
kpn

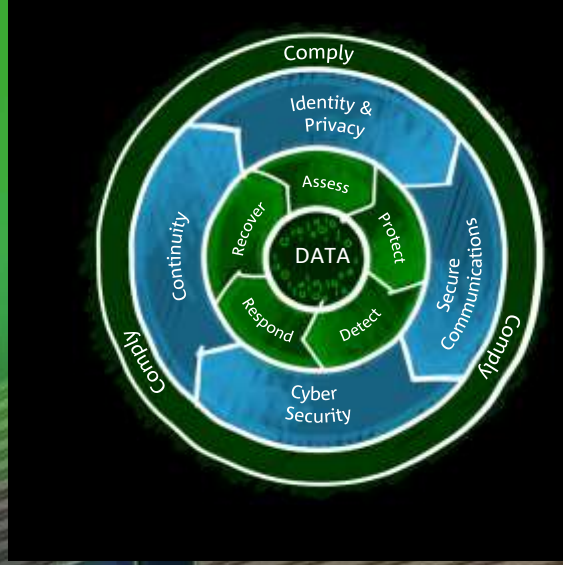
Workshops

		1e ronde	2e ronde
1	Business Continuity en Compliance	Zaal 1	Zaal 5
2		Zaal 2	Zaal 2
3	Hoe behoedt u uw organisatie voor ransomware?	Zaal 3	Zaal 3
4		Zaal 4	Zaal 4
5	Security- en Compliance-monitoring	Zaal 5	Zaal 1

Rondleiding: 17.30 / 18.00 / 18.30 – verzamelen bij de entree datacenter

Business Continuity en Compliance

Edgar Versteeg
KPN Security Services



Agenda

- Digitale transformatie en risico’s
- Wet & regelgeving
- Business Continuity
- Onze visie
- Afsluiting

Digitale transformatie en risico's

Brand verstoort online dienstverlening ADP

'Aanpak cybercrime door politie en OM schiet ernstig tekort'

Privégegevens inwoners Oegstgeest en Rotterdam online

woensdag 9 maart 2016, 15:22 door **Redactie**, 12 **reacties**

Swift waarschuwt voor meer aangevallen banken

dinsdag 26 april 2016, 09:44 door **Redactie**, 0 **reacties**

Elektriciteitsnetwerk Israël getroffen door 'ernstige hackaanval'

kpn

Wet & regelgeving

- Meldplichten datalekken
- General Data Protection Regulation (GDPR)
- De Wet Bescherming Persoonsgegevens
- Burgerlijk Wetboek (bijv. artikel 393 lid 4)
- De Regeling Organisatie en Beheersing van De Nederlandsche Bank (DNB)
- Het toetsingskader business continuity planning betalings- en effectenverkeer van DNB
- De Wet Computercriminaliteit

Stelling 1

- Uw organisatie heeft een protocol hoe om te gaan met het lekken van persoonsgegevens.
- U kunt derhalve binnen 72 uur melding doen bij de Autoriteit Persoonsgegevens en betrokkenen informeren.

Wet & regelgeving

Artikel 393 lid 4:

