ISO 27001
'To stay or not to stay?'

Security congres
8 oktober 2014

Gert Maneschijn – RDW, Security officer
Roland van der Knaap – PwC, Lead auditor

pwc

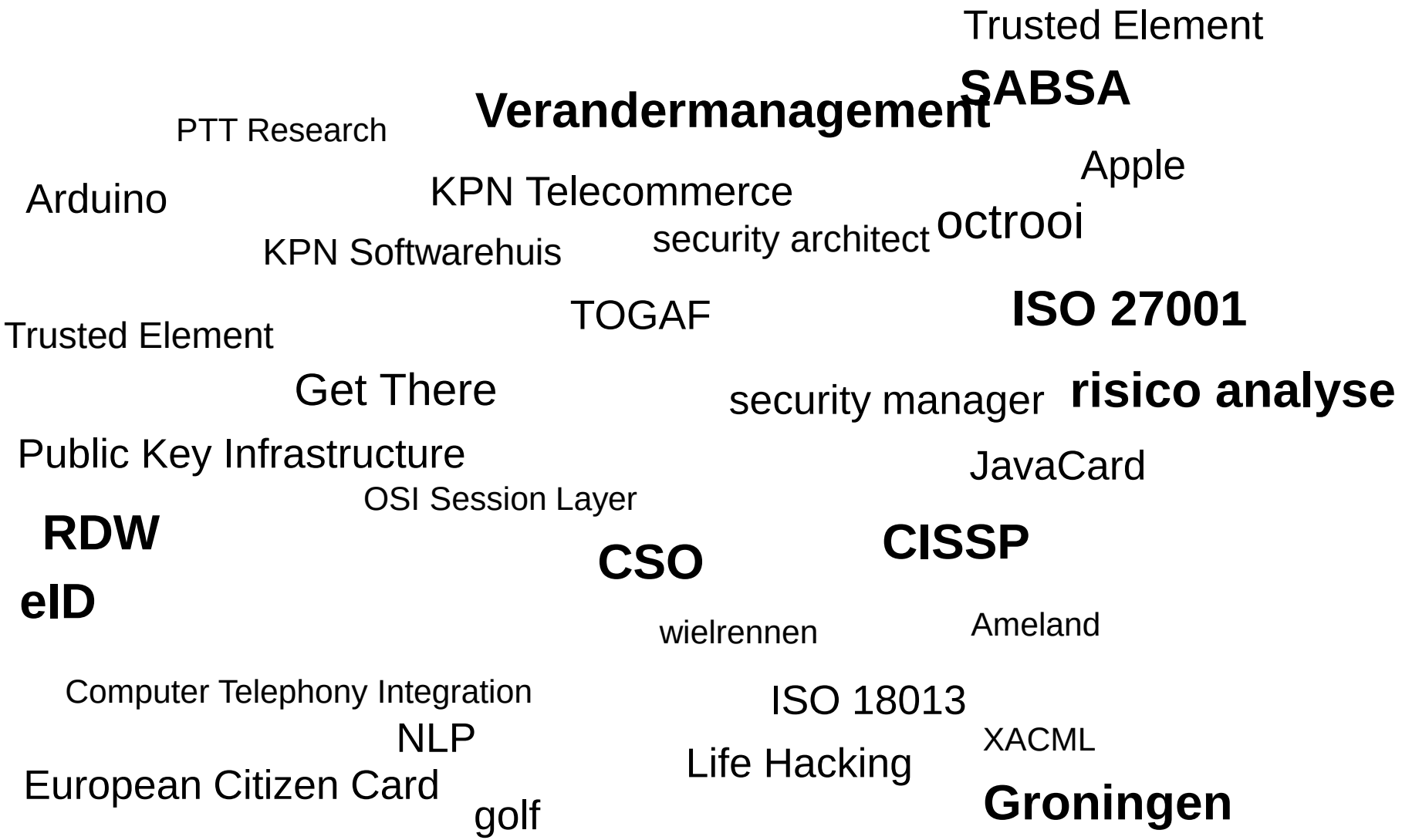
RDW

Achtergrond

Vanuit het perspectief van de gecertificeerde (RDW) en de certificeerder (PwC) wordt toegelicht hoe besloten is te starten met de certificering, hoe de (her)certificering is verlopen en wat het uiteindelijk oplevert als het gaat om behoorlijke beveiliging.

