COURSEWARE

Information Security Foundation

op basis van ISO 27002 Courseware

Courseware

Van Haren PUBLISHING

Information Security Foundation
op basis van ISO27002
Courseware

Colofon

Titel:	Information Security Foundation op basis van ISO 27002 Courseware
Auteurs:	Hans Baars, Jule Hintzbergen, André Smulders en Kees Hintzbergen
Uitgever:	Van Haren Publishing, Zaltbommel
ISBN Hard copy:	978 94 018 0179 9
Druk:	Eerste druk, eerste oplage, Mei 2017
Vormgeving:	Van Haren Publishing, Zaltbommel
Copyright:	© Van Haren Publishing 2017

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

The Certificate EXIN Information Security Foundation based on ISO/IEC 27002 is part of the qualification program Information Security. The module is followed up by the Certificates EXIN Information Security Management Advanced based on ISO/IEC 27002 and EXIN Information Security Management Expert based on ISO/IEC 27002.

Inhoud

Foundation of Information Security

EXIN INFORMATION SECURITY FOUNDATION
based on ISO/IEC 27002
e-CF Level e-2 / Professional

Introductie

- Kennismaking en doelstellingen
- Regels
- Agenda

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

Over het courseware

Studie boek

Courseware

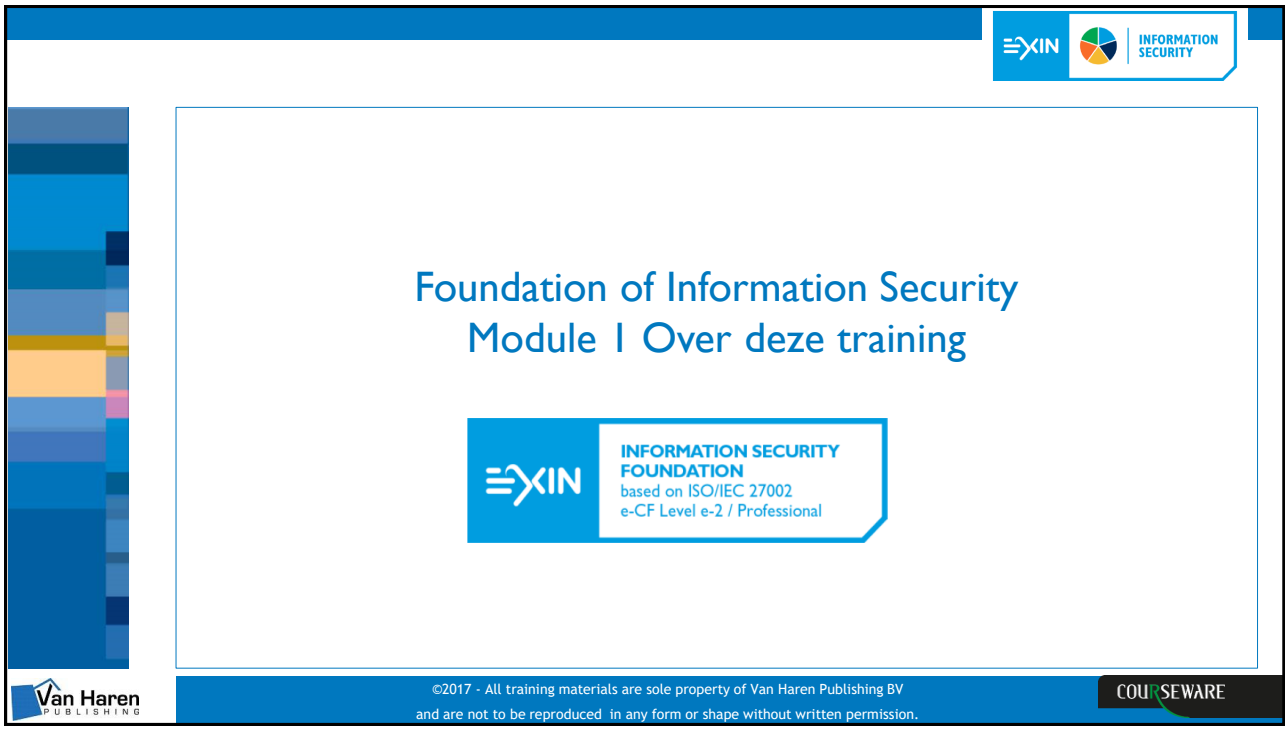
Trainer slides

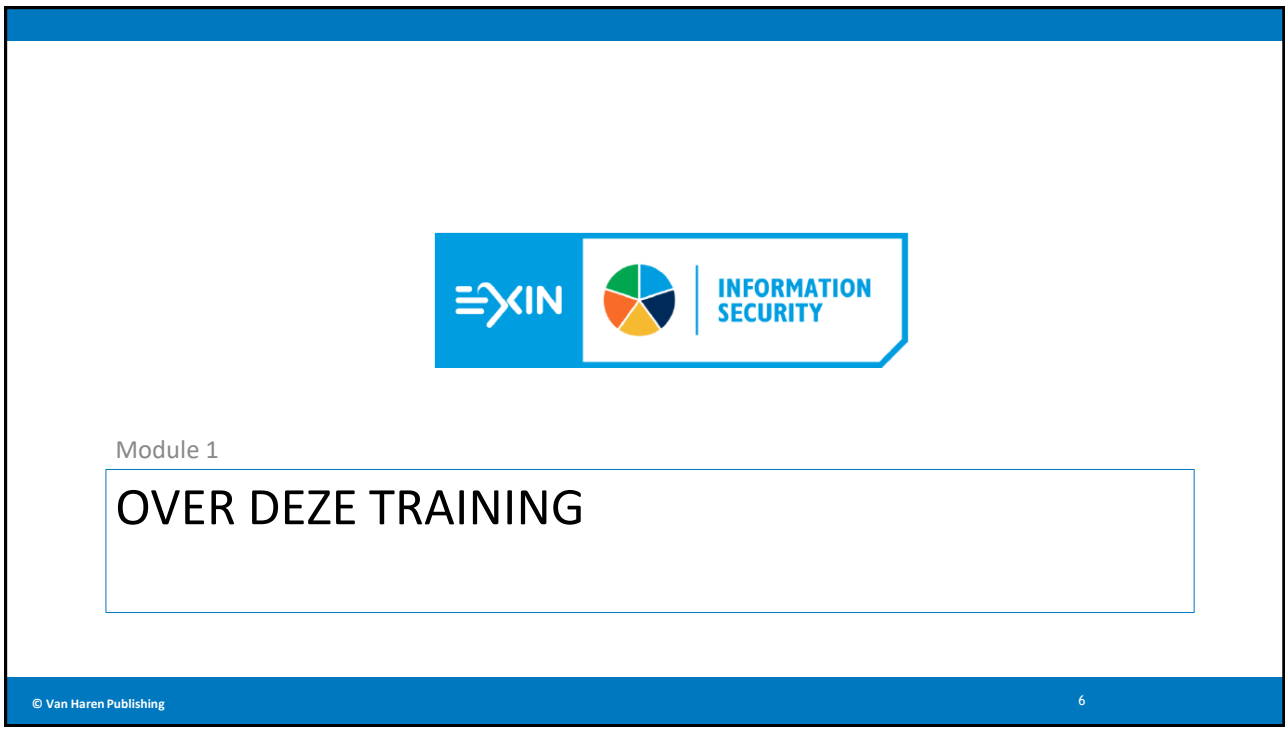
Contents

Agenda

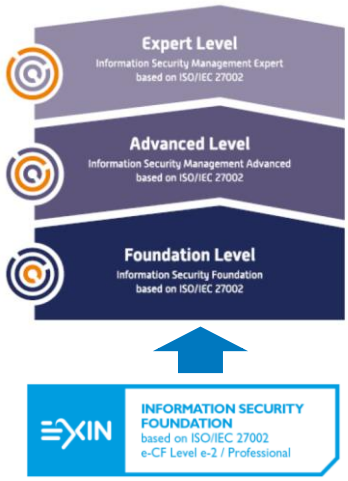
Dag 1	
09.00 - 9.30	Introductie
09.30 - 10.15	Module 1: Over deze training
10.15 – 12.00	Module 2: Informatie en beveiliging
12.00 - 12.30	Lunch
12.30 - 13.15	Module 3: Dreigingen en risico`s
13.15 – 14.45	Module 4: Aanpak en Organisatie
14.45 – 17.00	Module 5: Maatregelen

Dag 2	
09:00 – 09:20	Samenvatting dag 1
09:20 – 10:05	Module 6: Wet- en regelgeving
10:05 – 10:20	Pauze
10.20 – 12.20	Module 7: Examen training
12.20 – 13:00	Lunch
13:00 - 14:30	Zelf studie
14:30 – 14:50	Pauze
14:50 - 15:50	Examen





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

Exameneis	Examenspecificatie	Gewicht %
1. Informatie en beveiliging		10
	1.1 Het begrip informatie	2,5
	1.2 De waarde van informatie	2,5
	1.3 Betrouwbaarheidsaspecten	5
2. Dreigingen en risico's		30
	2.1 Dreiging en risico	15
	2.2 Relaties tussen dreigingen, risico`s en de betrouwbaarheid van informatie	15
3. Aanpak en organisatie		10
	3.1 Beveiligingsbeleid en beveiligingsorganisatie	2,5
	3.2 Onderdelen	2,5
	3.3 Incidentbeheer	5
4. Maatregelen		40
	4.1 Belang van maatregelen	10
	4.2 Fysieke maatregelen	10
	4.3 Technische maatregelen	10
	4.4 Organisatorische maatregelen	10
5. Wet- en regelgeving		10
	5.1 Wet- en regelgeving	10
	Totaal	100%

Examenspecificaties

1. **Informatie en beveiliging (10%)**

1.1 **Het begrip informatie (2,5%)**
De kandidaat begrijpt het begrip informatie.
De kandidaat kan:
1.1.1 uitleggen wat het verschil is tussen data en informatie;
1.1.2 informatiedragers beschrijven die onderdeel uitmaken van de basisinfrastructuur.

1.2 **De waarde van informatie (2,5%)**
De kandidaat begrijpt de waarde van informatie voor organisaties.
De kandidaat kan:
1.2.1 beschrijven wat de waarde is van data/informatie voor organisaties;
1.2.2 beschrijven hoe de waarde van data/informatie organisaties kan beïnvloeden;
1.2.3 uitleggen wat het nut is van informatiebeveiliging.

1.3 **Betrouwbaarheidsaspecten (5%)**
De kandidaat kent de betrouwbaarheidsaspecten (vertrouwelijkheid, integriteit, beschikbaarheid) van informatie.
De kandidaat kan:
1.3.1 de betrouwbaarheidsaspecten van informatie noemen;
1.3.2 de betrouwbaarheidsaspecten van informatie beschrijven.

2. **Dreigingen en risico`s (30%)**

2.1 **Dreiging en risico (15%)**
De kandidaat begrijpt de begrippen dreiging en risico.
De kandidaat kan:
2.1.1 de begrippen dreiging, risico en risicoanalyse uitleggen;
2.1.2 de relatie tussen een dreiging en een risico uitleggen;
2.1.3 verschillende soorten dreigingen beschrijven;
2.1.4 verschillende soorten schades beschrijven;
2.1.5 verschillende risicostrategieën beschrijven.

2.2 **Relaties tussen dreigingen, risico`s en de betrouwbaarheid van informatie (15%)**
De kandidaat begrijpt de relatie tussen dreigingen, risico`s en de betrouwbaarheid van informatie.
De kandidaat kan:
2.2.1 voorbeelden herkennen van de verschillende soorten dreigingen;
2.2.2 effecten beschrijven van de verschillende soorten dreigingen op informatie en informatieverwerking.

3. **Aanpak en Organisatie (10%)**

3.1 **Beveiligingsbeleid en beveiligingsorganisatie (2,5%)**
De kandidaat begrijpt de begrippen beveiligingsbeleid en beveiligingsorganisatie.
De kandidaat kan:
3.1.1 in grote lijnen beschrijven wat het doel en de inhoud is van een beveiligingsbeleid;
3.1.2 in grote lijnen beschrijven wat het doel en de inhoud is van een beveiligingsorganisatie.

3.2 **Onderdelen (2,5%)**
De kandidaat kent de verschillende onderdelen van de beveiligingsorganisatie.
De kandidaat kan:
3.2.1 het belang van een gedragscode uitleggen;
3.2.2 het belang van eigenaarschap uitleggen;
3.2.3 de belangrijkste rollen in de informatiebeveiligingsorganisatie noemen.

3.3 **Incidentbeheer (5%)**
De kandidaat begrijpt het belang van incidentbeheer en escalatie.
De kandidaat kan:
3.3.1 samenvatten hoe beveiligingsincidenten worden gemeld en welke informatie daarbij nodig is;
3.3.2 voorbeelden geven van beveiligingsincidenten;
3.3.3 duidelijk maken wat de consequenties zijn van het niet melden van beveiligingsincidenten;
3.3.4 uitleggen wat een escalatie inhoudt (functioneel en hiërarchisch);
3.3.5 beschrijven wat de effecten zijn van escalatie in de organisatie;
3.3.6 de incidentcyclus toelichten.

4. **Maatregelen (40%)**

4.1 **Belang van maatregelen (10%)**
De kandidaat begrijpt het belang van beveiligingsmaatregelen.
De kandidaat kan:
4.1.1 verschillende indelingen van beveiligingsmaatregelen beschrijven;
4.1.2 per type beveiligingsmaatregel voorbeelden geven;
4.1.3 de relatie tussen risico`s en beveiligingsmaatregelen uitleggen;
4.1.4 het doel van het classificeren van informatie benoemen;
4.1.5 beschrijven wat de uitwerking is van classificatie.

4.2 **Fysieke maatregelen (10%)**
De kandidaat kent de inrichting en uitvoering van fysieke maatregelen.
De kandidaat kan:
4.2.1 voorbeelden geven van fysieke maatregelen;
4.2.2 de risico`s verbonden aan het ontbreken van fysieke beveiligingsmaatregelen beschrijven.

Examenspecificaties

4.3 Technische maatregelen (10%)
De kandidaat kent de inrichting en uitvoering van technische maatregelen.
De kandidaat kan:
4.3.1 voorbeelden geven van technische maatregelen;
4.3.2 de risico`s verbonden aan het ontbreken van technische beveiligingsmaatregelen beschrijven;
4.3.3 de begrippen cryptografie, digitale handtekening en certificaat plaatsen;
4.3.4 de drie stappen voor veilig internetbankieren benoemen (PC, website, betaling);
4.3.5 verschillende soorten kwaadaardige software noemen;
4.3.6 de maatregelen beschrijven die tegen kwaadaardige software kunnen worden ingezet.

4.4 Organisatorische maatregelen (10%)
De kandidaat kent de inrichting en uitvoering van organisatorische maatregelen.
De kandidaat kan:
4.4.1 voorbeelden geven van organisatorische maatregelen;
4.4.2 de gevaren en risico`s verbonden aan het ontbreken van organisatorische beveiligingsmaatregelen beschrijven;
4.4.3 toegangbeveiligingsmaatregelen beschrijven zoals functiescheiding en wachtwoordgebruik;
4.4.4 principes voor het beheer van toegang beschrijven;
4.4.5 de begrippen identificatie, authenticatie en autorisatie beschrijven;
4.4.6 uitleggen wat het belang is van goed ingerichte Business Continuity Management voor een organisatie;
4.4.7 duidelijk maken wat het belang is van het uitvoeren van oefeningen.

5. Wet- en regelgeving (10%)

5.1 Wet- en regelgeving (10%)
De kandidaat begrijpt het belang en de werking van wet- en regelgeving.
De kandidaat kan:
5.1.1 uitleggen waarom wet- en regelgeving van belang is voor de betrouwbaarheid van informatie;
5.1.2 voorbeelden geven van wetgeving gerelateerd aan informatiebeveiliging;
5.1.3 voorbeelden geven van regelgeving gerelateerd aan informatiebeveiliging;
5.1.4 aangeven waaruit maatregelen voor wet- en regelgeving kunnen bestaan.

Hoofdstuk 3

Begrippenlijst

• functionele escalatie • hiërarchische escalatie	• Functional escalation • Hierarchical escalation
• exclusiviteit	• Exclusivity
• functiescheiding	• Segregation of duties
• gedragscode	• Code of conduct
• geheimhoudingsovereenkomst	• Non-disclosure agreement
• hacken	• Hacking
• Hoax	• Hoax
• identificatie	• Identification
• impact	• Impact
• incidentcyclus	• Incident cycle
• indirecte schade	• Indirect damage
• informatie	• Information
• informatieanalyse	• Information analysis
• informatiearchitectuur	• Information architecture
• Informatiebeveiligingsrisico beoordeling	• Information security review
• informatiemanagement	• Information management
• informatiesysteem	• Information system
• infrastructuur	• Infrastructure
• integriteit	• Integrity
• interferentie	• Interference
• ISO/IEC 27001:2013	• ISO/IEC 27001:2013
• ISO/IEC 27002:2013	• ISO/IEC 27002:2013
kwalitatieve risicoanalyse	• Qualitative risk analysis
• kwantitatieve risicoanalyse	• Quantitative risk analysis
• kwetsbaarheid	• Vulnerability

• logisch toegangsbeheer	• Logical access management
• maatregel	• measure / control
• Malware	• Malware
• naleving (Compliance)	• Compliance
• nauwkeurigheid	• Precision
• onderhoudstoegang (Maintenace door)	• Maintenance door
• onweerlegbaarheid	• Non-repudiation
• opslagmedium	• Storage medium
• Patch	• Patch
• Personal Firewall	• Personal firewall
• Phishing	• Phishing
• preventief	• Preventive
• prioriteit	• Priority
• privacy	• Privacy
• productiefactor	• Production factor
• Public Key Infrastructure (PKI)	• Public Key Infrastructure (PKI)
• reductief	• Reductive
• redundantie	• Redundancy
• repressief	• Repressive
• risico	• Risk
• risicoafweging (A&K analyse)	• Risk assessment (Dependency & Vulnerability analysis)
• risicoanalyse	• Risk analysis

Hoofdstuk 3

Begrippenlijst

• risicodragend	• Risk bearing
• risicomijdend	• Risk avoidance
• risiconeutraal	• Risk neutral
• risicomanagement	• Risk management
• risicostrategie	• Risk strategy
• robuustheid	• Robustness
• Rootkit	• Rootkit
• schade	• Damage
• sleutel	• Key
• Social engineering	• Social engineering
• Spam	• Spam
• Spyware	• Spyware
• Stand by-regeling	• Stand-by arrangement
• systeemacceptatietesten	• System acceptance testing
• tijdigheid	• Timeliness
• toegangsbeheer (Access Control)	• Access control
• toekennen van gebruikerstoegang	• User access provisioning
• Trojan	• Trojan
• uitwijk	• Stand-by arrangement
• Uninterruptible Power Supply (UPS)	• Uninterruptible Power Supply (UPS)
• urgentie	• Urgency

• validatie	• Validation
• verificatie	• Verification
• vertrouwelijkheid	• Confidentiality
• vertrouwelijke authenticatie informatie	• Secret authentication information
• Virtual Private Network (VPN)	• Virtual Private Network (VPN)
• virus	• Virus
• volledigheid	• Completeness
• Voorschrift Informatiebeveiliging Rijksdienst (VIR) / Voorschrift Informatiebeveiliging Bijzondere Informatie (VIR-BI)	• Information security regulations for the government
• Wet Bescherming Persoonsgegevens (WBP)	• Personal data protection legislation
• Wet Computer Criminaliteit (WCC)	• Computer criminality legislation
• Wijzigingsbeheer / Change Management	• Change Management
• worm	• Worm

Literatuur

Examenliteratuur

K Hintzbergen, J., Hintzbergen, K., Smulders, A. and Baars, H.
Basiskennis informatiebeveiliging op basis van ISO 27001 en ISO 27002
Van Haren Publishing, 2e herziene druk, 2015
ISBN 978 94 018 0013 6
E-ISBN 978 94 018 0543 8

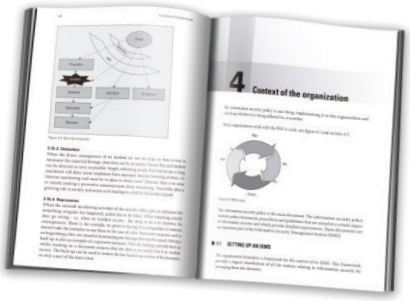
Samenhang literatuur en examenspecificaties

Examenels	Examen-specificatie	Literatuur	Literatuurverwijzing
1	1.1	A	Hoofdstuk 3 en §4.10
	1.2	A	Hoofdstuk 3 en 4
	1.3	A	Hoofdstuk 3 en4
2	2.1	A	Hoofdstuk 3
	2.2	A	Hoofdstuk 3 en 11
3	3.1	A	Hoofdstuk 3, 5 en 6
	3.2	A	Hoofdstuk 6, 7, 8 en 13
	3.3	A	Hoofdstuk 3, 15 en 16
4	4.1	A	Hoofdstuk 3, 8 en 16
	4.2	A	Hoofdstuk 3 en 11
	4.3	A	Hoofdstuk 6, 10, 11 en 12
	4.4	A	Hoofdstuk 3, 6, 9, 17 en 18
5	5.1	A	Hoofdstuk 18

Hoofdstuk 2

Over het boek

- Inhoud is aangepast aan de nieuwe versie van de standaards: ISO/IEC 27001:2013 en ISO/IEC 27002:2013.
- Officiële training gids voor het EXIN examen Information Security Foundation
- Bevat Casussen
- Bevat ISFS model exam
- Feedback op alle multiple choice examen vragen

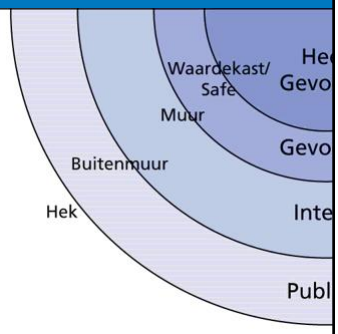


EXIN INFORMATION SECURITY

Foundation of Information Security
Module 2 Informatie en beveiliging

Van Haren PUBLISHING

COURSEWARE



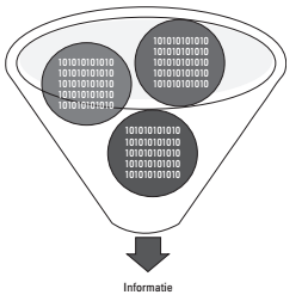
Module 2

HET BEGRIP INFORMATIE

Par. 4.10.1

Het verschil tussen data en information

- Data:
  - Kan 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. 4.10.7

Voorbeelden van elementen die de basis vormen van een infrastructuur

- Informatie Technologie
  - Werkstations
  - Data transport via een netwerk, bedraad of draadloos;
  - Servers;
  - Data opslag;
  - Mobiele telefoons;
  - Andere verbindingen
- Informatie Systemen
  - Ladenkast met geprinte documenten;
  - Een papieren telefoonboek;

Module 2

DE WAARDE VAN INFORMATIE

Par. 4.10.4

Waarde van data voor een organisatie

- Data kan grote betekenis hebben – afhankelijk van hoe het gebruikt wordt
- Waarde wordt primair bepaald door de gebruiker
  - Hoe belangrijk is de data om een bepaalde taak uit te voeren

Par. 4.10.5

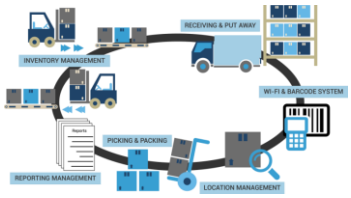
Waarde van informatie voor organisaties

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

Par. 4.10.6

Waarom is informatie/data waardevol?

- Een magazijn dat klanten en voorraad informatie kwijt raakt, functioneert doorgaans niet of nog maar zeer beperkt
- Voor een accountants kantoor is informatie vaak hun enige product.



Par. 3.4

Hoe toegepaste informatie security concepten helpen om waar 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 tussen organisatorische eenheden;
  - Strikte scheiding wordt gecreëerd tussen ontwikkeling, test en productieomgevingen;
  - Maatregelen zijn getroffen om privacy van personeel en derden te waarborgen.

Par. 3.5

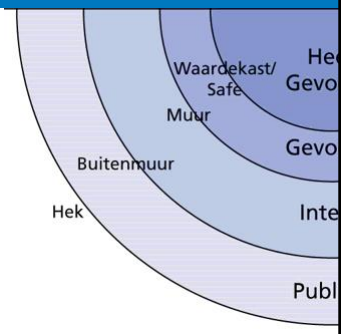
Hoe toegepaste informatie security concepten helpen om waar van data/informatie te beschermen

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

Par. 3.6

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

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



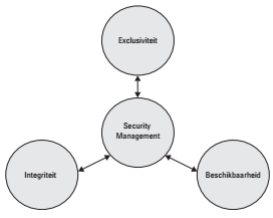
Module 2

BETROUWBAARHEIDSASPECTEN

Par. 3.6

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 BIE principes te schaden



Figuur 3.1 De BEI-driehoek

Bron: Basiskennis informatiebeveiliging op basis van ISO27001 en ISO27002

Par. 3.4

VERTROUWELIJKHEID

- Beperking, in termen van wie mag bij welke informatie.

Par. 3.5

INTEGRITEIT

- Integriteit verwijst naar het correct of consistent zijn op basis van een gewenste staat van informatie.
- Elke ongeautoriseerd wijziging van data, dan wel opzettelijk of per ongeluk is een inbreuk op data integriteit.

Par. 3.6

BESCHIKBAARHEID

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

Bijlage c.1

Oefenvraag

1. Wat is de relatie tussen data en informatie?

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

Bijlage c.1

Oefenvraag

2. 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 kan worden
C. De mate waarin data essentieel is voor het uitvoeren van bedrijfsprocessen
D. Het belang van het bedrijfsproces dat deze data gebruikt

Bijlage c.1

Oefenvraag

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

A. Beschikbarheid
B. Exclusiviteit
C. Integriteit