COURSEWARE

INFORMATION SECURITY FOUNDATION

OP BASIS VAN ISO/IEC 27001'22

COURSEWARE

Van Haren PUBLISHING

Information Security Foundation
op basis van ISO/IEC 27001 ’22
Courseware

Colofon

Titel:	Information Security Foundation op basis van ISO/IEC 27001 ’22 Courseware
Auteurs:	Hans Baars, Jule Hintzbergen en Kees Hintzbergen
Uitgever:	Van Haren Publishing, ‘s-Hertogenbosch
ISBN Hard copy:	978 94 018 1051 7
Druk:	Vijfde druk, eerste impressie, januari 2024
Vormgeving:	Van Haren Publishing, ‘s-Hertogenbosch
Copyright:	© Van Haren Publishing 2024

Voor verdere informatie over Van Haren Publishing, e-mail naar: info@vanharen.net

Over deze courseware

Deze courseware is opgesteld door experts in het vakgebied van Business informatiemanagement, met veel praktijkervaring op het gebied van het produceren en verzorgen van trainingen. De input voor het materiaal bestaat uit bestaande publicaties en de ervaring en expertise van de auteur(s). Het materiaal sluit aan op de exameneisen van APMG en is tevens door APMG geaccrediteerd.

Het doel van de courseware is om de trainer en cursist maximaal te ondersteunen bij zijn of haar opleiding/cursus of voorbereiding op een examen. Het materiaal is modulair opgebouwd en sluit qua opbouw en volgorde aan op de hoofdstukindeling van het BiSL-frameworkboek en op de exameneisen van het BiSL Foundation-examen van APMG.

Om de trainer en deelnemer van de training optimaal te ondersteunen in de beheersing van de theorie, zijn er oefenexamens, opdrachten en uitwerkingen toegevoegd aan het materiaal. Tevens zijn discussievragen opgenomen waarin veelal een verwijzing is opgenomen naar de eigen ervaringen van de cursisten om zo de vertaling van praktijk naar theorie te maken, waardoor de leerstof mogelijk beter "landt".

Waar van toepassing en noodzakelijk voor het Foundation-examen wordt in de sheets verwezen naar de bijbehorende literatuur, waarin de cursist additionele informatie kan vinden over een bepaald onderwerp. Op alle pagina’s is voldoende ruimte opengelaten voor het maken van persoonlijke aantekeningen. Er zijn dus geen aparte notitiepagina’s opgenomen.

Dit courseware-pakket is compleet, en het biedt voldoende vrijheid aan de trainer om in zijn verhaal af te wijken van de opbouw van de sheets ofwel om niet alle sheets of opdrachten te behandelen. En hopelijk voegt de trainer eigen ervaringen en voorbeelden toe! De cursist heeft altijd zelf de mogelijkheid deze onderwerpen in eigen tijd nogmaals door te nemen. Dit wordt eenvoudig gemaakt doordat deze courseware en het BiSL-frameworkboek dezelfde structuur hebben.

De laatste module bevat enkele tips en trucs voor het examen. Daarmee vormt deze courseware, samen met het frameworkboek, de perfecte combinatie om de theorie eigen te maken en goed te begrijpen.

Andere uitgaven van Van Haren Publishing

Van Haren Publishing (VHP) is gespecialiseerd in uitgaven op gebied van Best Practices, methodes en standaarden in de volgende vier domeinen:

- IT en IT Management
- Architectuur (Enterprise en IT)
- Business Management en
- Project Management

Van Haren Publishing publiceert ook voor organisaties en bedrijven zoals: ASLBiSL Foundation, BRMI, CA, Centre Henri Tudor, Gaming Works, IACCM, IAOP, IFDC, Innovation Value Institute, IPMA-NL, ITSqc, NAF, KNVI, PMI-NL, PON, The Open Group, The SOX Institute.

Onderwerpen zijn (per domein):

IT and IT Management
ABC of ICT
ASL®
CATS
CM®
CMMI®
COBIT®
e-CF
ISO/IEC 20000
ISO/IEC 27001/27002
ISPL
IT4IT®
IT-CMF™
IT Service CMM
ITIL®
MOF
MSF
SABSA
SAF
SIAM™
TRIM
VeriSM™

Enterprise Architecture
ArchiMate®
GEA®
Novius Architectuur
Methode
TOGAF®

Business Management
BABOK® Guide
BiSL® and BiSL® Next
BRMBOK™
BTF
EFQM
eSCM
IACCM
ISA-95
ISO 9000/9001
OPBOK
SixSigma
SOX
SqEME®

