



Stichting NIOC

Stichting NIOC en de NIOC kennisbank

Stichting NIOC (www.nioc.nl) stelt zich conform zijn statuten tot doel: het realiseren van congressen over informatica onderwijs en voorts al hetgeen met een en ander rechtstreeks of zijdelings verband houdt of daartoe bevorderlijk kan zijn, alles in de ruimste zin des woords.

De stichting NIOC neemt de archivering van de resultaten van de congressen voor zijn rekening. De website www.nioc.nl ontsluit onder "Eerdere congressen" de gearchiveerde websites van eerdere congressen. De vele afzonderlijke congresbijdragen zijn opgenomen in een kennisbank die via dezelfde website onder "NIOC kennisbank" ontsloten wordt.

Op dit moment bevat de NIOC kennisbank alle bijdragen, incl. die van het laatste congres (NIOC2025, gehouden op donderdag 27 maart 2025 jl. en georganiseerd door Hogeschool Windesheim). Bij elkaar zo'n 1500 bijdragen!

We roepen je op, na het lezen van het document dat door jou is gedownload, de auteur(s) feedback te geven. Dit kan door je te registreren als gebruiker van de NIOC kennisbank. Na registratie krijg je bericht hoe in te loggen op de NIOC kennisbank.

Het eerstvolgende NIOC vindt plaats op 18 maart 2027 in Arnhem en wordt georganiseerd door HAN University of Applied Sciences.

Reacties over de NIOC kennisbank en de inhoud daarvan kun je richten aan de beheerder:

R. Smedinga kennisbank@nioc.nl.

Vermeld bij reacties jouw naam en telefoonnummer voor nader contact.



Cyber Security Council



Dutch
Government



Loopbaanperspectieven voor cybersecurity

Fred van Noord
voorzitter PvIB

Marcel Spruit
*lector Cybersecurity
Haagse Hogeschool*

NIOC
23 april 2015

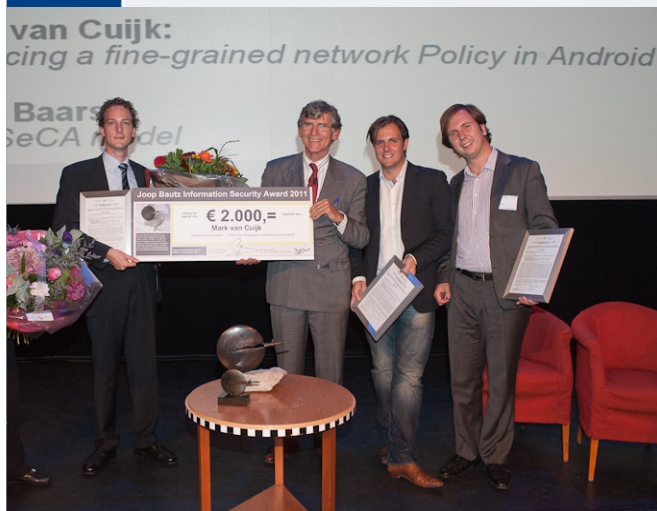
Fred van Noord

- Voorzitter PvIB
- Projectleider QIS:
kwalificatiestelsel voor informatiebeveiligers
- Projectleider Rijksoverheid:
ontwikkelen van één risicoanalyse methodiek voor de gehele
Rijksdienst (departementen en hun agentschappen)

PvIB – beroepsver. Informatiebeveiligers



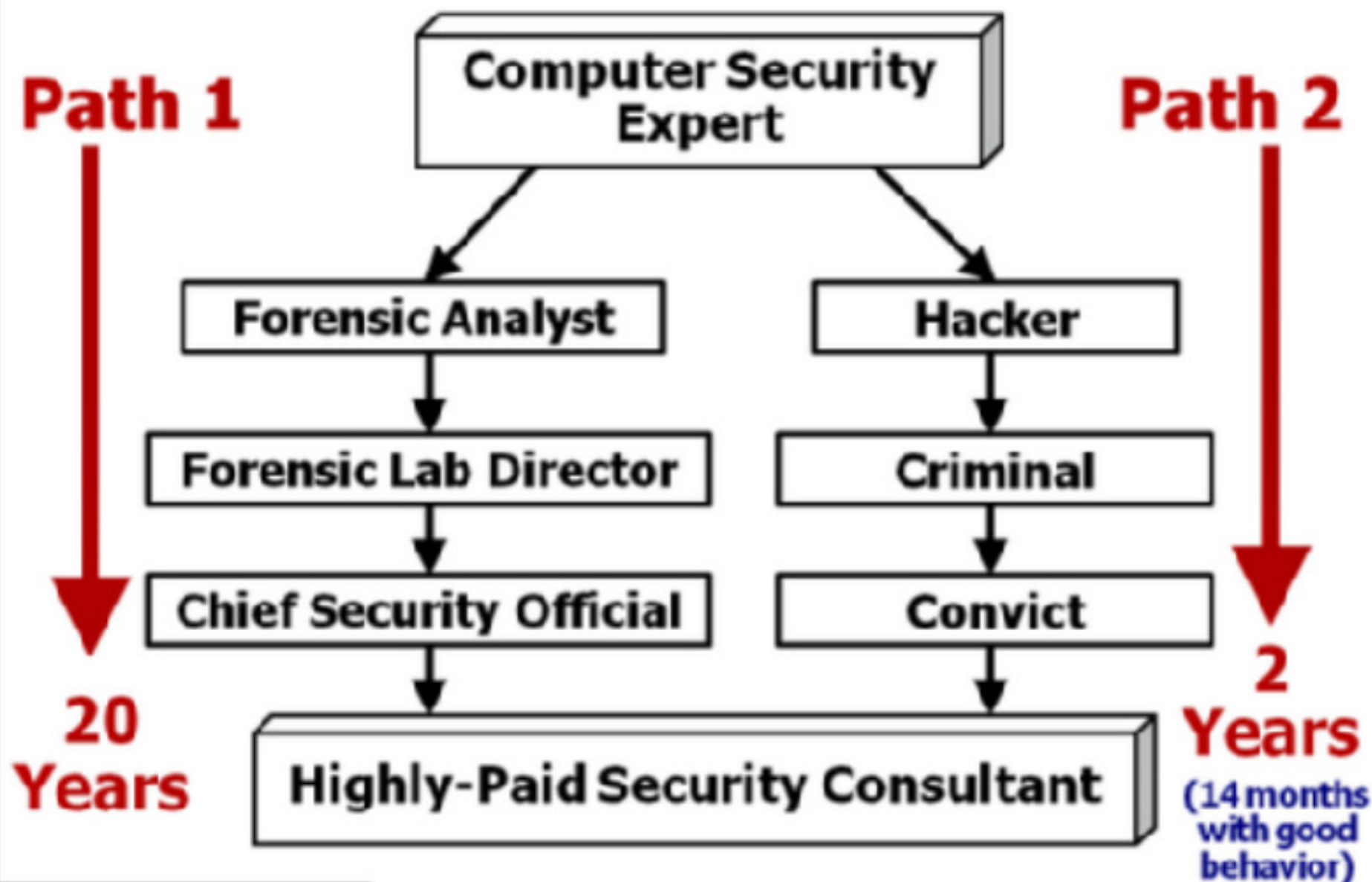
- Onafhankelijk en non-profit
- Vrijwillige inzet van professionals uit de praktijk (± 60)
- Groeiend aantal leden: 1500 (vele sectoren; 100 studenten)
- Kennis delen & netwerken:
 - Vakblad Informatiebeveiliging, Expertbrieven
 - Themasesies, Young Professionals, CISO bijeenkomsten
 - Security congres, Award voor potentials: scripties, dissertaties
 - Kwalificatie: 2-jaarlijkse Opleidingenmarkt, QIS Publiek Privaat Programma



