EXIN Information Security Management ISO/IEC 27001

EXPERT

Certified by EXIN

Preparation guide

Editie 201804

Inhoud

1. Overzicht

EXIN Information Security Management Expert based on ISO/IEC 27001 (ISMES.NL[1])

Scope

De module ISMES toetst specialistische kennis, inzicht en vaardigheden op het gebied van het inrichten, onderhouden en optimaliseren van informatiebeveiliging in een organisatie. Hiertoe behoren onder meer het opstellen van een informatiebeveiligingsbeleid en implementatieplan, het inrichten en organiseren van de informatiebeveiliging, bevorderen van beveiligingsbewustzijn, het uitvoeren van risicoanalyses en het voorstellen en beoordelen van technische en procedurele maatregelen.

Samenvatting

Informatiebeveiliging wordt steeds belangrijker. De globalisering van de economie leidt tot een toenemende uitwisseling van informatie tussen organisaties (medewerkers, klanten en leveranciers), een toenemend gebruik van netwerken, zoals het interne bedrijfsnetwerk, de koppeling met netwerken van andere bedrijven en Internet.
Andere trends die in dit kader van belang zijn:

- (internationale) standaarden en certificering op het gebied van informatiebeveiliging
- de verdere automatisering van het beheer
- ontwikkeling van geautomatiseerde informatiebeveiligingstools
- beheer op afstand
- uitbesteding van beheertaken
- naleving

Bovendien zijn de activiteiten van veel bedrijven nu afhankelijk van ICT, waarbij informatie een kostbaar bedrijfsmiddel is geworden. Informatiebeveiliging is essentieel om de goede werking en de continuïteit van de organisatie te waarborgen: informatie moet betrouwbaar zijn.
De internationale norm voor Informatiebeveiliging ISO/IEC 27001:2017 geeft structuur bij het inrichten van informatiebeveiliging en is daarom een belangrijk uitgangspunt van de module.
In de Information Security modulen wordt de volgende definitie gebruikt: Informatiebeveiliging betreft het definiëren, implementeren, onderhouden, handhaven en evalueren van een samenhangend stelsel van maatregelen die de beschikbaarheid, de integriteit en de vertrouwelijkheid van de (handmatige en geautomatiseerde) informatievoorziening waarborgen.

De onderwerpen van de module zijn:

- Organisatie van de informatiebeveiliging (opstellen Information Security Management System)
  - risicomanagementproces
  - taken, verantwoordelijkheden, bevoegdheden
  - rapportagesysteem
- Informatiebeveiligingsbeleid
  - het proces van totstandkoming
  - opstellen, presenteren en uitdragen
- Risicoanalyse
  - selecteren
  - uitvoeren of de uitvoering begeleiden
  - resultaten beoordelen

[1] De S in de modulecode staat voor: gebaseerd op de standaard.

- Organisatieverandering en –ontwikkeling met betrekking tot Information Security
  - veranderplan op- of bijstellen
  - awareness-programma opstellen, communiceren en uitvoeren
  - veranderplan doorvoeren
- Standaarden en normen
  - relevante standaard kiezen en hanteren
  - normenkaders ofwel baselineconstructie implementeren
- Audit en certificatie
  - uitvoering van audits organiseren
  - managementbeoordeling ISMS

Context

De module ISMES is een vervolg op EXIN Information Security Foundation based on ISO/IEC 27001 (ISFS.NL) en Information Security Management Professional based on ISO/IEC 27001 (ISMP.NL). ISMES rondt het onderwerp Information Security af op het niveau van het inrichten van de informatiebeveiliging.

De module ISFS toetst de basisbegrippen van informatiebeveiliging en de onderlinge relaties. De ISFS doelgroep is iedere medewerker, van de administratie tot de directie, die met vertrouwelijke informatie omgaat.
De module ISMP toetst de kennis van de organisatorische- en beheeraspecten van de informatiebeveiliging. De doelgroep is iedereen die vanuit zijn/haar functie is betrokken bij onder andere de implementatie, evaluatie van en rapportage over informatiebeveiliging, zoals de Manager Informatiebeveiliging (Information Security Manager, ISM) en de Information Security Officer, (ISO), een procesmanager, een lijnmanager of een projectmanager.
.