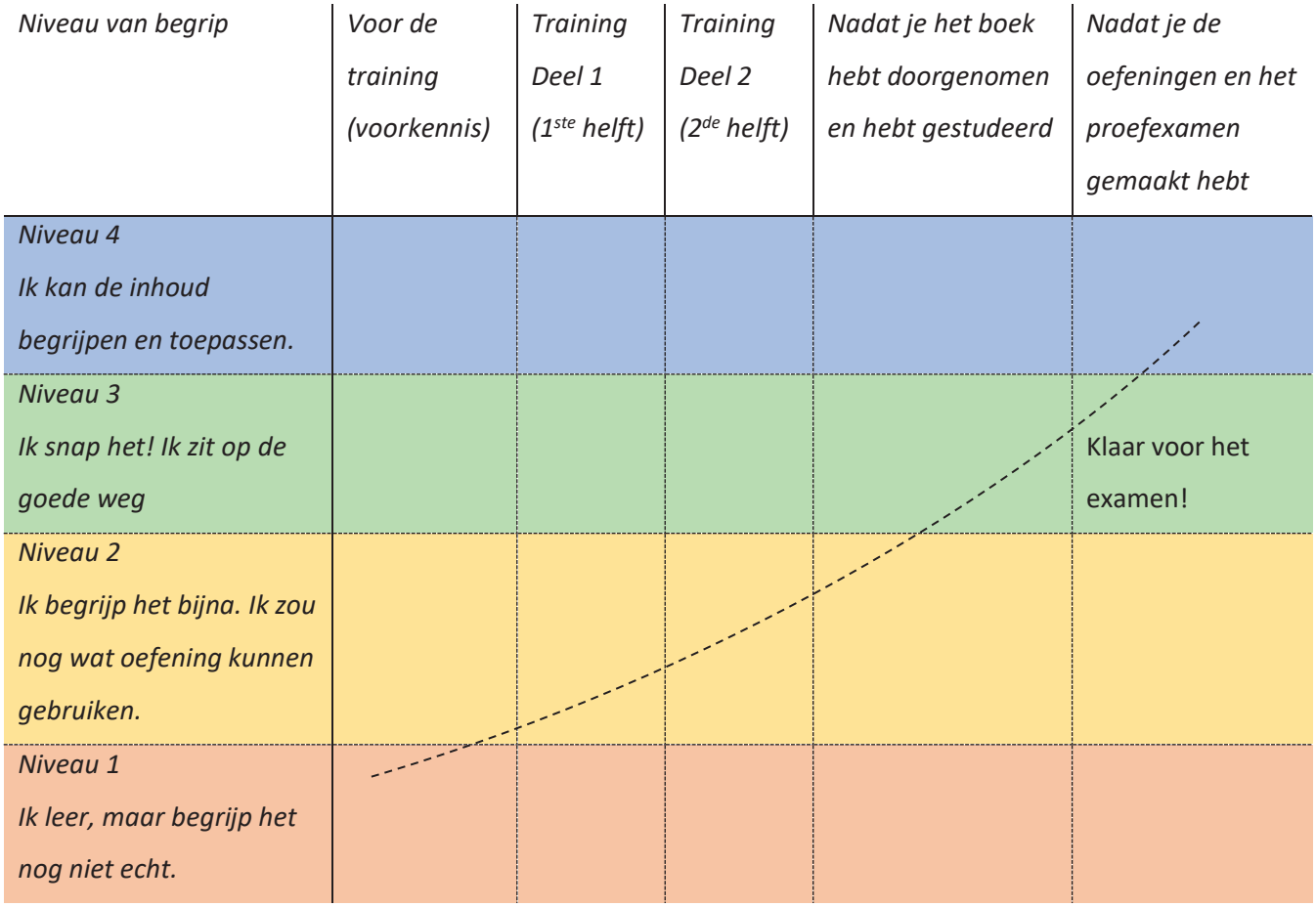
Project Management
A4-Projectmanagement
DSDM/Atern
ICB / NCB
ISO 21500
MINCE®
M_o_R®
MSP®
P3O®
PMBOK® Guide
Praxis®
PRINCE2®

Voor de meest recente informatie over VHP uitgaven, bezoek onze website: www.vanharen.net.

Inhoudsopgave

Diagram Zelfreflectie op begrip

Met deze diagram kun je je kennis en begrip van het materiaal evalueren. Vul hem in om te kijken hoe je ervoor staat. Om voor het examen te slagen zou je ernaar moeten streven om in het bovenste gedeelte van niveau 3 uit te komen. Wil je echt een pro worden? Richt je pijlen dan op niveau 4. Je algemene niveau van begrip zal natuurlijk de leercurve volgen. Daarom is het belangrijk dat je op ieder moment van de training weet waar je zit in het diagram en dat je aandacht besteedt aan de knelpunten. Op basis van je positie in de diagram Zelfreflectie op begrip, kun je de voortgang van je eigen training evalueren.



(Diagram Zelfreflectie op begrip)

Noteer welke knelpunten je nog tegenkomt zodat je ze zelf of met je trainer kunt oplossen. Evalueer daarna met behulp van het diagram of je beter begrijpt waar je staat op de leercurve.

Probleemoplossing

Knelpunt:	*Onderwerp:*
Deel 1	
Deel 2	
Nadat je het boek hebt doorgenomen en hebt gestudeerd	
Nadat je oefeningen en het proefexamen gemaakt hebt	

Agenda

Agenda met examen

Dag 1

- Introductie
- Module 1: Over Exin
- Module 2: Informatie en beveiliging
- Lunch
- Module 3: Dreigingen en risico's
- Module 4: Aanpak en organisatie
- Module 5: Maatregelen
  - 5.1: Organisatie
  - 5.2: Mens
  - 5.3: Fysiek
  - 5.4: Techniek

Dag 2

- Samenvatting dag 1
- Module 5: Maatregelen vervolg
- Pauze
- Zelfstudie
- Lunch
- Module 6: Examen training
- Module 7: Examen uitleg
- Samenvatting / evaluatie