Cybersecurity vs. informatiebeveiliging

- Cybersecurity (NCTV, Nationaal Coörd. Terrorismebestrijding en Veiligheid)
= het vrij zijn van gevaar of schade veroorzaakt door **verstoring of uitval van ICT of door misbruik van ICT**.
Het gevaar of de schade door misbruik, verstoring of uitval kan bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van de ICT, schending van de vertrouwelijkheid van in ICT opgeslagen informatie of schade aan de integriteit van die informatie.
- Informatiebeveiliging (ISO-normen: 27001 en 27002):
= het behouden van de vertrouwelijkheid, integriteit en beschikbaarheid van **informatie**.
Omvat ook de beveiliging van de niet-geautomatiseerde informatievoorziening.
- 16-17 april 2015: Global Conference on Cyber Space
Global Forum on Cyber Expertise (GFCE) gelanceerd
Het forum voor internetveiligheid
Secretariaat in Den Haag
Richt zich op cybersecurity, cybercrime, databescherming en e-development.

Computer Security Career Paths



Waarom beroepsprofielen nodig?

- **Context**

- afhankelijkheid bedrijfsprocessen van informatie groeit
- IB-beroepen zijn niet goed gedefinieerd
- te veel certificaten, niet-geharmoniseerd
- te weinig IB-opleidingen
- te weinig IB-professionals.

- **Behoefte**

- IB-beroepen zijn gedefinieerd
- kwalificaties zijn uniform, transparant en erkend.
- opleiden gaat sneller en gericht dan vanuit de praktijk
- meer opleidingsmogelijkheden

Acronym	Meaning
ABCP	Associate Business Continuity Professional
CAP	Certified Authorization Professional
CBCP	Certified Business Continuity Professional
CEH	Certified Ethical Hacker
CGEIT	Certified in the Governance of Enterprise IT
CIA	Certified Internal Auditor
CIPP	Certified Information Privacy Professional
CISA	Certified Information Systems Auditor
CISM	Certified Information Security Manager
CISSP	Certified Information Systems Security Prof.
CITP	Certified Information Technology Prof.
CRISC	Certified Risk and Information Syst. Control
CSSLP	Certified Secure Software Lifecycle Prof.
FBCI	Fellow of the Business Continuity Institute
FBCS	Fellow of the British Computer Society
ISMAS	Information Security Management Advanced
ISMES	Information Security Management Expert
ISSAP	Information Syst. Security Architecture Prof.
ISSEP	Information Systems Security Eng. Prof.
ISSMP	Information Systems Security Mngt Prof.
MBCP	Master Business Continuity Professional
MISM	Master of Information Security Management
MSIT	Master of Science in Information Technology
OPSA	OSSTMM Professional Security Analyst
OPST	OSSTMM Professional Security Tester
QICA	Qualification in Computer Auditing
RE	Register EDP auditor
RIB	Register Informatie Beveiliging
RO	Register Operational auditor
RSE	Register Security Expert
SSCP	Systems Security Certified Practitioner

ASML-hack is symptoom van cyberwapenwedloop



 Cleanroom van chipmachinefabrikant ASML. Het Veldhovense bedrijf is doelwit geweest van computerin...

- april: vier Belgische dagbladen: DDoS aanvallen
- februari: Gemalto (simkaarten), internationale banken
 - eind 2014: Sony Pictures

14 Z & Z Cybercrime

```
props PROXY_SERVER_KEY = "GATOR.PROXY_DATA.PROXY.SERVER"
props getFlameId = function()
config.hasKey( flame_props.FLAME_ID_CONFIG_KEY) then
cal l_l_0 = config.get
cal l_l_1 = flame_props.FLAME_ID_CONFIG_KEY
turn l_l_0(l_l_1)

rn nil
```

Tekort van honderden specialisten

Digitalisering maakt de samenleving kwetsbaar. De overheid komt specialisten tekort om haar systemen te beschermen. „De politieke ambities zetten praktische mogelijkheden op de tweede plaats”, zegt Steven Luitjens.

