LIO NOREA bijeenkomst 4 februari 2019

DNB meting inzake informatiebeveiliging door Self Assessments CZ

"Het COBIT model is net een set winterbanden"

Soms doen ze wat maar echt nodig heb je ze bijna nooit.

De context van CZ

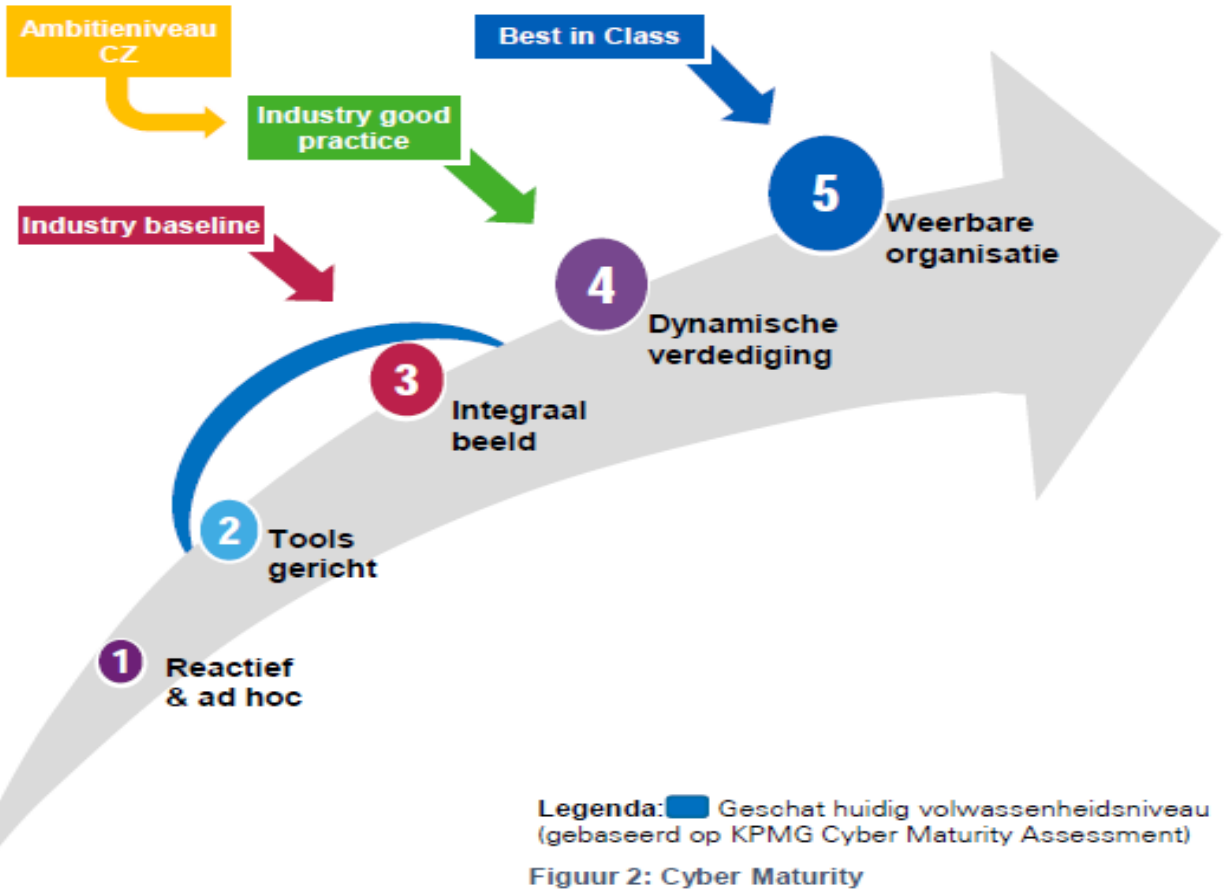
CZ Zorgverzekeraar

- Onderlinge waarborg maatschappij met 3,6 miljoen verzekerden
- Omvang zorgdeclaraties: €10,6 miljard
- Zorgkantoor ongeveer € 5 miljard
- 240 miljoen nota’s met bijzondere persoonsgegevens
- 5 miljoen klantcontacten waarin bijzondere persoonsgegevens aan de orde kunnen komen
- Ca. 2500 medewerkers
- Valt onder toezicht door DNB op verzekeraars
- CZ voert op verzoek DNB tweejaarlijks een self assessment Informatiebeveiliging uit