Agenda zonder examen

Dag 1

- Introductie
- Module 1: Over Exin
- Module 2: Informatie en beveiliging
- Lunch
- Module 3: Dreigingen en risico's
- Module 4: Aanpak en organisatie
- Module 5: Maatregelen
  - 5.1: Organisatie
  - 5.2: Mens
  - 5.3: Fysiek
  - 5.4: Techniek

Dag 2

- Samenvatting dag 1
- Module 5: Maatregelen vervolg
- Pauze
- Lunch
- Zelfstudie
- Module 6: Examen training
- Module 7: Examen uitleg
- Samenvatting / evaluatie

Foundation of Information Security

EXIN INFORMATION SECURITY MANAGEMENT PROFESSIONAL based on ISO/IEC 27001

COURSEWARE

Introductie

Kennismaking en doelstellingen

Hier staat de verwijzing bij de betreffende slide naar de theorie in het boek met het nummer van het hoofdstuk of de (sub)paragraaf (§) uit het boek

Over het materiaal

Studieboek

Courseware

Trainer slides

Inhoud

Agenda met examen

Dag 1	
09.00 - 09.30	Introductie
09.30 - 10.15	Module 1: Over Exin
10.15 - 12.00	Module 2: Informatie en beveiliging
12.00 - 12.30	Lunch
12.30 - 13.15	Module 3: Dreigingen en risico's
13.15 - 14.45	Module 4: Aanpak en organisatie
14.45 - 17.00	Module 5: Maatregelen 5.1: Organisatie 5.2: Mens 5.3: Fysiek 5.4: Techniek

Dag 2	
09.00 - 09.20	Samenvatting dag 1
09.20 - 11.00	Module 5: Maatregelen vervolg
10.05 - 10.20	Pauze
11.00 - 12.00	Zelfstudie
12.00 - 13.00	Lunch
13.00 - 14.00	Module 6: Examen training
14.00 - 15.00	Module 7: Examen uitleg
15.00 - 16.00	Samenvatting / evaluatie

Inhoud

Agenda zonder examen

Dag 1	
09.00 - 09.30	Introductie
09.30 - 10.15	Module 1: Over Exin
10.15 - 12.00	Module 2: Informatie en beveiliging
12.00 - 12.30	Lunch
12.30 - 13.15	Module 3: Dreigingen en risico's
13.15 - 14.45	Module 4: Aanpak en organisatie
14.45 - 17.00	Module 5: Maatregelen 5.1: Organisatie 5.2: Mens 5.3: Fysiek 5.4: Techniek

Dag 2	
09.00 - 09.20	Samenvatting dag 1
09.20 - 12.00	Module 5: Maatregelen vervolg
10.05 - 10.20	Pauze
12.00 - 13.00	Lunch
13.00 - 14.00	Zelfstudie
14.00 - 15.00	Module 6: Examen training
15.00 - 16.00	Module 7: Examen uitleg
16.00 - 16.30	Samenvatting / evaluatie

Foundation of Information Security
Module 1 Over deze training

EXIN INFORMATION SECURITY MANAGEMENT PROFESSIONAL based on ISO/IEC 27001

COURSEWARE

Wat is informatiebeveiliging?

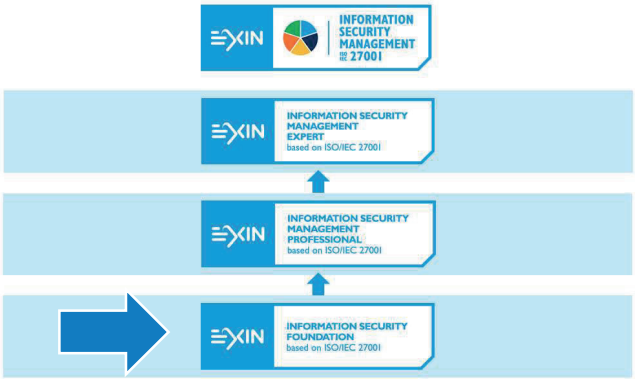
Informatiebeveiliging betreft het definiëren, implementeren, onderhouden, handhaven en evalueren van een samenhangend stelsel van maatregelen die de beschikbaarheid, de integriteit en de vertrouwelijkheid van de (handmatige en geautomatiseerde) informatievoorziening waarborgen.

Bron: PvIB

ISO/IEC 27001 en 27002

- 27001: **Standaard** voor managen van informatiebeveiliging
  - Internationale standaard voor procesmatig inrichten van informatiebeveiliging binnen een organisatie
  - Aanbevelingen voor het initiëren, implementeren en onderhouden van een ISMS
  - Beschrijft wat beveiligd moet worden
  - Bedrijven kunnen zich hiervoor certificeren
- 27002: **Best Practices**
  - Beschrijft hoe beveiligd kan worden
  - Bevat controls en en maatregelen
  - Personen kunnen zich hiervoor certificeren

Over deze training



Training doelen

- Informatie en beveiliging
- Dreigingen en risico`s
- Aanpak en Organisatie
- Maatregelen
- Wet- en regelgeving
- Examen training

Over ISFS

- Wat is ISFS
- Inhoud
- Doelgroep
- e-Competence Framework (e-CF)

Over EXIN

- EXIN en Information Security Foundation based on ISO/IEC 27002 (ISFS.NL)

e-CF Area	e-Competence		Level e-1	e-2	e-3	e-4	e-5
RUN	C.2.	Change Support					
	C.3.	Service Delivery					
ENABLE	D.9.	Personnel Development					
	D.10.	Information and Knowledge Management					
MANAGE	E.3.	Risk Management					
	E.8.	Information Security Management					

Legend for coverage:
- General - The competence is covered at the level indicated
- Partial - The competence is covered to some extent
- Superficial - Relevant knowledge is covered to some extent
- The competence level is available in the framework
- The competence level is **not** available in the framework

Exameneisen en weging

Exameneisen	Examenspecificaties	Gewicht
1. Informatie en beveiliging		27,5%
	1.1 Concepten met betrekking tot informatie	10%
	1.2 Betrouwbaarheidsaspecten	7,5%
	1.3 Informatie beveiligen in de organisatie	10%
2. Dreigingen en risico's		12,5%
	2.1 Dreigingen en risico's	12,5%
3. Beheersmaatregelen		52,5%
	3.1 Schetsen van beheersmaatregelen	2,5%
	3.2 Organisatorische beheersmaatregelen	15%
	3.3 Menselijke beheersmaatregelen	7,5%
	3.4 Fysieke beheersmaatregelen	10%
	3.5 Technische beheersmaatregelen	17,5%
4. Wet- en regelgeving en normen		7,5%
	4.1 Wet- en regelgeving	2,5%
	4.2 Normen	5%
	Totaal	100%

Examenspecificaties

1	Informatie en beveiliging		
	1.1	Concepten met betrekking tot informatie	
		De kandidaat kan...	
		1.1.1	het verschil tussen data en informatie uitleggen.
		1.1.2	concepten met betrekking tot informatiebeveiligingsmanagement uitleggen.
	1.2	Betrouwbaarheidsaspecten	
		De kandidaat kan...	
		1.2.1	de waarde van de BIV-driehoek uitleggen.
		1.2.2	de concepten eindverantwoordelijkheid en controleerbaarheid beschrijven.
	1.3	Informatie beveiligen in de organisatie	
		De kandidaat kan...	
		1.3.1	de doelstellingen en inhoud van een informatiebeveiligingsbeleid schetsen.
		1.3.2	uitleggen hoe informatiebeveiliging kan worden gewaarborgd wanneer er met leveranciers wordt gewerkt.
		1.3.3	rollen en verantwoordelijkheden schetsen die verband houden met informatiebeveiliging.
2	Dreigingen en risico's		
	2.1	Dreigingen en risico's	
		De kandidaat kan...	
		2.1.1	dreigingen, risico's en risicomanagement uitleggen.
		2.1.2	soorten schade beschrijven.
		2.1.3	risicostrategieën beschrijven.
		2.1.4	risicoanalyse beschrijven.

3	Beheersmaatregelen		
	3.1	Schetsen van beheersmaatregelen	
		De kandidaat kan...	
		3.1.1	voorbeelden geven van elke soort beheersmaatregelen.
	3.2	Organisatorische beheersmaatregelen	
		De kandidaat kan...	
		3.2.1	uitleggen hoe informatiemiddelen worden geclassificeerd.
		3.2.2	beheersmaatregelen voor de toegang tot informatie beschrijven.
		3.2.3	dreigings- en kwetsbaarhedenmanagement, projectmanagement en incidentmanagement uitleggen in de context van informatiebeveiliging.
		3.2.4	de waarde van bedrijfscontinuïteit uitleggen.
		3.2.5	de waarde van audits en controles beschrijven.
	3.3	Menselijke beheersmaatregelen	
		De kandidaat kan...	
		3.3.1	uitleggen hoe informatiebeveiliging wordt verbeterd met contracten en overeenkomsten.
		3.3.2	uitleggen hoe bewustwording met betrekking tot informatiebeveiliging wordt verhoogd.
	3.4	Fysieke beheersmaatregelen	
		De kandidaat kan...	
		3.4.1	beheersmaatregelen voor fysieke toegang beschrijven.
		3.4.2	beschrijven hoe informatie binnen beveiligde gebieden wordt beschermd.
		3.4.3	uitleggen hoe beschermingsringen werken.

Examenspecificaties

	3.5	Technische beheersmaatregelen	
		De kandidaat kan...	
		3.5.1	schetsen hoe informatiemiddelen worden beheerd.
		3.5.2	beschrijven hoe systemen worden ontwikkeld met aandacht voor informatiebeveiliging.
		3.5.3	beheersmaatregelen noemen die de netwerkbeveiliging waarborgen.
		3.5.4	technische beheersmaatregelen voor toegangsbeheer (access control) beschrijven.
		3.5.5	beschrijven hoe informatiesystemen worden beschermd tegen malware, phishing en spam.
		3.5.6	uitleggen hoe logging en monitoring bijdragen aan informatiebeveiliging.
4	Wet- en regelgeving en normen		
	4.1	Wet- en regelgeving	
		De kandidaat kan...	
		4.1.1	voorbeelden geven van wet- en regelgeving met betrekking tot informatiebeveiliging.
	4.2	Normen	
		De kandidaat kan...	
		4.2.1	de inhoud van de normen ISO/IEC 27000, ISO/IEC 27001 en ISO/IEC 27002 schetsen.
		4.2.2	de inhoud van andere normen met betrekking tot informatiebeveiliging schetsen.