Aanname: basiskennis van ISO 27001

Gert Maneschijn



RDW


RDW erkend
KENTEKENBEWIJS
RDW
00-RDW-1
01-05-2007
01-05-2007
Janssen
Skager Rak 10
9642 CZ Veendam
SPECIMEN
1234567890
RIJBEWIJS
Zilverberk p/v Klaverbeek
Lisanne J M P
29.07.1976 Groningen
01.10.2006
01.10.2016
Gemeente Groningen
Groningen
1234567890
A-BE-C1
AM
00-PJ-TX
TA-XI-01
1-9-2003
EF
RP-10
12F
RP3
01-GBB-1

Roland van der Knaap

Agenda

Inleiding

1. Waarom certificering?
2. Nulmeting
3. Initiële certificering
4. Certificering
5. Wat heeft het opgeleverd?
6. Misverstanden rondom 27001 certificering
7. Hoe ziet de toekomst eruit?

Inleiding

Net als ISO9001 heeft ISO27001 heeft als managementsysteemstandaard voortdurende verbetering voor ogen.

Processen voor risicomanagement en risicobehandeling maken daar integraal deel uit van de standaard. Tegelijkertijd wijst ISO27001 op de verantwoordelijkheid en betrokkenheid van het topmanagement als het gaat om informatiebeveiliging.

Deze sessie maakt duidelijk hoe ISO27001 op een risk based manier kan bijdragen aan behoorlijke beveiliging door dit onderwerp te belichten vanuit zowel de gecertificeerde als vanuit de certificeerder. Ook de beperkingen van ISO27001 certificering komen aan bod.

Behoorlijk bestuur en behoorlijke beveiliging kunnen niet zonder elkaar.

Samenvatting

Waarom certificering?

- Alle neuzen zelfde kant op
- Medewerkers hebben beter inzicht in het beleid en doelstellingen van hun organisatie en zien ook beter hun eigen aandeel daarin
- Management neemt verantwoordelijkheid

Wat levert het op?

- Een certificaat
- Interne aandacht voor informatiebeveiliging
- Fouten worden eerder opgemerkt en in principe permanent opgelost
- Transparantie naar buiten over wat je doet aan beveiliging
- Accreditatie kan extra vertrouwen schenken

Stap 1: Waarom?

Informatiebeveiliging is van Gert

Informatiebeveiliging staat op zichzelf

Informatiebeveiliging is alleen een ICT-ding

Stap 1: Waarom?

Informatiebeveiliging is van Gert

- informatiebeveiliging is de verantwoordelijkheid van de eigenaar

Informatiebeveiliging staat op zichzelf

- een attribuut en geen entiteit

Informatiebeveiliging is alleen een ICT-ding

- zeker ook processen, dienst, juridisch etc

Stap 1: Waarom?

imago: ISO is een bekende norm buiten Nederland, VIR niet

risicoanalyse: pragmatisch risico's expliciet maken

eigenaarschap: eigenaar is verantwoordelijk voor risico's

samenhang: tussen beleid, praktijk en de audit

toekomstvast: ISO is dé standaard voor RDW

best practice: maximaal hergebruik

kwaliteit: ISO breder is dan huidige beleid

Stap 1: Waarom?

imago: ISO is een bekende norm buiten Nederland, VIR niet

risicoanalyse: pragmatisch risico's expliciet maken

eigenaarschap: eigenaar is verantwoordelijk voor risico's

samenhang: tussen beleid, praktijk en de audit

toekomstvast: ISO is dé standaard voor RDW

best practice: maximaal hergebruik

kwaliteit: ISO breder is dan huidige beleid

En later: ISO 27001 binnen de overheid

Forum Standaardisatie – comply or explain richtlijnen

NEN-ISO/IEC 27001:2005 nl meer informatie	NEN	IT-beveiliging	Alle overheden
NEN-ISO/IEC 27002:2007 nl meer informatie	NEN	IT-beveiliging	Alle overheden

De norm is een specificatie van managementsystemen van informatiebeveiliging. Het beschrijft een model dat ingevuld kan worden met de elementen uit de ISO27002.
Deze norm is gebaseerd op de 17799 standaard en wordt omschreven als een set van 'best practices' in informatiebeveiliging waaruit gekozen kan worden bij de implementatie van een beveiligingsstrategie. De norm dient in samenhang met NEN-ISO/IEC 27001:2005 nl gehanteerd te worden.

VIR 2007

Een andere methode is certificering. Hierbij valt bijvoorbeeld te denken aan certificering op basis van de Code voor Informatiebeveiliging (ISO27001). Hierbij onderzoekt een externe partij of de betrouwbaarheidseisen en maatregelen overeenkomen met de Code voor informatiebeveiliging.

