# EXIN Information Security Management ISO/IEC 27001 FOUNDATION

Certified by EXIN

## Voorbeeldexamen

Editie 202404

# Inhoud

# Inleiding

Dit is het EXIN Information Security Foundation based on ISO/IEC 27001 (ISFS.NL) voorbeeldexamen. Op dit examen is het Reglement voor de Examens van EXIN van toepassing.

Dit examen bestaat uit 40 meerkeuzevragen. Elke vraag heeft een aantal antwoorden, waarvan er één correct is.

Het maximaal aantal te behalen punten is 40. Elke goed beantwoorde vraag levert u 1 punt op. U hebt minimaal 26 punten nodig om te slagen.

De beschikbare tijd is 60 minuten.

Veel succes!

# Voorbeeldexamen

**1 / 40**
Een database bevat enkele miljoenen transacties van een telefoonmaatschappij. Er wordt een factuur voor een klant gegenereerd en verzonden.

Wat bevat deze factuur voor de klant?

**A)** Data
**B)** Informatie
**C)** Data en informatie

**2 / 40**
Wat is het verschil tussen data en informatie?

**A)** Data kan allerlei feiten of cijfers zijn. Informatie is data met betekenis.
**B)** Data bestaat uit ongestructureerde cijfers. Informatie bestaat uit gestructureerde cijfers.
**C)** Data hoeft niet te worden beveiligd. Informatie moet wel worden beveiligd.
**D)** Data heeft geen waarde. Informatie is verwerkte data en heeft wel waarde.

**3 / 40**
Wat is de focus van informatiemanagement?

**A)** Zorgen dat bedrijfsactiviteiten en -processen zonder onderbrekingen blijven doorgaan
**B)** Zorgen dat de waarde van informatie wordt vastgesteld en benut
**C)** Voorkomen dat onbevoegde personen toegang krijgen tot geautomatiseerde systemen
**D)** Begrijpen hoe informatie door een organisatie stroomt

**4 / 40**
Organisaties moeten weten met welke risico's ze te maken hebben voordat ze passende maatregelen kunnen nemen.

Wat moet een organisatie weten om risico's te kunnen bepalen?

**A)** Wat de waarschijnlijkheid is dat iets gebeurt en wat de gevolgen daarvan zijn voor de organisatie
**B)** Wat de meest voorkomende gevaren zijn en hoe deze kunnen worden ondervangen, zoals beschreven in best practices
**C)** Met welke dreigingen de organisatie te maken heeft en hoe kwetsbaar de organisatie hiervoor is
**D)** Met welke ongeplande gebeurtenissen de organisatie te maken heeft en wat moet worden gedaan wanneer zo'n gebeurtenis zich voordoet

**5 / 40**
Wat is, naast integriteit en vertrouwelijkheid, het derde betrouwbaarheidsaspect van informatie?

**A)** Nauwkeurigheid
**B)** Beschikbaarheid
**C)** Volledigheid
**D)** Waarde

**6 / 40**
In de hal van een organisatie staat een netwerkprinter. Veel medewerkers halen hun afdrukken niet direct op en laten ze op de printer liggen.

Wat is het gevolg voor de betrouwbaarheid van de informatie?

**A)** De beschikbaarheid van de informatie kan niet langer worden gegarandeerd.
**B)** De vertrouwelijkheid van de informatie kan niet langer worden gegarandeerd.
**C)** De integriteit van de informatie kan niet langer worden gegarandeerd.

**7 / 40**
Wat is het verschil tussen eindverantwoordelijkheid en controleerbaarheid?

**A)** Eindverantwoordelijkheid betekent dat een organisatie de financiële boekhouding goed op orde heeft. Controleerbaarheid betekent dat een organisatie een audit met succes heeft doorlopen.
**B)** Eindverantwoordelijkheid is aansprakelijkheid voor de resultaten van activiteiten van een organisatie. Controleerbaarheid verwijst naar de gereedheid van een organisatie om onafhankelijk te worden gecontroleerd.
**C)** Eindverantwoordelijkheid is het dragen van verantwoordelijkheid voor de acties van een persoon. Controleerbaarheid is het dragen van verantwoordelijkheid voor de acties van een organisatie.
**D)** Eindverantwoordelijkheid betekent dat een organisatie voldoet aan Sarbanes-Oxley (SOX). Controleerbaarheid betekent dat een organisatie voldoet aan ISO/IEC 27001.

**8 / 40**
Hoe kan het doel van een informatiebeveiligingsbeleid het **beste** worden beschreven?

**A)** Een informatiebeveiligingsbeleid is waar de analyse van risico's en de zoektocht naar toepasselijke beheersmaatregelen zijn gedocumenteerd.
**B)** Een informatiebeveiligingsbeleid biedt de organisatie richting en ondersteuning ten behoeve van de informatiebeveiliging.
**C)** Een informatiebeveiligingsbeleid maakt het beveiligingsplan concreet door er de benodigde details aan toe te voegen.
**D)** Een informatiebeveiligingsbeleid biedt inzicht in dreigingen en mogelijke gevolgen daarvan.

**9 / 40**
Sara heeft opdracht gekregen de naleving (compliance) van alle wetgeving inzake de bescherming van persoonsgegevens binnen haar organisatie te waarborgen.

Wat moet zij als **eerste** doen?

**A)** Iemand aanstellen om managers te helpen bij de naleving van het beleid
**B)** Een verbod op het verzamelen en opslaan van persoonlijke informatie afkondigen
**C)** Medewerkers verantwoordelijk maken voor het verstrekken van hun persoonsgegevens
**D)** Wetgeving inzake de bescherming van persoonsgegevens vertalen naar een privacybeleid

**10 / 40**
Een organisatie besluit een deel van de IT uit te besteden.

Hoe kan de informatiebeveiliging het **beste** worden gewaarborgd wanneer er met een leverancier wordt gewerkt?

**A)** Door een nieuwe information security officer (ISO) aan te stellen in de organisatie van de leverancier
**B)** Door de vereisten voor informatiebeveiliging van de leverancier te formaliseren in een overeenkomst
**C)** Door beide organisaties volledig gescheiden te houden, zodat iedereen eindverantwoordelijk is voor de eigen data
**D)** Door te eisen dat de leverancier de processen en procedures van de klantorganisatie volgt

**11 / 40**
Wie is verantwoordelijk om de bedrijfsstrategie en -doelstellingen te vertalen naar de beveiligingsstrategie en -doelstellingen?

**A)** Chief information security officer (CISO)
**B)** Algemeen bestuur
**C)** Information security officer (ISO)
**D)** Information security policy officer

**12 / 40**
Wat is het **beste** voorbeeld van een menselijke dreiging?

**A)** Een lekkage veroorzaakt een storing in de elektriciteitsvoorziening.
**B)** Een virus belandt via een USB-stick op een netwerk.
**C)** Er ligt te veel stof in de serverruimte.

**13 / 40**
Een databasesysteem waarop niet alle patches waren toegepast, werd gehackt. De hackers kregen toegang tot de data en hebben die verwijderd.

Welk informatiebeveiligingsconcept beschrijft het gebrek aan beveiligingspatches?

**A)** Impact
**B)** Risico
**C)** Dreiging
**D)** Kwetsbaarheid

**14 / 40**
Er is brand geweest in een bedrijf. De brandweer was snel ter plaatse en wist de brand te blussen voordat deze zich kon verspreiden en het hele gebouw afbrandde. Door de brand is echter wel de server vernietigd. De back-uptapes, die in een andere ruimte werden bewaard, zijn gesmolten en veel andere documenten zijn verloren gegaan.

Welke **indirecte** schade heeft deze brand veroorzaakt?

**A)** Verbrande computersystemen
**B)** Verbrande documenten
**C)** Gesmolten back-uptapes
**D)** Waterschade

**15 / 40**
Bedrijven kunnen verschillende risicostrategieën hanteren, afhankelijk van het type bedrijf.

Welke risicostrategie is voor een ziekenhuis het **beste** geschikt?

**A)** Risicoaanvaardend
**B)** Risicomijdend
**C)** Risicodragend
**D)** Risiconeutraal

**16 / 40**
Een goed uitgevoerde risicoanalyse levert veel nuttige informatie op. Een risicoanalyse heeft verschillende hoofddoelen.

Wat is **geen** hoofddoel van een risicoanalyse?

**A)** De kosten van een incident en de kosten van een beheersmaatregel uitbalanceren
**B)** Relevante kwetsbaarheden en dreigingen bepalen
**C)** Middelen en hun waarde identificeren
**D)** Beheersmaatregelen implementeren

**17 / 40**
Wat is een repressieve beheersmaatregel in geval van brand?

**A)** Een brand blussen nadat deze is ontdekt
**B)** Door de brand veroorzaakte schade herstellen
**C)** Een brandverzekering afsluiten

**18 / 40**
Wat is het doel van classificatie van informatie?

**A)** Het aanbrengen van labels om informatie beter herkenbaar te maken
**B)** Het opstellen van een handleiding voor de omgang met mobiele apparatuur
**C)** Het ordenen van informatie op basis van de gevoeligheid ervan

**19 / 40**
Wat is de **belangrijkste** reden om functiescheiding toe te passen?

**A)** Voorkomen dat verschillende medewerkers tegelijkertijd hetzelfde werk verrichten
**B)** Alle medewerkers collectief verantwoordelijk houden voor gemaakte vergissingen
**C)** Duidelijk maken wie verantwoordelijk is voor welke taken en activiteiten
**D)** De kans op onbevoegde of onbedoelde wijzigingen beperken

**20 / 40**
Wat is de **beste** manier om gepaste toegang tot informatie te waarborgen?

**A)** Workflows automatiseren
**B)** Bedieningsprocedures definiëren
**C)** Werkinstructies voor alle taken ontwikkelen
**D)** Trainingen verzorgen

**21 / 40**
Er breekt brand uit in een vestiging van een organisatie. De medewerkers worden overgeplaatst naar naburige vestigingen van de organisatie, zodat ze kunnen blijven doorwerken.

Waar in de incidentcyclus stapt een organisatie over op een hot site op afroep?

**A)** Tussen de stadia 'schade' en 'herstel'
**B)** Tussen de stadia 'incident' en 'schade'
**C)** Tussen de stadia 'herstel' en 'dreiging'
**D)** Tussen de stadia 'dreiging' en 'incident'

**22 / 40**
Een medewerker ontdekt dat de vervaldatum van een beleidsdocument zonder haar medeweten is gewijzigd. Ze is de enige persoon die hiertoe bevoegd is en meldt dit beveiligingsincident bij de helpdesk.

De helpdeskmedewerker registreert de volgende informatie over dit incident:
- datum en tijd
- beschrijving van het incident
- mogelijke gevolgen van het incident

Welke belangrijke informatie over het incident ontbreekt hier?

**A)** De naam van de melder van het incident
**B)** De naam van het softwarepakket
**C)** Het nummer van de pc

**23 / 40**
Waarom is het belangrijk om het managementsysteem voor informatiebeveiliging (ISMS) van een organisatie regelmatig te onderwerpen aan een audit?

**A)** Audits zijn in contracten met klanten vaak een vereiste om informatiebeveiliging te waarborgen.
**B)** Audits zijn een verplicht onderdeel om te voldoen aan wettelijke of regelgevende vereisten.
**C)** Audits brengen kwesties aan het licht waardoor een organisatie financiële targets mogelijk niet haalt.
**D)** Audits brengen zwakheden in de implementatie van beheersmaatregelen voor informatiebeveiliging aan het licht.

**24 / 40**
Welk document bevat een regel die het gebruik van bedrijfs-e-mail voor privédoeleinden verbiedt?

**A)** Verklaring Omtrent Gedrag (VOG)
**B)** Gedragscode
**C)** Algemene verordening gegevensbescherming (AVG)
**D)** Geheimhoudingsverklaring (NDA)

**25 / 40**
Aan wie moet een medewerker het als **eerste** melden wanneer deze medewerker een incident vaststelt?

**A)** De helpdesk
**B)** De information security manager (ISM)
**C)** De information security officer (ISO)
**D)** De manager

**26 / 40**
Wat is de **effectiefste** manier om medewerkers bewust te maken van informatiebeveiliging?

**A)** Een bewustwordingstraining toespitsen op het managementteam
**B)** Een externe training over informatiebeveiliging laten volgen door alle medewerkers
**C)** Een bewustwordingsprogramma opzetten dat speciaal voor de organisatie is
**D)** Een algemene, online cursus over informatiebeveiliging aanbieden

**27 / 40**
Met welke fysieke beheersmaatregel wordt toegang tot de informatie van een organisatie beheerd?

**A)** De installatie van airconditioning
**B)** Een verbod op het gebruik van USB-sticks
**C)** Het verplichte gebruik van een gebruikersnaam en wachtwoord
**D)** Het gebruik van onbreekbaar glas

**28 / 40**
In een datacenter worden accu's gebruikt, maar er is geen stroomgenerator.

Welk risico vormt deze situatie voor de beschikbaarheid van het datacenter?

**A)** De hoofdvoeding is na herstel mogelijk niet automatisch weer beschikbaar, omdat hiervoor een stroomgenerator nodig is.
**B)** Een stroomonderbreking kan langer dan enkele minuten of uren duren, waarna er geen stroom beschikbaar is.
**C)** De gebruiksduur van de accu's is beperkt, want na enkele dagen raakt de diesel mogelijk op en werken ze niet meer.
**D)** De accu's moeten na enkele uren worden aangedreven door de stroomgenerator, en ze bieden dus slechts een beperkte bescherming.

**29 / 40**
Waarom wordt er airconditioning geïnstalleerd in de serverruimte?

**A)** Back-uptapes zijn gemaakt van dun plastic dat niet bestand is tegen hoge temperaturen. Als het te warm wordt in de serverruimte, kunnen ze beschadigd raken.
**B)** Het mag niet te warm worden voor medewerkers die in de serverruimte werken. Hoe warmer het wordt, hoe groter de kans dat zij fouten maken.
**C)** De lucht in de serverruimte moet worden gekoeld en de warmte die de apparatuur produceert moet worden afgevoerd. Op deze manier wordt de lucht in de ruimte ontvochtigd en gefilterd.
**D)** De lucht voor het hele kantoor kan het beste via de serverruimte worden gekoeld. Voor zo'n grote installatie moet geen kostbare kantoorruimte worden opgeofferd.

**30 / 40**
Bij fysieke beveiliging kunnen meerdere beschermingsringen worden toegepast waarbinnen verschillende maatregelen worden genomen.

Wat is **geen** beschermingsring?

**A)** Gebouw
**B)** Middenring
**C)** Beveiligde ruimte
**D)** Buitenring

**31 / 40**
De benodigde beheersmaatregel om een middel te beveiligen, is afhankelijk van het middel.

Wat is de **geschiktste** manier om een middel te beveiligen?

**A)** Een formulier beveiligen door het te laten invullen en ondertekenen
**B)** Een laptop beveiligen door deze aan één gebruiker toe te wijzen
**C)** Een USB-stick beveiligen door middel van encryptie
**D)** Een internetverbinding beveiligen met een back-up

**32 / 40**
Welke beheersmaatregel voor informatiebeveiliging draagt bij aan de ontwikkeling van systemen waarin informatiebeveiliging voorop staat?

**A)** Redundantie van de servers waarborgen
**B)** Fysieke beheersmaatregelen voor toegang implementeren
**C)** Een antecedentenonderzoek van personeel uitvoeren
**D)** Gebruikmaken van dataclassificatie voor informatiemiddelen

**33 / 40**
Het beleid van een organisatie wordt gewijzigd. Medewerkers mogen voortaan ook thuiswerken.

Welke beheersmaatregel moet nu worden ingevoerd?

**A)** V-LAN's maken om het bedrijfsnetwerk te segmenteren
**B)** De informatie op het bedrijfsnetwerk versleutelen
**C)** Firewalls installeren in het bedrijfsnetwerk
**D)** Een VPN gebruiken om verbinding te maken met het bedrijfsnetwerk

**34 / 40**
De medewerkers van een organisatie werken op laptops die worden beschermd door asymmetrische cryptografie. Alle consultants gebruiken hetzelfde sleutelpaar, zodat het management van de sleutels betaalbaar blijft.

Zodra bepaalde informatie wordt beschadigd, moeten er nieuwe sleutels worden verstrekt.

In welk geval moeten er nieuwe sleutels worden verstrekt?

**A)** Wanneer de persoonlijke sleutel bekend wordt
**B)** Wanneer de openbare sleutel bekend wordt
**C)** Wanneer de Public Key Infrastructure (PKI) bekend wordt

**35 / 40**
Welke vorm van beveiliging biedt een Public Key Infrastructure (PKI)?

**A)** Een PKI zorgt dat er regelmatig back-ups van bedrijfsdata worden gemaakt.
**B)** Een PKI toont klanten dat een online bedrijf veilig is.
**C)** Een PKI controleert welke persoon of welk systeem bij een specifieke openbare sleutel hoort.

**36 / 40**
Welke vorm van malware is een programma dat, behalve de functie die het ogenschijnlijk uitvoert, opzettelijk secundaire activiteiten verricht?

**A)** Logic bomb
**B)** Spyware
**C)** Trojan
**D)** Worm

**37 / 40**
Welke vorm van malware creëert een netwerk van geïnfecteerde computers door zichzelf te vermenigvuldigen?

**A)** Logic bomb
**B)** Spyware
**C)** Trojan
**D)** Worm

**38 / 40**
Welk wettelijk of regelgevend besluit met betrekking tot informatiebeveiliging kan aan alle organisaties worden opgelegd?

**A)** Algemene verordening gegevensbescherming (AVG)
**B)** Intellectueel eigendomsrecht
**C)** ISO/IEC 27001
**D)** ISO/IEC 27002

**39 / 40**
Welke ISO-norm is gericht op de implementatie van beheersmaatregelen voor informatiebeveiliging?

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

**40 / 40**
De normen van welke organisatie worden het **meest** gebruikt in Europa?

**A)** American National Standards Institute (ANSI)
**B)** Internationale Organisatie voor Standaardisatie (ISO)
**C)** National Institute of Standards and Technology (NIST)

# Antwoordsleutel

**1 / 40**
Een database bevat enkele miljoenen transacties van een telefoonmaatschappij. Er wordt een factuur voor een klant gegenereerd en verzonden.

Wat bevat deze factuur voor de klant?

**A)** Data
**B)** Informatie
**C)** Data en informatie

**A)** Incorrect. De database bevat data. Wanneer er echter een factuur wordt gegenereerd en naar een ontvanger wordt verzonden, is dit informatie voor de ontvanger.
**B)** Correct. De waarde van informatie wordt bepaald door de ontvanger. De factuur bevat waardevolle data voor de ontvanger en is daarom informatie. (Literatuur: A, hoofdstuk 4.8.5)
**C)** Incorrect. De factuur bevat alleen informatie voor de ontvanger.

**2 / 40**
Wat is het verschil tussen data en informatie?

**A)** Data kan allerlei feiten of cijfers zijn. Informatie is data met betekenis.
**B)** Data bestaat uit ongestructureerde cijfers. Informatie bestaat uit gestructureerde cijfers.
**C)** Data hoeft niet te worden beveiligd. Informatie moet wel worden beveiligd.
**D)** Data heeft geen waarde. Informatie is verwerkte data en heeft wel waarde.

**A)** Correct. Informatie wordt afgeleid van data door er betekenis aan te geven in een bepaalde context. (Literatuur: A, hoofdstuk 3.1)
**B)** Incorrect. Data kan zowel gestructureerd als ongestructureerd zijn. Informatie is doorgaans gestructureerd.
**C)** Incorrect. Zowel data als informatie moet worden beveiligd.
**D)** Incorrect. Zowel data als informatie heeft waarde.

**3 / 40**
Wat is de focus van informatiemanagement?

**A)** Zorgen dat bedrijfsactiviteiten en -processen zonder onderbrekingen blijven doorgaan
**B)** Zorgen dat de waarde van informatie wordt vastgesteld en benut
**C)** Voorkomen dat onbevoegde personen toegang krijgen tot geautomatiseerde systemen
**D)** Begrijpen hoe informatie door een organisatie stroomt

**A)** Incorrect. Dit is de focus van bedrijfscontinuïteitsbeheer (business continuity management, BCM). Het doel van BCM is voorkomen dat bedrijfsactiviteiten worden verstoord, bescherming van cruciale bedrijfsprocessen tegen de gevolgen van omvangrijke storingen in informatiesystemen en een snel herstel mogelijk maken.
**B)** Correct. Informatiemanagement beschrijft hoe een organisatie informatie efficiënt plant, verzamelt, ordent, gebruikt, beheert, verspreidt en verwijdert. Ook beschrijft het hoe de waarde van die informatie wordt bepaald en optimaal wordt benut. (Literatuur: A, hoofdstuk 4.9)
**C)** Incorrect. Dit is de focus van toegangsbeheer. Het zorgt ervoor dat onbevoegde personen of processen geen toegang krijgen tot geautomatiseerde systemen, databases en programma's.
**D)** Incorrect. Dit is de focus van informatieanalyse. Het schetst een duidelijk beeld van de manier waarop een organisatie omgaat met informatie en hoe de informatie door de organisatie stroomt.

**4 / 40**
Organisaties moeten weten met welke risico's ze te maken hebben voordat ze passende maatregelen kunnen nemen.

Wat moet een organisatie weten om risico's te kunnen bepalen?

**A)** Wat de waarschijnlijkheid is dat iets gebeurt en wat de gevolgen daarvan zijn voor de organisatie
**B)** Wat de meest voorkomende gevaren zijn en hoe deze kunnen worden ondervangen, zoals beschreven in best practices
**C)** Met welke dreigingen de organisatie te maken heeft en hoe kwetsbaar de organisatie hiervoor is
**D)** Met welke ongeplande gebeurtenissen de organisatie te maken heeft en wat moet worden gedaan wanneer zo'n gebeurtenis zich voordoet

**A)** Correct. Risico's worden bepaald door twee factoren op hoger niveau: de waarschijnlijkheid dat iets zich voordoet en de impact ervan op het bedrijf. (Literatuur: A, hoofdstuk 3.1)
**B)** Incorrect. Het is onverstandig om dit als uitgangspunt te nemen om de risico's voor een organisatie te bepalen. Een organisatie wordt niet veilig door te doen wat andere organisaties doen.
**C)** Incorrect. Dit is een beschrijving van de term waarschijnlijkheid. Hoewel het belangrijk is om te weten wat waarschijnlijkheid inhoudt, ontbreekt hier een belangrijk aspect: de invloed ervan op het bedrijf.
**D)** Incorrect. Uiteindelijk is het nodig om risico's te koppelen aan beheersmaatregelen, maar dit is eerder een reactie op risico's dan een manier om ze überhaupt te begrijpen.

**5 / 40**
Wat is, naast integriteit en vertrouwelijkheid, het derde betrouwbaarheidsaspect van informatie?

**A)** Nauwkeurigheid
**B)** Beschikbaarheid
**C)** Volledigheid
**D)** Waarde

**A)** Incorrect. De drie betrouwbaarheidsaspecten van informatie zijn beschikbaarheid, integriteit en vertrouwelijkheid. Nauwkeurigheid is een onderdeel van de integriteit.
**B)** Correct. De drie betrouwbaarheidsaspecten van informatie zijn beschikbaarheid, integriteit en vertrouwelijkheid. (Literatuur: A, hoofdstuk 3.4.3)
**C)** Incorrect. De drie betrouwbaarheidsaspecten van informatie zijn beschikbaarheid, integriteit en vertrouwelijkheid. Volledigheid is een onderdeel van de integriteit.
**D)** Incorrect. De drie betrouwbaarheidsaspecten van informatie zijn beschikbaarheid, integriteit en vertrouwelijkheid.

**6 / 40**
In de hal van een organisatie staat een netwerkprinter. Veel medewerkers halen hun afdrukken niet direct op en laten ze op de printer liggen.

Wat is het gevolg voor de betrouwbaarheid van de informatie?

**A)** De beschikbaarheid van de informatie kan niet langer worden gegarandeerd.
**B)** De vertrouwelijkheid van de informatie kan niet langer worden gegarandeerd.
**C)** De integriteit van de informatie kan niet langer worden gegarandeerd.

**A)** Incorrect. De informatie is nog steeds beschikbaar in het systeem dat werd gebruikt om de documenten te maken en af te drukken.
**B)** Correct. De informatie kan in handen vallen van of gelezen worden door personen die er geen toegang toe zouden mogen hebben. (Literatuur: A, hoofdstuk 3.4.1)
**C)** Incorrect. De integriteit van de informatie op de afdrukken kan nog steeds worden gegarandeerd, aangezien alles op papier staat.

**7 / 40**
Wat is het verschil tussen eindverantwoordelijkheid en controleerbaarheid?

**A)** Eindverantwoordelijkheid betekent dat een organisatie de financiële boekhouding goed op orde heeft. Controleerbaarheid betekent dat een organisatie een audit met succes heeft doorlopen.
**B)** Eindverantwoordelijkheid is aansprakelijkheid voor de resultaten van activiteiten van een organisatie. Controleerbaarheid verwijst naar de gereedheid van een organisatie om onafhankelijk te worden gecontroleerd.
**C)** Eindverantwoordelijkheid is het dragen van verantwoordelijkheid voor de acties van een persoon. Controleerbaarheid is het dragen van verantwoordelijkheid voor de acties van een organisatie.
**D)** Eindverantwoordelijkheid betekent dat een organisatie voldoet aan Sarbanes-Oxley (SOX). Controleerbaarheid betekent dat een organisatie voldoet aan ISO/IEC 27001.

**A)** Incorrect. Eindverantwoordelijkheid heeft niet direct te maken met de financiële boekhouding. Controleerbaarheid heeft niets te maken met het succesvol doorlopen van een audit.
**B)** Correct. Dit zijn de juiste definities van eindverantwoordelijkheid en controleerbaarheid. (Literatuur: A, hoofdstuk 3.4.4)
**C)** Incorrect. De definitie van eindverantwoordelijkheid is juist, maar de definitie van controleerbaarheid niet. Controleerbaarheid heeft niets te maken met verantwoordelijkheid voor de acties van een organisatie.
**D)** Incorrect. Zowel eindverantwoordelijkheid als controleerbaarheid heeft geen betrekking op naleving (compliance) van SOX- of ISO/IEC-normen.

**8 / 40**
Hoe kan het doel van een informatiebeveiligingsbeleid het **beste** worden beschreven?

**A)** Een informatiebeveiligingsbeleid is waar de analyse van risico's en de zoektocht naar toepasselijke beheersmaatregelen zijn gedocumenteerd.
**B)** Een informatiebeveiligingsbeleid biedt de organisatie richting en ondersteuning ten behoeve van de informatiebeveiliging.
**C)** Een informatiebeveiligingsbeleid maakt het beveiligingsplan concreet door er de benodigde details aan toe te voegen.
**D)** Een informatiebeveiligingsbeleid biedt inzicht in dreigingen en mogelijke gevolgen daarvan.

**A)** Incorrect. De analyse van risico's en de zoektocht naar beheersmaatregelen zijn doelen van risicoanalyse en risicomanagement.
**B)** Correct. Het beveiligingsbeleid biedt het management richting en ondersteuning ten behoeve van de informatiebeveiliging. (Literatuur: A, hoofdstuk 4.2.1)
**C)** Incorrect. Het beveiligingsplan maakt het informatiebeveiligingsbeleid concreet. Het plan benoemt onder andere welke beheersmaatregelen zijn gekozen, wie waarvoor verantwoordelijk is, wat de richtlijnen voor de implementatie van beheersmaatregelen zijn, et cetera.
**D)** Incorrect. Inzicht bieden in dreigingen en mogelijke gevolgen is het doel van een dreigingsanalyse.

**9 / 40**
Sara heeft opdracht gekregen de naleving (compliance) van alle wetgeving inzake de bescherming van persoonsgegevens binnen haar organisatie te waarborgen.

Wat moet zij als **eerste** doen?

**A)** Iemand aanstellen om managers te helpen bij de naleving van het beleid
**B)** Een verbod op het verzamelen en opslaan van persoonlijke informatie afkondigen
**C)** Medewerkers verantwoordelijk maken voor het verstrekken van hun persoonsgegevens
**D)** Wetgeving inzake de bescherming van persoonsgegevens vertalen naar een privacybeleid

**A)** Incorrect. Iemand die managers helpt is geen vereiste voor de naleving van wetgeving inzake de bescherming van persoonsgegevens. Bovendien moet het beleid eerst worden afgestemd op de wetgeving.
**B)** Incorrect. Dit is niet de beste manier om te zorgen voor naleving van wetgeving inzake de bescherming van persoonsgegevens.
**C)** Incorrect. Dit is geen manier om te zorgen voor naleving van wetgeving inzake de bescherming van persoonsgegevens.
**D)** Correct. De eerste stap om te zorgen voor naleving van de wetgeving, is het opstellen van een intern beleid voor de organisatie. (Literatuur: A, hoofdstuk 5.1)

**10 / 40**
Een organisatie besluit een deel van de IT uit te besteden.

Hoe kan de informatiebeveiliging het **beste** worden gewaarborgd wanneer er met een leverancier wordt gewerkt?

**A)** Door een nieuwe information security officer (ISO) aan te stellen in de organisatie van de leverancier
**B)** Door de vereisten voor informatiebeveiliging van de leverancier te formaliseren in een overeenkomst
**C)** Door beide organisaties volledig gescheiden te houden, zodat iedereen eindverantwoordelijk is voor de eigen data
**D)** Door te eisen dat de leverancier de processen en procedures van de klantorganisatie volgt

**A)** Incorrect. Als de organisatie van de leverancier al een ISO heeft, is het niet nodig een nieuwe ISO aan te stellen.
**B)** Correct. Hoewel het aangaan van een overeenkomst geen onfeilbaar vangnet is om het leveranciersrisico te beheersen, is het wel de effectiefste manier hiervoor. (Literatuur: A, hoofdstuk 5.20)
**C)** Incorrect. De klantorganisatie blijft eindverantwoordelijk voor alle informatie. Een volledige scheiding van organisaties heeft vaak tot gevolg dat de klantorganisatie niet weet hoe deze de informatiebeveiliging in de organisatie van de leverancier kan waarborgen of beïnvloeden.
**D)** Incorrect. Dit is niet de beste manier, omdat een leverancier zijn eigen informatiebeveiligingsprocessen moet kunnen volgen.

**11 / 40**
Wie is verantwoordelijk om de bedrijfsstrategie en -doelstellingen te vertalen naar de beveiligingsstrategie en -doelstellingen?

**A)** Chief information security officer (CISO)
**B)** Algemeen bestuur
**C)** Information security officer (ISO)
**D)** Information security policy officer

**A)** Correct. De CISO bevindt zich op het hoogste managementniveau van de organisatie en ontwikkelt de algemene beveiligingsstrategie voor het hele bedrijf. (Literatuur: A, hoofdstuk 5.2)
**B)** Incorrect. Het algemeen bestuur bepaalt de strategie op basis waarvan de CISO vervolgens de algemene beveiligingsstrategie bepaalt.
**C)** Incorrect. De ISO ontwikkelt het informatiebeveiligingsbeleid van een business-unit op basis van het bedrijfsbeleid en zorgt dat dit wordt nageleefd.
**D)** Incorrect. De information security policy officer is verantwoordelijk voor het onderhoud van het beleid dat wordt afgeleid van de beveiligingsstrategie.

**12 / 40**
Wat is het **beste** voorbeeld van een menselijke dreiging?

**A)** Een lekkage veroorzaakt een storing in de elektriciteitsvoorziening.
**B)** Een virus belandt via een USB-stick op een netwerk.
**C)** Er ligt te veel stof in de serverruimte.

**A)** Incorrect. Een lekkage is geen menselijke dreiging, maar een niet-menselijke dreiging.
**B)** Correct. Een USB-stick wordt altijd geplaatst door een persoon. Als zodoende een virus op het netwerk belandt, is dat dus een menselijke dreiging. (Literatuur: A, hoofdstuk 3.9.1)
**C)** Incorrect. Stof is geen menselijke dreiging, maar een niet-menselijke dreiging.

**13 / 40**
Een databasesysteem waarop niet alle patches waren toegepast, werd gehackt. De hackers kregen toegang tot de data en hebben die verwijderd.

Welk informatiebeveiligingsconcept beschrijft het gebrek aan beveiligingspatches?

**A)** Impact
**B)** Risico
**C)** Dreiging
**D)** Kwetsbaarheid

**A)** Incorrect. Impact is het effect van een gebeurtenis op een organisatie of op de informatie van de organisatie.
**B)** Incorrect. Een risico is de combinatie van de waarschijnlijkheid dat een gebeurtenis zich voordoet en de impact ervan.
**C)** Incorrect. Een dreiging is bijvoorbeeld wanneer een externe entiteit misbruik probeert te maken van een kwetsbaarheid. In dit geval vormen de hackers de dreiging.
**D)** Correct. Onvoldoende bescherming is een voorbeeld van een kwetsbaarheid. (Literatuur: A, hoofdstuk 3.5.3)

**14 / 40**
Er is brand geweest in een bedrijf. De brandweer was snel ter plaatse en wist de brand te blussen voordat deze zich kon verspreiden en het hele gebouw afbrandde. Door de brand is echter wel de server vernietigd. De back-uptapes, die in een andere ruimte werden bewaard, zijn gesmolten en veel andere documenten zijn verloren gegaan.

Welke **indirecte** schade heeft deze brand veroorzaakt?

**A)** Verbrande computersystemen
**B)** Verbrande documenten
**C)** Gesmolten back-uptapes
**D)** Waterschade

**A)** Incorrect. Verbrande computersystemen zijn directe schade ten gevolge van de brand.
**B)** Incorrect. Verbrande documenten zijn directe schade ten gevolge van de brand.
**C)** Incorrect. Gesmolten back-uptapes zijn directe schade ten gevolge van de brand.
**D)** Correct. Waterschade door de inzet van blusapparatuur is indirecte schade ten gevolge van de brand. Het is een neveneffect van de bluswerkzaamheden, die erop zijn gericht de schade ten gevolge van de brand te beperken. (Literatuur: A, hoofdstuk 3.10)

**15 / 40**
Bedrijven kunnen verschillende risicostrategieën hanteren, afhankelijk van het type bedrijf.

Welke risicostrategie is voor een ziekenhuis het **beste** geschikt?

**A)** Risicoaanvaardend
**B)** Risicomijdend
**C)** Risicodragend
**D)** Risiconeutraal

**A)** Incorrect. Een ziekenhuis kan niet zomaar risico's aanvaarden, met het oog op financiële verliezen of het overlijden van patiënten.
**B)** Correct. Ziekenhuizen moeten elk risico proberen te mijden. (Literatuur: A, hoofdstuk 3.11)
**C)** Incorrect. Risicodragend betekent dat bepaalde risico's worden aanvaard. Een reden hiervoor kan zijn dat de kosten van beheersmaatregelen de mogelijke schade overtreffen. In een ziekenhuis is dit niet de beste manier om met risico's om te gaan.
**D)** Incorrect. Risiconeutraal betekent dat er beveiligingsmaatregelen worden genomen om te voorkomen dat dreigingen zich voordoen of, mocht dit toch het geval zijn, om te zorgen dat de voortvloeiende schade tot een minimum beperkt blijft. Omdat schade aan cliënten nooit goed is, moeten ziekenhuizen risicomijdend zijn.

**16 / 40**
Een goed uitgevoerde risicoanalyse levert veel nuttige informatie op. Een risicoanalyse heeft verschillende hoofddoelen.

Wat is **geen** hoofddoel van een risicoanalyse?

**A)** De kosten van een incident en de kosten van een beheersmaatregel uitbalanceren
**B)** Relevante kwetsbaarheden en dreigingen bepalen
**C)** Middelen en hun waarde identificeren
**D)** Beheersmaatregelen implementeren

**A)** Incorrect. Dit is een van de hoofddoelen van een risicoanalyse.
**B)** Incorrect. Dit is een van de hoofddoelen van een risicoanalyse.
**C)** Incorrect. Dit is een van de hoofddoelen van een risicoanalyse.
**D)** Correct. Dit is geen doel van een risicoanalyse. (Literatuur: A, hoofdstuk 3.7)

**17 / 40**
Wat is een repressieve beheersmaatregel in geval van brand?

**A)** Een brand blussen nadat deze is ontdekt
**B)** Door de brand veroorzaakte schade herstellen
**C)** Een brandverzekering afsluiten

**A)** Correct. Deze repressieve beheersmaatregel beperkt de schade door een brand. (Literatuur: A, hoofdstuk 3.8)
**B)** Incorrect. Dit is geen repressieve beheersmaatregel. Hiermee wordt de schade door de brand niet beperkt.
**C)** Incorrect. Een verzekering biedt bescherming tegen de financiële gevolgen van een brand en is een vorm van verzekering tegen risico's.

**18 / 40**
Wat is het doel van classificatie van informatie?

**A)** Het aanbrengen van labels om informatie beter herkenbaar te maken
**B)** Het opstellen van een handleiding voor de omgang met mobiele apparatuur
**C)** Het ordenen van informatie op basis van de gevoeligheid ervan

**A)** Incorrect. Het labelen van informatie is rubricering: een speciale vorm van informatiecategorisering die volgt op de classificatie van informatie.
**B)** Incorrect. Het opstellen van een handleiding heeft betrekking op gebruiksrichtlijnen en classificeert geen informatie.
**C)** Correct. Informatie wordt geclassificeerd om de verschillende gevoeligheidsniveaus te definiëren waarbinnen informatie kan worden gestructureerd. (Literatuur: A, hoofdstuk 5.12)

**19 / 40**
Wat is de **belangrijkste** reden om functiescheiding toe te passen?

**A)** Voorkomen dat verschillende medewerkers tegelijkertijd hetzelfde werk verrichten
**B)** Alle medewerkers collectief verantwoordelijk houden voor gemaakte vergissingen
**C)** Duidelijk maken wie verantwoordelijk is voor welke taken en activiteiten
**D)** De kans op onbevoegde of onbedoelde wijzigingen beperken

**A)** Incorrect. Functiescheiding wordt gebruikt om onbevoegde of onbedoelde wijzigingen of misbruik van de middelen van een organisatie te voorkomen. Het bepaalt niet wanneer activiteiten moeten worden uitgevoerd.
**B)** Incorrect. Functiescheiding wordt gebruikt om taken en verantwoordelijkheden van elkaar te scheiden. Het maakt groep mensen niet collectief verantwoordelijk.
**C)** Incorrect. Functiescheiding wordt gebruikt om onbevoegde of onbedoelde wijzigingen of misbruik van de middelen van een organisatie te voorkomen. Het doel ervan is niet om duidelijk te maken wie waarvoor verantwoordelijk is.
**D)** Correct. Functies moeten worden gescheiden om onbevoegde of onbedoelde wijzigingen of misbruik van de middelen van een organisatie te voorkomen. (Literatuur: A, hoofdstuk 5.3)

**20 / 40**
Wat is de **beste** manier om gepaste toegang tot informatie te waarborgen?

**A)** Workflows automatiseren
**B)** Bedieningsprocedures definiëren
**C)** Werkinstructies voor alle taken ontwikkelen
**D)** Trainingen verzorgen

**A)** Incorrect. Automatisering van workflows draagt zeker bij aan de informatiebeveiliging, maar niet aan gepaste toegang.
**B)** Correct. Het gebruik van procedures om te zorgen dat werk gepast, veilig en verantwoord wordt verricht, is een effectieve manier om effectieve informatiebeveiliging te bewerkstelligen. (Literatuur: A, hoofdstuk 5.36.1)
**C)** Incorrect. Dit is te gedetailleerd en te voorschrijvend, waardoor het niet de beste manier is.
**D)** Incorrect. Training is belangrijk maar garandeert geen gepaste toegang tot informatie.

**21 / 40**
Er breekt brand uit in een vestiging van een organisatie. De medewerkers worden overgeplaatst naar naburige vestigingen van de organisatie, zodat ze kunnen blijven doorwerken.

Waar in de incidentcyclus stapt een organisatie over op een hot site op afroep?

**A)** Tussen de stadia 'schade' en 'herstel'
**B)** Tussen de stadia 'incident' en 'schade'
**C)** Tussen de stadia 'herstel' en 'dreiging'
**D)** Tussen de stadia 'dreiging' en 'incident'

**A)** Incorrect. 'Schade' en 'herstel' worden beperkt door de hot site op afroep.
**B)** Correct. Een hot site op afroep is een repressieve maatregel die in gang wordt gezet om de schade te beperken. (Literatuur: A, hoofdstuk 3.8.4)
**C)** Incorrect. Het stadium 'herstel' vindt plaats nadat een hot site op afroep in het leven in werking is getreden.
**D)** Incorrect. Het is duur om over te stappen op een hot site op afroep zonder dat er sprake is van een incident.

**22 / 40**
Een medewerker ontdekt dat de vervaldatum van een beleidsdocument zonder haar medeweten is gewijzigd. Ze is de enige persoon die hiertoe bevoegd is en meldt dit beveiligingsincident bij de helpdesk.

De helpdeskmedewerker registreert de volgende informatie over dit incident:
- datum en tijd
- beschrijving van het incident
- mogelijke gevolgen van het incident

Welke belangrijke informatie over het incident ontbreekt hier?

**A)** De naam van de melder van het incident
**B)** De naam van het softwarepakket
**C)** Het nummer van de pc

**A)** Correct. Wanneer een incident wordt gemeld, moet minimaal de naam van de melder worden vastgelegd. (Literatuur: A, hoofdstuk 5.25)
**B)** Incorrect. Dit is aanvullende informatie die later kan worden toegevoegd.
**C)** Incorrect. Dit is aanvullende informatie die later kan worden toegevoegd.

**23 / 40**
Waarom is het belangrijk om het managementsysteem voor informatiebeveiliging (ISMS) van een organisatie regelmatig te onderwerpen aan een audit?

**A)** Audits zijn in contracten met klanten vaak een vereiste om informatiebeveiliging te waarborgen.
**B)** Audits zijn een verplicht onderdeel om te voldoen aan wettelijke of regelgevende vereisten.
**C)** Audits brengen kwesties aan het licht waardoor een organisatie financiële targets mogelijk niet haalt.
**D)** Audits brengen zwakheden in de implementatie van beheersmaatregelen voor informatiebeveiliging aan het licht.

**A)** Incorrect. Contracten met klanten bevatten zelden auditvereisten.
**B)** Incorrect. Wettelijke of regelgevende vereisten stellen audits doorgaans niet verplicht.
**C)** Incorrect. Audits worden doorgaans niet gebruikt om financiële prestaties te controleren.
**D)** Correct. Het doel van audits is het vinden van zwakheden in geïmplementeerde beheersmaatregelen. (Literatuur: A, hoofdstuk 5.35)

**24 / 40**
Welk document bevat een regel die het gebruik van bedrijfs-e-mail voor privédoeleinden verbiedt?

**A)** Verklaring Omtrent Gedrag (VOG)
**B)** Gedragscode
**C)** Algemene verordening gegevensbescherming (AVG)
**D)** Geheimhoudingsverklaring (NDA)

**A)** Incorrect. Een VOG wordt afgegeven door het ministerie van Justitie en Veiligheid en bewijst dat iemand geen strafbare feiten heeft gepleegd.
**B)** Correct. De gedragscode is een document (vaak onderdeel van het personeelshandboek) waarin de beleidsregels worden beschreven die binnen een bedrijf gelden voor het personeel. (Literatuur: A, hoofdstuk 6.2)
**C)** Incorrect. De AVG heeft betrekking op de bescherming van persoonsgegevens.
**D)** Incorrect. Een NDA is een contract waaronder het verboden is bepaalde informatie openbaar te maken. Het gebruik van bedrijfs-e-mail voor privédoeleinden valt niet onder zo'n document.

**25 / 40**
Aan wie moet een medewerker het als **eerste** melden wanneer deze medewerker een incident vaststelt?

**A)** De helpdesk
**B)** De information security manager (ISM)
**C)** De information security officer (ISO)
**D)** De manager

**A)** Correct. Incidenten moeten doorgaans aan de helpdesk worden gemeld voor evaluatie, toepassing van de eerste procedures en, zo nodig, escalatie. Ze moeten niet onmiddellijk verticaal worden geëscaleerd. (Literatuur: A, hoofdstuk 6.8)
**B)** Incorrect. Incidenten moeten niet onmiddellijk verticaal worden geëscaleerd. Bovendien is niet elk incident een beveiligingsincident. Het incident moet daarom eerst door de helpdesk worden beoordeeld om te bepalen of er überhaupt sprake is van een beveiligingsincident.
**C)** Incorrect. Incidenten moeten niet onmiddellijk verticaal worden geëscaleerd. Bovendien is niet elk incident een beveiligingsincident. Het incident moet daarom eerst door de helpdesk worden beoordeeld om te bepalen of er überhaupt sprake is van een beveiligingsincident.
**D)** Incorrect. Incidenten moeten niet onmiddellijk verticaal worden geëscaleerd.

**26 / 40**
Wat is de **effectiefste** manier om medewerkers bewust te maken van informatiebeveiliging?

**A)** Een bewustwordingstraining toespitsen op het managementteam
**B)** Een externe training over informatiebeveiliging laten volgen door alle medewerkers
**C)** Een bewustwordingsprogramma opzetten dat speciaal voor de organisatie is
**D)** Een algemene, online cursus over informatiebeveiliging aanbieden

**A)** Incorrect. Alle medewerkers moeten zich bewust zijn van informatiebeveiliging, niet alleen managers.
**B)** Incorrect. Een externe training voorziet mogelijk niet volledig in de specifieke behoeften van een organisatie.
**C)** Correct. Het is het effectiefst om het bewustwordingsprogramma af te stemmen op de specifieke behoeften van de organisatie. (Literatuur: A, hoofdstuk 6.3)
**D)** Incorrect. Een algemene training over informatiebeveiliging voorziet mogelijk niet volledig in de specifieke behoeften van een organisatie.

**27 / 40**
Met welke fysieke beheersmaatregel wordt toegang tot de informatie van een organisatie beheerd?

**A)** De installatie van airconditioning
**B)** Een verbod op het gebruik van USB-sticks
**C)** Het verplichte gebruik van een gebruikersnaam en wachtwoord
**D)** Het gebruik van onbreekbaar glas

**A)** Incorrect. Met airconditioning kan de toegang tot informatie van een organisatie niet worden beheerd.
**B)** Incorrect. Dit is een organisatorische beheersmaatregel.
**C)** Incorrect. Dit is een technische beheersmaatregel.
**D)** Correct. Het gebruik van onbreekbaar glas is een voorbeeld van een fysieke beheersmaatregel om te voorkomen dat onbevoegde personen toegang krijgen tot het gebouw. (Literatuur: A, hoofdstuk 7.4)

**28 / 40**
In een datacenter worden accu's gebruikt, maar er is geen stroomgenerator.

Welk risico vormt deze situatie voor de beschikbaarheid van het datacenter?

**A)** De hoofdvoeding is na herstel mogelijk niet automatisch weer beschikbaar, omdat hiervoor een stroomgenerator nodig is.
**B)** Een stroomonderbreking kan langer dan enkele minuten of uren duren, waarna er geen stroom beschikbaar is.
**C)** De gebruiksduur van de accu's is beperkt, want na enkele dagen raakt de diesel mogelijk op en werken ze niet meer.
**D)** De accu's moeten na enkele uren worden aangedreven door de stroomgenerator, en ze bieden dus slechts een beperkte bescherming.

**A)** Incorrect. Een stroomgenerator wordt niet gebruikt om de hoofdvoeding te activeren.
**B)** Correct. Accu's bieden alleen bescherming tegen tijdelijke stroomstoringen en -pieken, terwijl een stroomgenerator beschermt tegen langere storingen. (Literatuur: A, hoofdstuk 7.11.1)
**C)** Incorrect. Diesel wordt gebruikt om de generator aan te drijven; een accu wordt gevoed door batterijen.
**D)** Incorrect. De accu's werken slechts korte tijd, maar worden niet gevoed door de generator. De generator neemt de voeding simpelweg over van de accu's.

**29 / 40**
Waarom wordt er airconditioning geïnstalleerd in de serverruimte?

**A)** Back-uptapes zijn gemaakt van dun plastic dat niet bestand is tegen hoge temperaturen. Als het te warm wordt in de serverruimte, kunnen ze beschadigd raken.
**B)** Het mag niet te warm worden voor medewerkers die in de serverruimte werken. Hoe warmer het wordt, hoe groter de kans dat zij fouten maken.
**C)** De lucht in de serverruimte moet worden gekoeld en de warmte die de apparatuur produceert moet worden afgevoerd. Op deze manier wordt de lucht in de ruimte ontvochtigd en gefilterd.
**D)** De lucht voor het hele kantoor kan het beste via de serverruimte worden gekoeld. Voor zo'n grote installatie moet geen kostbare kantoorruimte worden opgeofferd.

**A)** Incorrect. Back-uptapes moeten niet in de serverruimte worden bewaard. Bij brand zouden zowel de gebruikte informatie als de back-ups worden vernietigd.
**B)** Incorrect. Dit is niet de reden om airconditioning te installeren in de serverruimte.
**C)** Correct. Voor de fysieke beveiliging van serverruimtes gelden andere afwegingen. Ze bevatten gevoelige apparatuur die gevoelig is voor vocht en warmte, en zelf ook warmte produceert. (Literatuur: A, hoofdstuk 7.11.2)
**D)** Incorrect. De lucht voor het hele kantoor moet niet worden gekoeld via de serverruimte.

**30 / 40**
Bij fysieke beveiliging kunnen meerdere beschermingsringen worden toegepast waarbinnen verschillende maatregelen worden genomen.

Wat is **geen** beschermingsring?

**A)** Gebouw
**B)** Middenring
**C)** Beveiligde ruimte
**D)** Buitenring

**A)** Incorrect. Gebouw is de ring voor toegang tot de locatie.
**B)** Correct. Er zijn vier beschermingsringen: buitenring, gebouw, werkruimten en beveiligde ruimte. (Literatuur: A, hoofdstuk 7.0.1)
**C)** Incorrect. De beveiligde ruimte is een geldige zone, waarin het middel dat moet worden beschermd zich bevindt.
**D)** Incorrect. De buitenring is een geldige zone, die het gebied rondom de locatie beslaat.

**31 / 40**
De benodigde beheersmaatregel om een middel te beveiligen, is afhankelijk van het middel.

Wat is de **geschiktste** manier om een middel te beveiligen?

**A)** Een formulier beveiligen door het te laten invullen en ondertekenen
**B)** Een laptop beveiligen door deze aan één gebruiker toe te wijzen
**C)** Een USB-stick beveiligen door middel van encryptie
**D)** Een internetverbinding beveiligen met een back-up

**A)** Incorrect. Het archiveren van een vel papier met informatie is geen geschikte beheersmaatregel.
**B)** Incorrect. Het is natuurlijk beter als een laptop slechts door één persoon wordt gebruikt, maar dit is niet de geschiktste optie. Gebruikersaccountbeheer en wachtwoordcontrole zijn betere beheersmaatregelen.
**C)** Correct. Encryptie is een deugdelijke beheersmaatregel om USB-sticks te beveiligen. Veel organisaties gebruiken deze beheersmaatregel, ongeacht de classificatie van de informatie op een USB-stick. (Literatuur: A, hoofdstuk 8.12)
**D)** Incorrect. Het gebruik van back-ups is niet de beste, directe manier om internetverbindingen te beveiligen.

**32 / 40**
Welke beheersmaatregel voor informatiebeveiliging draagt bij aan de ontwikkeling van systemen waarin informatiebeveiliging voorop staat?

**A)** Redundantie van de servers waarborgen
**B)** Fysieke beheersmaatregelen voor toegang implementeren
**C)** Een antecedentenonderzoek van personeel uitvoeren
**D)** Gebruikmaken van dataclassificatie voor informatiemiddelen

**A)** Correct. Serverredundantie is een beheersmaatregel die tijdens de ontwikkeling van een systeem moet worden overwogen. (Literatuur: A, hoofdstuk 8.14)
**B)** Incorrect. Dit is een deugdelijke beheersmaatregel om informatiebeveiliging te verbeteren, maar deze staat los van de systeemontwikkeling.
**C)** Incorrect. Dit is een deugdelijke beheersmaatregel om informatiebeveiliging te verbeteren, maar deze staat los van de systeemontwikkeling.
**D)** Incorrect. Dit is een deugdelijke beheersmaatregel om informatiebeveiliging te verbeteren, maar deze staat los van de systeemontwikkeling.

**33 / 40**
Het beleid van een organisatie wordt gewijzigd. Medewerkers mogen voortaan ook thuiswerken.

Welke beheersmaatregel moet nu worden ingevoerd?

**A)** V-LAN's maken om het bedrijfsnetwerk te segmenteren
**B)** De informatie op het bedrijfsnetwerk versleutelen
**C)** Firewalls installeren in het bedrijfsnetwerk
**D)** Een VPN gebruiken om verbinding te maken met het bedrijfsnetwerk

**A)** Incorrect. Netwerksegmentering om vertrouwelijkheid en functiescheiding te waarborgen zou al moeten worden toegepast. Deze hebben niet specifiek betrekking op wijzigingen in het thuiswerkbeleid.
**B)** Incorrect. Encryptie is onmisbaar om informatie te beschermen, maar heeft niet specifiek betrekking op het thuiswerken van medewerkers.
**C)** Incorrect. Firewalls tussen het bedrijfsnetwerk en de buitenwereld zijn belangrijk, maar zouden al aanwezig moeten zijn. Bovendien bieden firewalls geen directe bescherming van externe verbindingen.
**D)** Correct. Het gebruik van VPN's is een beheersmaatregel die moet worden ingevoerd wanneer medewerkers thuis mogen werken. (Literatuur: A, hoofdstuk 8.2)

**34 / 40**
De medewerkers van een organisatie werken op laptops die worden beschermd door asymmetrische cryptografie. Alle consultants gebruiken hetzelfde sleutelpaar, zodat het management van de sleutels betaalbaar blijft.

Zodra bepaalde informatie wordt beschadigd, moeten er nieuwe sleutels worden verstrekt.

In welk geval moeten er nieuwe sleutels worden verstrekt?

**A)** Wanneer de persoonlijke sleutel bekend wordt
**B)** Wanneer de openbare sleutel bekend wordt
**C)** Wanneer de Public Key Infrastructure (PKI) bekend wordt

**A)** Correct. Bij asymmetrische encryptie is het belangrijk om de persoonlijke sleutel privé te houden. De openbare sleutel mag bekend zijn. (Literatuur: A, hoofdstuk 8.24.5)
**B)** Incorrect. De hele wereld mag toegang hebben tot de openbare sleutel. De persoonlijke sleutel moet geheim blijven om de integriteit en beschikbaarheid van informatie te waarborgen.
**C)** Incorrect. PKI wordt gebruikt om sleutels voor asymmetrische encryptiesystemen uit te wisselen.

**35 / 40**
Welke vorm van beveiliging biedt een Public Key Infrastructure (PKI)?

**A)** Een PKI zorgt dat er regelmatig back-ups van bedrijfsdata worden gemaakt.
**B)** Een PKI toont klanten dat een online bedrijf veilig is.
**C)** Een PKI controleert welke persoon of welk systeem bij een specifieke openbare sleutel hoort.

**A)** Incorrect. Een PKI zorgt niet dat er back-ups worden gemaakt.
**B)** Incorrect. Een PKI garandeert welke persoon of welk systeem bij een specifieke openbare sleutel hoort.
**C)** Correct. Een kenmerk van een PKI is dat deze, dankzij overeenkomsten, procedures en een organisatiestructuur, garanties biedt over welke persoon of welk systeem bij een specifieke openbare sleutel hoort. (Literatuur: A, Hoofdstuk 8.24.6)

**36 / 40**
Welke vorm van malware is een programma dat, behalve de functie die het ogenschijnlijk uitvoert, opzettelijk secundaire activiteiten verricht?

**A)** Logic bomb
**B)** Spyware
**C)** Trojan
**D)** Worm

**A)** Incorrect. Een logic bomb is een stukje code dat is ingebouwd in een softwaresysteem. Deze code voert vervolgens een functie uit wanneer er aan specifieke voorwaarden wordt voldaan. Een logic bomb wordt lang niet altijd gebruikt voor kwaadwillige doeleinden. Het voert niet altijd secundaire activiteiten uit.
**B)** Incorrect. Spyware is een computerprogramma dat informatie verzamelt op de computer van de gebruiker en deze informatie naar een andere partij verzendt.
**C)** Correct. Een trojan is een programma dat, naast de functie die het ogenschijnlijk uitvoert, opzettelijk secundaire activiteiten verricht die niet worden opgemerkt door de computergebruiker. Hierdoor kan de integriteit van het geïnfecteerde systeem worden aangetast. (Literatuur: A, hoofdstuk 8.7.2)
**D)** Incorrect. Een worm creëert een netwerk van geïnfecteerde computers door zichzelf te vermenigvuldigen.

**37 / 40**
Welke vorm van malware creëert een netwerk van geïnfecteerde computers door zichzelf te vermenigvuldigen?

**A)** Logic bomb
**B)** Spyware
**C)** Trojan
**D)** Worm

**A)** Incorrect. Een logic bomb is een stukje code dat is ingebouwd in een softwaresysteem. Deze code voert vervolgens een functie uit wanneer er aan specifieke voorwaarden wordt voldaan. Een logic bomb wordt lang niet altijd gebruikt voor kwaadwillige doeleinden.
**B)** Incorrect. Spyware is een computerprogramma dat informatie verzamelt op de computer van de gebruiker en deze informatie naar een andere partij verzendt.
**C)** Incorrect. Een trojan is een programma dat, naast de functie die het ogenschijnlijk uitvoert, opzettelijk secundaire activiteiten verricht die niet worden opgemerkt door de computergebruiker. Hierdoor kan de integriteit van het geïnfecteerde systeem worden aangetast.
**D)** Correct. Dit is wat een worm doet. (Literatuur: A, hoofdstuk 8.7)

**38 / 40**
Welk wettelijk of regelgevend besluit met betrekking tot informatiebeveiliging kan aan alle organisaties worden opgelegd?

**A)** Algemene verordening gegevensbescherming (AVG)
**B)** Intellectueel eigendomsrecht
**C)** ISO/IEC 27001
**D)** ISO/IEC 27002

**A)** Correct. Alle organisaties moeten een beleid en procedures voor de bescherming van persoonsgegevens hebben en iedereen die persoonsgegevens verwerkt, zou hiermee bekend moeten zijn. (Literatuur: A, hoofdstuk 5.33)
**B)** Incorrect. Deze regelgeving heeft geen betrekking op informatiebeveiliging door organisaties.
**C)** Incorrect. Dit is een norm met richtlijnen voor organisaties om hun informatiebeveiligingsproces op te zetten.
**D)** Incorrect. Deze norm, ook wel 'Informatiebeveiliging, cyberbeveiliging en privacybescherming - Beheersmaatregelen voor informatiebeveiliging' genoemd, bevat richtlijnen voor een informatiebeveiligingsbeleid en bijbehorende beheersmaatregelen.

**39 / 40**
Welke ISO-norm is gericht op de implementatie van beheersmaatregelen voor informatiebeveiliging?

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

**A)** Incorrect. Dit is de algemene inleiding in de reeks ISO/IEC 27000-normen.
**B)** Incorrect. Dit is de norm met vereisten voor een managementsysteem voor informatiebeveiliging (ISMS).
**C)** Correct. Dit is de norm waarin beheersmaatregelen voor informatiebeveiliging worden beschreven met adviezen voor de implementatie ervan. (Literatuur A, hoofdstuk 4.12)
**D)** Incorrect. ISO/IEC 27005 is gericht op risicomanagement binnen informatiebeveiliging.

**40 / 40**
De normen van welke organisatie worden het **meest** gebruikt in Europa?

**A)** American National Standards Institute (ANSI)
**B)** Internationale Organisatie voor Standaardisatie (ISO)
**C)** National Institute of Standards and Technology (NIST)

**A)** Incorrect. De ANSI-normen worden vooral gebruikt in de Verenigde Staten.
**B)** Correct. In Europa worden de ISO-normen het meest gebruikt. (Literatuur: A, hoofdstuk 5.36)
**C)** Incorrect. De NIST-norm wordt vooral gebruikt in de Verenigde Staten.

# Evaluatie

De juiste antwoorden op de vragen in dit voorbeeldexamen staan in onderstaande tabel.

| Vraag | Antwoord | Vraag | Antwoord |
|---|---|---|---|
| **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 |


## Contact EXIN

www.exin.com