DOOR KEES VERSTEEGH

Dinsdagnacht 13 december ging het mis in de Rotterdamse haven. Vanaf 23.31 uur kwam de handelsstroom via de belangrijkste Nederlandse haven goeddeels stil te liggen. Het centrale computersysteem (Digipoort OTP) voor elektronische aangiftes van im- en exportgoederen bij de douanedienst en de belastingdienst viel uit.

„De boel gaat vaker op tilt, maar dit was een fors incident”, vertelt Hans Maessen, directeur van Maco Customs Service in Rotterdam. Zijn bedrijf zorgt voor de elektronische afhandeling van douane- en belas-

van Binnenlandse Zaken. Logius is verantwoordelijk voor Digipoort en KPN doet in opdracht van Logius het dagelijkse operationele werk. Het zou tot het begin van de volgende middag duren totdat de storing bij Digipoort verholpen was.

KPN wil niet veel kwijt over het incident, dat werd veroorzaakt in haar datacentrum in Aalsmeer. Wel zegt een woordvoerder: „Dat de CEO van KPN door een betrokken klant persoonlijk is gebeld, bleek achteraf onnodig en is het gevolg van een misverstand.”

Het incident in de Rotterdamse haven kwam niet in het nieuws. Andere incidenten wel, zoals in april de dagenlange storing bij Vodafone na

computers van het Rijk.

Na aanleiding van deze incidenten noemt Logius-directeur Steven Luitjens het „volstrekt begrijpelijk dat er een stevig debat is ontstaan of Nederland voldoende is voorbereid op de hoge eisen die een steeds verder gedigitaliseerde samenleving stelt aan de overheid en het bedrijfsleven.”

„Storingen zoals in de Rotterdamse haven en aanvallen van hackers nemen hand over hand toe. Dat bleek deze week weer met de geslaagde hackersaanval op LinkedIn. Het internet is een onveilige plaats waar kwaadwillenden op het oog bijna vrij baan hebben. Tegelijkertijd is er hype: we moeten niet blijven hangen in het uitvergroten van incidenten, maar kijken naar de achterliggende patronen”, aldus Luitjens.

In hoeverre is de overheid weer 'in control' na de grote DigiNotar-crisis?

„Uit evaluaties blijkt dat de overheid adequaat heeft gereageerd. Tegelijk hebben we veel geleerd van die crisis. We zitten nu dichterbij de bal. We voeren – ook onaangekondigd – veelvuldiger zelf controles en testen uit. We zijn in onze contracten met leveranciers meer gedetailleerde eisen

gaan stellen. Daarnaast willen we ons niet meer afhankelijk maken van één leverancier van veiligheidscertificaten [certificaten die waarborgen dat een website echt is, red.] Het DigiNotar-probleem heeft ons bewust gemaakt van nieuwe risico's.”

Er werd door de overheid, behalve meer toezicht, ook meer professionaliteit bij organisaties als de uwe beloofd.

„Er is meer toezicht. Maar goede mensen, dat is een aanzienlijk lastiger verhaal. Er wordt gesuggereerd dat mensen die je nodig hebt aan een boom groeien. Dat is helaas niet het geval. Neem mijn eigen organisatie: de afdeling die toezicht houdt op de zeven leveranciers van certificaten waarmee het vorig jaar mis ging, groeide van 1,5 fte naar 3. Maar zelfs voor die paar plekken kan ik nauwelijks geschikte mensen vinden, ondanks intensieve wervingspogingen. Juist als je dichterbij je leveranciers en de markt gaat zitten, realiseer je je welke lacunes er in je eigen kennis en organisatie zitten. Op sleutelposities voor ict komen overheid én bedrijfsleven naar mijn schatting minimaal ettelijke honderden experts tekort.”

Wat betekent deze schaarste voor

en expertise vragen dan we dachten.

„De overheid heeft, net als het bedrijfsleven, enorme plannen met het verder toepassen van ict. Politieke ambities zetten praktische mogelijkheden daarbij te vaak op de tweede plaats. Zo bevat het huidige innovatiebeleid van het kabinet ambitieuze plannen voor de toepassing van ict in transport en logistiek. Maar de uitval van het computersysteem in de Rotterdamse haven laat juist zien dat we beter eerst zulke incidenten kunnen voorkomen. Het Rotterdamse voorbeeld laat ook de kwetsbaarheid zien van allerlei organisaties die via ict zijn verbonden. Een storing in een klein deel van de keten heeft grote gevolgen elders.”

Hoe kan de overheid die kwetsbaarheid verkleinen, los van het terugschakelen van ambities?

„We moeten in elk geval snel nieuwe opleidingsinitiatieven starten. We moeten met kennisinstituten zoals de TU Delft en andere universiteiten, en het bedrijfsleven afspraken maken zodat er meer mensen worden opgeleid. Er zijn genoeg jongeren die geïnteresseerd zijn, ik ben daar niet fatalistisch over. Terugkijkend hadden wij als overheid en bedrijfsleven veel eerder moeten zeggen: we moe-

Het belang van gekwalificeerde informatiebeveiligers

Europa - Neelie Kroes, de Digitale Agenda 2010

- Stem nationale kwalificaties af met die van andere Europese landen
- Wellicht kan PvIB een beroepsregister organiseren en dat afstemmen met zusterorganisaties in andere landen



Nederland

- Nationale Cybersecurity Strategie 2 (2014-2016)
'Van bewust naar bekwaam'

Doelstelling 5:

Nederland beschikt over voldoende cybersecuritykennis en -kunde en investeert in ICT-innovatie om onze cybersecuritydoelstellingen te behalen

Actie	Wie	Wanneer
31. Er zal een PPS taskforce Cybersecurity Onderwijs worden ingesteld, die zich richt op advisering over het cybersecurity onderwijsaanbod. Onder andere certificering, diplomering en het (verder) ontwikkelen van lesmodules.	VenI, EZ, OCW	2014



Video

Algemeen Overleg min. V&J

april 2012

m.m.v.

Opstelten

Spies

Teeven

Hennis-Plasschaert



European e-Competence Framework (e-CF)

- Het Europese referentiemodel voor ICT-competenties
- (Internationaal) vergelijkbaar maken van competenties ICT-professionals:
 - voor **werkgevers** wordt het makkelijker om het juiste personeel aan te trekken
 - **opleidingsinstituten** kunnen hun onderwijs beter afstemmen op behoeften van de markt
 - **werknemers** kunnen makkelijker hun kennis en kunde 'verkopen'.
- 40 e-competenties
- 23 ICT-beroepsprofielen gedefinieerd
- e-CF wordt in 2015 Europese standaard
- Ministerie van EZ ondersteunt het e-CF vanuit Digivaardig & Digiveilig
- e-CF is geadopteerd door Rijksoverheid: Functiegebouw Rijk.



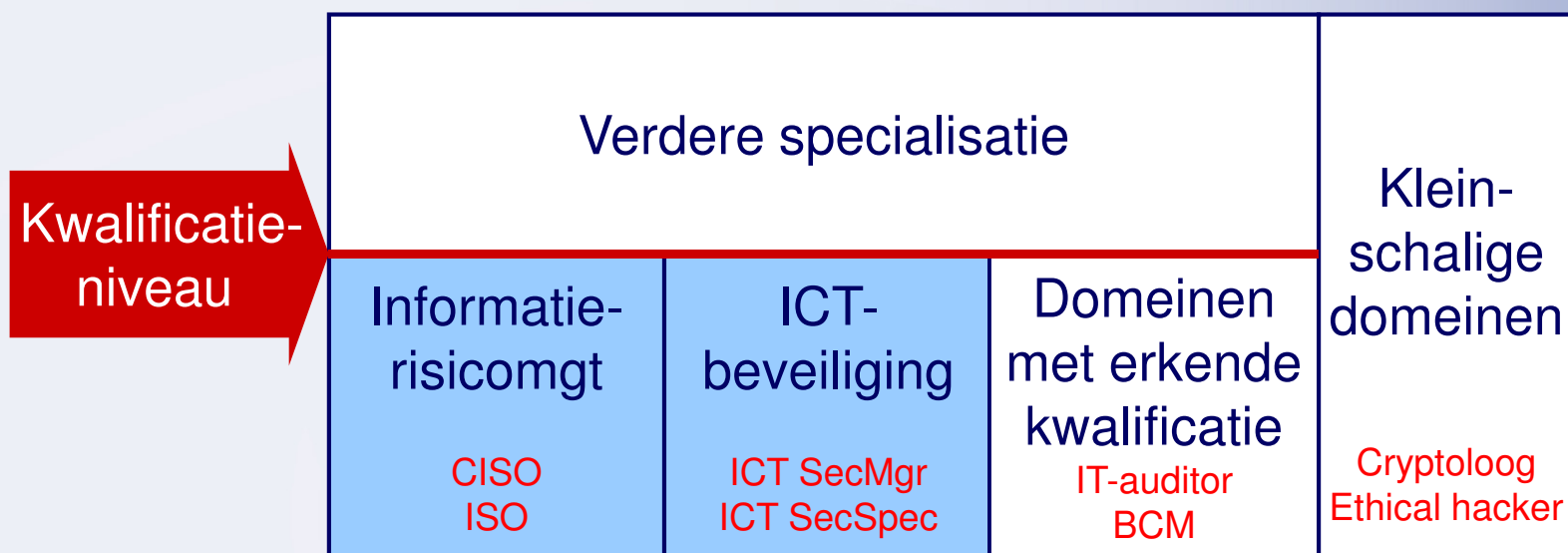
Dimension 1	Dimension 2	Dimension 3				
5 e-competence areas (A - E)	40 e-competences Identified	e-competence proficiency levels e-1 to e-5 (related to EQF levels 3-8)				
		e-CF levels Identified for each competence				
		e-1	e-2	e-3	e-4	e-5
A. PLAN	A.1. IS and Business Strategy Alignment					
	A.2. Service Level Management					
	A.3. Business Plan Development					
	A.4. Product/ Service Planning					
	A.5. Architecture Design					
	A.6. Application Design					
	➡ A.7. Technology Trend Monitoring					
	A.8. Sustainable Development					
	A.9. Innovating					
B. BUILD	B.1. Application Development					
	B.2. Component Integration					
	B.3. Testing					
	➡ B.4. Solution Deployment					
	B.5. Documentation Production					
	B.6. Systems Engineering					
C. RUN	C.1. User Support					
	C.2. Change Support					
	C.3. Service Delivery					
	C.4. Problem Management					
D. ENABLE	➡ D.1. Information Security Strategy Development					
	D.2. ICT Quality Strategy Development					
	D.3. Education and Training Provision					
	D.4. Purchasing					
	D.5. Sales Proposal Development					
	D.6. Channel Management					
	D.7. Sales Management					
	D.8. Contract Management					
	D.9. Personnel Development					
	D.10. Information and Knowledge Management					
	D.11. Needs Identification					
	D.12. Digital Marketing					
E. MANAGE	E.1. Forecast Development					
	E.2. Project and Portfolio Management					
	➡ E.3. Risk Management					
	➡ E.4. Relationship Management					
	E.5. Process Improvement					
	E.6. ICT Quality Management					
	E.7. Business Change Management					
	➡ E.8. Information Security Management					
	E.9. IS Governance					

European e-Competence Framework 3.0

A common European framework for ICT Professionals in all industry sectors



Domeinen informatiebeveiliging





4 representatieve beroepsprofielen
ontwikkeld met 60 professionals,
gereviewed door de organisaties van de
Stuurgroep QIS en
Klankbordgroep QIS



Definieert de informatiebeveiligingsstrategie en organiseert en stuurt informatiebeveiliging van de organisatie overeenkomstig de behoeften en de risicobereidheid van de organisatie.

Definieert de ICT-beveiligingsrichtlijnen voor de organisatie in overeenstemming met de informatiebeveiligingsstrategie en -architectuur van de organisatie en organiseert en managet de ICT-beveiliging van de organisatie.

	Informatie risico management	ICT beveiliging
Strategisch/ tactisch	Chief Information Security Officer (CISO)	ICT Security Manager
Tactisch/ operationeel	Information Security Officer (ISO)	ICT Security Specialist

Implementeert informatiebeveiliging in overeenstemming met de informatiebeveiligingsstrategie van de organisatie

Geeft invulling aan de ICT-beveiligingsrichtlijnen van de organisatie.

Profieltitel	CHIEF INFORMATION SECURITY OFFICER		
Samenvatting	Definieert de informatiebeveiligingsstrategie en organiseert en stuurt de informatiebeveiliging van de organisatie overeenkomstig de behoeften en de risicobereidheid van de organisatie.		
Missie			
Producten	Eindverantw.	Realiseert	Draagt bij
	•	•	•
Kerntaken	• Definieert de informatiebeveiligingsstrategie • Organiseert informatiebeveiliging en expertise •		
e-Competenties (uit e-CF)	D.1. Strategieontwikkeling informatiebev.		Niveau 5
	E.3. Risicomanagement		Niveau 4
	E.4. Relatiemanagement		Niveau 4
	E.8. Informatiebeveiligingsmanagement		Niveau 5
Algemene competenties	G.1. Leiderschap		Niveau 4
	G.6. Management		Niveau 4
	G.3. Communicatie en overtuigingskracht		Niveau 4
	G.5. Organisationsensitiviteit		Niveau 4
	G.7. Analytisch vermogen		Niveau 4
	G.8. Integriteit		Niveau 4
Ervaring	• Een relevante Master-opleiding of vergelijkbaar • Senioriteit op het gebied van informatiebeveiliging		
KPI			



= Generieke beroeps-
beschrijving

Uitgewerkt in
whitepaper

Opleidingsprofiel

Competentie	Kennis / vaardigheden	Leerdoelen [niveau]
E.3 Risico-management	Kent / is zich bewust van / is bekend met:	•Heeft kennis van en inzicht in:
Level 4	K1 Bedrijfswaarden en bedrijfsbelangen waarop risicoanalyses moeten worden toegepast K2 Rentabiliteit van investeringen vergeleken met risicomijding K3 'Best practices' (methoden) en standaarden voor risicoanalyse S1 S2 S3	– De belangrijkste principes en modellen uit de organisatiekunde, hun kenmerken en toepassingen [4] – De belangrijkste principes en modellen voor governance en alignment, hun kenmerken en toepassingen [4] – De belangrijkste principes en modellen voor financiële stelsels, hun kenmerken en toepassingen [4] – De belangrijkste modellen, methoden en technieken voor risicomanagement, hun kenmerken en toepassingen [4] –

Opleidingsprofielen - inhoudelijk



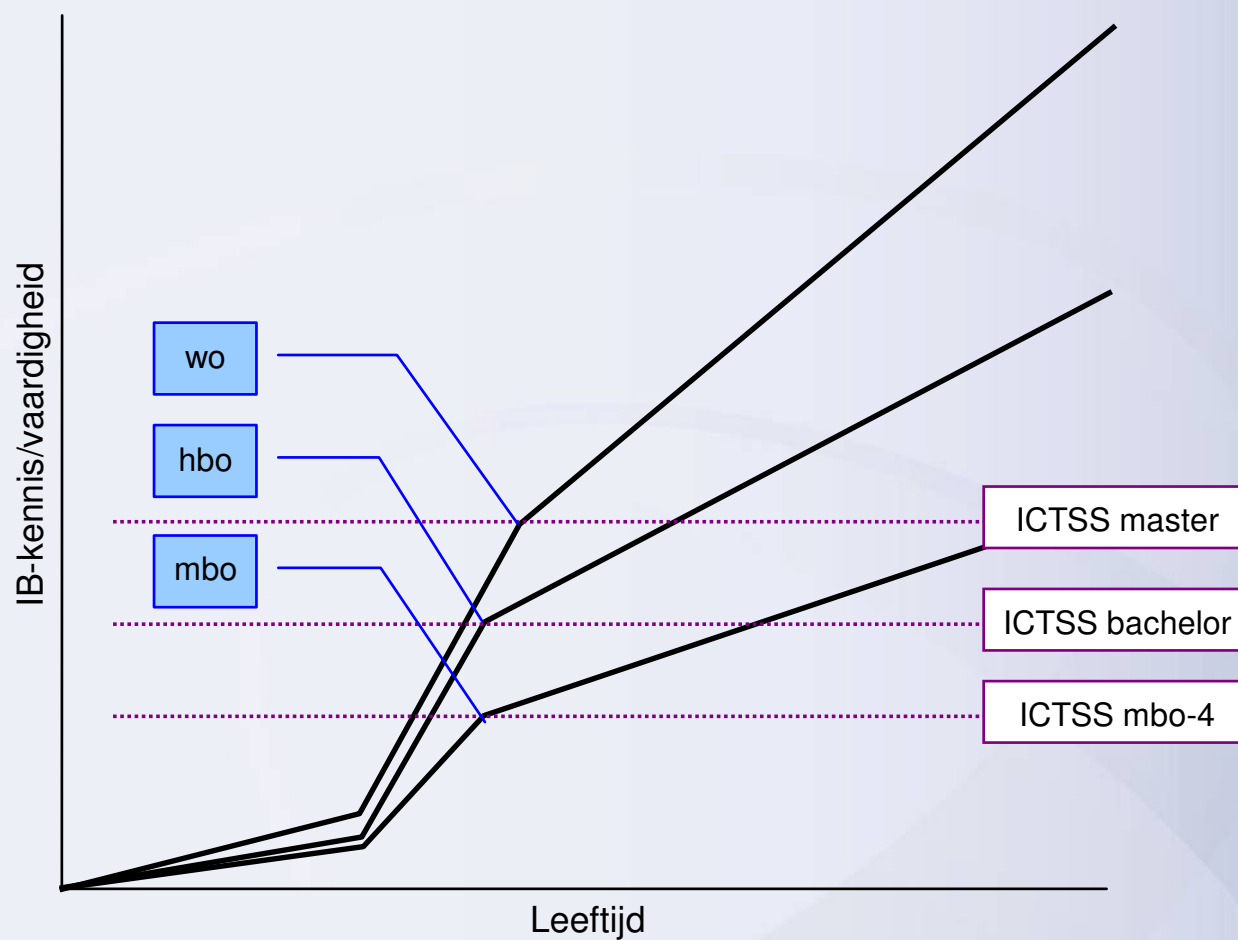
Onderwerp \ Opleiding	IRM Strat.	IRM Tact.	IT-bev. Strat.	IT-bev. Tact.
Organisatie				
Organisatiekunde	X	X		
Veranderkunde	X			
Projectmanagement	X	X	X	
Beveiligingsarchitectuur	X		X	
Risico- en security management	X	X		
Risicoanalyse	X	X	X	X
Business continuity management	X			
Wet- en regelgeving en compliance	X	X	X	
Financieel management	X		X	
Beveiligingsstandaarden	X	X		
Mens en gedrag				
Psychologie	X	X		
Menselijk falen	X	X		
Communicatie	X	X	X	
Techniek				
Informatietechnologie			X	X
Malware- en fraudetechnieken			X	X
Cryptografie			X	X
Computer- en netwerkbeveiliging			X	X
Softwarebeveiliging			X	X
SCADA-beveiliging			X	X
Technische beveiligingsstandaarden			X	X
Vaardigheden				
Leiding geven	X	X	X	
Samenwerken	X	X	X	X
Analyseren	X	X	X	X
Presenteren (mondeling, schriftelijk)	X	X	X	X
Adviseren	X	X	X	X
Auditen	X	X	X	X

Risk en security in niet-security gerelateerde e-competenties (2)



e-Competence	Knowledge	Skills	Level
B.1. Application Development Interprets the application design to develop a suitable application in accordance with customer needs. Adapts existing solutions by e.g. porting an application to another operating system. Codes, debugs, tests and documents and communicates product development stages. Selects appropriate technical options for development such as reusing, improving or reconfiguration of existing components. Optimises efficiency, cost and quality. Validates results with user representatives, integrates and commissions the overall solution.	K1 appropriate software programs / modules K2 hardware components, tools and hardware architectures K3 functional & technical designing K4 state of the art technologies K5 programming languages K6 Power consumption models of software and / or hardware K7 DBMS K8 operating Systems and software platforms K9 Integrated development environment (IDE) K10 rapid application development (RAD) K11 IPR issues K12 modeling technology and languages K13 interface definition languages (IDL) K14 security	S1 explain and communicate the design / development to the customer S2 perform and evaluate test results against product specifications S3 apply appropriate software and / or hardware architectures S4 develop user interfaces, business software components and embedded software components S5 manage and guarantee high levels of cohesion and quality S6 use data models S7 perform and evaluate test in the customer or target environment S8 cooperate with development team and with application designers	1 - Acts under guidance to develop, test and document applications. 2 - Systematically develops and validates applications. 3 - Acts creatively to develop applications and to select appropriate technical options. Accounts for others development activities. Optimizes application development, maintenance and performance by employing design patterns and by reusing proved solutions.

ICT Security Specialist – 3 niveaus



2014-2015: Uitwerken Opleidingsprofielen

1. Professionals

- Opleiders IB opleidingenmarkt
- ISACA, (ISC)²
- koepels: SPIH, VOI

2. Jong talent

Doelen: Bijeenkomst mei 2015

- 1) ontwikkelen keuzedelen MBO-4 ICT Security Specialist
- 2) aansluiting met HBO

- ROC Mondriaan (Den Haag), ROC van Amsterdam, ROC van Hilversum, ROC Nijmegen, ROC Aventus
- Haagse Hogeschool, Fontys, HvA
- ECABO
- NWO

eCF-niveau	EQF-niveau	Functioniveau	Opleidingsniveau
5	8	Principal	Master+
4	7	Senior-manager / Topspecialist	Master
3	6	Manager / Senior-specialist	Bachelor
2	4-5	Professional	Mbo4/vwo/havo
1	3	Associate	Mbo3

Level	Knowledge	Skills
5	Exceptionally comprehensive and detailed knowledge and understanding of the subject	Guiding others who carry out the activity in a very complex context
4	Very extensive and detailed knowledge and understanding of the subject	Carrying out the activity in a very complex context
3	Knowledge and understanding of the subject in detail	Carrying out the activity in a difficult context
2	Knowledge and understanding of all major aspects of the subject	Carrying out the activity in a simple context
1	Basic knowledge and understanding of the subject	Carrying out the activity in a simple context under guidance

Matchen opleidingen en certificaten

		curriculum		Security of the information (Information risk management)		Security of the ICT (ICT security)			
		level	G/P/S	CISO	ISO	ICT Sec. manager	ICT Security Specialist		
	e-CF Competency	Knowl	Skill	Knowl	Skill		master	bachelor	mbo-4
A7	Technology Trend Monitoring					3	4	3	2
B4	Solution Deployment						3	2	2
D1	Information Security Strategy Development			5					
E3	Risk Management				3	3	3		
E4	Relationship Management			4					
E8	Information Security Management			5	4	4	3	3	2
	General Competency								
G1	Leadership			4					
G2	Project management				3	3			
G3	Communication and persuasion			4	3	3	4	2	2
G4	Technical research				3		4	3	2
G5	Organisational sensitivity				3				
G6	Management			4		3			
G7	Analytical skills			4	3	3	4	3	
G8	Integrity			4	4	4	3	3	2

General

Someone with this certificate will most likely have the competence.

Partial

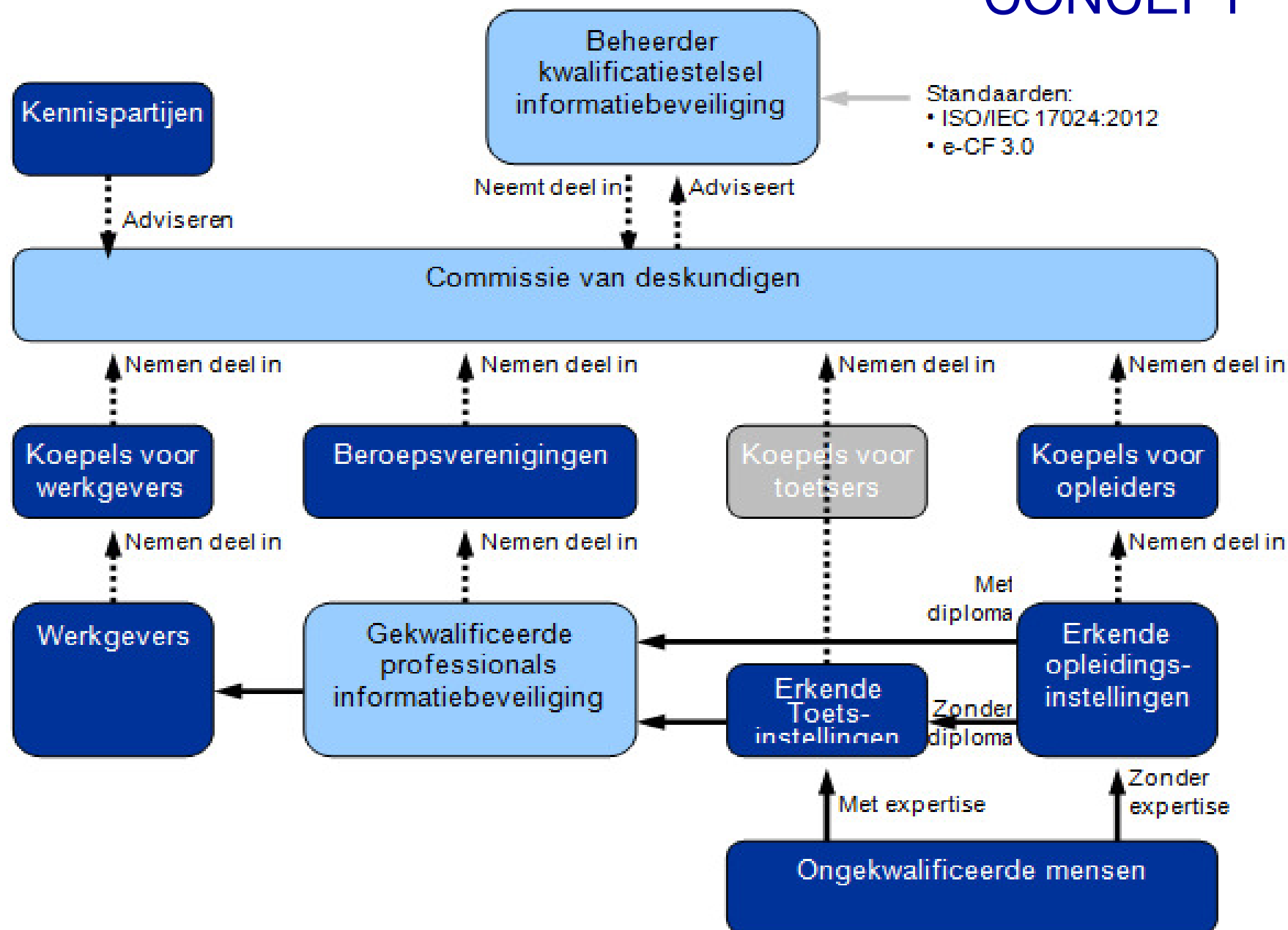
The content of the requirements for the certificate match with the description of the competence but some parts of the competence are missing (e.g. no evidence of some of the practical skills).

Superficial

The content of the requirements mentions parts of the competence description, but there is *no* evidence that obtaining the certificate will show possession of this competence.

Actoren m.b.t. uniform kwalificatiestelsel informatiebeveiliging

CONCEPT





Stuurgroep QIS

- Toetsen van opleidingsprofielen in pilots
- Mapping van bestaande opleidingen
- Selecteren van onafhankelijke beheerpartij
- Inrichten van kwalificatiestelsel
- Ontwerpen van kwalificatiestelsel
- Internationale erkenning
- Definiëren van erkende opleidingen
- Onderzoek haalbaarheid certificatieregister

Klankbordgroep QIS



Cyber Security Raad



Rijksoverheid



VNO NCW



vereniging van
opleidingsinstituten
voor ICT



Platform
ICT
Hogescholen



HOGER BEROEPSONDERWIJS
ICT-OPLEIDINGEN

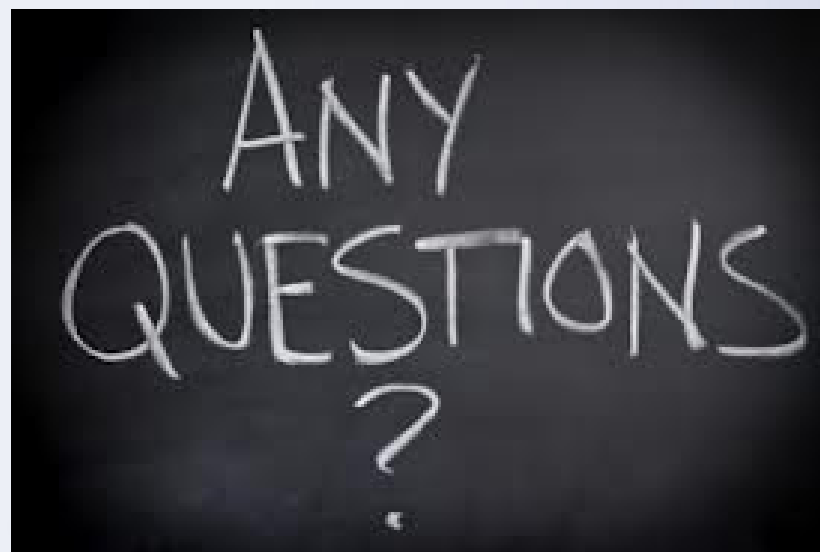




Video

“What are you sinking about ?”

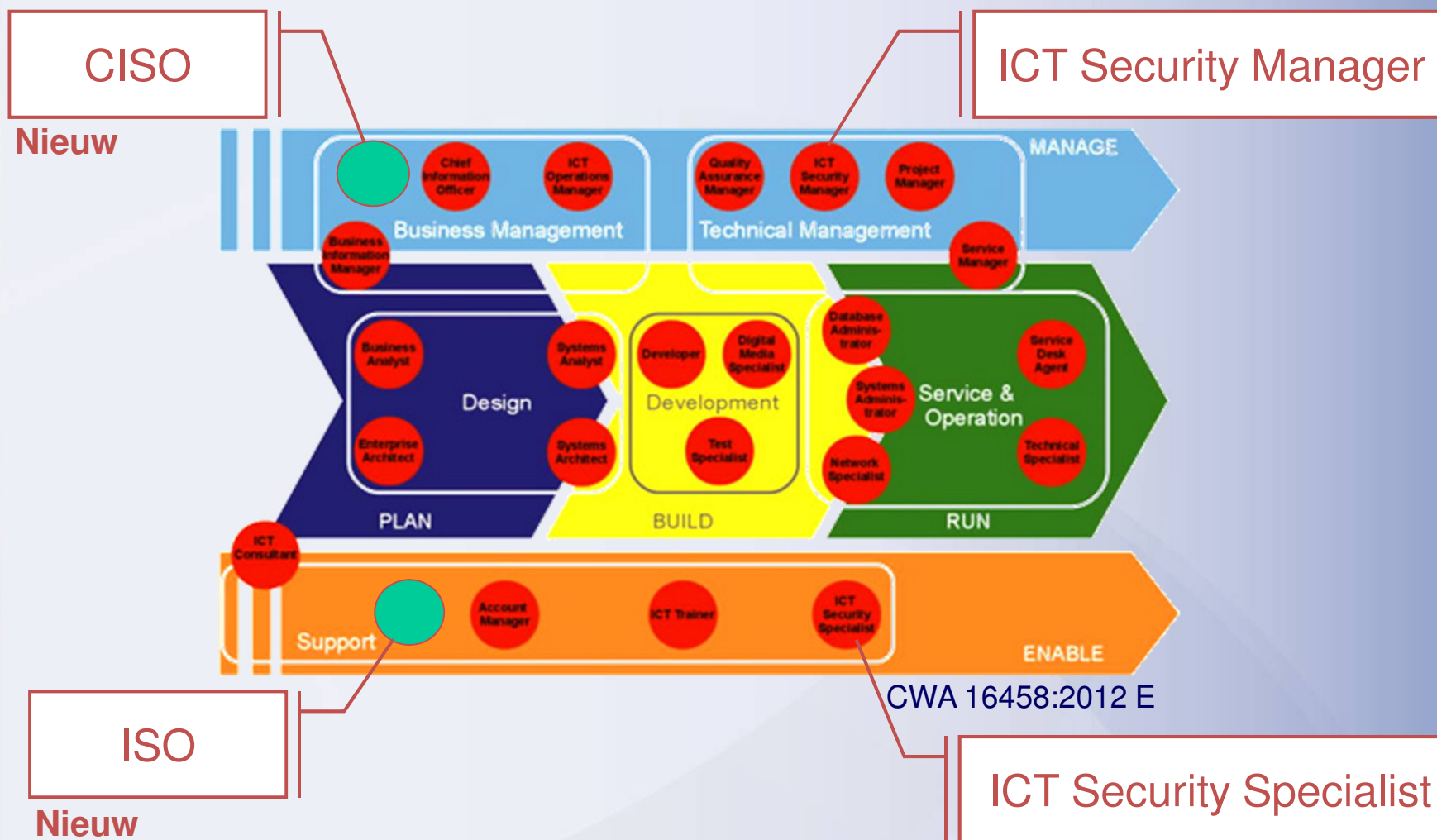




PvIB.nl
CEN.eu

fredvannoord@pvib.nl

Beroepsprofielen



2014-2016: Uitwerken Opleidingsprofielen

Samen met opleidingsinstituten en werkgevers (profielen/pilots)

- MBO: **ICT-Security Specialist**
 - ECABO
2 kwalificatiedossiers: ICT-beheerder en Netwerkbeheerder (MBO niveau 4)
 - ROC Mondriaan, Den Haag
 - ROC van Amsterdam + MBO College Hilversum
 - ROC van Flevoland
- HBO: **ISO, ICT-Security Manager, ICT-Security Specialist (bachelor)**
 - Haagse Hogeschool (Information Security Management: 2010)
 - NOVI, LOI
 - Fontys
 - Hogeschool Utrecht
- WO: **CISO, ICT-Security Specialist (master)**
 - Cyber security Academy (TU Delft, Univ. Leiden, HHS)
 - EuroCIO (Universiteit Tilburg en Business School Antwerpen)
 - NWO