Doelgroep

IT Professionals belast met het geheel of gedeeltelijk inrichten en ontwikkelen van structurele informatiebeveiliging, zoals de Concernmanager Informatiebeveiliging (Chief Information Security Officer, CISO), de Manager Informatiebeveiliging (Information Security Manager, ISM) of de Procesarchitect Informatiebeveiliging (Business Information Security Architect, BISA). Het bezit van het certificaat Information Security Management Professional wordt ten zeerste aangeraden.

Certificeringseisen

- Aantoonbare praktijkervaring op managementniveau, minimaal 2 jaar, op tenminste twee van de hoofdonderwerpen (exameneisen) van deze module
- Succesvolle afronding van:
  - een door EXIN geaccrediteerde training Information Security Management Expert based on ISO/IEC 27001

  of
  - coaching traject Information Security Management Expert based on ISO/IEC 27001
- De kandidaat heeft met goed gevolg het examen Information Security Management Expert based on ISO/IEC 27001 afgelegd.

Examendetails

De module Information Security Management Expert bestaat uit twee onderdelen:

1. Het schriftelijke deel, een praktijkwerkstuk
   In het hoofdstuk over de examenopzet wordt de procedure van het praktijkwerkstuk toegelicht.
2. Het mondeling examen
   In het hoofdstuk over de examenopzet wordt de procedure van het mondeling examen toegelicht.

Het schriftelijke deel van het examen moet voorafgaand aan het mondeling examen behaald zijn.

Ter voorbereiding op het examen kunnen kandidaten een Guide aanvragen op http://www.exin.com.

Aantal vragen:	Niet van toepassing
Cesuur:	55%
Open boek/notities:	Powerpoint presentatie
Elektronische hulpmiddelen toegestaan:	Ja, voor de Powerpoint presentatie
Examenduur:	90 minuten

Op dit examen is het Reglement voor de examens van EXIN van toepassing.

Training

Contacturen

De training kan bestaan uit een cursus van enkele dagen, aangevuld met coachen, of kan uit enkel coachen bestaan. Het aantal contacturen hangt af van de begeleiding die de deelnemer nodig heeft om klaar te zijn voor het examen.

Indicatie studielast

De studiebelasting van de module Information Security Management Expert based on ISO/IEC 27001 is ongeveer 200 uur, afhankelijk van bestaande kennis en ervaring.

Procedure

Een procedure voor de ISMES training kan zijn:

- Intake
- Vastlegging
- Beoordeling van de voorvereisten (certificaten, ervaring)
- Analyse van het verschil tussen het huidige kennisniveau enerzijds en de gevraagde competenties en op te leveren producten voor ISMES anderzijds
- Diensten die aangeboden worden om het verschil te overbruggen (bijvoorbeeld training, coaching, evaluatie van het werkstuk, uitwisseling met andere kandidaten)
- Ontwerp van een individueel trainingsplan
- Examen registratie bij EXIN
- Examen voorbereiding (bijvoorbeeld oefenen van het mondeling examen, individueel of met andere kandidaten)
- Evaluatie

Trainingsorganisaties

Een lijst van geaccrediteerde trainingsorganisaties kunt u vinden op de website van EXIN http://www.exin.com.

2. Exameneisen

De exameneisen zijn de onderwerpen van de module. In onderstaande tabel staan de onderwerpen van de module (exameneisen). De exameneisen zijn uitgewerkt in examenspecificaties.

Exameneis	Examenspecificatie	Gewicht
1. Organisatie van de informatiebeveiliging (opstellen ISMS)		**20%**
	1.1 Risicomanagement	
	1.2 Rollen	
	1.3 Rapportage	
2. Informatiebeveiligingsbeleid		**10%**
	2.1 Totstandkoming	
	2.2 Uitdragen	
3. Risicoanalyse		**10%**
	3.1 Uitvoering	
	3.2 Analyseren	
4. Organisatieverandering en –ontwikkeling met betrekking tot Information Security		**40%**
	4.1 Veranderplan	
	4.2 Awareness	
	4.3 Verandering doorvoeren	
5. Standaarden en normen		**10%**
	5.1 Standaard kiezen	
	5.2 Baseline	
6. Audit en certificatie		**10%**
	6.1 Uitvoering	
	6.2 Managementbeoordeling ISMS	
	Totaal	100%

Toelichting

Het aantal vragen per examenspecificatie is afhankelijk van wat de kandidaat al heeft gepresenteerd/beantwoord. De examinatoren bepalen tijdens het examen over welke specificaties nog moet worden doorgevraagd en houden hierbij de gewichtsverdeling in gedachten.

Examenspecificaties

1 Organisatie van de informatiebeveiliging (opstellen ISMS)

1.1 De kandidaat kan het risicomanagementproces in relatie met het ISMS beargumenteren.
De kandidaat kan binnen een organisatie, in een gegeven situatie…

1.1.1 van de verschillende activiteiten uit het ISMS het belang en de consequenties voor de organisatie aangeven.

1.1.2 de scope van het ISMS definiëren in termen van de karakteristieken van de bedrijfsactiviteiten, de organisatie, de locatie, bezittingen en technologie.

1.1.3 op een overtuigende wijze het belang van ISMS beargumenteren.

1.2 De kandidaat kan de rollen voor informatiebeveiliging definiëren.
De kandidaat kan binnen een organisatie, in een gegeven situatie…

1.2.1 de verschillende taken, verantwoordelijkheden en bevoegdheden vaststellen en uitleggen.

1.2.2 de verschillende procedures, richtlijnen en voorschriften vaststellen en implementeren.

1.3 De kandidaat kan een rapportagesysteem ten behoeve van het management inrichten en toepassen.
De kandidaat kan binnen een organisatie, in een gegeven situatie…

1.3.1 het ISMS reviewen op geschiktheid en effectiviteit.

1.3.2 mogelijkheden voor verbetering definiëren.

2 Informatiebeveiligingsbeleid

2.1 De kandidaat kan meewerken aan het proces van het tot stand komen van het informatiebeveiligingsbeleid.
De kandidaat kan binnen een organisatie, in een gegeven situatie…

2.1.1 aangeven welke stappen genomen moeten worden om een informatiebeveiligingsbeleid tot stand te brengen.

2.2 De kandidaat kan een informatiebeveiligingsbeleid opstellen, presenteren en uitdragen.
De kandidaat kan binnen een organisatie, in een gegeven situatie…

2.2.1 het informatiebeveiligingsbeleid opstellen, rekening houdend met de doelstellingen van de organisatie, de juridische kaders en organisatorische en technische mogelijkheden.

2.2.2 het opgestelde informatiebeveiligingsbeleid presenteren en uitdragen.

2.2.3 zorgen voor acceptatie van de consequenties op managementniveau.

3 Risicoanalyse

3.1 De kandidaat kan op basis van inzicht in de verschillende risicoanalysemethoden een risicoanalyse uitvoeren of de uitvoering van een risicoanalyse begeleiden.
De kandidaat kan binnen een organisatie, in een gegeven situatie…

3.1.1 de geselecteerde risicoanalysemethode toepassen.

3.1.2 de verschillende stappen uit de risicoanalyse toelichten.

3.2 De kandidaat kan de resultaten van een risicoanalyse analyseren.
De kandidaat kan binnen een organisatie, in een gegeven situatie…

3.2.1 de verschillende tussenresultaten uit de risicoanalyse beoordelen.

3.2.2 de onderlinge samenhang van de tussenresultaten uit de risicoanalyse op consistentie beoordelen.

3.2.3 het eindresultaat van de risicoanalyse op bruikbaarheid en volledigheid beoordelen.

4 Organisatieverandering en –ontwikkeling met betrekking tot Information Security

4.1 De kandidaat kan in een gegeven situatie een veranderplan op- of bijstellen.

De kandidaat kan binnen een organisatie, in een gegeven situatie…

4.1.1 het ontwikkelingsniveau (groeistadium) van het ISMS beoordelen.

4.1.2 de kenmerken van de organisatiecultuur benoemen en de mogelijkheden en beperkingen voor ontwikkeling van het ISMS benoemen.

4.1.3 een veranderstrategie en de beoogde resultaten definiëren.

4.2 De kandidaat kan in een gegeven situatie een awareness programma opstellen, communiceren, presenteren en uitvoeren.

De kandidaat kan binnen een organisatie, in een gegeven situatie…

4.2.1 voor de verschillende doelgroepen identificeren welke veranderingen in kennis, houding en gedrag een bijdrage aan verbetering van het ISMS leveren.

4.2.2 de succesfactoren benoemen en de effectiviteit van hulpmiddelen vergelijken.

4.2.3 een aanpak voor een communicatieplan ontwikkelen.

4.2.4 op managementniveau zowel schriftelijk als mondeling voorstellen voor veranderingen of beleid van het ISMS presenteren, verdedigen en zo nodig aanpassen.

4.3 De kandidaat kan in een gegeven situatie de veranderingen doorvoeren of dit proces begeleiden.

De kandidaat kan binnen een organisatie, in een gegeven situatie…

4.3.1 interventies toelichten en in de organisatie doorvoeren en borgen.

4.3.2 effectief omgaan met meningen en gevoelens van organisatieleden en wisselen in de aanpak van interventies.

4.3.3 de toegepaste interventies evalueren en reflecteren op de eigen rol.

5 Standaarden en normen

5.1 De kandidaat kan in een gegeven situatie een relevante standaard kiezen en hanteren

De kandidaat kan binnen een organisatie, in een gegeven situatie:

5.1.1 de consequenties aangeven bij een keuze voor een bepaalde standaard.

5.1.2 het proces begeleiden om een standaard te hanteren.

5.1.3 de kandidaat kan normenkaders ofwel baselineconstructies implementeren.

5.2 De kandidaat kan in een gegeven situatie een normenkader ofwel baseline constructie opstellen, uitdragen, evalueren en onderhouden.

De kandidaat kan binnen een organisatie, in een gegeven situatie:

5.2.1 een normenkader ofwel baselineconstructie opstellen;

5.2.2 het vastgestelde normenkader ofwel baselineconstructie uitdragen;

5.2.3 het geïmplementeerde normenkader ofwel baselineconstructie evalueren en onderhouden.

6 Audit en certificatie

6.1 De kandidaat kan de uitvoering van audits organiseren.

De kandidaat kan binnen een organisatie, in een gegeven situatie:

6.1.1 een auditprogramma opstellen.

6.1.2 de uitvoering van een audit begeleiden;

6.1.3 verbeteringen voorstellen op grond van die auditresultaten.

6.2 De kandidaat kan meewerken aan een managementbeoordeling van het ISMS.
De kandidaat kan binnen een organisatie, in een gegeven situatie:
6.2.1 de invoer van de managementbeoordeling verzorgen;
6.2.2 verbeteringen voorstellen op grond van de beoordelingsresultaten;
6.2.3 de resultaten van de managementbeoordeling vastleggen.

Toelichting

Exameneis 4 vormt de kern van het inrichten van informatiebeveiliging binnen een organisatie, exameneis 1 geeft aan wat er ingericht moet worden en de overige eisen detailleren de inrichting. De examenspecificaties bevatten geen concrete technieken, omdat deze technieken onderdeel vormen van het eerder door de kandidaat gevolgde leertraject. Per kandidaat kunnen inhoudelijke verschillen ontstaan enerzijds door de inhoud van de presentatie en anderzijds door het gevolgde leertraject.

Examenopzet

Het examen voor de module Information Security Management Expert based on ISO/IEC 27001 (ISMES) bestaat uit twee onderdelen:
1. het werkstuk van de kandidaat;
2. het mondeling examen.