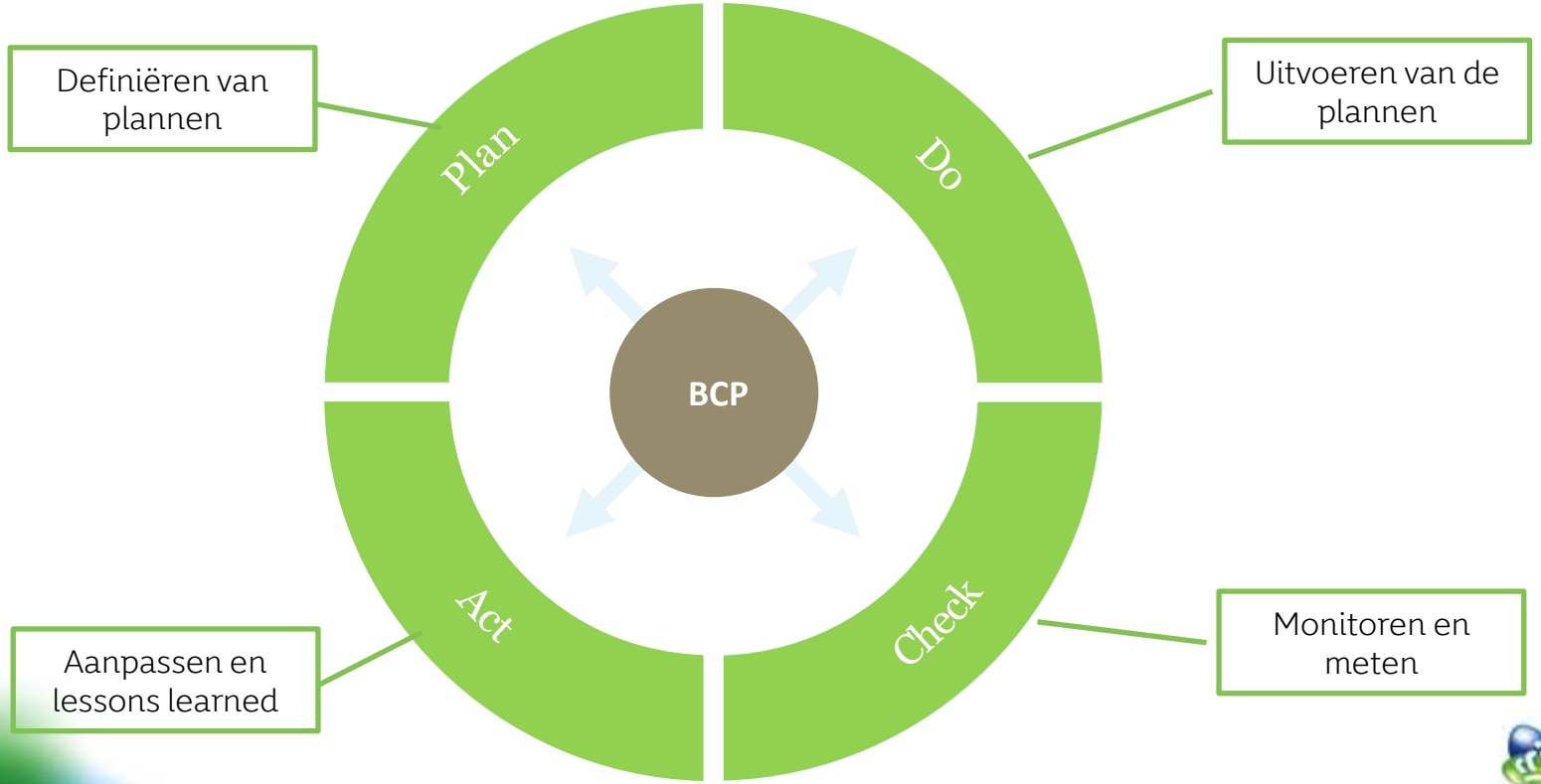
- *De accountant brengt omtrent zijn onderzoek verslag uit aan de raad van commissarissen en aan het bestuur. Hij maakt daarbij ten minste melding van zijn bevindingen met betrekking tot de **betrouwbaarheid** en **continuïteit** van de geautomatiseerde gegevensverwerking*

- Van *tell* me, *show* me naar *prove* me

Stelling 2

- Uw externe en/of interne accountant heeft uw Business Continuity plan in de afgelopen 12 maanden beoordeeld.

Business Continuity Planning is een continue proces waarbij voorbereiding cruciaal is



Stelling 3

- Uw organisatie heeft een actueel Business Continuity plan dat u jaarlijks test.

Business Continuity Management

Een stapsgewijs proces

1 Ready

Voorbereiding, orientatie, stip op de horizon in strategie

2 Set

Alle schaakstukken goed zetten:
assessment › scenario's › vastleggen

3 Go!

De gemaakte plannen uitvoeren en continu optimaliseren en beheren

Stap 1
Oriëntation

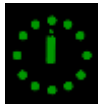
Bewustwording en begrippen duiden

Stap 2
Strategy

Strategische IT roadmap, afgestemd met de beslissers

Stap 3
Asses & Define

Scenario van de huidige naar de gewenste situatie



Stap 4
Design & Plan

Alles vastgelegd in ontwerpen

Stap 5
Implementation

De daadwerkelijke implementatie

Stap 6
Optimization

Beheren en optimaliseren

Business Continuity – meest gemaakte fouten

GEEN RAMPENPLAN

86% van alle organisaties hebben in de afgelopen 24 maanden wel eens een ramp te verduren gekregen

- Gartner -

TE KORTE BCM PROGRAMMA'S

De BCM-programma's hebben een veel te korte horizon:

75% plant voor een week of minder.

GEEN INZICHT IN PLAN

De meeste bedrijven hebben geen idee of hun plan wel adequaat is:

- Slechts een op de drie oefent en leert daarvan;
- Slechts 30% heeft metrics voor de status;
- Slechts 27% gebruikt scorecards;
- Bijna de helft vertrouwt geheel en al op auditrapporten.

Bron: *BCM Survey Provides Program Posture and Maturity Improvement Actions for BCM Leaders in 2015*

Tevens zien wij…

- Bij controle wordt af en toe op BCM gelet, maar zelfs dan moet er iets bij het bedrijf gebeurd zijn voordat accountants erop wijzen (reactief beoordelen).

- Accountants geven een 'going concern'-verklaring af. Dit betekent dat ze de komende 12 maanden geen liquiditeitsproblemen verwachten op basis van de financiële situatie en resultaten.

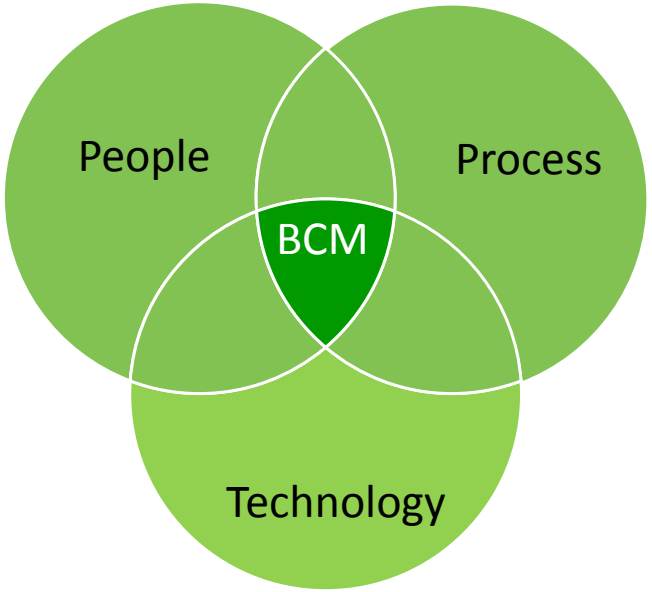
- Derhalve worden alleen zichtbare financiële risico's gemeten en beoordeeld. Mogelijke calamiteiten als brand, een cyberattack, stroomstoringen of explosies worden niet besproken en bedrijven zijn hier dus niet op voorbereid.

Stelling 4

- Uw organisatie heeft in de laatste 24 maanden een beveiligingsincident gehad waardoor de bedrijfsprocessen negatief werden beïnvloed, terwijl er geen plannen en/of maatregelen waren om het incident te beheersen.

Visie van KPN: integrale benadering

Wij geloven in een integrale aanpak over de drie assen:



Wij hanteren *Sungard Assurance Continuity Management* t.b.v. modelleren van continuiteitsplannen, assessments, Incident Management en alarmering

Van aanleiding naar pain, oplossing en gain

SITUATIE / AANLEIDING

- Ontbreekt Crisis management organisatie en plan
- Continuiteitsplannen zijn verouderd
- Geen inzicht in kritische bedrijfsprocessen met de maximale hersteltijd en maximale verlies van data
- Oefening en Testen worden niet uitgevoerd

PAIN

- Niet bekend wat te doen ingeval van crisis situatie
- Geen uitwijk, alleen tape back-up
- Klanten eisen snel herstel
- Geen tijd om te oefenen en te testen

OPLOSSING

- Continuiteitsplannen
- Backup Online XL
- Business Impact Analyse, Risico Analyse
- DRaaS (VM Continuïteit, RPO tot minuten)
- Impact assessments
- Oefenen en testen (Testen as a Service)
- Awareness en crisis management team oefening
- Systeem recovery

GAIN

- Snellere recovery door voorzieningen en getrainde medewerkers
- Actuele plannen beschikbaar
- Inzicht in kritieke bedrijfsprocessen
- Compliant wet- en regelgeving
- Vertrouwen
- Reputatie

KPN biedt support

Awareness	Privacy	Security	Business Continuity*
Oceans'99	Quick Scan Meldplicht Datalekken	ISO 27001/2	Business Impact Analyse (BIA)
	Privacy Impact analyses (PIA)	NEN7510	Business Continuity Planning
		Baseline Informatiebeveiliging Gemeenten (BIG)	Disaster Recovery Planning

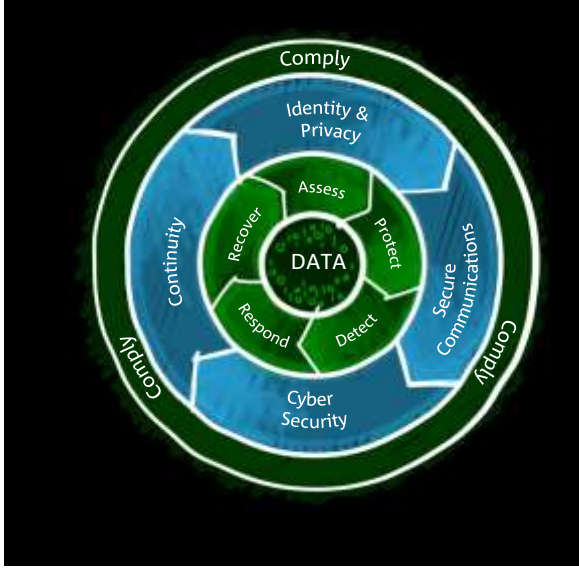
*Wij hanteren Sungard Assurance t.b.v. het modelleren van uw BCP

Bedankt voor uw aandacht

Meer weten …?

KPN

E: managedsecurityservices@kpn.com
W: www.kpn.com/security



Het security portfolio van KPN

Identity & Privacy	Secure Communications	Cyber Security	Business Continuity
Managed PKI	Anti-DDoS NL	Security & Compliance Monitoring	Disaster Recovery Services
Secure Access & Strong Authentication	Mobile Device Management	Vulnerability Management	DR Testing
eID	Mobile Guard	PenTesting	DRaaS (VM Continuity)
Secure Identity	Secure Information Exchange	Incident Response & Forensics	Back-up Online XL
eHerkenning	Secure File Transfer	Threat Intelligence	Tape Back-Up (MTS)
Cloud Identity	Secure Network, WLAN, Internet, Communication		Werkplek en Telefonie Uitwijk

Workshops

		1e ronde	2e ronde
1	Business Continuity en Compliance	Zaal 1	Zaal 5
2		Zaal 2	Zaal 2
3	Hoe behoedt u uw organisatie voor ransomware?	Zaal 3	Zaal 3
4		Zaal 4	Zaal 4
5	Security- en Compliance-monitoring	Zaal 5	Zaal 1

Rondleiding: 17.30 / 18.00 / 18.30 – verzamelen bij de entree datacenter