Preparation Guide

Editie 201811

Inhoud

1. Overzicht

EXIN Information Security Management Professional based on ISO/IEC 27001 (ISMP.NL)

Scope

In de module EXIN Information Security Management Professional based on ISO/IEC 27001 (ISMP.NL) wordt de kennis van de organisatorische- en beheeraspecten van de informatiebeveiliging getoetst.

De onderwerpen van de module zijn:

- Perspectieven informatiebeveiliging: organisatie, klant, (service)leverancier
- Risicobeheer: analyse, maatregelen, restrisico's
- Maatregelen informatiebeveiliging: organisatorische, technische, fysieke maatregelen.

Samenvatting

Informatiebeveiliging is het beschermen van de vertrouwelijkheid, de integriteit en de beschikbaarheid van informatie (ISO/IEC 27000 definitie).

Informatiebeveiliging wordt steeds belangrijker in de wereld van de Informatie- en communicatietechnologie (ICT). De globalisering van de economie leidt tot een toenemende uitwisseling van informatie tussen organisaties (medewerkers, klanten en leveranciers), en een toenemend gebruik van computers en computerapparatuur in netwerken.

De kernactiviteiten van veel bedrijven zijn nu volledig afhankelijk van IT. Enterprise Resource Planning (ERP)-managementsystemen, de controlesystemen die regelen hoe een gebouw of een productiemachine functioneert, dagelijkse communicatie, alles is afhankelijk van een computer. De overgrote meerderheid aan informatie, het meest waardevolle goed in de wereld, wordt overgedragen via IT. Informatie is essentieel voor de continuïteit en het juist functioneren van organisaties en de economieën waar ze onderdeel van uitmaken; deze informatie moet beschermd worden tegen toegang door onbevoegde personen, tegen abusievelijke of kwaadwillende aanpassing of vernietiging en dient beschikbaar te zijn wanneer het nodig is. Bedrijven en individuele gebruikers van technologie beginnen nu ook in te zien hoe belangrijk beveiliging is en baseren hun keuze van een leverancier steeds vaker op de beveiliging van de technologie of dienst.

Er zijn nog een aantal trends die ervoor zorgen dat informatiebeveiliging steeds belangrijker wordt:

- Verplichtingen nemen toe: De meeste landen kennen meerdere wetten of regels die het gebruik en de beveiliging van verschillende soorten gegevens regelen. Er komen steeds meer van dit soort wetten en de eisen worden steeds strenger.
- Veel industrieën, vooral in de financiële wereld, kennen naast door de overheid opgelegde regels nog andere regels. Deze nemen in aantal toe en worden steeds complexer.
- Er worden op industrieel, nationaal en internationaal niveau beveiligingsstandaarden ontwikkeld en aangescherpt.
- Soms worden beveiligingscertificaten of ander te controleren bewijs gevraagd dat een organisatie beveiligingsnormen en/of best practices naleeft, als voorwaarde om zaken te doen met een specifieke organisatie of in een specifiek land of gebied.

De Code voor Informatiebeveiliging ISO/IEC 27001:2013, is een algemeen geaccepteerde standaard en geeft structuur bij het inrichten van informatiebeveiliging. Ze biedt een raamwerk voor de organisatie en het beheer van de informatiebeveiliging. Implementatie van een programma gebaseerd op deze standaard ondersteunt een organisatie om te voldoen aan de hoge eisen die worden gesteld aan de huidige complexe operationele omgeving. Een grondige kennis van deze standaard is belangrijk voor de persoonlijke ontwikkeling van iedere informatiebeveiligingsprofessional.

In de Information Security modulen van EXIN wordt de definitie van het PvIB (Platform voor Informatiebeveiliging) 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.

Context

Het EXIN Information Security Management Professional certificaat sluit aan op het EXIN Information Security Foundation certificaat, waarin de basisbegrippen van informatiebeveiliging worden getoetst.

Doelgroep

Beveiligingsprofessionals. Deze module richt zich op 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.

Het hebben over basiskennis van Information Security wordt aangeraden. Dit kan bijvoorbeeld worden verkregen door het EXIN Information Security Foundation based on ISO/IEC 27001 examen

Certificeringseisen

- De training EXIN Information Security Professional based on ISO/IEC 27001 bij een door EXIN accredited training organization (ATO), en de twee praktische opdrachten als onderdeel van de training met succes afgerond hebben.
- Het examen EXIN Information Security Management Professional based on ISO/IEC/27001 behaald hebben.