Informatiebeveiliging is bij CZ van groot belang onder andere omdat zij persoonsgegevens beheert met een grote persoonlijke waarde voor de verzekerden

- Verlies van data oid. beïnvloedt in ernstige mate de persoonlijke sfeer van verzekerden
- Omvang geldstromen is zeer groot
- Uitstekende reputatie is onontbeerlijk voor zorg sector
- Cybercrime ontwikkelingen vormen een nooit afnemende bedreiging en als in een schaakspel; “we spelen met zwart”
- Informatiebeveiligingsstrategie ontwikkeld i.s.m. extern adviseur

De strategie voor informatiebeveiliging is ontwikkeld met behulp van externe consultancy en wordt gerealiseerd met een 5-stappen model



Legenda: Geschat huidig volwassenheidsniveau (gebaseerd op KPMG Cyber Maturity Assessment)

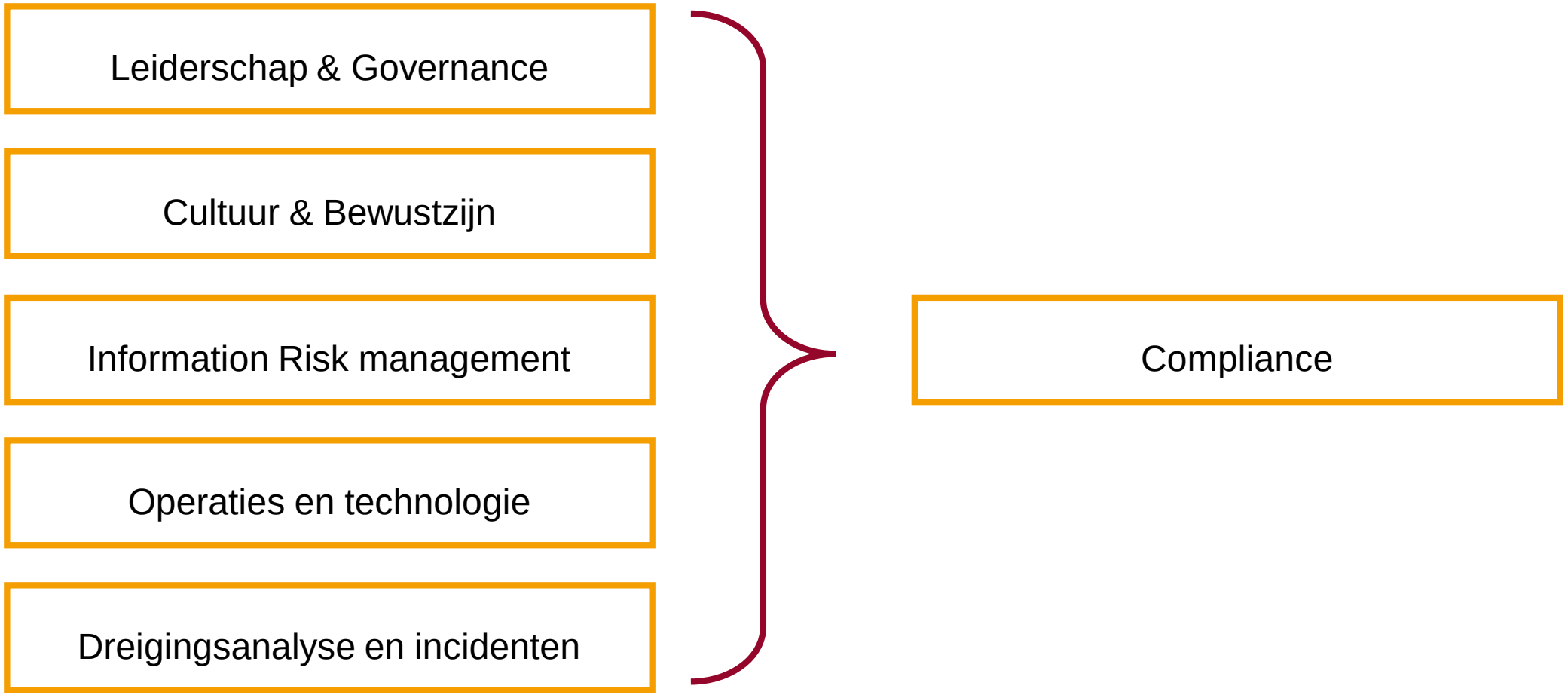
Figuur 2: Cyber Maturity

Realisatie strategie levert resultaten als:

- Security awareness programma 2017-2018 afgerond. Jaargang 2019-2020 gestart
- CZ breed zichtbare leadership vanuit RvB
- Implementatie van een Secure Development Lifecycle
- Modernisering van alle IAM processen m.b.v. nieuw RBAC model
- Herinrichting Security Monitoring dienst
- Frequente security assessments door bv Secura, Deloitte en FoxIt

Pragmatische inzet van frameworks en kennis van NIST, ISF, ISO en…. Cobit!

Terugkomend op de stelling van slide 1: het gaat niet om het model maar om intrinsieke motivatie. Die leidt vanzelf naar compliance met het model (of een ander model ☺), maar veel belangrijker tot informatiebeveiliging



De compliance van CZ moet een gevolg zijn van onze informatiebeveiligingsprogramma's en kan geen op zichzelf staand programma zijn

- Laten we eerlijk zijn: welke collega in een operationele functie staat 's morgens op en denkt "ik ga vandaag eens lekker aan compliance werken"?
- De uitdaging is dus intrinsieke motivatie in zijn of haar denken te krijgen gebaseerd op het dagelijks werk
- Het betrekken van relevante sleutelrol spelers in bijv. risico analyses levert waardevolle informatie en leidt tot draagvlak.
- Het herinrichten van het Security Operating Center naar een hoger niveau is daar een gevolg van en heeft een zeer betrokken projectomgeving
  - Dit levert een doorontwikkeling van maatregelen van objective "DS0509 Malicious software prevention, detection and correction", maar ook een nieuwe CZ-SOC organisatie.
- Besturing van het programma door CZ's Security Office om de vakmatige kwaliteit te garanderen

CZ streeft met het programma naar een situatie waarbij het uitvoeren van het self assessment niet een tweejaarlijkse piek in activiteit is

- We realiseren onze ambitie duurzaam
- Het realiseren van een ambitie zodanig dat het bereikte maturity level per objective niet daalt
- Alle maatregelen altijd onderdeel zijn van ”going concern” van de verantwoordelijke afdelingen
- Heldere toewijzing van verantwoordelijkheden met ingebouwde samenwerking
- Eenduidige control implementatie waarvan opzet, bestaan en werking eenduidig toetsbaar zijn
- Self Assessment documenten, inclusief bewijsvoering, zijn altijd actueel en toegankelijk (voor bevoegden!)

Nog even terugkomend op die winterbanden... Cobit is geen heel slechte winterband, maar we zijn er geen fan van.

- Cobit helpt niet om de mensen in de organisatie uit te leggen wat er van ze verwacht wordt;
  - Control Objectives zijn voor hen te abstract, te hoog over
  - Control practices zijn moeilijk te "mappen" op de (IT-) omgeving en de eigen alledaagse werkelijkheid
  - Met het "Test the control design" lijstje kun je vele kanten op
- Cobit teksten zijn lastig, bijna juridisch. Consistente interne beoordeling van self assessments en bijgeleverde evidence wordt bepaald door de lezer, en die wisselen nu eenmaal door de tijd heen
- Vaststellen of maatregelen een control objective realiseren leidt soms tot academische discussies

Desondanks:

- Staat CZ wel achter de selectie van control objectives al zijn ze soms (deels) achterhaald
- Is het self assessment toch nog een welkome prikkel voor het doorvoeren van verbeteringen
- Heeft CZ een stap gemaakt door toepassing van het NBA Maturity model