Hoofdstuk 3

Begrippenlijst

Engels	Nederlands
access control	toegangsbeheer (access control)
accountability	eindverantwoordelijkheid
annualized loss expectancy (ALE)	annualized loss expectancy (ALE)
annualized rate of occurrence (ARO)	annualized rate of occurrence (ARO)
asset	middel
auditability	controleerbaarheid
authentication	authenticatie
authorization	autorisatie
availability	beschikbaarheid
backup	back-up
biometrics	biometrie
business continuity management (BCM)	bedrijfscontinuïteitsbeheer (business continuity management, BCM)
certificate	certificaat
change management	wijzigingsbeheer (change management)
chief information security officer (CISO)	chief information security officer (CISO)
classification	classificatie
code of conduct	gedragscode
compliance	naleving (compliance)
confidentiality	vertrouwelijkheid

Engels	Nederlands
controls	beheersmaatregelen
· corrective	· correctief
· detective	· detectief
· insurance	· verzekering
· preventive	· preventief
· reductive	· reductief
· repressive (suppressive)	· repressief
cryptography	cryptografie
cyber crime	cybercrime
damage	schade
· direct damage	· directe schade
· indirect damage	· indirecte schade
data	data
digital signature	digitale handtekening
due care	due care
due diligence	due dilligence
escalation	escalatie
exposure	blootstelling
(business) impact	(bedrijfs)impact
incident cycle	incidentcyclus

Hoofdstuk 3

Begrippenlijst

Engels	Nederlands
information	informatie
information analysis	informatieanalyse
information management	informatiemanagement
information security management system (ISMS)	managementsysteem voor informatiebeveiliging (ISMS)
information security manager (ISM)	information security manager (ISM)
information security officer (ISO)	information security officer (ISO)
information security policy	informatiebeveiligingsbeleid
information security strategy	informatiebeveiligingsstrategie
information system	informatiesysteem
integrity	integriteit
likelihood	waarschijnlijkheid
non-disclosure agreement (NDA)	geheimhoudingsverklaring (NDA)
Plan, Do, Check, Act (PDCA)	Plan, Do, Check, Act (PDCA)
personally identifiable information (PII)	persoonlijk identificeerbare informatie (PII)
phishing	phishing
privacy	privacy
protection ring	beschermingsringen
public key infrastructure (PKI)	Public Key Infrastructure (PKI)
reliability	betrouwbaarheid

Engels	Nederlands
risk	risico
risk analysis	risicoanalyse
· qualitative risk analysis	· kwalitatieve risicoanalyse
· quantitative risk analysis	· kwantitatieve risicoanalyse
risk assessment	risicobeoordeling
risk management	risicomanagement
risk strategy	risicostrategie
· risk avoiding	· risicomijdend
· risk bearing (risk acceptance)	· risicodragend (risicoacceptatie)
· risk neutral	· risiconeutraal
risk treatment	risicobehandeling
security incident	beveiligingsincident
segregation of duties	functiescheiding
single loss expectancy (SLE)	single loss expectancy (SLE)
stand-by arrangement	hot site op afroep
threat	dreiging
· human threat	· menselijke dreiging
· non-human threat	· niet-menselijke dreiging
threat agent	aanvaller
validation	validatie
verification	verificatie
virtual private network (VPN)	virtual private network (VPN)
vulnerability	kwetsbaarheid

Literatuur

Examenliteratuur

Basiskennis informatiebeveiliging op basis van ISO 27001 en ISO 27002
Van Haren Publishing, 4e herziene druk, 2023
K. Hintzbergen, J. Hintzbergen, en H. Baars
ISBN: 978 94 018 0991 7
eBoek: 978 94 018 0993 4
ePub: 978 94 018 0993 1

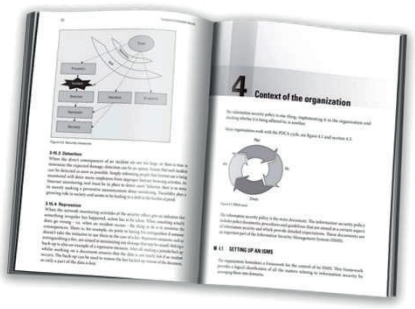
Samenhang literatuur en examenspecificaties

Exameneisen	Examenspecificaties	Referentie
1. Informatie en beveiliging		
	1.1 Concepten met betrekking tot informatie	Hoofdstuk 3.1 - 3.3, 4.7 - 4.9
	1.2 Betrouwbaarheidsaspecten	Hoofdstuk 3.4, 4.4 - 4.6
	1.3 Informatie beveiligen in de organisatie	Hoofdstuk 4.2, 4.3, 4.11 - 4.14, 5.1 - 5.6, 5.14, 5.19 - 5.23, 5.35, 7.7, 7.9, 7.10, 8.30
2. Dreigingen en risico's		
	2.1 Dreigingen en risico's	Hoofdstuk 3.5, 3.7, 3.9 – 3.11
3. Beheersmaatregelen		
	3.1 Schetsen van beheersmaatregelen	Hoofdstuk 3.8
	3.2 Organisatorische beheersmaatregelen	Hoofdstuk 3.6.2, 5.3, 5.7 – 5.18, 5.24 – 5.30, 5.35, 5.36, 6.8
	3.3 Menselijke beheersmaatregelen	Hoofdstuk 6
	3.4 Fysieke beheersmaatregelen	Hoofdstuk 7
	3.5 Technische beheersmaatregelen	Hoofdstuk 4.10, 8
4. Wet- en regelgeving en normen		
	4.1 Wet- en regelgeving	Hoofdstuk 5.31 – 5.34
	4.2 Normen	Hoofdstuk 1, 3.6, 3.12, 4.1, 4.12, 5.36

Hoofdstuk 2

Over het boek

- De inhoud is aangepast aan de nieuwe versie van de standaards: ISO/IEC 27001:2022 en ISO/IEC 27002:2022.
- Is de officiële trainingsgids voor het EXIN examen Information Security Foundation
- Bevat casuïstiek
- Bevat het ISFS model examen
- Geeft feedback op alle multiple choice examen vragen



Foundation of Information Security
Module 2 Informatie en beveiliging

EXIN INFORMATION SECURITY MANAGEMENT PROFESSIONAL based on ISO/IEC 27001

COURSEWARE

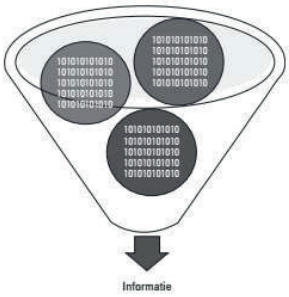
Module 2

HET BEGRIP INFORMATIE

Par. 4.8.1

Het verschil tussen data en information

- Data:
  - Kunnen verwerkt worden met informatietechnologie
- Informatie:
  - Is data waaraan een bepaalde waarde wordt toegekend



Figuur 4.2 Aggregatie van gegevens genereert informatie

Bron: Basiskennis informatiebeveiliging op basis van ISO27001 en ISO27002

Par. 4.8.7

Informatiesysteem

Voorbeelden van informatie technologie:

- Werkstations;
- Data transport via een netwerk;
- Bekabeling of draadloos;
- Servers;
- Data opslag;
- Mobiele telefoons.

Informatiesysteem:

de interactie tussen mensen, processen, data en technologie.

Maar ook:

- Ladenkast met geprinte documenten;
- Een papieren telefoonboek.

Module 2

WAARDE VAN INFORMATIE

Par 4.8, 4.9

Informatie management en informatie analyse

Informatie Management

- Het managen van informatie
- Informatie zien als bedrijfsmiddel
- Beheersing van informatie
- Onafhankelijk van de vorm
- Betreft stakeholders / belanghebbenden

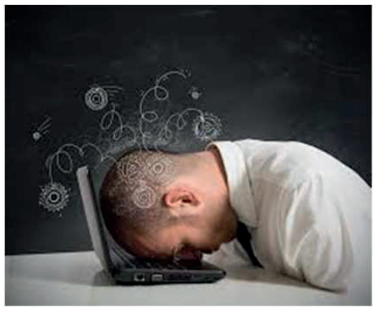
Informatie Analyse

- Het gebruik van informatie in een (bedrijfs)proces
- Focus op het gebruik van informatie in een organisatie

Par. 4.8.4

Waarde van data voor een organisatie

- Data kunnen grote betekenis hebben – afhankelijk van hoe ze gebruikt worden
- Waarde wordt primair bepaald door de gebruiker
  - Hoe belangrijk zijn de data om een bepaalde taak uit te voeren



Par. 4.8.4

Waarde van informatie voor organisaties

- Voor sommige personen is een bepaalde dataset oninteressant
- Anderen zijn mogelijk in staat om daar toch waarde aan te onttrekken

Par. 4.10.6

Waarom is informatie/zijn data waardevol?

- Een magazijn dat klant- en voorraad informatie kwijt raakt, functioneert doorgaans niet of nog maar zeer beperkt
- Voor een accountantskantoor is informatie vaak het enige product.

Par 3.6

Nieuw in ISO 27002:2022; De introductie van attributen

Maatregelsoorten:
- Preventief
- Detectief
- Correctief

Informatiebeveiligingsbegrippen:
- Beschikbaarheid
- Integriteit
- Vertrouwelijkheid

Cybersecurity concepten:
- Identificeren
- Beschermen
- Detecteren
- Reageren
- Herstellen

Operationele mogelijkheden (KPI's)
- Beheer van bedrijfsmiddelen
- Beheer van de beveiligingsorganisatie
- Beheersing van dreigingen en kwetsbaarheden
- Beheersing van Incidenten
- Beveiliging van leveranciersrelaties
- Applicatiebeveiliging
- Configuratiebeveiliging
- Business Continuïty Management
- Fysieke beveiliging
- Governance
- Identiteits- en toegangsbeheer
- Informatiebeveiliging
- Juridisch en compliance
- Persoonsbeveiliging
- Systeem en netwerkbeveiliging

Doel is goed na te denken over de wijze waarop je de beveiliging in je organisatie vorm geeft

 27

Module 2

BETROUWBAARHEIDSASPECTEN

 28

Par 3.3

Betrouwbaarheidsaspecten

Informatie beveiliging, bescherming van:

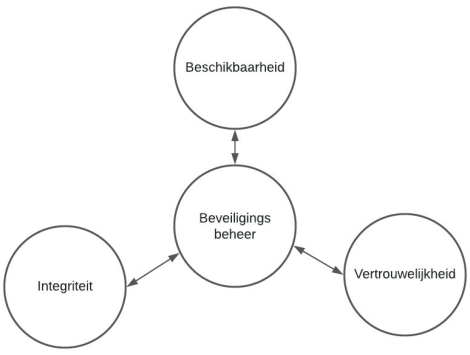
- Beschikbaarheid
- Integriteit
- Vertrouwelijkheid (exclusiviteit)

(BIV)

Par. 3.3

Fundamentele security principes

- Alle security maatregelen, mechanismen en technische implementatie zijn ter ondersteuning van een of meer van deze principes
- Alle risico's, dreigingen en kwetsbaarheden worden beoordeeld op de potentie om een of meerdere BIV principes te schaden



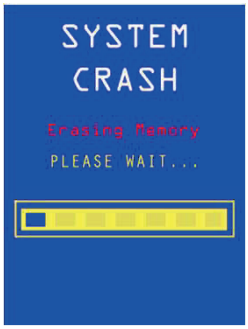
De BIV-Driehoek

Bron: Basiskennis informatiebeveiliging op basis van ISO27001 en ISO27002

Par. 3.4.1

BESCHIKBAARHEID

- De karakteristieken van beschikbaarheid zijn:
  - Tijdigheid
  - Continuïteit
  - Robuustheid



Par. 3.2/3.43

Hoe toegepaste informatie security concepten helpen om de betrouwbaarheid van data/informatie te beschermen

- Beschikbaarheid
  - Het beheer en de opslag van data is zodanig dat de kans op verlies van informatie minimaal is
  - Er zijn back-up procedures aanwezig
  - Juridische eisen geven aan hoe lang data moeten of mogen worden opgeslagen. Dit varieert van land tot land in de EU, de VS en andere continenten

Par. 3.4.2

INTEGRITEIT

- Integriteit is de mate waarin informatie actueel en zonder fouten is
- Elke ongeautoriseerde wijziging van data, opzettelijk danwel per ongeluk is een inbreuk op data integriteit

Par. 3.2/3.4.2

Hoe toegepaste informatie security concepten helpen om de betrouwbaarheid van data/informatie te beschermen

- Integriteit
  - Veranderingen in systemen en data zijn geautoriseerd
  - Waar mogelijk zijn mechanismen ingebouwd die afdwingen dat de juiste terminologie gebruikt wordt
  - Acties van gebruikers worden vastgelegd (logging) zodat kan worden vastgesteld wie informatie veranderd heeft
  - Acties in vitale systemen, zoals bijvoorbeeld het installeren van nieuwe software, kunnen niet worden uitgevoerd door slechts één persoon

Par. 3.4.3

VERTROUWELIJKHEID

- Beperking, in termen van wie mag bij welke informatie

Par 3.2 / 3.4.3

Hoe toegepaste informatie security concepten helpen om de betrouwbaarheid van data/informatie te beschermen

- Vertrouwelijkheid
  - Toegang tot informatie is op basis van **"need to know"**
  - **Logische toegangscontrole zorgt** ervoor dat ongeautoriseerde personen of processen geen toegang krijgen tot geautomatiseerde systemen, databases en programma's
  - Er wordt een **scheiding** aangebracht tussen **verantwoordelijkheden** van organisatorische eenheden
  - Strikte **scheiding** wordt gecreëerd tussen **ontwikkeling, test en productieomgevingen**
  - Maatregelen worden getroffen om **privacy** van personeel en derden te waarborgen

Bijlage c.1

Oefenvraag

- Wat is de relatie tussen data en informatie?

A. Data zijn gestructureerde informatie
B. Informatie is de betekenis en waarde die toegekend wordt aan een data verzameling.

Bijlage c.1

Oefenvraag

- Om een brandverzekering af te kunnen sluiten, moet een administratiekantoor de waarde van data die het beheert vaststellen. Welke factor is niet van belang om deze waarde voor een organisatie vast te stellen?

A. De inhoud van de data
B. De mate waarin ontbrekende of incorrecte data hersteld kunnen worden
C. De mate waarin data essentieel zijn voor het uitvoeren van bedrijfsprocessen
D. Het belang van het bedrijfsproces dat deze data gebruikt

Bijlage c.1

Oefenvraag

- Een hacker krijgt toegang tot een webserver en kan bestanden inzien op de server die credit card nummers bevatten. Welke van de principes van beschikbaarheid, exclusiviteit en integriteit (BEI) worden hiermede geschonden?

A. Beschikbarheid
B. Vertrouwelijkheid
C. Integriteit

Bijlage c.1

Oefenvraag

- Er staat een printer in de hal van het bedrijf waar je voor werkt. Veel werknemers halen de prints die ze maken niet direct op en laten ze liggen op de printer. Wat is de consequentie hiervan voor de betrouwbaarheid van deze informatie?

A. De integriteit is niet langer gegarandeerd
B. De beschikbaarheid van de informatie is niet langer gegarandeerd
C. De vertrouwelijkheid van de informatie is niet langer gegarandeerd

Foundation of Information Security
Module 3 Dreigingen en risico`s

COURSEWARE

Module 3

DREIGING EN RISICO

Par. 3.5.2

Dreiging en Aanvaller

- Een **dreiging** is een potentiële bron van een ongewenst incident
- Een 'threat agent' of aanvaller is een entiteit die misbruik maakt van een **kwetsbaarheid**
- Bijvoorbeeld, een aanvaller kan een indringer zijn die het netwerk binnenkomt via een firewall poort
- Of een proces dat toegang heeft tot data zodanig dat dit een inbreuk is op de security policy

Par. 3.5.1

Risico

- Een risico is de kans dat een 'threat agent' misbruikt maakt van een kwetsbaarheid en de resulterende impact op de bedrijfsvoering
- Bijvoorbeeld, een brand breekt uit in uw kantoor
- Of een medewerker die niet op de personeelszaken afdeling werkt krijgt toegang tot gevoelige informatie

Par. 3.7

Risico analyse

- Een risico analyse is een proces dat:
  - Bedrijfsmiddelen identificeert op basis van hun waarde
  - Een balans vaststelt tussen kosten van een incident en de kosten van maatregelen
  - Relevante kwetsbaarheden en dreigingen identificeert
- Risicomanagement
  - Het continue proces (PDCA) waarbij risicoanalyses worden uitgevoerd en waarbij risico's worden beheerst door het treffen van passende maatregelen.
- Een risico analyse is bedoeld om:
  - Te komen tot een passende set van maatregelen tegen een dreiging
  - Maatregelen kosteneffectief en tijdig te kunnen toepassen
- Types
  - Kwalitatief
  - Kwantitatief
  - Combinatie van beide

Par. 3.7

Doelstellingen risicoanalyses

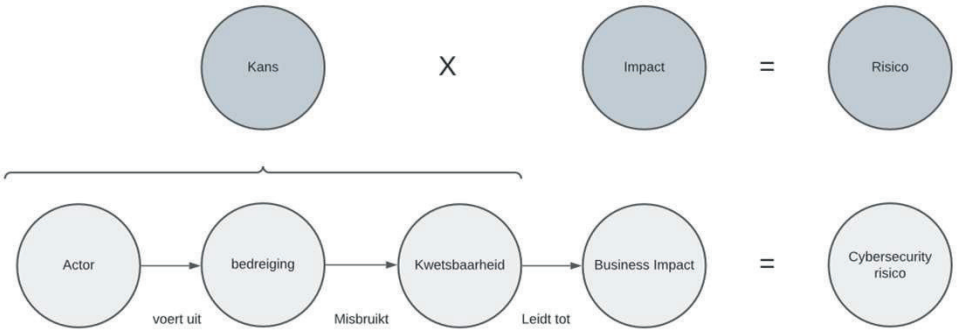
Een risicoanalyse heeft vijf hoofddoelstellingen:

1. identificeren van assets en hun waarde;
2. bepalen van kwetsbaarheden en bedreigingen;
3. bepalen van het risico dat bedreigingen werkelijkheid worden en het operationele proces verstoren;
4. bepalen van een evenwicht tussen de kosten van een incident en de kosten van een beveiligingsmaatregel;
5. risico's ten opzichte van elkaar kunnen vergelijken om prioritering te bepalen in wat het eerst te doen (80/20-regel).

Par. 3.7

Risico formule

- In de basis is de risico formule (kans x impact = risico)
- Hier bestaan ook oneindig veel varianten op
- Bijvoorbeeld de actor kan ook weer uitgedrukt worden in (kennis/middelen)
- De informatie kan meer of minder waardevol zijn voor de aanvaller



Par. 3.7

Kwantitatieve formules

Met de kwantitatieve aanpak is het de bedoeling dat men op vergelijkbare kosten per jaar komt, daarvoor heb je de volgende parameters nodig:

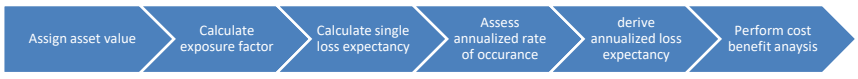
AV - asset value (waarde asset, betrek alle kosten)

EF - exposure factor (hoe veel schade kan er zijn, als het risico optreedt)

SLE - single loss expectancy (AV x EF = SLE)

ARO - Annualized rate of occurrence (Hoe vaak per jaar kan het voorkomen)

ALE – Annualized Loss Expectancy (SLE x ARO = ALE) (wat is de verwachte schade per jaar)



Par. 5.7

Informatie en analyses over dreigingen

- Dreigings- en kwetsbaarheidsbeheer zorgt ervoor dat kwetsbaarheden tijdig worden ontdekt en weggewerkt.
- Beveiligingspatches worden geïnstalleerd zodra ze bekend zijn.
- Wanneer patches niet beschikbaar zijn, worden, indien mogelijk, tijdelijk andere beveiligingsmaatregelen genomen om ervoor te zorgen dat de kwetsbaarheid niet kan worden misbruikt.

Threat intelligence loopt daarbij voorop.

De organisatie wacht dan niet op een bericht van de leverancier dat er een kwetsbaarheid is gevonden en dat er aan een patch wordt gewerkt. De organisatie onderzoekt zelf actief of er nieuwe kwetsbaarheden zijn gevonden.

Par. 3.5, 3.5.1, 3.5.2

De relatie tussen een dreiging en een risico

- Een dreiging heeft de potentie om een ongewenst incident te veroorzaken. Zo'n incident kan negatieve gevolgen hebben voor de systemen of de organisatie (kans)
- De impact geeft aan in welke mate een dreiging negatieve gevolgen kan hebben voor een organisatie
- Risico = kans x impact