Examendetails

Examenvorm:	Multiple-choice-vragen
Aantal vragen:	30
Cesuur:	65%
Open boek/notities:	Nee
Elektronische hulpmiddelen toegestaan:	Nee
Examenduur:	90 minuten

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

Bloom level

Het EXIN Information Security Management Professional based on ISO/IEC 27001 examen toetst kandidaten op Bloom Levels 3 en 4 volgens de Bloom's Revised Taxonomy:

- Bloom Level 3: Toepassen – laat zien dat kandidaten in staat zijn om informatie in een andere context te gebruiken dan die waarin deze is geleerd. Dit type vragen onderzoekt of de kandidaat in staat is problemen in nieuwe situaties op te lossen door verworven kennis, feiten, technieken en regels op een andere of nieuwe manier toe te passen. Deze vragen bevatten meestal een korte voorbeeldsituatie.
- Bloom Level 4: Analyseren – laat zien dat kandidaten in staat zijn geleerde informatie in stukjes op te breken om hem te begrijpen. Dit Bloom Level wordt voornamelijk getest tijdens de praktijkopdrachten. De praktijkopdrachten zijn bedoeld om te kijken of de kandidaat kan onderzoeken en informatie in delen kan opbreken door redenen of oorzaken te herkennen, zelf dingen uit de informatie af te leiden en bewijs te vinden voor generalisaties.

Training

Contacturen

Het minimumaantal contacturen tijdens de training is 20. Dit omvat praktijkopdrachten, voorbereiding op het examen en korte pauzes. Dit aantal uren is exclusief huiswerk, logistieke voorbereiding van het examen, het examen en lunchpauzes.

Indicatie studielast

120 uur, afhankelijk van bestaande kennis.

Trainingsorganisaties

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

2. Exameneisen

De exameneisen staan vermeld in de examenspecificaties. De volgende tabel bevat de onderwerpen van de module (exameneisen) en de sub-onderwerpen (examenspecificaties).

Exameneis	Examenspecificatie	Gewicht
1. Perspectieven op informatiebeveiliging		**10%**
	1.1 De kandidaat begrijpt het zakelijke belang van informatiebeveiliging.	3.3%
	1.2 De kandidaat kent het perspectief van de klant ten aanzien van informatiebeheer.	3.3%
	1.3 De kandidaat kent de verantwoordelijkheden van de leverancier ten aanzien van veiligheidsgaranties.	3.3%
2. Risicobeheer		**30%**
	2.1 De kandidaat kent de principes van risicobeheer.	10%
	2.2 De kandidaat weet hoe risico's beheerd worden.	10%
	2.3 De kandidaat weet hoe om te gaan met restrisico's.	10%
3. Maatregelen voor informatiebeveiliging		**60%**
	3.1 De kandidaat heeft kennis van organisatorische maatregelen.	20%
	3.2 De kandidaat heeft kennis van technische maatregelen.	20%
	3.3 De kandidaat heeft kennis van fysieke, werknemer-gerelateerde en continuïteitsmaatregelen.	20%
	Total	100%

Examenspecificaties

1 Perspectieven op informatiebeveiliging

1.1 De kandidaat begrijpt het zakelijke belang van informatiebeveiliging.

De kandidaat kan…

1.1.1 verschillende soorten informatie op basis van hun zakelijke waarde onderscheiden.

1.1.2 de eigenschappen van een managementsysteem voor informatiebeveiliging uitleggen.

1.2 De kandidaat kent het perspectief van de klant ten aanzien van informatiebeheer.

De kandidaat kan…

1.2.1 het belang van informatiebeheer bij uitbesteding uitleggen.

1.2.2 een leverancier op basis van garanties aanbevelen.

1.3 De kandidaat kent de verantwoordelijkheden van de leverancier ten aanzien van veiligheidsgaranties.

De kandidaat kan…

1.3.1 beveiligingsaspecten in servicemanagementprocessen onderscheiden.

1.3.2 nalevingsactiviteiten ondersteunen.

2 Risicobeheer

2.1 De kandidaat kent de principes van risicobeheer.

De kandidaat kan…

2.1.1 principes voor het analyseren van risico's uitleggen.

2.1.2 risico's voor geclassificeerde bedrijfsmiddelen identificeren.

2.1.3 risico's voor geclassificeerde bedrijfsmiddelen berekenen.

2.2 De kandidaat weet hoe risico's beheerd worden.

De kandidaat kan…

2.2.1 maatregelen op basis van Vertrouwelijkheid, Integriteit en Beschikbaarheid (Confidentiality, Integrity and Availability (CIA)) indelen.

2.2.2 maatregelen op basis van de fasen van de incidentcyclus kiezen.

2.2.3 relevante richtlijnen voor het toepassen van maatregelen kiezen.