Werkstuk van de kandidaat

De criteria hiervoor staan beschreven in de Guide, bestemd voor kandidaten. Deze is op te vragen bij EXIN. Het schriftelijke gedeelte betreft een praktijkwerkstuk van ongeveer 6000 woorden over één van de volgende onderdelen van ISMES:
- Security Awareness-plan
- Risicoanalyse
- Veranderingsplan
- ISMS plan
- Auditplan
- Quickscan
- Informatiebeveiligingsbeleid

Dit werkstuk wordt in drievoud naar EXIN gestuurd, ongeveer acht weken voor de beoogde datum van het mondeling examen. De kandidaat dient met het werkstuk een managementsamenvatting van het werkstuk op te sturen.
Samen met het werkstuk stuurt de kandidaat ook een kort curriculum vitae, waaruit blijkt dat hij/zij minstens 2 jaar werkervaring heeft, op managementniveau, op het gebied van ten minste 2 exameneisen. De opleider voegt een verantwoording toe voor de relatie tussen het gekozen onderwerp en de gekozen exameneis.

De inhoud van het praktijkwerkstuk dient gerelateerd te zijn aan de werkcontext van de kandidaat. De kern van het werkstuk kan een bestaand document zijn (een van de hiervoor genoemde), op voorwaarde dat de kandidaat daarvan de auteur of co-auteur met voldoende inhoudelijke inbreng is. Het dient in dat geval - minimaal - aangevuld te worden met een start- en slothoofdstuk waarin de rol van de kandidaat duidelijk naar voren komt.

Onderdelen van het starthoofdstuk zijn onder andere:
- de aanleiding voor het tot stand komen van het betreffende document in de organisatie, daaraan gerelateerd een vraag- en doelstelling;
- de rol van de kandidaat bij het tot stand komen van het document;
- de rol/status van het document in de organisatie.

Onderdelen van het slothoofdstuk zijn onder andere:

- zorgvuldige reflecties op de verschillende onderdelen van het proces. Hierin wordt het functioneren van de kandidaat zichtbaar; waar liep de kandidaat tegenaan, welke alternatieven waren er, welke keuzes werden gemaakt, wat kan een volgende keer beter etc.
- een terugkoppeling naar het starthoofdstuk, onder andere naar de vraag- en doelstelling.

Idealiter is het praktijkwerkstuk in zijn geheel voor de module ISMES geschreven; bijvoorbeeld als logisch vervolg in een lopend traject of omdat de organisatie waar de kandidaat werkzaam is er behoefte aan heeft. Ook in dat geval gelden de hiervoor genoemde richtlijnen voor het start- en slothoofdstuk.

Voor elk van de hiervoor genoemde typen werkstukken zijn criteria geformuleerd. Deze zijn uitgebreid beschreven in de Guide. Het is sterk aanbevolen dat de kandidaat het plan voor het werkstuk naar EXIN stuurt in een vroeg stadium om te laten controleren dat het aan de minimum eisen voldoet.

Wanneer het voor een kandidaat niet mogelijk is een praktijkwerkstuk te schrijven op basis van de werkomgeving, kan de kandidaat in overleg met de opleider besluiten een werkstuk te schrijven op basis van de casus. Deze casus is in de Guide van ISMES toegevoegd. In het geval van een werkstuk op basis van de casus dient de kandidaat wel de eigen inbreng uit werkervaring en werkcontext duidelijk te maken. In het laatste hoofdstuk kan dan worden aangegeven bij welke onderdelen is geput uit eigen ervaring, wat relevante overeenkomsten/verschillen zijn met de eigen werkcontext, wat de leerpunten van de casus zijn voor de eigen werkomgeving etc.

Twee examinatoren van EXIN beoordelen het werkstuk. Voor de verschillende onderdelen van ISMES, zoals hiervoor genoemd, zijn criteria geformuleerd waaraan het werkstuk moet voldoen. Naast de inhoud zal ook de vormgeving en verwoording van het werkstuk (inclusief correct gebruik van taal en stijl) worden beoordeeld. Na de beoordeling stuurt EXIN feedback op het werkstuk naar de opleider.

Mondeling examen

De kandidaat kan worden aangemeld voor het mondeling examen als het werkstuk met een voldoende (55% of hoger) is beoordeeld. Het mondeling examen van Information Security Management Expert based on ISO/IEC 27001 (ISMES) bestaat uit vier onderdelen:

I Presentatie door de kandidaat
Het examen begint met een presentatie door de examenkandidaat. Hij of zij geeft een presentatie over het werkstuk. Tijdens de presentatie wordt uitgegaan van een situatie waarin de kandidaat een presentatie verzorgt voor een managementteam met het doel het management te overtuigen en eventuele voorstellen aanvaard te krijgen. Hierbij wordt beoordeeld of de presentatie voldoende afgestemd is op het MT. Deze presentatie duurt (maximaal) 15 minuten. Een overzicht van de criteria waarop wordt getoetst is opgenomen in de Guide behorende bij ISMES (mondeling gedeelte).

II Examengesprek naar aanleiding van de presentatie
Het tweede deel van het examen bestaat uit een gesprek met de examinatoren over de presentatie. De examinatoren bevragen de kandidaat kritisch, als leden van een managementteam. De examinatoren kunnen hierbij vragen stellen over de inhoud van de presentatie. Dit gesprek duurt 15 minuten. Een overzicht van de criteria waarop wordt getoetst is opgenomen in de Guide.

III Examengesprek met betrekking tot de overige exameneisen
In het derde en laatste deel van het examen stellen de examinatoren vragen over de exameneisen die nog niet of onvoldoende aan bod zijn gekomen in de presentatie of in het examengesprek naar aanleiding van de presentatie. De examinatoren zijn hierbij niet meer in hun rol als

managementteam. Er wordt getoetst of de kandidaat in staat is de inhoud van ISMES ook buiten de eigen werkcontext te plaatsen, verbanden te leggen tussen het werkstuk, de presentatie, de eigen werkcontext en recente ontwikkelingen in het vakgebied. Daarnaast kan getoetst worden of de kandidaat in staat is te reflecteren op het eigen handelen in relatie tot de inhoud van de module. De kandidaat dient dus ook buiten de context van zijn eigen functie of bedrijf inzicht te hebben in de onderwerpen die in de exameneisen staan. Dit laatste examengesprek duurt 25 minuten.
Een overzicht van de criteria waarop wordt getoetst is opgenomen in de Guide.

IV Eindoordeel
Direct na het examen bepalen de examinatoren in onderling overleg het eindoordeel en stellen daarbij het eindcijfer vast. Dit duurt 25 minuten. Aansluitend delen de examinatoren het eindcijfer mondeling mede aan de examenkandidaat en lichten het eindoordeel toe. Dit duurt 10 minuten. Het hele examen zal 90 minuten in beslag nemen.

De examenzitting

- Bij de presentatie dient de examenkandidaat gebruik te maken van powerpointdia's op een cd of een eigen laptop.
- Direct voorafgaande aan de presentatie worden twee setjes enkelzijdig bedrukte afdrukken van de dia's aan de examinatoren verstrekt.
- De presentatie start met:
    - Eén dia met de titel van de presentatie.
    - Eén dia met de naam van de kandidaat, de functie, het bedrijf, en de aard van het bedrijf.
- De presentatie gaat over het werkstuk, dus niet over de biografie van de examenkandidaat en is **geen** beschrijving van het bedrijf waar de kandidaat werkt of het eigen bedrijf van de kandidaat.
- Tijdens de presentatie kunnen de examinatoren alleen vragen stellen ter verheldering.
- Het gehele mondelinge examen wordt vastgelegd met opnameapparatuur.
- Het is niet toegestaan de examinatoren te beïnvloeden met mededelingen over zakelijke of privéomstandigheden.

Bij het mondeling examen zijn de volgende personen aanwezig:
- de kandidaat
- twee examinatoren

De opleider/begeleider van de kandidaat kan het mondeling examen als toehoorder bijwonen, als de kandidaat hier toestemming voor geeft.

Tijdsduur

De gehele examensessie duurt maximaal 90 minuten, inclusief het verstrekken van de uitslag. De opbouw van het examen is als volgt:
- 15 minuten (maximaal) voor de presentatie
- 15 minuten voor het gesprek over de presentatie
- 25 minuten voor het examengesprek over de overige exameneisen
- 25 minuten beoordelingsoverleg examinatoren
- 10 minuten bespreken uitslag met de examenkandidaat

Conclusie

De examinatoren beoordelen de drie examenonderdelen aan de hand van drie beoordelingsinstrumenten. De examinatoren vullen tijdens het mondeling deze beoordelingsinstrumenten in. Na afloop van het examen bepalen de examinatoren in onderling overleg het eindcijfer en lichten hun eindoordeel toe.

3. Begrippenlijst

De begrippenlijst van de ISFS en ISMP worden als bekend verondersteld.

4. Literatuur

Examenliteratuur

De literatuur zoals voorgeschreven bij ISFS en ISMP worden als bekend verondersteld. Hierna worden suggesties gegeven voor literatuur die betrekking heeft op de exameneisen en examenspecificaties van dit examen.

A. ISO/IEC 27001:2017 (EN)
Information technology – Security techniques – Information security management systems – Requirements
Zwitserland, ISO/IEC, 2017
www.iso.org

B. ISO/IEC 27002:2017 (EN)
Information technology – Security techniques – Code of practice for information security controls
Zwitserland, ISO/IEC, 2017
www.iso.org

C. ISO/IEC 27000:2018 (EN)
Information technology – Security techniques – Information security management systems – Overview and vocabulary
Zwitserland, ISO/IEC, 2018
www.iso.org

D. ISO/IEC 27005:2011 (EN)
Information technology – Security Techniques – Information security risk management
Zwitserland, ISO/IEC, 2011
www.iso.org

E. NEN 7510:2011 (NL)
Medische informatica – Informatiebeveiliging in de zorg
www.NEN.nl

F. **Besluit Voorschrift Informatiebeveiliging Rijksdienst (VIR)**
Ministerie van Binnenlandse Zaken en Koninkrijkrelaties, 1994 en 2007
www.erfgoedinspectie.nl

G. NEN-ISO/IEC 21827:2008 (EN)
Information technology – Security techniques – Systems Security Engineering – Capability Maturity Model® (SSE-CMM®)
www.NEN.nl

H. ISO/IEC 27035:2016
Information technology – Security techniques – Information security incident management
Switzerland, ISO/IEC, 2016
www.iso.org

I. Carnal, C.A.
Managing Change in Organizations
Financial Times/Prentice, vierde editie, 2007
ISBN-10: 0273704141
ISBN-13: 9780273704140

J. Boonstra, J.J., Stedensma, H.O., Demenint, M.I., e.a.
Ontwerpen en Ontwikkelen van Organisaties
Reed Business Information, 2003
ISBN-10: 90 590 1092 2
ISBN-13: 9789059010925
www.managementboek.nl

K. Gerrichhauzen, J., Kampermann, A., Kluytmans, F., e.a.
Interventies bij Organisatieverandering
Kluwer, 1994
ISBN-10: 90 267 1979 5
ISBN-13: 9789026719790
www.managementboek.nl

L. Robbins, S.P
Organizational Behavior
Prentice Hall, 13e editie, 2008
ISBN-10: 013207964X
ISBN-13: 9780132079648

M. Bokhorst, B., Noord, F., van, e.a.
Functies in de informatiebeveiliging
Expertbrief GVIB, 2005
www.pvib.nl

N. Cazemier, J. A., Overbeek, P., Peters, L.
Security Management Best Practice
Van Haren, januari 2010
ISBN: 978-90-8753-548 3

O. Calder, A.
Information Security based on ISO 27001/ISO 27002 – A Management Guide
Van Haren, 2009
ISBN-13: 978-90-8753-540 7

P. Calder, A.
Implementing Information Security based on ISO 27001/ISO 27002 – A Management Guide
Van Haren, 2009
ISBN-13: 978-90-8753-541 4

Toelichting

Op expertniveau worden deelnemers geacht te kunnen voorzien in hun eigen informatiebehoefte; om deze te sturen zijn suggesties opgenomen voor te raadplegen literatuur, artikelen etc. Deze lijst is niet uitputtend en biedt zeker niet de garantie van volledigheid qua dekking van de te bestuderen stof. Anderzijds is de hoeveelheid beschikbare literatuur zo groot dat het maken van keuzes arbitrair zou zijn en geen recht zou doen aan de keuzevrijheid die de kandidaat op dit niveau dient te hebben.

Contact EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER