks
Prohibiting the use of USB sticks
C) Erfordernis von Benutzernamen und Password
Requiring username and password
D) Verwendung von Sicherheitsglas
Using unbreakable glass

A) Falsch. Klimaanlagen haben nichts mit der Regelung des Zugriffs auf die Informationen einer Organisation zu tun.
Incorrect. Air conditioning does not manage access to an organization's information.
B) Falsch. Dies ist eine organisatorische Sicherheitsmaßnahme.
Incorrect. This is an organizational control.
C) Falsch. Dies ist eine technische Sicherheitsmaßnahme.
Incorrect. This is a technical control.
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)
Correct. The use of unbreakable glass is an example of a physical control to prevent unauthorized persons from entering the building. (Literature: A, Chapter 7.4)

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

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

A data center uses battery packs but has no power generator.

What is the risk associated with this setup for the availability of the data center?

A) Bei einer Wiederherstellung der Stromversorgung schaltet sich die Hauptstromversorgung möglicherweise nicht automatisch wieder ein, da dazu ein Generator benötigt wird.
The main power may not come up again automatically when restored, because this needs a power generator.

B) Der Ausfall der Hauptstromversorgung kann länger als nur ein paar Minuten oder Stunden dauern und in diesem Fall wäre kein Strom verfügbar.
The main power outage may last for longer than a few minutes or hours, which will cause unavailability of power.

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.
The battery packs' lifespan is limited, so they may run out of diesel and stop functioning after a couple of days.

D) Die Akkus müssen nach ein paar Stunden vom Stromgenerator mit Strom versorgt werden und bieten daher nur eingeschränkt Schutz.
The battery packs must be powered by the power generator after a few hours, so they only provide limited protection.

A) Falsch. Ein Stromgenerator dient nicht dazu, die Hauptstromversorgung einzuschalten.
Incorrect. A power generator is not used to trigger the main power supply.

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)
Correct. Battery packs only protect against temporary power outages and surges, whereas a power generator protects for longer-duration outages. (Literature: A, Chapter 7.11.1)

C) Falsch. Diesel dient als Treibstoff für den Generator. Akkus werden mit Hilfe von Batterien betrieben.
Incorrect. Diesel is used to power the generator; a battery pack is powered by batteries.

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.
Incorrect. The battery packs will only work for a short period but are not powered by the generator. The generator simply takes over from the battery pack.

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

Why is air conditioning placed in the server room?

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.
Backup tapes are made from thin plastic that cannot withstand high temperatures. Therefore, if it gets too hot in the server room, they may get damaged.

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.
Employees that work in the server room should not work in the heat. The heat increases the chance that they make errors.

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.
In the server room the air must be cooled, and the heat produced by the equipment must be extracted. It also dehumidifies and filters the air in the room.

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.
The server room is the best way to cool the air in the office. No office space must be sacrificed for such a large piece of equipment.

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.
Incorrect. Backup tapes should not be stored in the server room. A fire would then destroy both the information in use and the backup.

B) Falsch. Dies ist nicht der Grund, warum im Server-Raum eine Klimaanlage installiert werden sollte.
Incorrect. This is not the reason why air conditioning should be installed in the server room.

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)
Correct. Server rooms must be approached separately when considering physical security. Server rooms contain sensitive equipment that is vulnerable to humidity and warmth and produce heat themselves. (Literature: A, Chapter 7.11.2)

D) Falsch. Im Server-Raum wird nicht die Raumluft für die gesamte Niederlassung gekühlt.
Incorrect. The server room is not the place to cool the air in the entire office.

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?

In physical security, multiple protection rings can be applied in which different measures can be taken.

*What is **not** a protection ring?*

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

A) Falsch. Das Gebäude ist ein Sicherheitsring mit Zugang zum Betriebsgelände.
Incorrect. The building is a ring that deals with access to the premises.
B) Richtig. Man unterscheidet zwischen den folgenden vier Sicherheitsringen: Outer Ring, Building, Workspaces, und Secure Room. (Literatur: A, Kapitel 7.0.1)
Correct. There are four protection rings: outer ring, building, workspaces, and secure room. (Literature: A, Chapter 7.0.1)
C) Falsch. Der Secure Room Ring ist ein gültiger Bereich, in dem sich der zu schützende Wert (Asset) befindet.
Incorrect. The secure room ring is a valid zone and deals with the asset that is to be protected.
D) Falsch. Der Outer Ring ist ein gültiger Bereich und bezeichnet das Gebiet rund um das Betriebsgelände.
Incorrect. The outer ring is a valid zone and deals with the area around the premises.

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?

The control to secure an asset depends on the asset.

*What is the **most** appropriate way to secure the asset?*

A) Indem man ein Formular sichert durch ausfüllen und abzeichnen
Secure a form by having it filled out and signed off
B) Indem man einen Laptop sichert und diesen einem einzigen Benutzer zuweist
Secure a laptop by assigning it to a single user
C) Indem man einen USB-Stick mittels Verschlüsselung sichert
Secure a USB-stick with encryption
D) Indem man eine Internetverbindung mittels Backup sichert
Secure an internet connection with a backup

A) Falsch. Ein Stück Papier mit Informationen abzulegen ist keine angemessene Sicherheitsmaßnahme.
Incorrect. Filing a piece of paper with information is not an appropriate control.
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.
Incorrect. It is obviously better if a single person uses a single laptop, but this is not the most appropriate option. User account management and password control are better controls.
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)
Correct. Encryption is a valid control for securing a USB-stick. Many organizations apply this control regardless of the classification of the information stored on the USB-stick. (Literature: A, Chapter 8.12)
D) Falsch. Ein Backup zu nutzen ist nicht die beste direkte Lösung, um eine Internetverbindung zu sichern.
Incorrect. Using a backup is not the best, direct way to secure the internet connection.

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

What information security control helps to develop systems with information security in mind?

A) Die Redundanz der Server sicherzustellen
Ensuring redundancy of the servers

B) Physische Zugangskontrollen zu implementieren
Implementing physical entry controls

C) Background Checks bei Mitarbeitenden durchzuführen
Performing background checks on employees

D) Datenklassifizierung bei Informationswerten (Informationsassets) zu nutzen
Using data classification on information assets

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)
Correct. Server redundancy is a control that should be considered during system development. (Literature: A, Chapter 8.14)

B) Falsch. Dies ist zwar eine valide Sicherheitsmaßnahme zur Verbesserung der Informationssicherheit, hat aber nichts mit der Systementwicklung zu tun.
Incorrect. This is a valid control to enhance information security but is not related to system development.

C) Falsch. Dies ist zwar eine valide Sicherheitsmaßnahme zur Verbesserung der Informationssicherheit, hat aber nichts mit der Systementwicklung zu tun.
Incorrect. This is a valid control to enhance information security but is not related to system development.

D) Falsch. Dies ist zwar eine valide Sicherheitsmaßnahme zur Verbesserung der Informationssicherheit, hat aber nichts mit der Systementwicklung zu tun.
Incorrect. This is a valid control to enhance information security but is not related to system development.

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?

An organization changes its policy. Employees are now allowed to work remotely.

What control should now be put in place?

A) Erstellen von V-Lans zur Segmentierung des Unternehmensnetzwerks
Create V-LANs to segment the corporate network

B) Verschlüsselung der Informationen im Unternehmensnetzwerk
Encrypt the information on the corporate network

C) Einrichtung von Firewalls im Unternehmensnetzwerk
Install firewalls on the corporate network

D) Verbindung mit dem Unternehmensnetzwerk über virtuelles privates Netzwerk (VPN)
Use a VPN to connect to the corporate network

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.
Incorrect. Segmenting networks to ensure confidentiality and segregation of duties should already be in place. These do not specifically apply to changing the remote-working policy.

B) Falsch. Zwar ist Verschlüsselung zum Schutz von Informationen unabdingbar, sie gilt aber nicht speziell dafür, Mitarbeitenden Remote- oder Telearbeit zu ermöglichen.
Incorrect. Encryption is a vital tool to use to protect information, but it does not specifically apply to allowing employees to work remotely.

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.
Incorrect. Firewalls between the corporate network and the outside world are important but these should already be in place. Also, firewalls do not directly secure remote connections.

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)
Correct. The use of VPNs is a control that should be put in place when employees are allowed to work remotely. (Literature: A, Chapter 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?

The employees of an organization work on laptops that are protected by asymmetrical cryptography. To keep the management of the keys cheap, all consultants use the same key pair. If certain information is compromised, new keys should be supplied.

In what case should new keys be supplied?

A) Wenn der private Schlüssel bekannt wird
When the private key becomes known
B) Wenn der öffentliche Schlüssel bekannt wird
When the public key becomes known
C) Wenn die Infrastruktur mit öffentlichem Schlüssel (PKI) bekannt wird
When the public key infrastructure (PKI) becomes known

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)
Correct. In asymmetric encryption, it is important to keep the private key private. The public key may be known. (Literature: A, Chapter 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.
Incorrect. The public key may be open to the whole world. The private key should be kept secret to ensure integrity and availability.
C) Falsch. Die PKI wird genutzt, um die Schlüssel für asymmetrische Verschlüsselungssysteme auszutauschen.
Incorrect. PKI is used for the exchange of keys for asymmetrical encryption systems.

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

What sort of security does a public key infrastructure (PKI) offer?

A) Eine PKI stellt regelmäßige Backups der Unternehmensdaten sicher.
A PKI ensures that backups of company data are made on a regular basis.

B) Eine PKI weist gegenüber den Kunden nach, dass ein webbasiertes Geschäft sicher ist.
A PKI shows customers that a web-based business is secure.

C) Eine PKI verifiziert, ob eine Person oder ein System zu einem bestimmten öffentlichen Schlüssel gehört.
A PKI verifies which person or system belongs to a specific public key.

A) Falsch. Eine PKI stellt nicht sicher, dass Backups erstellt werden.
Incorrect. A PKI does not ensure making backups.

B) Falsch. Eine PKI garantiert, dass eine bestimmte Person oder ein bestimmtes System zu einem öffentlichen Schlüssel gehören.
Incorrect. A PKI provides guarantees regarding which person or system belongs to a specific public key.

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)
Correct. A characteristic of a PKI is that through agreements, procedures, and an organization structure, it provides guarantees regarding which person or system belongs to a specific public key. (Literature: A, Chapter 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?

Which type of malware is a program which, in addition to the function that it appears to perform, purposely conducts secondary activities?

A) Logikbombe (Logic Bomb)
Logic bomb
B) Spyware
Spyware
C) Trojaner
Trojan
D) Wurm
Worm

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.
Incorrect. A logic bomb is a piece of code that is built into a software system. This code will then carry out a function when specific conditions are met. This is not always used for malicious purposes. It does not always conduct secondary activities.

B) Falsch. Spyware ist ein Computer-Programm, das Informationen über den Benutzer des Computers sammelt und diese an eine andere Partei schickt.
Incorrect. Spyware is a computer program that collects information on the user's computer and sends this information to another party.

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)
Correct. A trojan is a program which, in addition to the function that it appears to perform, purposely conducts secondary activities, unnoticed by the computer user, which can harm the integrity of the infected system. (Literature: A, Chapter 8.7.2)

D) Falsch. Ein Wurm erstellt ein Netzwerk aus infizierten Computern, indem sie sich selbst repliziert.
Incorrect. A worm builds a network of contaminated computers by replicating itself.

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

Which type of malware builds a network of contaminated computers by replicating itself?

A) Logikbombe (Logic Bomb)
Logic bomb
B) Spyware
Spyware
C) Trojaner
Trojan
D) Wurm
Worm

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.
Incorrect. A logic bomb is a piece of code that is built into a software system. This code will then carry out a function when specific conditions are met. This is not always used for malicious purposes.
B) Falsch. Spyware ist ein Computer-Programm, das Informationen über den Benutzer des Computers sammelt und diese an eine andere Partei schickt.
Incorrect. Spyware is a computer program that collects information on the computer user and sends this information to another party.
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.
Incorrect. A trojan is a program which, in addition to the function that it appears to perform, purposely conducts secondary activities, unnoticed by the computer user, which can harm the integrity of the infected system.
D) Richtig. Genau das macht ein Wurm. (Literatur: A, Kapitel 8.7)
Correct. This is what a worm does. (Literature: A, Chapter 8.7)

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

Which is a legislative or regulatory act related to information security that can be imposed upon all organizations?

A) Datenschutz-Grundverordnung (DSGVO)
General Data Protection Regulation (GDPR)
B) Geistige Eigentumsrechte
Intellectual property (IP) rights
C) ISO/IEC 27001
ISO/IEC 27001
D) ISO/IEC 27002
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)
Correct. All organizations should have a policy and procedures for personal data protection, which should be known by everybody who processes personal data. (Literature: A, Chapter 5.33)
B) Falsch. Diese Vorschrift hat nichts mit der Informationssicherheit von Organisationen zu tun.
Incorrect. This regulation is not related to information security for organizations.
C) Falsch. Hierbei handelt es sich um eine Norm, die Organisationen einen Leitfaden für die Einführung von Informationssicherheitsprozessen an die Hand gibt.
Incorrect. This is a standard with guidelines for organizations on how to deal with the set-up of an information security process.
D) Falsch. Diese Norm mit dem Titel ‚Informationssicherheit, Cybersicherheit und Datenschutz – Informationssicherheitsmaßnahmen' enthält Leitlinien zur Informationssicherheitsrichtlinie und zu Sicherheitsmaßnahmen.
Incorrect. This standard, also known as 'Information security, cybersecurity and privacy protection - Information security controls', contains guidelines for information security policy and controls.

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

Which ISO standard is focused on the implementation of information security controls?

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

A) Falsch. Dies ist die Norm zur allgemeinen Einführung der Normenreihe ISO/IEC 27000.
Incorrect. This is the general introduction to the ISO/IEC 27000 series of standards.
B) Falsch. Diese Norm enthält die Anforderungen an ein Informationssicherheitsmanagementsystem (ISMS).
Incorrect. This is the standard with requirements for an information security management system (ISMS).
C) Richtig. Diese Norm spezifiziert die Informationssicherheitsmaßnahmen und bietet Orientierung bezüglich deren Implementierung. (Literatur: A, Kapitel 4.12)
Correct. This is the standard specifying information security controls with guidance on their implementation. (Literature A, Chapter 4.12)
D) Falsch. Die Norm ISO/IEC 27005 befasst sich hauptsächlich mit dem Risikomanagement im Bereich der Informationssicherheit.
Incorrect. ISO/IEC 27005 focuses on information security risk management.

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

---
*The standards of which organization is **most** commonly used in Europe?*

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

A) Falsch. ANSI-Normen werden eher in den Vereinigten Staaten von Amerika genutzt.
Incorrect. The ANSI standards are more common in the United States of America.
B) Richtig. ISO-Normen werden in Europa am häufigsten genutzt. (Literatur: A, Kapitel 5.36)
Correct. In Europe, the ISO standards are the most common. (Literature: A, Chapter 5.36)
C) Falsch. NIST-Normen werden eher in den Vereinigten Staaten von Amerika genutzt.
Incorrect. The NIST standard is more common in the United States of America.

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