Stap 2: de nulmeting

RDW zoekt ondersteuning

Belangrijkste vraag: moeten wij voor 600 systemen risicoanalyses doen?

PwC:

- Clusteren van systemen
- Gedifferentieerde risicoanalyses

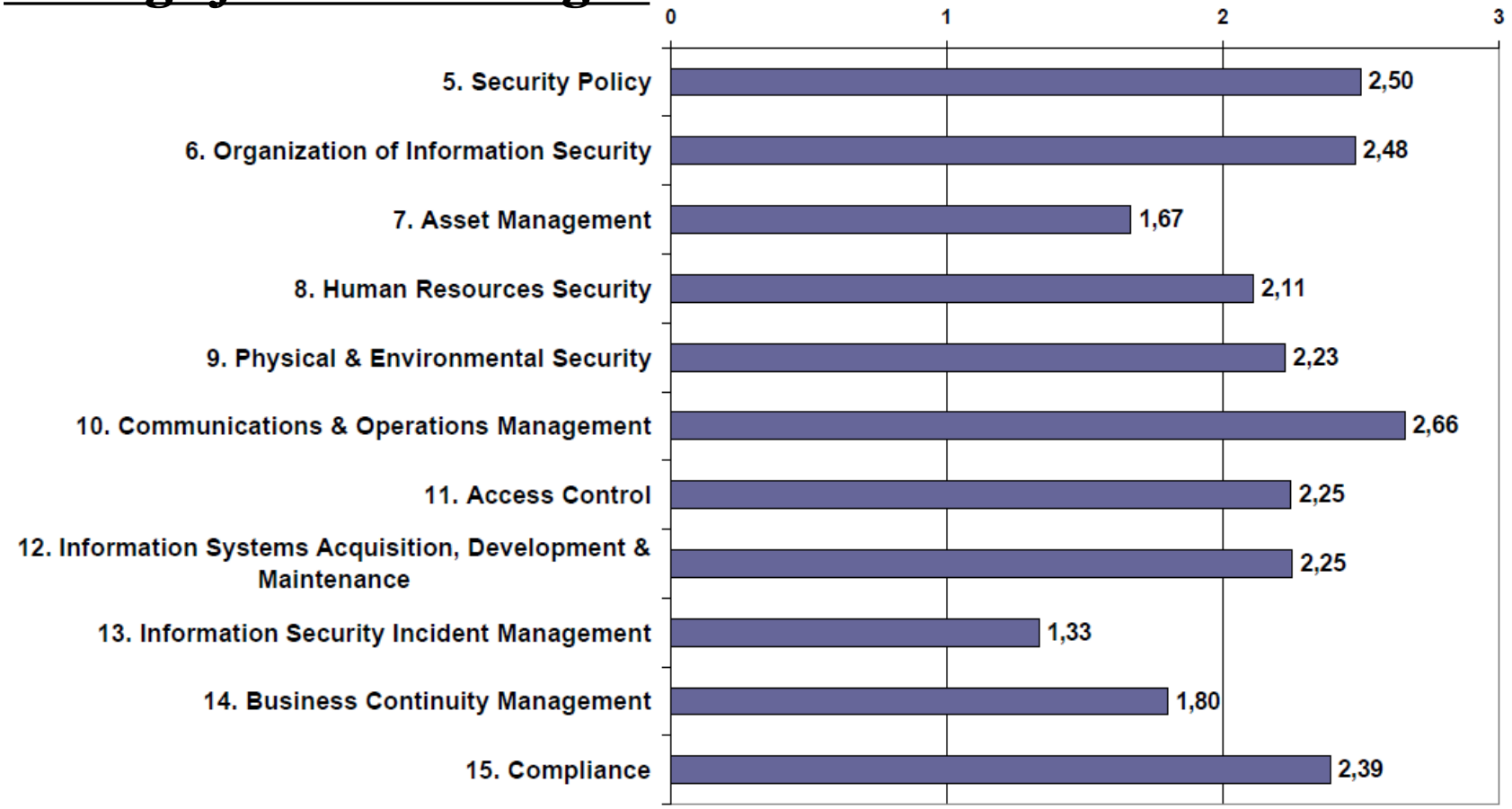
→ Keuze voor PwC!!

Stap 2: aanpak nulmeting

- documentatie informatiebeveiliging beoordeeld tegen ISO27001
- interviews rond het ISMS en elk van de Annex A hoofdstukken
- maatregelen onderzocht op bestaan en werking
- per onderscheiden locatie
- classificatie bevindingen

Stap 2: uitkomsten nulmeting (2007)

Belangrijkste bevindingen

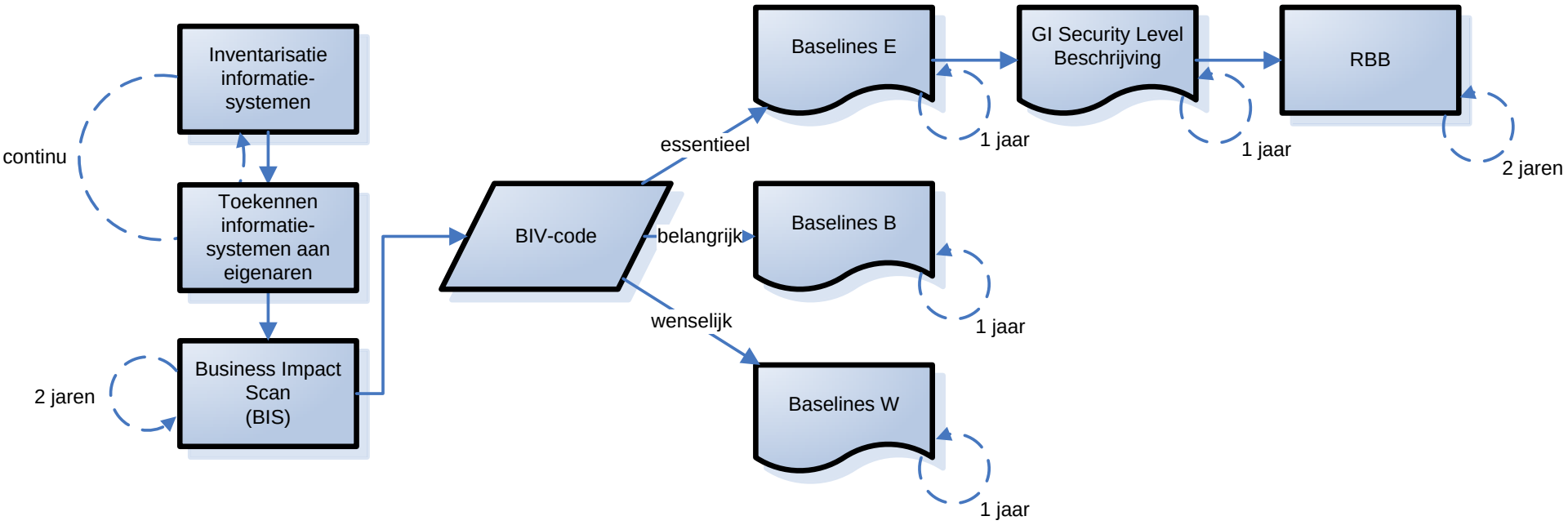


Stap 3: de initiële certificering, voorbereiding

- Bepaal de scope
  - Eerst het ICT-bedrijf
  - Na drie jaren RDW als geheel

- Information Security Management System
  - De lat niet hoger: Formuleer beleid aan de huidige praktijk
  - Vervolgens focus op voortdurende verbetering
  - Maak handboeken per afdeling (HR, FB, ICT etc)
  - Houd het praktisch

Stap 3: de initiële certificering, voorbereiding



Stap 4: de certificering

<u>Opmerking vooraf</u>

1. Kan wel of niet onder accreditatie plaatsvinden
2. Accreditatie biedt aan de gebruiker van het certificaat:
   - ✓ Meer zekerheid over kwaliteit van het certificaat
   - ✓ Meer uniformiteit over organisaties heen, ook internationaal

Markt is zich niet altijd bewust van het bestaan van het verschil

Stap 4: de certificering

Organisatie (certificerende instelling)

1. Audit team: gekwalificeerde (Lead) Auditor(s)
   - Voert onderzoek uit
   - Lead Auditor adviseert over certificering ja/nee
2. Back-office:
   - Ziet toe op kwalificatie personeel
   - Ziet toe op juiste uitvoering processen en audit planning
   - Neemt advies tot certificering over of niet
   - Verzorgt certificeringsovereenkomst en het certificaat

Stap 4: de certificering

Proces

1. Client Intake / Scopebepaling
2. Certificeringsprogramma voor 3 jaar
3. Audit plan per jaar
4. Uitvoering onderzoek jaar 1 (stage 1, stage 2, NCF, CAR)
5. Advies tot certificering / Besluit tot certificering
6. Certificeringsovereenkomst / Onderhouden certificering
7. Herhaalaudits (jaar 2 en jaar 3)

5. *Wat heeft het opgeleverd?*

1. informatiebeve eid van de eigenaar ✓
2. een attribuut e
3. Informatiebeve ng ✓

1. Bewust omgaa
2. Eigenaarschap
3. Best practice ✓
4. Kwaliteit ✓
5. Imago, samenh

Certificate No.: 12-0010

pwc

CERTIFICAAT

Het Information Security Management System (ISMS) van

RDW

Voldoet aan de eisen van:

ISO/IEC 27001:2005

Het toepassingsgebied van dit certificaat omvat het ISMS van de RDW gericht op het realiseren van informatiebeveiliging binnen de dienstverlening van de RDW. Het betreft de dienstverlening verzorgd vanuit Directie & Staven alsmede vanuit de Divisies (Registratie & Informatie, Voertuigtechniek en ICT-bedrijf) met inbegrip van de kantoren in Zoetermeer, Groningen (Hoogkerk en Zernike), Veendam, Test Centrum Lelystad en Keuringstations/Regiokantoren.

De geselecteerde risico compenserende beheersmaatregelen zijn beschreven in de Verklaring van Toepasselijkheid (= RDW document ISMS004, v2.0 van 12 oktober 2012).

Uitgifte van dit certificaat is gebaseerd op het rapport van de initiële audit met referentie: PwCC-0002-2013.

Het certificaat is voor de eerste keer uitgegeven op 28 februari 2013 en zal geldig zijn tot 28 februari 2016.

Het ISMS is onderworpen aan jaarlijkse surveillance audits gedurende de geldigheidsduur van het certificaat.

PricewaterhouseCoopers Certification B.V.
Amsterdam, 28 februari 2013

Dit certificaat wordt elektronisch gepubliceerd en blijft eigendom van PricewaterhouseCoopers Certification B.V. en is gehouden aan de voorwaarden van de certificeringsovereenkomst. Zie http://www.pwc.nl/nl/pwc-certification voor achtergrond en geldigheid van dit certificaat.
Dit certificaat gaat over het information security management system, en niet over de producten of diensten van de gecertificeerde organisatie. Het certificaat referentienummer, het handelsmerk van de certificerende instelling en/of het accreditatiemerkteken mag niet worden getoond op producten of opgenomen in documenten over producten of diensten. Promotiemateriaal, advertenties of andere documenten die of wel tonen ofwel verwijzen naar het certificaat, het handelsmerk van de certificerende instelling of het accreditatiemerkteken, moeten in overeenstemming zijn met de intentie van het certificaat. Het certificaat verleent niet uit zich zelf aan de gecertificeerde organisatie ontheffing van (het voldoen aan) wettelijke plichten.

RvA MGMT. SYS. RvA C 203

6. Misverstanden over ISO27001 certificering

1. Met een certificaat ben ik veilig
2. Ik heb niets aan een ISO27001 certificaat
3. Kosten van certificering zijn hoog

   - > Wat zijn de kosten van geen certificering?
4. Certificering is niet voor mijn organisatie
5. Klanten moeten erom vragen

   -> Waarom wachten?
6. Security waait wel weer over

   -> Is dat zo?
7. ISO27001 is voor ICT

   -> Beveiliging van informatie gaat veel verder dan ICT
8. Certificeren is alleen op basis van maatregelen

   -> geeft geen blijvende aandacht

7. Hoe ziet de toekomst van certificering eruit?

1. Toenemende afhankelijkheid van informatie
2. Cyber security blijft nog wel even
3. Verhoogde aandacht voor bescherming van informatie (Privacy, (Business) Continuity)
4. Management verantwoordelijkheid wordt steeds meer beseft
5. Management systemen kunnen bijdragen aan verhoging van interne beheersing van informatiebeveiliging
6. Certificering van dergelijke management systemen dwingt intern tot nadenken en bedrijfsmatig inrichten en beheersen van informatiebeveiliging
7. 100 % beveiliging bestaat niet, maar 27001 certificering kan bijdragen aan transparantie naar maatschappelijk verkeer

7. De toekomst vanuit RDW-perspectief

- De werkplek is niet meer te vertrouwen!

  ?? Air gap PC?

- RDW/Nederland heeft een hoger authenticatieniveau nodig.

- Versleutel gevoelige documenten
  - doel: beveilig de bron en niet de end-points (Jericho)

Dank voor uw aandacht!