2.3 De kandidaat weet hoe om te gaan met restrisico's.

De kandidaat kan…

2.3.1 risicostrategieën onderscheiden.

2.3.2 business cases voor maatregelen opstellen.

2.3.3 over risicoanalyses rapporteren.

3 Maatregelen voor informatiebeveiliging

3.1 De kandidaat heeft kennis van organisatorische maatregelen.

De kandidaat kan…

3.1.1 beleid en procedures voor informatiebeveiliging schrijven.

3.1.2 incidentafhandeling bij informatiebeveiliging implementeren.

3.1.3 een bewustzijnscampagne binnen de organisatie uitvoeren.

3.1.4 rollen en verantwoordelijkheden voor informatiebeveiliging implementeren.

3.2 De kandidaat heeft kennis van technische maatregelen.

De kandidaat kan…

3.2.1 het doel van beveiligingsarchitecturen uitleggen.

3.2.2 het doel van beveiligingsdiensten uitleggen.

3.2.3 het belang van beveiligingselementen in de IT-infrastructuur uitleggen.

3.3 De kandidaat heeft kennis van fysieke, werknemer-gerelateerde en continuïteitsmaatregelen.
De kandidaat kan…

3.3.1 maatregelen voor fysieke toegang aanbevelen.

3.3.2 beveiligingsmaatregelen in de levenscyclus van dienstverbanden aanbevelen.

3.3.3 de ontwikkeling en het testen van een bedrijfscontinuïteitsplan ondersteunen.

3. Begrippenlijst

Dit hoofdstuk bevat de begrippen die kandidaten moeten kennen.

Let op! Uitsluitend kennis van deze termen is niet voldoende voorbereiding voor het examen; de kandidaten moeten de begrippen begrijpen en in staat zijn om voorbeelden te geven.

Engels	Nederlands
acceptance	acceptatie
access management	toegangsbeheer
asset	bedrijfsmiddel
attack	aanval
audit	audit
authentication	authenticatie
authorization	autorisatie
availability	beschikbaarheid
avoidance	vermijding
awareness (campaigns)	bewustzijn(scampagnes)
business continuity (plan)	business continuity (plan)
Business Impact Analysis (BIA)	Business Impact Analyse (BIA)
Certificate Authority (CA)	Certificate Authority (CA)
Cloud computing	Cloud computing
code of practice for information security	code voor informatiebeveiliging
compliance	naleving (compliance)
confidentiality	vertrouwelijkheid
controls	maatregelen
cryptography	cryptografie
defense	verdediging
Delphi	Delphi
disaster recovery plan	Disaster recovery plan
encryption	versleuteling
escrow agreement	Escrow-overeenkomst
event management	eventbeheer
FAIR	FAIR
firewall	firewall
Host-Based Intrusion Detection and Protection System (Host-Based IDPS)	Host-Based Intrusion Detection and Protection System (Host-Based IDPS)
incident management	incidentbeheer
incident response plan	incident response plan
Information Security Management System (ISMS)	Information Security Management System (ISMS)
information security perspectives	perspectieven van informatiebeveiliging
information security program	informatiebeveiligingsprogramma
integrity	Integriteit
Intrusion Detection System	indringerdetectiesysteem (IDS)

ISO/IEC 27001	ISO/IEC 27001
ISO/IEC 27002	ISO/IEC 27002
IT strategy	IT-strategie
legislation	wetgeving
logical access control	logische toegangscontrole
Microsoft Risk Management Approach	Microsoft Risk Management-aanpak
mitigation	verkleinen
mitigation plan	risicobeheerplan
network content filter	filter voor netwerkinhoud
Network-Based Intrusion Detection and Protection System (Network-Based IDPS)	Network-Based Intrusion Detection and Protection System (Network-Based IDPS)
open design	open ontwerp
perimeter	cirkel
physical access control	fysieke toegangscontrole
Plan-Do-Check-Act (PDCA) cycle	Plan-Do-Check-Act (PDCA) cyclus
policy	beleid
private key	geheime sleutel
problem management	probleembeheer
procedure	procedure
protocol	protocol
public key	openbare sleutel
Public Key Infrastructure (PKI)	Public Key Infrastructure (PKI)
Recovery Point Objective (RPO)	Recovery Point Objective (RPO)
Recovery Time Objective (RTO)	Recovery Time Objective (RTO)
residual risk	restrisico
retention policy	beleid voor het bewaren van gegevens
risk	risico
risk analysis	risicoanalyse
risk appetite	risicobereidheid
risk assessment	risicoanalyse
risk management framework	framework voor risicomanagement
risk manager	beveiligingsmanager
risk strategy	risicostrategie
risk treatment (plan)	(plan van) aanpak van risico's
security architecture	beveiligingsarchitectuur
security governance	bestuur van beveiliging
security services	beveiligingsdiensten
Service Oriented Architecture (SOA)	servicegeoriënteerde architectuur
Statement of Applicability	Statement of Applicability
third party	externe partij
threats	dreigingen
topic-specific policy	onderwerp-specifiek beleidsdocument
Total Cost of Ownership (TCO)	Total Cost of Ownership (TCO)
transference	overdragen
Virtual Private Network (VPN)	Virtual Private Network (VPN)

vulnerability	kwetsbaarheid
zoning	zonering

4. Literatuur

Examenliteratuur

De vereiste kennis voor het examen EXIN Information Security Management Professional based on ISO/IEC 27001 wordt behandeld in de volgende literatuur:

A. Cazemier, J.A., Overbeek, P. en Peters, L.
Information Security Management with ITIL V3
Van Haren Publishing: 2010
ISBN: 978 90 8753 552 0

B. Whitman, M.E., Mattord, H.J.
Management of Information Security
Cengage learning: 2018 (zesde editie)
ISBN: 978 1 337 40571 3
https://www.cengagebrain.co.uk/shop/isbn/9780357192795

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

Aanvullende literatuur

D. BSI-standard 100-2
IT-Grundschutz Methodology
Bundesamt für Sicherheit in der Informationstechnik
De Engelse versie is te downloaden via Partnernet of http://bit.ly/bsi-standard_100-2

E. ISO/IEC 27005:2018 (EN)
Information technology -- Security techniques -- Information security risk management
Zwitserland, ISO/IEC, 2018
www.iso.org

F. Pfleeger, Charles P. and Pfleeger, Shari Lawrence
Security in Computing, 4th edition
Upper Saddle River NJ, Prentice Hall, 2006
ISBN 978 0132390774

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

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

Opmerkingen

- Aanvullende literatuur dient alleen ter referentie en het verdiepen van kennis.
- Literatuur **B** bevat een **woordenlijst** met termen die, indien met betrekking tot de hoofdstukken die vermeld worden in het literatuuroverzicht hieronder, de basisbegrippen vormen voor de examens.
- Literatuur **B** Hoofdstuk 6, Modellen vermeld op pagina 222 hoeven **niet** gekend te worden.
- Literatuur **B** Hoofdstuk 6, Figuur 6-3 op pagina 230; de pijl moet naar rechts wijzen in plaats van naar links (Plan – Do – Check – Act)

Literatuurmatrix

Exameneis	Examenspecificatie	Literatuur
1. Perspectieven op informatiebeveiliging		
	1.1 De kandidaat begrijpt het zakelijke belang van informatiebeveiliging.	A: §1.1.1-1.1.4, §2.1, H. 3, §5.6 B: §1.1, §6.2
	1.2 De kandidaat kent het perspectief van de klant ten aanzien van informatiebeheer.	A: §5.3.4, §5.7, Annex A C: Annex A 15
	1.3 De kandidaat kent de verantwoordelijkheden van de leverancier ten aanzien van veiligheidsgaranties.	A: H. 4, Annex A B: §1.1, §9.2, §9.4 C: Annex A 12.7, 15, 18
2. Risicobeheer		
	2.1 De kandidaat kent de principes van risicobeheer.	A: §4.3 B: H. 6 C: Annex A 8
	2.2 De kandidaat weet hoe risico's beheerd worden.	A: §2.1, §3.2 B: H. 5, §6.2, H. 7, §8.3 C: Annex A 6, 14
	2.3 De kandidaat weet hoe om te gaan met restrisico's.	A: §2.1, §4.5 B: H. 7, §12.2 C: §7.5, Annex A 16
3. Maatregelen voor informatiebeveiliging		
	3.1 De kandidaat heeft kennis van organisatorische maatregelen.	A: §2.1, §3.2, §4.5, §5.2, 5.3, §5.5, Annex A B: H. 10, §2.4, §3.3, H. 4, H. 5, §7.1, H. 8 C: H. 5, Annex A 5, 6.1, 7, 9, 16
	3.2 De kandidaat heeft kennis van technische maatregelen.	A: H. 2 B: H. 8, H. 12 C: Annex A 9, §12.1-12.4, §13.1-13.2
	3.3 De kandidaat heeft kennis van fysieke, werknemer-gerelateerde en continuïteitsmaatregelen.	A: §2.2, §5.3 B: H. 10, H. 11, §12.1 C: Annex A 7, 11, 17

Contact EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER