EXIN Information Security Management ISO/IEC 27001

FOUNDATION

Certified by EXIN

Voorbeeldexamen

Editie 201804

Inhoud

Introductie

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

Dit voorbeeldexamen 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. Bij 26 punten of meer bent u geslaagd.

De beschikbare tijd is 60 minuten.

Veel succes!

Voorbeeldexamen

1 / 40
Wat is de relatie tussen gegevens en informatie?

A. Gegevens zijn gestructureerde informatie.
B. Informatie is de zinvolle betekenis en waarde die aan een verzameling gegevens wordt toegekend.

2 / 40
Een administratiekantoor moet voor het afsluiten van een brandverzekering inventariseren wat de waarde is van de gegevens die ze beheert.

Welke factor is **niet** van belang voor het bepalen van de waarde van gegevens voor een organisatie?

A. de inhoudelijke aspecten van gegevens
B. de mate van herstelbaarheid waarin ontbrekende, incomplete of onjuiste gegevens hersteld kunnen worden
C. de onmisbaarheid van gegevens voor de bedrijfsprocessen
D. het belang van de bedrijfsprocessen die gebruik maken van de gegevens

3 / 40
Een hacker verschaft zich toegang tot een webserver en kan een bestand met creditcardgegevens op de server bekijken.

Welk van de principes beschikbaarheid, integriteit, vertrouwelijkheid (BIV) van het creditcardbestand wordt daarmee geschonden?

A. Beschikbaarheid
B. Vertrouwelijkheid
C. Integriteit

4 / 40
In de organisatie waar u werkt, staat een netwerkprinter op de gang. Veel medewerkers halen hun afdrukken niet tijdig op en laten ze liggen.

Wat is het gevolg voor de betrouwbaarheid van de informatie?

A. De integriteit van de gegevens is niet meer gewaarborgd.
B. De beschikbaarheid van de gegevens is niet meer gewaarborgd.
C. De vertrouwelijkheid van de gegevens is niet meer gewaarborgd.

5 / 40
Een goed uitgevoerde risicoanalyse levert veel bruikbare informatie op. Daarbij zijn vier hoofddoelen te onderscheiden.

Wat hoort niet bij de vier hoofddoelen van een risicoanalyse?

A. het identificeren van de waarde van bedrijfsmiddelen.
B. het nemen van maatregelen
C. het vinden van een evenwicht tussen de kosten van een incident en de kosten van een beveiligingsmaatregel
D. het vaststellen van relevante kwetsbaarheden en bedreigingen

6 / 40
Een administratiekantoor gaat inventariseren aan welke gevaren ze blootstaat.

Hoe wordt een mogelijke gebeurtenis genoemd die een verstorende invloed kan hebben op de betrouwbaarheid van informatie?

A. afhankelijkheid
B. dreiging
C. kwetsbaarheid
D. risico

7 / 40
Wat is het doel van risicomanagement?

A. De kans bepalen dat een bepaald risico zich manifesteert.
B. De schade bepalen van mogelijke beveiligingsincidenten.
C. In kaart brengen van de bedreigingen waaraan IT objecten bloot staan.
D. Met behulp van maatregelen risico's tot een aanvaardbaar niveau terugbrengen.

8 / 40
U bent een paar jaar geleden begonnen met uw bedrijf en dit is inmiddels flink gegroeid, van 1 naar 20 medewerkers. Uw bedrijfsinformatie wordt steeds meer waard en de tijd dat u alles zelf onder controle had is voorbij. U weet dat u maatregelen moet gaan nemen, maar welke? U schakelt een externe deskundige in en die adviseert u te beginnen met een kwalitatieve risicoanalyse.

Wat is een kwalitatieve risicoanalyse?

A. Een kwalitatieve risicoanalyse volgt een nauwkeurige statistische kansberekening om later exacte schades te kunnen berekenen.
B. Een kwalitatieve risicoanalyse gaat uit van scenario's en situaties en levert een subjectief bedreigingsgevoel op.

9 / 40
In een regiokantoor van Verzekeringskantoor Euregio is brand geweest. De brandweer was vrij snel ter plekke en kon met blussen voorkomen dat het volledige pand uitbrandde. De server is echter verbrand. De back-up tapes die in een andere ruimte lagen zijn gesmolten. Helaas waren ook veel andere documenten niet te redden.

Wat is een voorbeeld van indirecte schade van deze brand?

A. gesmolten back-up tapes
B. verbrande computersystemen
C. verbrande documenten
D. waterschade door bluswerkzaamheden

10 / 40
U bent eigenaar van de koeriersdienst SpeeDelivery. U hebt een risicoanalyse gedaan en wilt nu uw risicostrategie gaan bepalen. U besluit voor de grote risico's maatregelen te treffen, voor de kleine risico's niet.

Hoe wordt deze strategie genoemd?

A. risicodragend
B. risicomijdend
C. risiconeutraal

11 / 40
Wat is een voorbeeld van een menselijke dreiging?

A. Een USB-stick brengt een virus over op het netwerk.
B. In de serverruimte ligt teveel stof.
C. Lekkage veroorzaakt de uitval van de stroomvoorziening.

12 / 40
Wat is een voorbeeld van een menselijke dreiging?

A. blikseminslag
B. brand
C. phishing

13 / 40
U werkt op het directiesecretariaat van een grote onderneming. U ontvangt een telefoontje van iemand die zegt van de Helpdesk te zijn. Hij vraagt om uw wachtwoord.

Om welk soort dreiging gaat het hier?

A. natuurlijke dreiging
B. organisatorische dreiging
C. Social Engineering

14 / 40

In een lokale vestiging van een zorgverzekeraar breekt brand uit. De medewerkers worden overgebracht naar vestigingen in naburige plaatsen zodat zij hun werkzaamheden kunnen voortzetten.

Waar wordt het uitvoeren van een dergelijke uitwijk in de incidentcyclus geplaatst?

A. tussen bedreiging en incident
B. tussen herstel en bedreiging
C. tussen schade en herstel
D. tussen incident en schade

15 / 40
Informatie kent een aantal betrouwbaarheidsaspecten.
Die betrouwbaarheid wordt voortdurend bedreigd. Voorbeelden van dreigingen zijn: een kabel komt los te liggen, iemand kan per ongeluk gegevens wijzigen, gegevens worden privé gebruikt of ze worden vervalst.

Welke van deze voorbeelden is een bedreiging van het aspect integriteit?

A. een losliggende kabel
B. per ongeluk wissen van gegevens
C. privégebruik van gegevens

16 / 40
Een medewerker ontkent een bepaald bericht te hebben verstuurd.

Welk betrouwbaarheidsaspect van informatie is hier in gevaar?

A. beschikbaarheid
B. correctheid
C. integriteit
D. vertrouwelijkheid

17 / 40
Hoe wordt het doel van informatiebeveiligingsbeleid omschreven?

A. het analyseren van risico's en het zoeken van tegenmaatregelen
B. het bieden van een richting en ondersteuning aan het management ten behoeve van informatiebeveiliging
C. het concreet maken van het beveiligingsplan door er invulling aan te geven
D. het verschaffen van inzicht in dreigingen en de mogelijke gevolgen

18 / 40
Een beveiligingsincident met betrekking tot een webserver wordt gemeld aan een helpdeskmedewerker. Zijn collega heeft meer ervaring met webservers, dus hij draagt de zaak aan haar over.

Welke term beschrijft deze overdracht?

A. Functionele escalatie
B. Hiërarchische escalatie

19 / 40
Een medewerkster van Verzekeringskantoor Euregio ontdekt dat de einddatum van een polis is gewijzigd terwijl zij de enige is die de bevoegdheid heeft dit te doen. Ze meldt dit beveiligingsincident bij de Helpdesk. De Helpdeskmedewerker registreert de volgende informatie over het incident:
• datum en tijd
• omschrijving van het incident
• de mogelijke gevolgen van het incident

Welke belangrijke informatie over het incident mist hier?

A. de melder van het incident
B. de naam van het softwarepakket
C. het PC nummer
D. wie is nog meer op de hoogte

20 / 40
In de incidentcyclus worden achtereenvolgens vier stappen onderscheiden.

Welke stap volgt na Incident?

A. Bedreiging
B. Schade
C. Herstel

21 / 40
Welke maatregel is een preventieve maatregel?

A. een logging-systeem dat er voor zorgt dat wijzigingen in een systeem terug gevonden kunnen worden
B. het afsluiten van al het internetverkeer nadat een hacker toegang tot de bedrijfssystemen heeft gekregen
C. het in een kluis leggen van gevoelige informatie

22 / 40
Wat is, in geval van brand, een repressieve maatregel?

A. een brandverzekering afsluiten
B. een brand blussen nadat deze is gedetecteerd door een brandmelder
C. schade ten gevolge van de brand herstellen

23 / 40
Wat is het doel van het classificeren van informatie?

A. een handleiding maken over hoe om te gaan met mobiele apparatuur
B. een merkteken aanbrengen zodat de informatie beter herkend wordt
C. het indelen van informatie naar gevoeligheid

24 / 40
Wie is bevoegd de classificatie van een document te wijzigen?

A. de auteur van het document
B. de beheerder van het document
C. de eigenaar van het document
D. de manager van de eigenaar van het document

25 / 40
De toegang tot de computerruimte wordt afgesloten met een paslezer. Alleen de afdeling Systeembeheer heeft een pasje.

Welk type beveiligingsmaatregel is dit?

A. een correctieve beveiligingsmaatregel
B. een fysieke beveiligingsmaatregel
C. een logische beveiligingsmaatregel
D. een repressieve beveiligingsmaatregel

26 / 40
Voor de toegang tot streng beveiligde gebieden is sterke authenticatie nodig. Bij sterke authenticatie wordt de identiteit van een persoon op drie aspecten gecontroleerd.

Welk aspect wordt gecontroleerd als we een toegangspas moeten tonen?

A. iets dat je bent
B. iets dat je hebt
C. iets dat je weet

27 / 40
Bij fysieke beveiliging kunnen meerdere zones (beschermingsringen) worden onderscheiden, waarin verschillende maatregelen kunnen worden genomen.

Wat is geen beschermingsring?

A. Gebouw
B. Middenring
C. Object
D. Buitenring

28 / 40
Welke bedreiging komt voort uit het ontbreken van een fysieke maatregel?

A. Een gebruiker kan bestanden inzien van een andere gebruiker.
B. Een server valt uit door oververhitting.
C. Een vertrouwelijk document blijft bij de printer liggen en wordt gelezen door een onbevoegde.
D. Indringers kunnen ongehinderd het computernetwerk binnendringen.

29 / 40
Welke beveiligingsmaatregel is een technische maatregel?

A. een eigenaar aan informatie toewijzen
B. encryptie van bestanden
C. vastleggen wat met e-mailen wel en niet mag
D. wachtwoorden van systeembeheer in de kluis bewaren

30 / 40
De back-ups van de centrale server worden bewaard in dezelfde afgesloten ruimte als de server.

Welk risico loopt de organisatie?

A. Als de server crasht, duurt het lang voordat de systemen weer beschikbaar zijn.
B. Bij brand is het onmogelijk de systemen weer in oude staat te herstellen.
C. Niemand is verantwoordelijk voor de back-ups.
D. Onbevoegden hebben eenvoudig toegang tot de back-ups.

31 / 40
Welke kwaadaardige software bouwt een netwerk op van besmette computers?

A. Logic Bomb
B. Stormworm of Botnet
C. Trojan
D. Spyware

32 / 40
De beveiligingsmedewerker van een bedrijf ontdekt kwaadaardige software op het werkstation van één van de medewerkers. De kwaadaardige software is geïnstalleerd na een doelgerichte phishing-aanval.

Welke maatregel kan het beste worden genomen om dergelijke incidenten in de toekomst te voorkomen?

A. MAC-technologie implementeren
B. een bewustwordingscampagne starten
C. de firewallregels updaten
D. de code van het spamfilter updaten

33 / 40
U werkt op de IT afdeling van een middelgroot bedrijf. Vertrouwelijke informatie uit uw bedrijf is meerdere malen in verkeerde handen gekomen. Dit levert veel imagoschade op. U krijgt het verzoek organisatorische beveiligingsmaatregelen voor de laptops van uw bedrijf voor te stellen.

Welke stap zou als eerste moeten worden gezet?

A. beleid opstellen ten aanzien van mobiele gegevensdragers (PDA's, laptops, smartphones, USB-sticks)
B. bewakers aannemen
C. de harde schijven van laptops en USB-sticks versleutelen
D. inrichten van toegangscontrolebeleid

34 / 40
Hoe heet het systeem waarmee de samenhang van informatiebeveiliging in de organisatie wordt gewaarborgd?

A. Information Security Management System (ISMS)
B. Rootkit
C. Voorschrift Informatie Rijksoverheid – Bijzondere Informatie (VIR-BI)

35 / 40
Hoe heet het 'vaststellen of iemands identiteit juist is'?

A. Authenticatie
B. Autorisatie
C. Identificatie

36 / 40
Waarom is het nodig een calamiteitenplan actueel te houden en regelmatig te testen?

A. om altijd te beschikken over recente back-ups, die zich buiten het kantoor bevinden
B. om normale dagelijks optredende storingen het hoofd te kunnen bieden
C. omdat anders bij een ingrijpende verstoring de getroffen maatregelen en incident-procedures te kort schieten of verouderd blijken
D. omdat de Wet Bescherming Persoonsgegevens (WBP) dit voorschrijft

37 / 40
Op grond van welke wetgeving kan iemand om inzage verzoeken in de gegevens die van hem of haar zijn geregistreerd?

A. de archiefwet
B. de wet bescherming persoonsgegevens
C. de wet computercriminaliteit
D. de wet openbaarheid van bestuur

38 / 40
Welke wet- en regelgeving is opgelegd aan alle organisaties en gerelateerd aan informatiebeveiliging?

A. Intellectueel Eigendomsrecht
B. ISO/IEC 27001
C. ISO/IEC 27002
D. Wet Bescherming Persoonsgegevens (WBP)

39 / 40
U bent eigenaar van koeriersdienst SpeeDelivery. U hebt een paar mensen in dienst die, in afwachting van een bezorgopdracht, andere karweitjes kunnen doen. U merkt echter dat ze die tijd gebruiken om hun privémail te behandelen en op internet surfen.

Op welke wijze kan het gebruik van de internet en e-mailvoorzieningen juridisch gezien het beste worden gereguleerd?

A. een applicatie installeren waarmee bepaalde websites niet meer toegankelijk zijn en die bijlagen in e-mails filtert
B. een gedragscode voor internet- en e-mailgebruik waarin de rechten en plichten van zowel de werkgever als de medewerkers zijn vastgelegd
C. een privacyreglement invoeren
D. een virusscanner installeren

40 / 40

Onder welke voorwaarde mag de werkgever controleren hoe de Internet en e-mailvoorzieningen op het werk, bijvoorbeeld voor privédoeleinden, worden gebruikt?

A. De werkgever mag dit controleren als de werknemer na iedere controle wordt geïnformeerd.
B. De werkgever mag dit controleren als de werknemers weten dat dit kan gebeuren.
C. De werkgever mag dit controleren als ook een firewall is geïnstalleerd.

Antwoordsleutel

1 / 40
Wat is de relatie tussen gegevens en informatie?

A. Gegevens zijn gestructureerde informatie.
B. Informatie is de zinvolle betekenis en waarde die aan een verzameling gegevens wordt toegekend.

A. Onjuist. Informatie is de betekenis die aan gegevens toegekend wordt.
B. Juist. Informatie is gegevens die in een bepaalde context betekenis hebben voor zijn ontvanger. (Hoofdstuk 3 en §4.10)

2 / 40
Een administratiekantoor moet voor het afsluiten van een brandverzekering inventariseren wat de waarde is van de gegevens die ze beheert.

Welke factor is **niet** van belang voor het bepalen van de waarde van gegevens voor een organisatie?

A. de inhoudelijke aspecten van gegevens
B. de mate van herstelbaarheid waarin ontbrekende, incomplete of onjuiste gegevens hersteld kunnen worden
C. de onmisbaarheid van gegevens voor de bedrijfsprocessen
D. het belang van de bedrijfsprocessen die gebruik maken van de gegevens

A. Juist. De inhoudelijke aspecten van gegevens bepalen niet de waarde ervan. (Hoofdstuk 4)
B. Onjuist. Ontbrekende, incomplete of onjuiste gegevens die eenvoudig hersteld kunnen worden zijn minder waardevol dan gegevens die niet of nauwelijks hersteld kunnen worden.
C. Onjuist. Onmisbaarheid van gegevens voor bedrijfsprocessen bepaalt mede de waarde.
D. Onjuist. Gegevens die in belangrijke bedrijfsprocessen gebruikt worden zijn daardoor waardevol.

3 / 40
Een hacker verschaft zich toegang tot een webserver en kan een bestand met creditcardgegevens op de server bekijken.

Welk van de principes beschikbaarheid, integriteit, vertrouwelijkheid (BIV) van het creditcardbestand wordt daarmee geschonden?

A. Beschikbaarheid
B. Vertrouwelijkheid
C. Integriteit

A. Onjuist. De hacker heeft het bestand niet verwijderd of de toegang door bevoegde entiteiten geblokkeerd. De beschikbaarheid is dus niet in het geding.
B. Juist. De hacker kon het bestand lezen (vertrouwelijkheid). (Hoofdstuk 3)
C. Onjuist. Er is geen informatie gewijzigd in het creditcardbestand, dus de integriteit van het bestand is niet geschonden.

4 / 40
In de organisatie waar u werkt, staat een netwerkprinter op de gang. Veel medewerkers halen hun afdrukken niet tijdig op en laten ze liggen.

Wat is het gevolg voor de betrouwbaarheid van de informatie?

A. De integriteit van de gegevens is niet meer gewaarborgd.
B. De beschikbaarheid van de gegevens is niet meer gewaarborgd.
C. De vertrouwelijkheid van de gegevens is niet meer gewaarborgd.

A. Onjuist. De gegevens op de afdrukken zijn nog steeds integer, ze staan immers op papier.
B. Onjuist. De gegevens zijn nog steeds beschikbaar op het systeem dat gebruikt is om het document te maken en te printen.
C. Juist. De gegevens kunnen in onbevoegde handen vallen en ingezien worden door anderen. (Hoofdstuk 3)

5 / 40
Een goed uitgevoerde risicoanalyse levert veel bruikbare informatie op. Daarbij zijn vier hoofddoelen te onderscheiden.

Wat hoort niet bij de vier hoofddoelen van een risicoanalyse?

A. het identificeren van de waarde van bedrijfsmiddelen
B. het nemen van maatregelen
C. het vinden van een evenwicht tussen de kosten van een incident en de kosten van een beveiligingsmaatregel.
D. het vaststellen van relevante kwetsbaarheden en bedreigingen

A. Onjuist. De middelen en de waarde die daaraan toegekend wordt, vormen de basis om de schade te bepalen in de risicoafweging.
B. Juist. Dit is geen hoofddoel van een risicoanalyse. Maatregelen worden genomen als uit een risicoanalyse is gebleken voor welke risico's beveiligingsmaatregelen moeten worden getroffen. (Hoofdstuk 3)
C. Onjuist. Het in balans brengen van de kosten van een incident en de kosten van een maatregel is een hoofddoel van een risicoanalyse. Vaak is dit ook de moeilijkste stap in het uitvoeren van een risicoanalyse.
D. Onjuist. De basis voor elke goede risicoanalyse is het identificeren van de relevante dreigingen en kwetsbaarheden. Als deze stap niet wordt uitgevoerd kan het zijn dat er onnodige risico's onderkend worden of dat er risico's niet meegenomen worden.

6 / 40
Een administratiekantoor gaat inventariseren aan welke gevaren ze blootstaat.

Hoe wordt een mogelijke gebeurtenis genoemd die een verstorende invloed kan hebben op de betrouwbaarheid van informatie?

A. afhankelijkheid
B. dreiging
C. kwetsbaarheid
D. risico

A. Onjuist. Een afhankelijkheid is geen gebeurtenis.
B. Juist. Een dreiging is een mogelijke gebeurtenis die een verstorende invloed kan hebben op de betrouwbaarheid van informatie. (Hoofdstuk 3)
C. Onjuist. Een kwetsbaarheid is de mate waarin een object van de informatievoorziening gevoelig is voor een bedreiging.
D. Onjuist. Een risico is de gemiddeld verwachte schade over een bepaalde tijdsperiode doordat één of meer dreigingen leiden tot verstoring(en).

7 / 40
Wat is het doel van risicomanagement?

A. De kans bepalen dat een bepaald risico zich manifesteert.
B. De schade bepalen van mogelijke beveiligingsincidenten.
C. In kaart brengen van de dreigingen waaraan IT objecten bloot staan.
D. Met behulp van maatregelen risico's tot een aanvaardbaar niveau terugbrengen.

A. Onjuist. Dit is een onderdeel van risicoanalyse
B. Onjuist. Dit is een onderdeel van risicoanalyse.
C. Onjuist. Dit is een onderdeel van risicoanalyse.
D. Juist. Het doel van risicomanagement is risico's tot een aanvaardbaar niveau terugbrengen. (Hoofdstuk 3)

8 / 40
U bent een paar jaar geleden begonnen met uw bedrijf en dit is inmiddels flink gegroeid, van 1 naar 20 medewerkers. Uw bedrijfsinformatie wordt steeds meer waard en de tijd dat u alles zelf onder controle had is voorbij. U weet dat u maatregelen moet gaan nemen, maar welke? U schakelt een externe deskundige in en die adviseert u te beginnen met een kwalitatieve risicoanalyse.

Wat is een kwalitatieve risicoanalyse?

A. Een kwalitatieve risicoanalyse volgt een nauwkeurige statistische kansberekening om later exacte schades te kunnen berekenen.
B. Een kwalitatieve risicoanalyse gaat uit van scenario's en situaties en levert een subjectief dreigingsgevoel op.

A. Onjuist. Exacte waarden worden in een kwantitatieve risicoanalyse berekend, niet in een kwalitatieve risicoanalyse.
B. Juist. Een kwalitatieve risicoanalyse inventariseert het gevoel over dreigingen. (Hoofdstuk 3)

9 / 40
In een regiokantoor van Verzekeringskantoor Euregio is brand geweest. De brandweer was vrij snel ter plekke en kon met blussen voorkomen dat het volledige pand uitbrandde. De server is echter verbrand. De back-up tapes die in een andere ruimte lagen zijn gesmolten. Helaas waren ook veel andere documenten niet te redden.

Wat is een voorbeeld van indirecte schade van deze brand?

A. gesmolten back-up tapes
B. verbrande computersystemen
C. verbrande documenten
D. waterschade door bluswerkzaamheden

A. Onjuist. Gesmolten back-uptapes zijn een direct gevolg van de brand.
B. Onjuist. Verbrande computersystemen zijn een direct gevolg van een brand.
C. Onjuist. Verbrande documenten zijn een direct gevolg van een brand.
D. Juist. Waterschade door bluswerkzaamheden is een voorbeeld van indirecte schade. Het blussen van een brand is er op gericht de gevolgen zoveel mogelijk te beperken. Dit kan neveneffecten hebben. Zo kan door blussen aanvullende schade ontstaan. (Hoofdstuk 3)

10 / 40
U bent eigenaar van de koeriersdienst SpeeDelivery. U hebt een risicoanalyse gedaan en wilt nu uw risicostrategie gaan bepalen. U besluit voor de grote risico's maatregelen te treffen, voor de kleine risico's niet.

Hoe wordt deze strategie genoemd?

A. risicodragend
B. risicomijdend
C. risiconeutraal

A. Juist. Dit betekent dat bepaalde risico's geaccepteerd worden. (Hoofdstuk 3)
B. Onjuist. Dit betekent dat maatregelen genomen worden om de bedreiging in zulke mate te neutraliseren, dat het niet langer leidt tot een incident.
C. Onjuist. Dit betekent dat de veiligheidsmaatregelen voorkomen dat de dreigingen zich manifesteren, of de schade tot een minimum beperken.

11 / 40
Wat is een voorbeeld van een menselijke dreiging?

A. Een USB-stick brengt een virus over op het netwerk.
B. In de serverruimte ligt teveel stof.
C. Lekkage veroorzaakt de uitval van de stroomvoorziening.

A. Juist. Een USB-stick wordt altijd door iemand ingebracht dus als hierdoor een virus in het netwerk komt is dit een menselijke dreiging. (Hoofdstuk 3)
B. Onjuist. Stof is een niet-menselijke dreiging.
C. Onjuist. Lekkage is een niet-menselijke dreiging.

12 / 40
Wat is een voorbeeld van een menselijke dreiging?

A. blikseminslag
B. brand
C. phishing

A. Onjuist. Blikseminslag is een voorbeeld van een niet-menselijke dreiging.
B. Onjuist. Brand is een voorbeeld van een niet-menselijke dreiging.
C. Juist. Phishing (het lokken van gebruikers naar valse websites) is een vorm van een menselijke dreiging. (Hoofdstuk 3)

13 / 40
U werkt op het directiesecretariaat van een grote onderneming. U ontvangt een telefoontje van iemand die zegt van de Helpdesk te zijn. Hij vraagt om uw wachtwoord.

Om welk soort dreiging gaat het hier?

A. natuurlijke dreiging
B. organisatorische dreiging
C. Social Engineering

A. Onjuist. Een telefoontje is een menselijke handeling en dat is geen natuurlijke dreiging.
B. Onjuist. Het begrip organisatorische bedreiging is niet gebruikelijk.
C. Juist. Het gebruiken van jargon of namen van medewerkers en hun afdeling geeft de indruk dat een college bedrijfs- en handelsgeheimen probeert te achterhalen. U moet controleren of u wel echt met de helpdesk telefoneert. Een helpdesk medewerker zal nooit naar uw wachtwoord vragen. (Hoofdstuk 3)

14 / 40
In een lokale vestiging van een zorgverzekeraar breekt brand uit. De medewerkers worden overgebracht naar vestigingen in naburige plaatsen zodat zij hun werkzaamheden kunnen voortzetten.

Waar wordt het uitvoeren van een dergelijke uitwijk in de incidentcyclus geplaatst?

A. tussen bedreiging en incident
B. tussen herstel en bedreiging
C. tussen schade en herstel
D. tussen incident en schade

A. Onjuist. Het uitwijken zonder dat er een incident is, is erg kostbaar.
B. Onjuist. Herstel vindt na een eventuele uitwijk plaats.
C. Onjuist. Schade en herstel moeten juist beperkt worden door de uitwijk.
D. Juist. Uitwijk is een repressieve maatregel die in gang gezet wordt om de schade te beperken. (Hoofdstuk 16)

15 / 40
Informatie kent een aantal betrouwbaarheidsaspecten.
Die betrouwbaarheid wordt voortdurend bedreigd. Voorbeelden van dreigingen zijn: een kabel komt los te liggen, iemand kan per ongeluk gegevens wijzigen, gegevens worden privé gebruikt of ze worden vervalst.

Welke van deze voorbeelden is een bedreiging van het aspect integriteit?

A. een losliggende kabel
B. per ongeluk wissen van gegevens
C. privégebruik van gegevens

A. Onjuist. Een losliggende kabel is een bedreiging van de beschikbaarheid van informatie.
B. Juist. Het onbedoeld wijzigen van gegevens is een bedreiging van de integriteit. (Hoofdstuk 3)
C. Onjuist. Het gebruiken van gegevens voor privédoeleinden is een vorm van misbruik en is een bedreiging van de vertrouwelijkheid.

16 / 40
Een medewerker ontkent een bepaald bericht te hebben verstuurd.

Welk betrouwbaarheidsaspect van informatie is hier in gevaar?

A. beschikbaarheid
B. correctheid
C. integriteit
D. vertrouwelijkheid

A. Onjuist. Overbelasting van de infrastructuur is een voorbeeld van een bedreiging m.b.t. het aspect beschikbaarheid.
B. Onjuist. Correctheid is geen betrouwbaarheidsaspect. Het is een kenmerk van het betrouwbaarheidsaspect integriteit.
C. Juist. Het ontkennen van het versturen van een bericht heeft te maken met onweerlegbaarheid en dat is een bedreiging van het aspect integriteit. (Hoofdstuk 3)
D. Onjuist. Misbruik of onthulling van gegevens zijn bedreigingen van het aspect vertrouwelijkheid.

17 / 40
Hoe wordt het doel van informatiebeveiligingsbeleid omschreven?

A. het analyseren van risico's en het zoeken van tegenmaatregelen
B. het bieden van een richting en ondersteuning aan het management ten behoeve van informatiebeveiliging.
C. het concreet maken van het beveiligingsplan door er invulling aan te geven
D. het verschaffen van inzicht in dreigingen en de mogelijke gevolgen

A. Onjuist. Dit is het doel van risicoanalyse en risicomanagement.
B. Juist. Het beveiligingsbeleid biedt richting en ondersteuning aan het management ten behoeve van informatiebeveiliging. (Hoofdstuk 5)
C. Onjuist. Het beveiligingsplan maakt het informatiebeveiligingsbeleid concreet. In het plan staat o.a. welke maatregelen er gekozen zijn, wie verantwoordelijk is voor wat, de richtlijnen voor implementatie van maatregelen etc.
D. Onjuist. Dit is het doel van een bedreigingenanalyse.

18 / 40
Een beveiligingsincident met betrekking tot een webserver wordt gemeld aan een helpdeskmedewerker. Zijn collega heeft meer ervaring met webservers, dus hij draagt de zaak aan haar over.

Welke term beschrijft deze overdracht?

A. Functionele escalatie
B. Hiërarchische escalatie

A. Juist. Als de helpdeskmedewerker het incident niet zelf kan afhandelen, kan het worden gemeld aan iemand met meer ervaring, die het probleem mogelijk wel kan oplossen. Dit heet een functionele (horizontale) escalatie. (Hoofdstuk 16)
B. Onjuist. Dit heet een functionele (horizontale) escalatie. Een hiërarchische escalatie vindt plaats wanneer een taak wordt overgedragen aan iemand met meer bevoegdheden.

19 / 40
Een medewerkster van Verzekeringskantoor Euregio ontdekt dat de einddatum van een polis is gewijzigd terwijl zij de enige is die de bevoegdheid heeft dit te doen. Ze meldt dit beveiligingsincident bij de Helpdesk. De Helpdeskmedewerker registreert de volgende informatie over het incident:
• datum en tijd
• omschrijving van het incident
• de mogelijke gevolgen van het incident

Welke belangrijke informatie over het incident mist hier?

A. de melder van het incident
B. de naam van het softwarepakket
C. het PC nummer
D. wie is nog meer op de hoogte

A. Juist. Bij het melden van een incident moet in ieder geval de naam van de melder worden geregistreerd. (Hoofdstuk 16)
B. Onjuist. Dit is eventueel aanvullende informatie.
C. Onjuist. Dit is eventueel aanvullende informatie
D. Onjuist. Dit is eventueel aanvullende informatie.

20 / 40
In de incidentcyclus worden achtereenvolgens vier stappen onderscheiden.

Welke stap volgt na Incident?

A. Bedreiging
B. Schade
C. Herstel

A. Onjuist. De schade volgt na incident. In de incidentcyclus worden achtereenvolgens onderscheiden: bedreiging, incident, schade, herstel.
B. Juist. In de incidentcyclus worden achtereenvolgens onderscheiden: bedreiging, incident, schade, herstel. (Hoofdstuk 16)
C. Onjuist. De schade volgt na incident. In de incidentcyclus worden achtereenvolgens onderscheiden: bedreiging, incident, schade, herstel.

21 / 40
Welke maatregel is een preventieve maatregel?

A. een logging-systeem dat er voor zorgt dat wijzigingen in een systeem terug gevonden kunnen worden
B. het afsluiten van al het internetverkeer nadat een hacker toegang tot de bedrijfssystemen heeft gekregen
C. het in een kluis leggen van gevoelige informatie

A. Onjuist. Via een logging-systeem kan alleen achteraf, wanneer een incident heeft plaatsgevonden, terug gezocht worden naar wat gebeurd is. Dat is dus een mengeling van detectief (het terugvinden van de oorzaak) en reactief, het reageren op een incident.
B. Onjuist. Het afsluiten van het internetverkeer is een repressieve actie op een incident.
C. Juist. Een kluis is een preventieve maatregel, waarmee je wilt voorkomen dat er iets met de inhoud van de kluis gebeurt. (Hoofdstuk 3)

22 / 40
Wat is, in geval van brand, een repressieve maatregel?

A. een brandverzekering afsluiten
B. een brand blussen nadat deze is gedetecteerd door een brandmelder
C. schade ten gevolge van de brand herstellen

A. Onjuist. Het afsluiten van een verzekering is een risicostrategie en geen maatregel. Door een verzekering af te sluiten kunnen de financiële gevolgen van bijvoorbeeld een brand afgedekt worden.
B. Juist. Een repressieve maatregel is bedoeld om de gevolgen van een incident te stoppen/te beperken. (Hoofdstuk 3)
C. Onjuist. De schade herstellen is een correctieve maatregel. Het minimaliseert niet de schade veroorzaakt door de brand.

23 / 40
Wat is het doel van het classificeren van informatie?

A. een handleiding maken over hoe om te gaan met mobiele apparatuur
B. een merkteken aanbrengen zodat de informatie beter herkend wordt
C. het indelen van informatie naar gevoeligheid

A. Onjuist. Het maken van een handleiding over hoe om te gaan met mobiele apparatuur heeft te maken met het gebruik van bedrijfsmiddelen en niet met de classificatie van informatie.
B. Onjuist. Merking is het aanbrengen van een bijzondere aanduiding, aanvullend op een classificatie. Het doel daarvan is aangeven voor welke speciale doelgroep de informatie bestemd is.
C. Juist. Classificeren is het indelen van informatie naar gevoeligheid. De gevoeligheid van informatie kan verschillen. De te treffen beveiligingsmaatregelen zullen dan ook verschillen. (Hoofdstuk 3 en 8)

24 / 40
Wie is bevoegd de classificatie van een document te wijzigen?

A. de auteur van het document
B. de beheerder van het document
C. de eigenaar van het document
D. de manager van de eigenaar van het document

A. Onjuist. De auteur mag de inhoud maar niet de classificatie wijzigen.
B. Onjuist. De beheerder van het document mag de classificatie niet wijzigen.
C. Juist. De eigenaar mag de classificatie wijzigen. (Hoofdstuk 3 en 8)
D. Onjuist. De manager van de eigenaar heeft hier geen zeggenschap over.

25 / 40
De toegang tot de computerruimte wordt afgesloten met een paslezer. Alleen de afdeling Systeembeheer heeft een pasje.

Welk type beveiligingsmaatregel is dit?

A. een correctieve beveiligingsmaatregel
B. een fysieke beveiligingsmaatregel
C. een logische beveiligingsmaatregel
D. een repressieve beveiligingsmaatregel

A. Onjuist. Een correctieve beveiligingsmaatregel is een herstellende maatregel.
B. Juist. Dit is een fysieke beveiligingsmaatregel. (Hoofdstuk 3 en 11)
C. Onjuist. Een logische beveiligingsmaatregel regelt de toegang tot software en informatie, niet de fysieke toegang tot ruimtes.
D. Onjuist. Een repressieve beveiligingsmaatregel is bedoeld om de gevolgen van een verstoring te minimaliseren.

26 / 40
Voor de toegang tot streng beveiligde gebieden is sterke authenticatie nodig. Bij sterke authenticatie wordt de identiteit van een persoon op drie aspecten gecontroleerd.

Welk aspect wordt gecontroleerd als we een toegangspas moeten tonen?

A. iets dat je bent
B. iets dat je hebt
C. iets dat je weet

A. Onjuist. Een toegangspas is geen voorbeeld van iets dat je bent.
B. Juist. Een toegangspas is iets dat je hebt. (Hoofdstuk 11)
C. Onjuist. Een toegangspas is niet iets dat je weet.

27 / 40
Bij fysieke beveiliging kunnen meerdere zones (beschermingsringen) worden onderscheiden, waarin verschillende maatregelen kunnen worden genomen.

Wat is geen beschermingsring?

A. Gebouw
B. Middenring
C. Object
D. Buitenring

A. Onjuist. Het gebouw is een geldige zone in verband met de toegang tot de locatie.
B. Juist. Beschermingsringen zijn: Buitenring (gebied rond de locatie), Gebouw (toegang tot de locatie), Werkruimte (de ruimten binnen de locatie, ofwel de 'binnenste ring'), Object (de asset die moet worden beschermd). Een middenring bestaat niet. (Hoofdstuk 11)
C. Onjuist. Het object is een geldige zone in verband met de bedrijfsmiddelen die moet worden beschermd.
D. Onjuist. De buitenring is een geldige zone in verband met het gebied rondom de locatie.

28 / 40
Welke bedreiging komt voort uit het ontbreken van een fysieke maatregel?

A. Een gebruiker kan bestanden inzien van een andere gebruiker.
B. Een server valt uit door oververhitting.
C. Een vertrouwelijk document blijft bij de printer liggen en wordt gelezen door een onbevoegde.
D. Indringers kunnen ongehinderd het computernetwerk binnendringen.

A. Onjuist. Logisch toegangsbeheer voorkomt dat een gebruiker ongeautoriseerd bestanden van anderen kan lezen. Logisch toegangsbeheer is een technische maatregel.
B. Juist. Klimaatbeheersing (het regelen van de temperatuur en luchtvochtigheid) in serverruimten is een fysieke maatregel. (Hoofdstuk 11)
C. Onjuist. Door beleid te maken en dit na te leven, had voorkomen kunnen worden dat vertrouwelijke documenten te lang bij de printer blijven liggen. Het maken en naleven van beleid is een organisatorische maatregel.
D. Onjuist. Het weren van indringers op het computernetwerk is een technische maatregel.

29 / 40
Welke beveiligingsmaatregel is een technische maatregel?

A. een eigenaar aan informatie toewijzen
B. encryptie van bestanden
C. vastleggen wat met e-mailen wel en niet mag
D. wachtwoorden van systeembeheer in de kluis bewaren

A. Onjuist. Een eigenaar aan informatie toewijzen is classificatie en valt onder de organisatorische maatregelen.
B. Juist. Dit is een technische maatregel die voorkomt dat onbevoegden de informatie kunnen lezen. (Hoofdstuk 8)
C. Onjuist. Dit is een organisatorische maatregel, een gedragscode die in het arbeidscontract kan worden vastgelegd.
D. Onjuist. Dit is een organisatorische maatregel.

30 / 40
De back-ups van de centrale server worden bewaard in dezelfde afgesloten ruimte als de server.

Welk risico loopt de organisatie?

A. Als de server crasht, duurt het lang voordat de systemen weer beschikbaar zijn.
B. Bij brand is het onmogelijk de systemen weer in oude staat te herstellen.
C. Niemand is verantwoordelijk voor de back-ups.
D. Onbevoegden hebben eenvoudig toegang tot de back-ups.

A. Onjuist. Dit zou juist een sneller operationeel zijn bevorderen.
B. Juist. De kans dat bij brand de back-up ook verloren gaat, is zeer groot. (Hoofdstuk 11)
C. Onjuist. De verantwoordelijkheid staat los van de plek van bewaring.
D. Onjuist. De computerruimte is afgesloten.

31 / 40
Welke kwaadaardige software bouwt een netwerk op van besmette computers?

A. Logic Bomb
B. Stormworm of Botnet
C. Trojan
D. Spyware

A. Onjuist. Een Logic Bomb is een stukje code die een functie uitvoert wanneer er aan specifieke voorwaarde wordt voldaan. Een Logic Bomb bouwt geen netwerk van besmette computers op.
B. Juist. Stormworm wordt gezien als de malware van de toekomst. De stormworm bouwt een netwerk van besmette computers: een botnet. (Hoofdstuk 12)
C. Onjuist. Een Trojan virus bouwt geen netwerk van besmette computers op.
D. Onjuist. Spyware is een computerprogramma dat informatie verzamelt van de computergebruiker en deze informatie naar een andere partij verzendt.

32 / 40
De beveiligingsmedewerker van een bedrijf ontdekt kwaadaardige software op het werkstation van één van de medewerkers. De kwaadaardige software is geïnstalleerd na een doelgerichte phishing-aanval.

Welke maatregel kan het beste worden genomen om dergelijke incidenten in de toekomst te voorkomen?

A. MAC-technologie implementeren
B. een bewustwordingscampagne starten
C. de firewallregels updaten
D. de code van het spamfilter updaten

A. Onjuist. MAC heeft te maken met toegangscontrole. Het kan niet voorkomen dat een gebruiker wordt overgehaald om een bepaalde actie uit te voeren na een doelgerichte aanval.
B. Juist. De bedreiging die aan de basis ligt van het probleem is de onwetendheid van de gebruiker. Bij dit soort aanvallen wordt de gebruiker overgehaald om bepaalde code uit te voeren die in strijd is met het beleid, zoals het installeren van verdachte software. Door de bewustwording over dergelijke aanvallen te vergroten, zullen dit soort situaties in de toekomst minder vaak voorkomen. (Hoofdstuk 12)
C. Onjuist. De firewall kan eventueel wel het verkeer blokkeren dat wordt gegenereerd door de kwaadaardige software, maar kan niet voorkomen dat de situatie opnieuw optreedt.
D. Onjuist. Dit type aanval maakt niet altijd gebruik van e-mail. De aanvaller kan bijvoorbeeld via sociale media of gewoon per telefoon contact opnemen met het slachtoffer.

33 / 40
U werkt op de IT afdeling van een middelgroot bedrijf. Vertrouwelijke informatie uit uw bedrijf is meerdere malen in verkeerde handen gekomen. Dit levert veel imagoschade op. U krijgt het verzoek organisatorische beveiligingsmaatregelen voor de laptops van uw bedrijf voor te stellen.

Welke stap zou als eerste moeten worden gezet?

A. beleid opstellen ten aanzien van mobiele gegevensdragers (PDA's, laptops, smartphones, USB-sticks)
B. bewakers aannemen
C. de harde schijven van laptops en USB-sticks versleutelen
D. inrichten van toegangscontrolebeleid

A. Juist. Beleid voor het omgaan met mobiele gegevensdragers is een organisatorische maatregel. In deze maatregel kan de beveiliging van laptops dwingend worden opgelegd. De uitvoering van het beleid (versleutelen van de harde schijf) is een technische maatregel. (Hoofdstuk 6)
B. Onjuist. Bewakers aannemen is een technische maatregel die geen effect heeft. Wanneer de gebruiker van de laptop gerechtigd is deze mee naar buiten te nemen blijft het risico van lekken aanwezig.
C. Onjuist. De harde schijven van laptops en USB-sticks versleutelen is een technische maatregel die op basis van een organisatorische maatregel kan worden uitgevoerd.
D. Onjuist. Een toegangscontrolebeleid is organisatorisch, maar regelt alleen de toegang tot gebouwen of tot ICT-systemen.

34 / 40
Hoe heet het systeem waarmee de samenhang van informatiebeveiliging in de organisatie wordt gewaarborgd?

A. Information Security Management System (ISMS)
B. Rootkit
C. Voorschrift Informatie Rijksoverheid – Bijzondere Informatie (VIR-BI)

A. Juist. Het Information Security Management System (ISMS) wordt beschreven in ISO/IEC 27001 en geeft samenhang aan informatiebeveiliging. (Hoofdstuk 3)
B. Onjuist. Een rootkit is kwaadaardige software, meestal gebruikt door een derde partij (meestal een hacker).
C. Onjuist. Voorschrift Informatie Rijksoverheid – Bijzondere Informatie (VIR-BI) is een voorschrift voor de Rijksoverheid met regels voor het omgaan met bijzondere informatie.

35 / 40
Hoe heet het 'vaststellen of iemands identiteit juist is'?

A. Authenticatie
B. Autorisatie
C. Identificatie

A. Juist. Het vaststellen of iemands identiteit juist is heet authenticatie. (Hoofdstuk 9)
B. Onjuist. Als iemand toegangsrechten tot een computer of netwerk krijgt heet dat autorisatie.
C. Onjuist. Identificatie is het kenbaar maken van een identiteit.

36 / 40
Waarom is het nodig een calamiteitenplan actueel te houden en regelmatig te testen?

A. om altijd te beschikken over recente back-ups, die zich buiten het kantoor bevinden
B. om normale dagelijks optredende storingen het hoofd te kunnen bieden
C. omdat anders bij een ingrijpende verstoring de getroffen maatregelen en incident-procedures te kort schieten of verouderd blijken
D. omdat de Wet Bescherming Persoonsgegevens (WBP) dit voorschrijft

A. Onjuist. Dit is een van de technische maatregelen om een systeem te kunnen herstellen.
B. Onjuist. Voor normale storingen zijn de getroffen maatregelen en incidentprocedures voldoende.
C. Juist. Bij een ingrijpende verstoring is een up to date en getest plan vereist. (Hoofdstuk 17)
D. Onjuist. De WBP gaat in op bescherming van persoonsgegevens.

37 / 40
Op grond van welke wetgeving kan iemand om inzage verzoeken in de gegevens die van hem of haar zijn geregistreerd?

A. de archiefwet
B. de wet bescherming persoonsgegevens
C. de wet computercriminaliteit
D. de wet openbaarheid van bestuur

A. Onjuist. De archiefwet regelt het bewaren en vernietigen van archiefbescheiden.
B. Juist. Het inzagerecht is geregeld in de wet bescherming persoonsgegevens. (Hoofdstuk 18)
C. Onjuist. De wet computercriminaliteit is een wijziging op het wetboek van strafrecht en wetboek van strafvordering om strafbare feiten door voortschrijdende informatietechniek beter mogelijk te maken. Een voorbeeld van een nieuw strafbaar feit is computervredebreuk.
D. Onjuist. De wet openbaarheid van bestuur regelt inzage in schriftelijke bestuurlijke stukken. Persoonsgegevens zijn geen bestuurlijke stukken.

38 / 40
Welke wet- en regelgeving is opgelegd aan alle organisaties en gerelateerd aan informatiebeveiliging?

A. Intellectueel Eigendomsrecht
B. ISO/IEC 27001
C. ISO/IEC 27002
D. Wet Bescherming Persoonsgegevens (WBP)

A. Onjuist. Dit recht is niet gerelateerd aan informatiebeveiliging voor organisaties.
B. Onjuist. Dit is een standaard met richtlijnen voor organisaties hoe om te gaan met het opzetten van een informatiebeveiligingsproces.
C. Onjuist. Deze standaard, bevat richtlijnen voor informatiebeveiliging regelgeving en maatregelen.
D. Juist. Alle organisaties zouden een regelgeving en procedures voor de beveiliging van persoonlijke gegevens moeten hebben, die bekend moet zijn bij iedereen die persoonlijke gegevens verwerkt. (Hoofdstuk 18)

39 / 40
U bent eigenaar van koeriersdienst SpeeDelivery. U hebt een paar mensen in dienst die, in afwachting van een bezorgopdracht, andere karweitjes kunnen doen. U merkt echter dat ze die tijd gebruiken om hun privémail te behandelen en op internet surfen.

Op welke wijze kan het gebruik van de internet en e-mailvoorzieningen juridisch gezien het beste worden gereguleerd?

A. een applicatie installeren waarmee bepaalde websites niet meer toegankelijk zijn en die bijlagen in e-mails filtert
B. een gedragscode voor internet- en e-mailgebruik waarin de rechten en plichten van zowel de werkgever als de medewerkers zijn vastgelegd
C. een privacyreglement invoeren
D. een virusscanner installeren

A. Onjuist. Het installeren van de hier bedoelde software reguleert voor een deel wel het gebruik, maar niet de hoeveelheid tijd die voor privédoeleinden gebruikt wordt. Dit is een zuiver technische maatregel.
B. Juist. Met een gedragscode kunnen afspraken met de medewerkers worden gemaakt over de wijze van internet- en mailgebruik. Hierin kan worden vermeld welke soort sites niet bezocht mogen worden en hoeveel tijd voor privégebruik wordt toegestaan, mits het werk er niet onder lijdt. Dit is interne regelgeving. (Hoofdstuk 18)
C. Onjuist. Het invoeren van een privacyreglement legt het gebruik van de persoonsgegevens van medewerkers en/of klanten vast. Dat heeft een andere doelstelling dan het gebruik van internet en e-mail.
D. Onjuist. Een virusscanner controleert inkomende mail, internetconnecties en (externe) gegevensdragers op de aanwezigheid van schadelijke (kwaadaardige) software. Dit reguleert het gebruik van internet en e-mail niet en is bovendien een technische maatregel.

40 / 40
Onder welke voorwaarde mag de werkgever controleren hoe de Internet en e-mailvoorzieningen op het werk, bijvoorbeeld voor privédoeleinden, worden gebruikt?

A. De werkgever mag dit controleren als de werknemer na iedere controle wordt geïnformeerd.
B. De werkgever mag dit controleren als de werknemers weten dat dit kan gebeuren.
C. De werkgever mag dit controleren als ook een firewall is geïnstalleerd.

A. Onjuist. De werknemer hoeft niet na iedere controle geïnformeerd te worden.
B. Juist. Als aan de proportionaliteitseis is voldaan kan een werkgever e-mailverkeer van de werknemer inzien. In de meeste bedrijven in Nederland is het zo geregeld dat de werkgever de werknemer op de hoogte dient te stellen dat dit gedaan wordt. De voorwaarden zoals die gelden in Nederland (en de EU) zijn:
1. Het moet de medewerker duidelijk zijn dat er controles worden of kunnen worden uitgevoerd. (Bijv. door schriftelijke mededeling of passage in contract/arbeidsvoorwaarden)
2. Er moet een gerede verdenking bestaan jegens de medewerker waardoor er sprake is van een gerechtvaardigd doel van de inbreuk. (Vermoeden van fraude of laster)
3. Het inlezen van het e-mailverkeer moet de enige mogelijkheid voor de werkgever zijn om de e-mails in te zien en dus ook de enige mogelijkheid zijn om te verifiëren of de verdenking gerechtvaardigd is. Hierbij is het wel van belang dat het feit waarvan de medewerker wordt verdacht dermate ernstig is dat het opweegt tegen de eventuele inbreuk op de privacy. (Hoofdstuk 3 en 18)
C. Onjuist. Een firewall beschermt tegen indringers van buitenaf. De aanwezigheid ervan heeft geen invloed op de bevoegdheid van de werkgever het gebruik van IT-voorzieningen te controleren.

Evaluatie

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

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

Contact EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER