COURSEWARE

Certified BIO Professional

Baseline Informatie-beveiliging Overheid – Courseware

Van Haren PUBLISHING

Certified BIO Professional
Baseline Informatiebeveiliging Overheid
Courseware

Colofon

Titel:	Certified BIO Professional - Baseline Informatiebeveiliging Overheid - Courseware – Nederlands
Hoofdauteur:	Ruben Zeegers
Co-auteur:	Boudewijn Cremers
Uitgever:	Van Haren Publishing, ‘s-Hertogenbosch
ISBN Hard Copy:	9789401806831
Editie:	Eerste druk, eerste oplage, oktober 2020
Vormgeving:	Van Haren Publishing, ‘s-Hertogenbosch
Copyright:	© Van Haren Publishing 2020

For further information about Van Haren Publishing please e-mail us at: info@vanharen.net or visit our website: www.vanharen.net

All rights reserved. No part of this publication may be reproduced, distributed, stored in a data processing system or Published in any form by print, photocopy or any other means whatsoever without the prior written Consent of the authors and publisher.

Other copyright statements

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.

Other publications by Van Haren Publishing

Van Haren Publishing (VHP) specializes in titles on Best Practices, methods and standards within four domains:

- IT and IT Management
- Architecture (Enterprise and IT)
- Business Management and
- Project Management

Van Haren Publishing is also publishing on behalf of leading organizations and companies: 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.

Topics are (per domain):

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®

For the latest information on VHP publications, visit our website: www.vanharen.net.

Inhoudsopgave

	--- Dianummer	--- Paginanummer
Diagram Zelfreflectie		7
Algemeen	(1)	9
Module 1: Achtergrond informatiebeveiliging en BIO	(9)	17
Overheidsvoorschriften en normenkaders	(11)	19
Begrippen Informatiebeveiliging	(17)	25
Risico's en Maatregelen	(21)	29
PDCA	(37)	45
Aanpak & Implementatie ISMS	(46)	54
Module 2: Beleid en Organisatie	(93)	101
Organiseren van informatiebeveiliging	(98)	106
Veilig personeel	(104)	112
Acquisitie, ontwikkeling en onderhoud van informatiesystemen	(109)	117
Leveranciersrelaties	(112)	120
Module 3: Tactische en operationele beheersmaatregelen	(121)	129
Beheer van bedrijfsmiddelen	(122)	130
Toegangsbeveiliging	(132)	140
Cryptografie	(141)	149
Fysieke beveiliging en beveiliging van de omgeving	(146)	154
Beveiliging bedrijfsvoering	(149)	157
Communicatiebeveiliging	(159)	167
Mobiele apparatuur en telewerken	(168)	176
Module 4: Incidenten & Bedrijfsconinuïteit	(172)	180
Beheer van informatiebeveiligingsincidenten	(173)	181
Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	(182)	190
Naleving	(189)	197
Praktijkopdracht: Implementatie stappenplan	(199)	207
Syllabus		209

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.

Niveau van begrip	*Voor de training (voorkennis)*	*Training Deel 1 (1ste helft)*	*Training Deel 2 (2de helft)*	*Nadat je het boek hebt doorgenomen en hebt gestudeerd*	*Nadat je de oefeningen en het proefexamen gemaakt hebt*
Niveau 4 *Ik kan de inhoud begrijpen en toepassen.*					
Niveau 3 *Ik snap het! Ik zit op de goede weg*					Klaar voor het examen!
Niveau 2 *Ik begrijp het bijna. Ik zou nog wat oefening kunnen gebruiken.*					
Niveau 1 *Ik leer, maar begrijp het nog niet echt.*					

(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	

Programma

- Algemeen

Module 1: Achtergrond informatiebeveiliging en BIO

Module 2: Beleid en Organisatie

Module 3: Tactische en operationele beheersmaatregelen

Module 4: Incidenten & Bedrijfscontinuïteit



Aantekeningen:

Per 1 januari 2019 is de Baseline Informatiebeveiliging Overheid (BIO) van kracht. De BIO is een gezamenlijk normenkader voor informatiebeveiliging binnen de gehele Nederlandse overheid. Het vervangt de voormalige baselines informatieveiligheid voor Rijk, Gemeenten, Waterschappen en Provincies. De BIO gebaseerd op de internationaal erkende ISO-normatiek voor informatiebeveiliging.

De BIO maakt informatiebeveiligingsrisico's binnen de Nederlandse overheid beter beheersbaar. Dat is noodzakelijk, want in de huidige 'informatiegestuurde' tijdperk zijn ondernemers, burgers en overheden steeds vaker afhankelijk van informatie. Daarbij delen zij in toenemende mate gevoelige en vertrouwelijke informatie.

Programma

- Algemeen

  Module 1: Achtergrond informatiebeveiliging en BIO

  Module 2: Beleid en Organisatie

  Module 3: Tactische en operationele beheersmaatregelen

  Module 4: Incidenten & Bedrijfscontinuïteit

Voorstellen

- Ik ben…
- En werk bij…
- Mijn functie heeft met de BIO te maken omdat…
- De reden dat ik deelneem aan de CBP training is omdat…

© Van Haren Publishing

Aantekeningen:

Programma

- Algemeen

  Module 1: Achtergrond informatiebeveiliging en BIO

  Module 2: Beleid en Organisatie

  Module 3: Tactische en operationele beheersmaatregelen

  Module 4: Incidenten & Bedrijfscontinuïteit



Aantekeningen:

Programma

- Algemeen

  Module 1: Achtergrond informatiebeveiliging en BIO

  Module 2: Beleid en Organisatie

  Module 3: Tactische en operationele beheersmaatregelen

  Module 4: Incidenten & Bedrijfscontinuïteit

Trainingsdoelen

Aantoonbare kennis van informatiebeveiliging voor overheid
Kennis van tactisch normen kader
BIO vertaling naar de praktijk

© Van Haren Publishing

Aantekeningen:

Programma

- Algemeen

  Module 1: Achtergrond informatiebeveiliging en BIO

  Module 2: Beleid en Organisatie

  Module 3: Tactische en operationele beheersmaatregelen

  Module 4: Incidenten & Bedrijfscontinuïteit

Exameneisen

Certificering bestaat uit 3 vereiste onderdelen:
- 16 uur training (inclusief praktijkopdracht)
- Behalen van de praktijkopdracht
- Behalen van het multiple-choice examen

Tijdens de training wordt invulling gegeven aan de praktijkopdracht.

© Van Haren Publishing

Aantekeningen:

Programma

- Algemeen

  Module 1: Achtergrond informatiebeveiliging en BIO

  Module 2: Beleid en Organisatie

  Module 3: Tactische en operationele beheersmaatregelen

  Module 4: Incidenten & Bedrijfscontinuïteit

Examenspecificaties

Aantal examenvragen	60 (multiple choice)
Examen duur	60 minuten
Cesuur	70% (42 goed)
Examen hulpmiddelen	Geen
Taal	Nederlands

© Van Haren Publishing

Aantekeningen:

Voor meer informatie over het examen zie de voorbereidingsgids achterin de courseware.

Programma

- Algemeen

  Module 1: Achtergrond informatiebeveiliging en BIO

  Module 2: Beleid en Organisatie

  Module 3: Tactische en operationele beheersmaatregelen

  Module 4: Incidenten & Bedrijfscontinuïteit



Aantekeningen:

De courseware is gebaseerd op de meest recente versie van de BIO en de ISO27001 / 2 aangevuld met relevantie informatie over begrippen en hulpmiddelen voor de vertaling van de BIO naar de praktijk.

Informatiebeveiligingsdienst
De Informatiebeveiligingsdienst (IBD) is onderdeel van de Vereniging Nederlandse Gemeenten (VNG) en ondersteunt gemeenten op het gebied van informatiebeveiliging en privacy.
De IBD heeft een grote hoeveelheid aan kennisproducten ontwikkeld, die van oorsprong gebaseerd waren op de Baseline Informatiebeveiliging Gemeenten (BIG).
Met de komst van de BIO voor de gehele Nederlands overheid is de BIG komen te vervallen. De IBD heeft steeds meer kennisproducten herschreven naar de BIO. Als gevolg hiervan kunnen deze kennisproducten breder worden ingezet dan alleen voor gemeenten. Hiermee kunnen security professionals vanuit de gehele Nederlandse overheid kosteloos gebruik maken van handreikingen en tools om snel en eenduidig invulling te kunnen geven aan informatiebeveiliging conform de BIO.

Programma

- Algemeen

  Module 1: Achtergrond informatiebeveiliging en BIO

  Module 2: Beleid en Organisatie

  Module 3: Tactische en operationele beheersmaatregelen

  Module 4: Incidenten & Bedrijfscontinuïteit



Aantekeningen:

De bovenstaande afbeelding is een uitsnede van een willekeurige pagina uit dit boek. Aan de hand hiervan wordt de layout toegelicht.

Modules
De training bestaat uit vier modules. Op elke pagina is door middel van het oranje bolletje te zien tot welke module de pagina behoord.

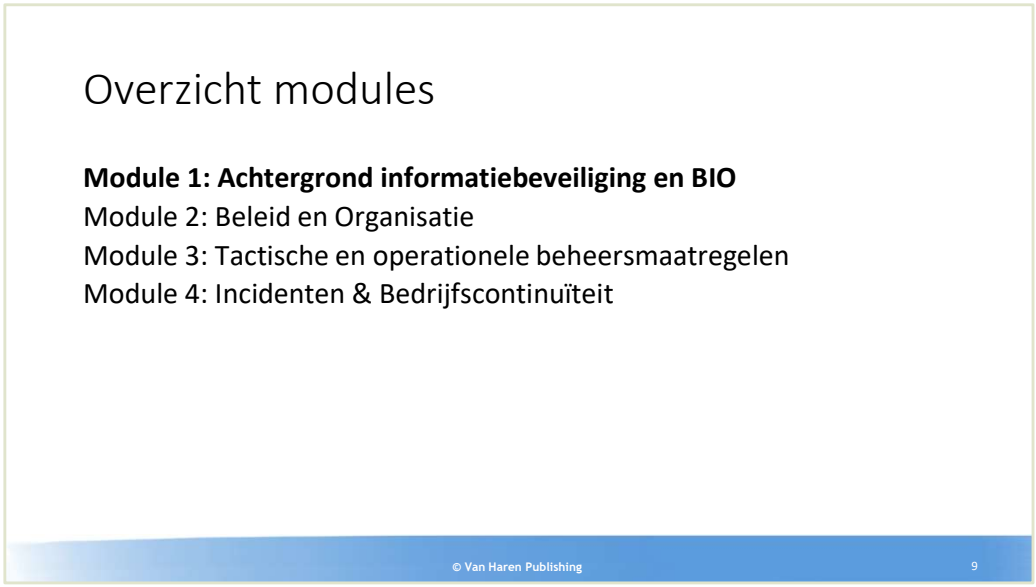
Verwijzing BIO hoofdstukken
Bij sommige sheets is er in de titel een hoofdstuknummer vermeld. Dit betreft een verwijzingen naar de hoofdstukkenindeling van de BIO. Omdat de courseware uitgebreider is dan de BIO alleen, is deze BIO hoofdstuknummering niet op elke sheet aanwezig. Omdat de opbouw van de training niet dezelfde volgorde heeft als de hoofdstukken van de BIO zijn de hoofdstuk verwijzingen niet in chronologische volgorde.

Aanvullende verdiepende informatie
De training sheets behandelen op hoofdlijnen de BIO. Relevante aanvullende of verdiepende informatie is onder de sheet opgenomen. Hiermee is de courseware niet alleen te gebruiken voor examen voorbereiding maar ook prima inzetbaar als naslagwerk.

Aantekeningen
Op elke pagina is ruimte opgenomen voor het maken van aantekeningen.

Programma

- Algemeen
- Module 1: Achtergrond informatiebeveiliging en BIO
- Module 2: Beleid en Organisatie
- Module 3: Tactische en operationele beheersmaatregelen
- Module 4: Incidenten & Bedrijfscontinuïteit



Aantekeningen:

Module 1: Achtergrond informatiebeveiliging en BIO
Overheidsvoorschriften en normenkaders
Begrippen Informatiebeveiliging
Risico's en Maatregelen
PDCA
Aanpak & Implementatie ISMS

Module 2: Beleid en Organisatie
5. Informatiebeveiligingsbeleid
6. Organiseren van informatiebeveiliging
7. Veilig personeel
14. Acquisitie, ontwikkeling en onderhoud van informatiesystemen
15. Leveranciersrelaties

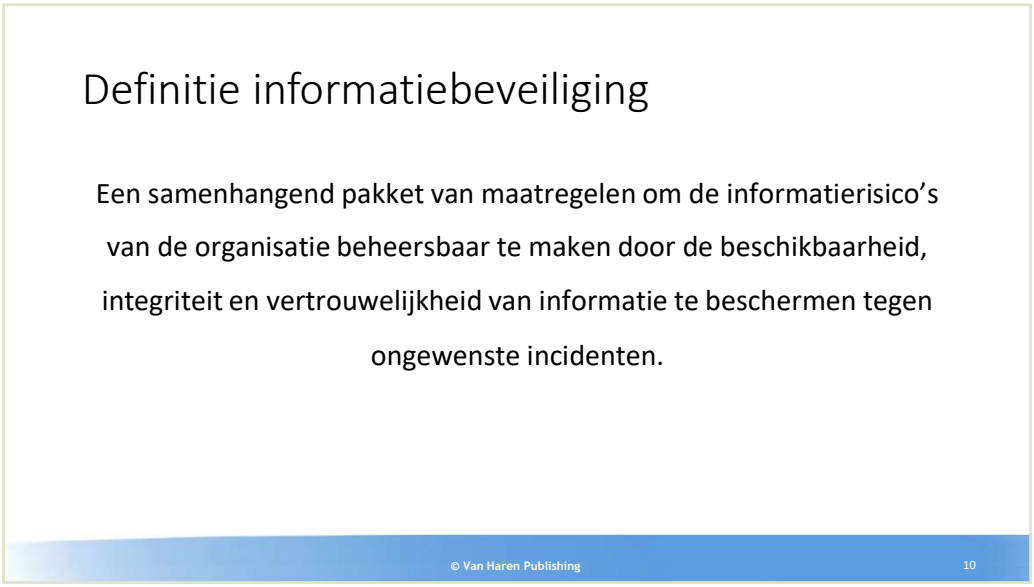
Module 3: Tactische en operationele beheersmaatregelen
8. Beheer van bedrijfsmiddelen
9. Toegangsbeveiliging
10. Cryptografie
11. Fysieke beveiliging en beveiliging van de omgeving
12. Beveiliging bedrijfsvoering
13. Communicatiebeveiliging

Module 4: Incidenten & Bedrijfscontinuïteit

16. Beheer van informatiebeveiligingsincidenten
17. Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer
18. Naleving

Programma

- Algemeen
- Module 1: Achtergrond informatiebeveiliging en BIO
- Module 2: Beleid en Organisatie
- Module 3: Tactische en operationele beheersmaatregelen
- Module 4: Incidenten & Bedrijfscontinuïteit

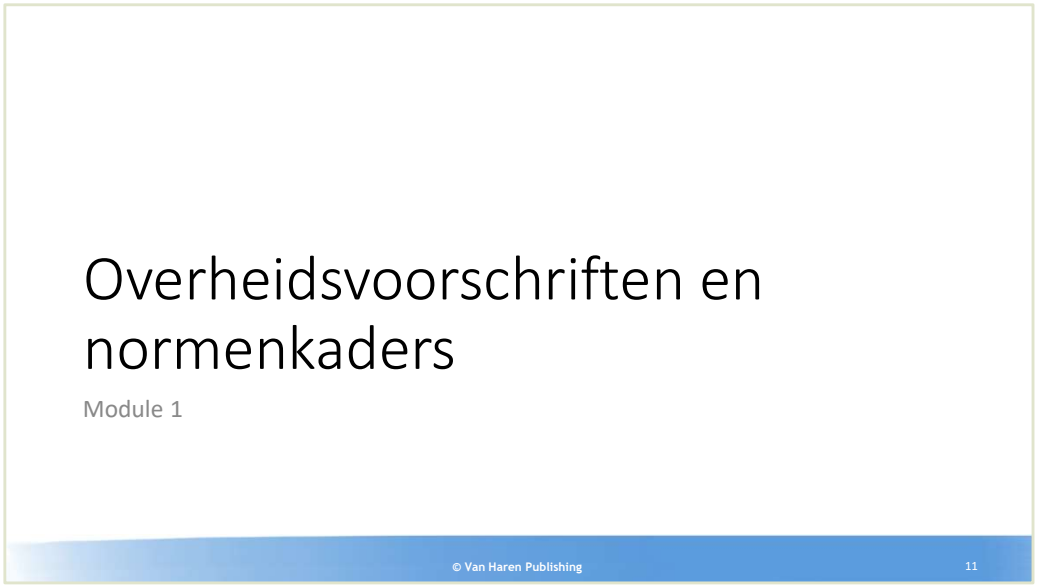


Aantekeningen:

Er zijn vele definities voor informatiebeveiliging. Doorgaans zijn ze vergelijkbaar en bijna altijd bevatten ze de componenten beschikbaarheid, integriteit en vertrouwelijkheid.

Programma

- Algemeen
- Module 1: Achtergrond informatiebeveiliging en BIO
- Module 2: Beleid en Organisatie
- Module 3: Tactische en operationele beheersmaatregelen
- Module 4: Incidenten & Bedrijfscontinuïteit



Aantekeningen:

Programma

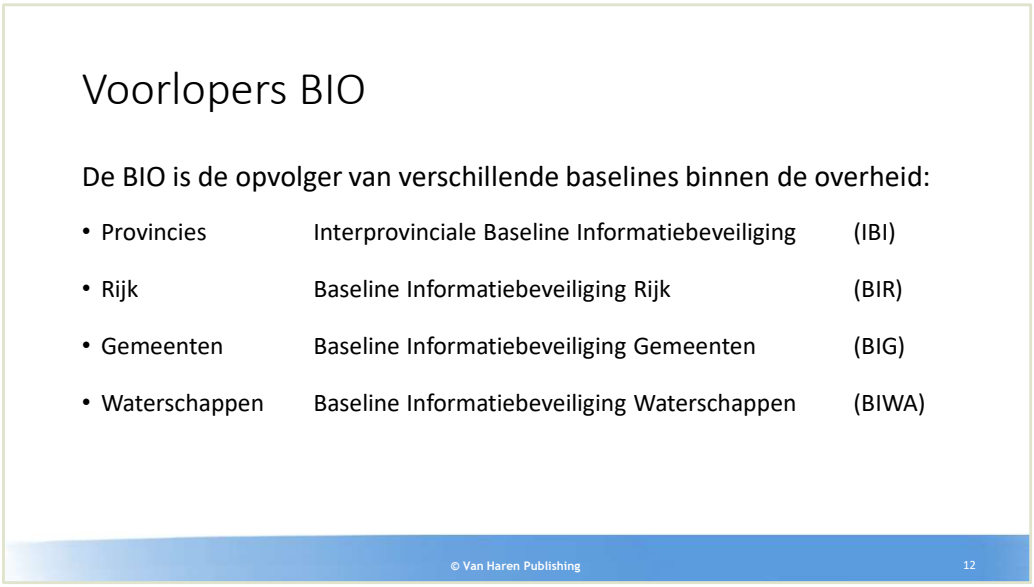
Algemeen

- Module 1: Achtergrond informatiebeveiliging en BIO

Module 2: Beleid en Organisatie

Module 3: Tactische en operationele beheersmaatregelen

Module 4: Incidenten & Bedrijfscontinuïteit



Aantekeningen:

Voorlopers

Interprovinciale Baseline Informatiebeveiliging
2010 IBI[1] (Provincies)

Baseline Informatiebeveiliging Rijk
2012 BIR1.0[1] (Rijksdiensten)
2018 BIR2017[2]

Baseline Informatiebeveiliging Gemeenten
2013 BIG[1] (Gemeenten)

Baseline Informatiebeveiliging Waterschappen2013
BIWA[1] (Waterschappen)

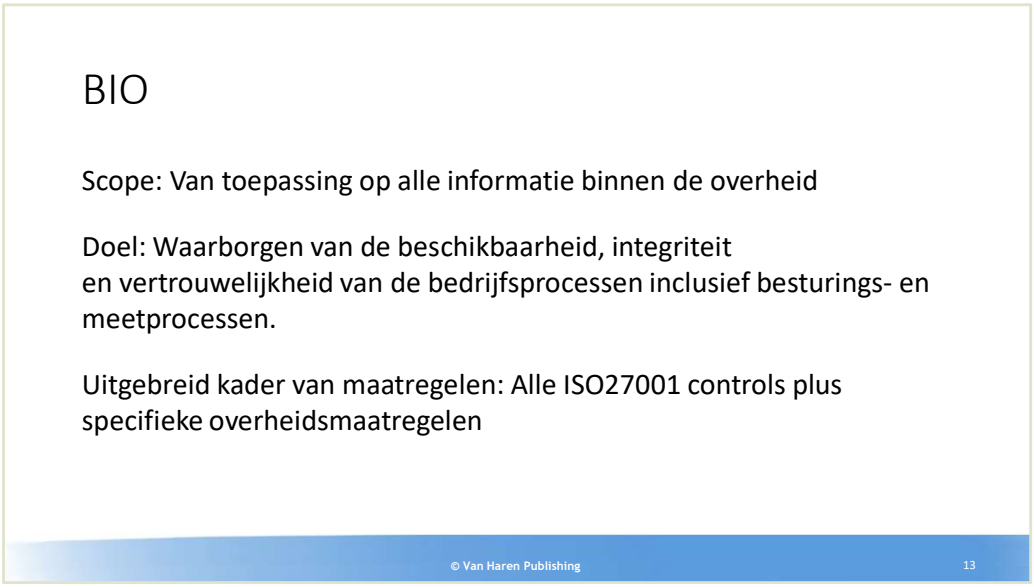
[1]gebaseerd op maatregelen uit de ISO27001:2005
[2]gebaseerd op maatregelen uit de ISO27001:2013

De interbestuurlijke werkgroep Normatiek onderhoudt de BIO (als onderdeel van het Overheidsbrede\ Beleidsoverleg Digitale Overheid (OBDO)). Het Directoraat-general Overheidsorganisatie (DGOO, onderdeel van BZ) is de trekker hiervan.

Afgeleid van de ISO27001 en 27002 norm
Bevat eigenlijk de controls uit de Annex A van de ISO27001 norm aangevuld met overheidsmaateregelen

Programma

- Algemeen
- Module 1: Achtergrond informatiebeveiliging en BIO
- Module 2: Beleid en Organisatie
- Module 3: Tactische en operationele beheersmaatregelen
- Module 4: Incidenten & Bedrijfscontinuïteit



Aantekeningen:

BIO is verplicht voor:
- rijksdiensten;
- provincies;
- waterschappen;
- gemeenten;
- andere organisaties waarvoor dit bij wet bepaald is.

Aanbevolen voor overige overheidsorganisaties en private samenwerkingen waarin de overheid enig aandeelhouder is.

De BIO: NEN-ISO/IEC 27001:2017 en de NEN-ISO/IEC 27002:2017 beschrijven details voor implementatie (implementatierichtlijnen) en eisen voor de procesinrichting (o.a. het ISMS uit NEN-ISO/IEC 27001:2017).

Die documenten geven dus de details voor de toepassing, die niet in de BIO zijn beschreven en die nodig blijven voor een goede implementatie van de BIO.

Om een effectieve implementatie van de BIO te doen is het noodzakelijk om ook de ISO27001 (voor het ISMS) en de ISO27002 (voor uitleg over de implementatie van controls) toe te passen.

Programma

- Algemeen
- Module 1: Achtergrond informatiebeveiliging en BIO
- Module 2: Beleid en Organisatie
- Module 3: Tactische en operationele beheersmaatregelen
- Module 4: Incidenten & Bedrijfscontinuïteit

Overige normenkaders

Enkele normenkaders:
DigiD, SUWInet, BRP, PUN, BAG, BGT, BRO, ENSIA

Scope:
Specifiek domein (bijvoorbeeld de webomgeving in geval van DigiD)

Doel:
Verantwoording. Bijvoorbeeld om aan te tonen te voldoen aan de eisen die aan het gebruik van een publieke dienst (zoals DigiD) gesteld worden of richting een toezichthouder.

© Van Haren Publishing

Aantekeningen:

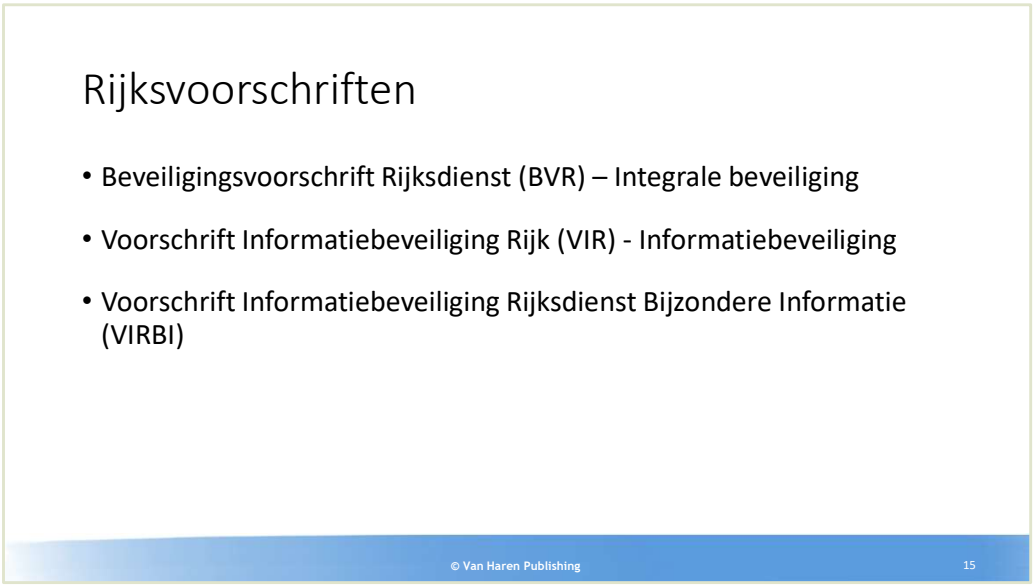
De overheid kent nog meer normenkaders. De relatie van een specifiek normenkader met de BIO is afhankelijk van de scope en het doel van deze overige normenkaders.

Deze normenkaders geven doorgaans een beperkte controlset aan die gericht is op het object waarover verantwoord moet worden.

Specifieke normenkaders kunnen van toepassing zijn voor overheid en niet overheid. Bijvoorbeeld verplicht voor afnemers van een dienst zoals bij DigiD.

Programma

- Algemeen
- Module 1: Achtergrond informatiebeveiliging en BIO
- Module 2: Beleid en Organisatie
- Module 3: Tactische en operationele beheersmaatregelen
- Module 4: Incidenten & Bedrijfscontinuïteit



Aantekeningen:

BVR
Beveiligingsvoorschrift Rijksdienst (BVR 2005) bevat richtlijnen voor de aanwijzing van de beveiligingsambtenaar (BVA) en verdere organisatie van integrale beveiliging bij de rijksdienst.

VIR
Het Voorschrift Informatiebeveiliging Rijksdienst (VIR 1995) is een besluit dat regelt hoe de Rijksoverheid omgaat met de informatiebeveiliging.

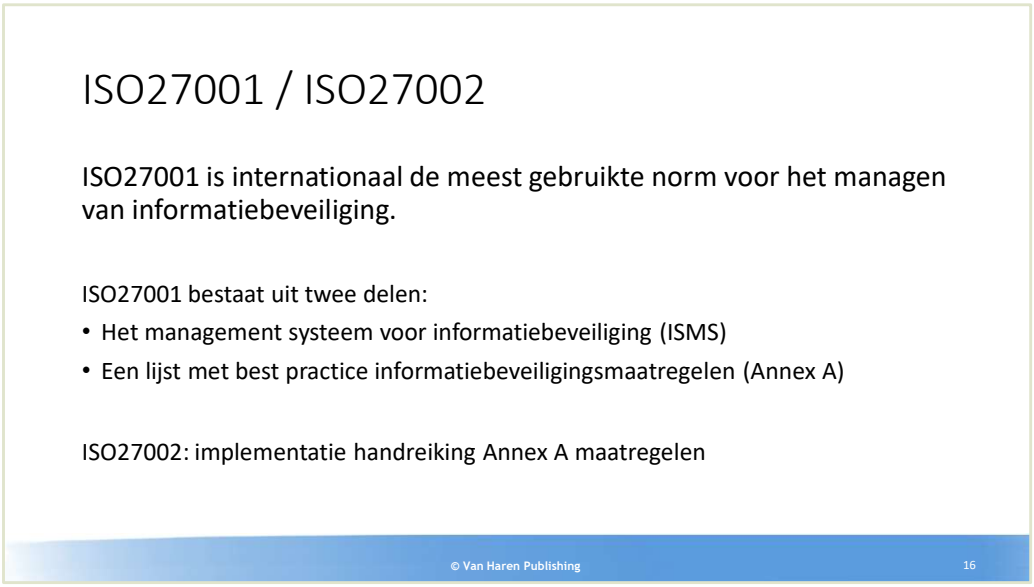
VIRBI
Voor de behandeling van vertrouwelijke informatie bij de Rijksoverheid is een aanvullende set van maatregelen van toepassing: Het Voorschrift Informatiebeveiliging Bijzondere Informatie (VIRBI).
In dit voorschrift wordt voor 4 categorieën van informatie extra eisen gesteld. Bijzondere informatie wordt als volgt gerubriceerd:

- Departementaal VERTROUWELIJK (Dep.V.)
- Staatsgeheim CONFIDENTIEEL (Stg.C)
- Staatsgeheim GEHEIM (Stg.G)
- Staatsgeheim ZEER GEHEIM (Stg.ZG)

Het VIRBI legt per beveiligingsniveau een niveau van beveiliging op aan de “beheerder” van vertrouwelijke informatie.

Programma

- Algemeen
- Module 1: Achtergrond informatiebeveiliging en BIO
- Module 2: Beleid en Organisatie
- Module 3: Tactische en operationele beheersmaatregelen
- Module 4: Incidenten & Bedrijfscontinuïteit



Aantekeningen:

ISO27001 is certificeerbaar. Dat wil zeggen dat een externe partij verklaart dat de organisatie het managementsysteem rond informatiebeveiliging aantoonbaar effectief ingericht heeft.

Relevante ISO standaarden voor informatiebeveiliging:

27000 Overzicht en terminologie
27001 Standaard voor Informatiebeveiliging
27002 Best practices voor Informatiebeveiliging
27005 Richtlijn Risk Management voor Informatiebeveiliging
27701 Privacy uitbreiding op de 27001/2

Geschiedenis:
Oorspronkelijk als BS 7799 gepubliceerd door BSI Group in 1995
Geadopteerd als ISO/IEC 17799, "Information Technology - Code of practice for information security management." in 2000.
In 2005 omgevormd naar de ISO27001:2005 en 27002
In 2013 herzien en ingericht volgens de High Level Structure ISO27001:2013

Programma

Algemeen

- Module 1: Achtergrond informatiebeveiliging en BIO

Module 2: Beleid en Organisatie

Module 3: Tactische en operationele beheersmaatregelen

Module 4: Incidenten & Bedrijfscontinuïteit



Aantekeningen:

Begrippen:

- Betrouwbaarheidsaspecten
- Persoonsgegevens
- Veiligheidsdomeinen
- Risico's
- Maatregelen
- Bedrijfsmiddel
- Waarde van bedrijfsmiddelen
- Kwetsbaarheid
- Dreiging
- Risico
- Incident
- Schade
- Risicomanagement
- Risicoanalyse
- Controls en overheidsmaatregelen
- Classificatie
- PDCA
- ISMS
- Basisbeveiligingsniveau (BBN)
- Diepgaande risicoanalyse (DRA)
- Beveiligingsvoorschrift Rijksdienst
- Voorschrift Informatiebeveiliging Rijksdienst
- Explains
- GAP-analyse

Programma

Algemeen

- Module 1: Achtergrond informatiebeveiliging en BIO

Module 2: Beleid en Organisatie

Module 3: Tactische en operationele beheersmaatregelen

Module 4: Incidenten & Bedrijfscontinuïteit



Aantekeningen:

Informatiebeveiliging wordt onderverdeeld in de volgende kwaliteitsaspecten

Beschikbaarheid:
Integriteit
Vertrouwelijkheid

De BIV in het Engels wordt vaak afgekort met CIA, Confidentiality, Integrity & Availability)

De betekenis kennen van de betrouwbaarheidsaspecten is belangrijk om de potentiële impact op deze aspecten te kunnen inschatten en voor het uitvoeren van de BBN toets

Vertrouwelijkheid
Informatie beschermen tegen ongeautoriseerde toegang tot informatie.
Gerelateerd begrippen:
bescherming van bedrijfsinformatie;
privacy bescherming;
“Need to know”.

Enkele maatregelen om vertrouwelijkheid te beschermen:
toegangscontrole, encryptie, geheimhoudingsverklaring.

Integriteit
Informatie beschermen tegen verwijdering of wijziging door onbevoegden.
Gerelateerd begrippen:
onweerlegbaarheid, compleet, accuraat.

Enkele maatregelen om integriteit te beschermen:
input validatie, vier ogen principe, hashing.

Beschikbaarheid
Informatie beschermen tegen het niet beschikbaar zijn.
Gerelateerd begrippen:
tijdigheid, continuïteit, robuustheid.

Enkele maatregelen om de beschikbaarheid te beschermen:
redundant, noodstroom voorziening, backup en restore.

Programma

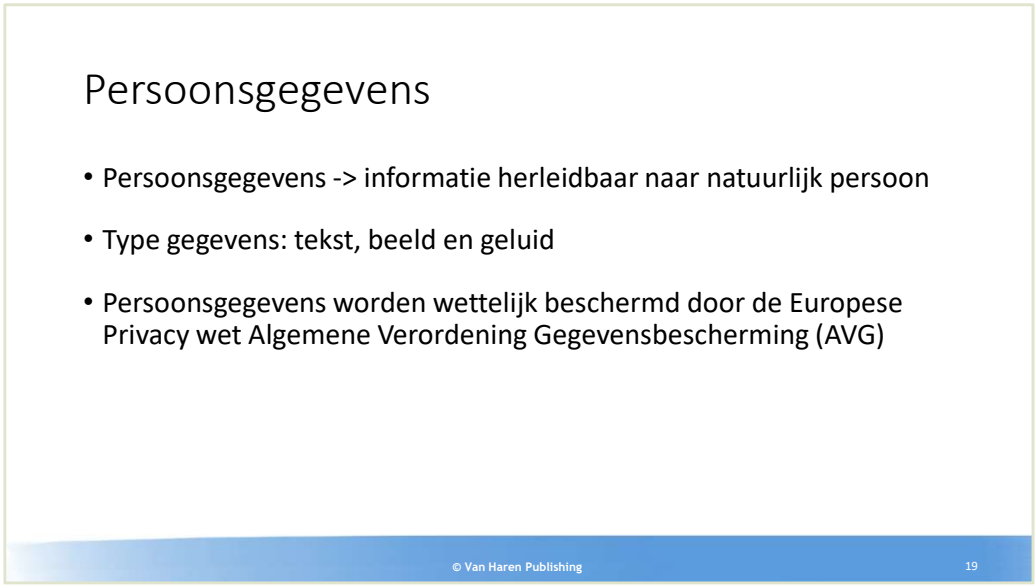
Algemeen

- Module 1: Achtergrond informatiebeveiliging en BIO

Module 2: Beleid en Organisatie

Module 3: Tactische en operationele beheersmaatregelen

Module 4: Incidenten & Bedrijfscontinuïteit



Aantekeningen:

Een **persoonsgegeven** is een gegeven dat herleidbaar is naar een natuurlijke persoon die geïdentificeerd is, of kan worden geïdentificeerd. De term “natuurlijk persoon” sluit rechtspersonen en overledenen uit. Persoonsgegevens vallen in de “privésfeer” (grondwettelijke term).

Informatiebeveiliging betreft het beschermen van de vertrouwelijkheid, integriteit en beschikbaarheid van “informatie” (in de breedste zin van het woord). Persoonsgegevens behoren tot die informatie. Maar naast persoonsgegevens beschikken organisaties ook over niet-persoonsgegevens. Dit is wel informatie maar niet herleidbaar naar een natuurlijk persoon en valt niet onder de AVG. Niet-persoonsgegevens worden ook wel bedrijfsgegevens genoemd. Informatiebeveiliging beschermd dus alle informatie dus zowel persoonsgegevens als bedrijfsgegevens. Alleen geldt er een wettelijke plicht voor de bescherming van persoonsgegevens terwijl er geen wettelijke plicht geldt voor de bescherming van bedrijfsgegevens.

Enkele voorbeelden:
• Persoonsgegevens: salaris administratie, personeelsadministratie, burgergegevens
• Bedrijfsgegevens: Bedrijfsadres, begroting, netwerk architectuur.

Informatie kan in sommige gevallen persoonsgegevens zijn terwijl dat in andere gevallen niet zo is. Dit kan afhangen van de aard van de gegevens of wie de gegevens beheerd. Zo kan bijvoorbeeld een adres herleidbaar zijn naar een rechtspersoon (bedrijfsadres) waardoor het geen persoonsgegeven is. Een kenteken van een voertuig, dat vaak geen persoonsgegeven is omdat het niet zondermeer herleidbaar is, kan een persoonsgegeven zijn wanneer het verzameld wordt door de Rijksdienst voor het Wegverkeer. Zij hebben kennis en expertise om het kenteken herleidbaar te maken. In het verlengde van het vorige voorbeeld kunnen technische ontwikkelingen en organisatie veranderingen er dus toe leiden dat niet-persoonsgegevens persoonsgegevens worden en andersom.
7

Programma

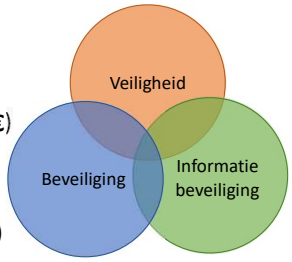
- Algemeen
- Module 1: Achtergrond informatiebeveiliging en BIO
- Module 2: Beleid en Organisatie
- Module 3: Tactische en operationele beheersmaatregelen
- Module 4: Incidenten & Bedrijfscontinuïteit

Gerelateerde veiligheidsdomeinen

Veiligheid
- Beschermen van het welzijn van mensen (♥)

Beveiliging (fysieke beveiliging)
- Beschermen van de continuïteit van de organisatie (€)

Informatiebeveiliging
- Beschermen van informatie (mens ♥ & organisatie €)



© Van Haren Publishing

Aantekeningen:

De termen veiligheid, (fysieke)beveiliging en informatiebeveiliging lijken op elkaar maar zijn niet hetzelfde. Ze hebben wel met elkaar te maken. Samen worden ze ook wel de veiligheidsdomeinen genoemd.

Organisaties kennen doorgaans verschillende afdelingen of verantwoordelijken voor veiligheid, beveiliging en informatiebeveiliging. Zo kan een organisatie als verantwoordelijke voor de bescherming van de veiligheidsdomeinen een veiligheidsfunctionaris, een afdeling beveiliging en een afdeling informatiebeveiliging hebben. Soms zijn er dezelfde maar soms ook tegenstrijdige belangen in de wijze van bescherming.

Vanuit het perspectief van informatiebeveiliging en fysieke beveiliging geldt bijvoorbeeld het uitgangspunt om de organisatie zoveel als mogelijk af te sluiten ter bescherming tegen diefstal. Maar vanuit het perspectief van veiligheid moet een organisatie juist open zijn om bij incidenten en calamiteiten te kunnen vluchten. De veiligheid van mensen gaat altijd voor de bescherming van de organisatie. Het vinden van een optimale bescherming van de verschillende domeinen vraagt om samenwerking, overeenstemming van risico's en afstemming van maatregelen.

Voorbeelden van incidenten:
- Veiligheid: Vallen, bedrijfsongeval, Arbo incident
- Fysieke beveiliging: Diefstal, inbraak, vernieling
- Informatiebeveiliging: Datalek, Hacking, stroomuitval

Er zijn incidenten (rampen) die twee of zelfs drie van de veiligheidsdomeinen raken. Bijvoorbeeld een grote aangestoken brand, of een overval waarbij met geweld en bedreiging van personen gegevensdragers buit zijn gemaakt.

Privacy is een onderwerp wat in feite alle drie de domeinen raakt. Informatiebeveiliging is het meest voor de hand liggende domein. Maar waar het bij veiligheid gaat om de lichamelijke bescherming van mensen gaat het bij privacy om de digitale veiligheid van mensen. Digitale veiligheid in de vorm van de bescherming van persoonsgegevens. En omdat persoonsgegevens ook fysiek voorkomen moet het ook fysiek beschermd worden.

Programma

- Algemeen
- Module 1: Achtergrond informatiebeveiliging en BIO
- Module 2: Beleid en Organisatie
- Module 3: Tactische en operationele beheersmaatregelen
- Module 4: Incidenten & Bedrijfscontinuïteit



Aantekeningen:

Programma

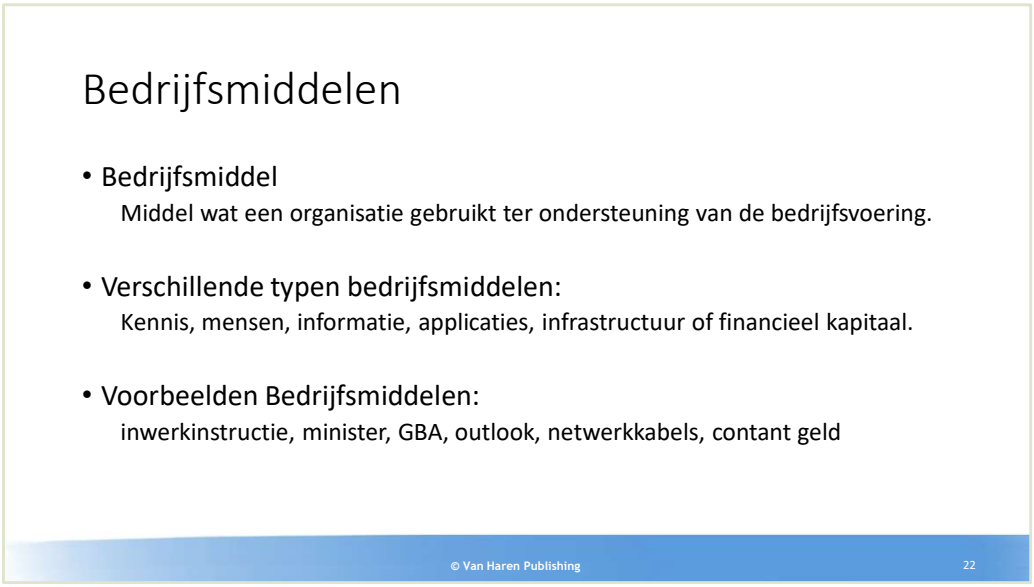
Algemeen

- Module 1: Achtergrond informatiebeveiliging en BIO

Module 2: Beleid en Organisatie

Module 3: Tactische en operationele beheersmaatregelen

Module 4: Incidenten & Bedrijfscontinuïteit



Aantekeningen:

Bedrijfsmiddel is een term die meer omvattend is dan alleen informatiebeveiliging. Bij financiële boekhouding is een bedrijfsmiddel elk middel dat eigendom is van een bedrijf of een economische entiteit. Het is alles (materieel of immaterieel) dat eigendom kan zijn of kan worden ingezet om waarde te produceren en dat in het bezit is van een economische entiteit en een positieve economische waarde kan opleveren. Eenvoudig gezegd vertegenwoordigen activa (bedrijfsmiddelen) de eigendomswaarde die kan worden omgezet in contant geld (hoewel contant geld zelf ook als een bedrijfsmiddel wordt beschouwd).

Bij informatiebeveiliging beschermen we een gedeelte van de totale bedrijfsmiddelen van de organisatie. Namelijk het “informatie-gedeelte”. Er worden maatregelen getroffen om de vertrouwelijkheid beschikbaarheid en integriteit van de informatie-bedrijfsmiddelen te beschermen. Als we binnen informatiebeveiliging spreken van bedrijfsmiddelen dan worden daar alleen die bedrijfsmiddelen bedoeld die betrekking hebben op informatiebeveiliging. Contant geld is bijvoorbeeld wel een bedrijfsmiddel maar valt niet onder informatiebeveiliging.

Een organisatie beschikt doorgaans over een diversiteit en aanzienlijke hoeveelheid aan bedrijfsmiddelen. Niet allemaal zijn ze even relevant voor informatiebeveiliging.
De uitkomst van de Business Impact Analyse (BIA) kan worden gebruikt om op basis van belangrijke bedrijfsprocessen overzicht en prioritering te verkrijgen in bedrijfsmiddelen die relevant zijn.