

PvIB rol van de CISO

Hoe succesvol te worden en wat te doen als het niet lukt

André Beerten

C-MMA

andre@octopus-ib.nl

06-12727238



Wie vindt zichzelf succesvol?

- Voelt het (informatie-)veilig bij jou?
 - Heb je alle audits soepel doorstaan?
 - Loopt het ISMS als een tierelier?
 - Zijn er (bijna) geen incidenten of meldingen?
 - ..
-
- Hoe meet je jouw succes eigenlijk?

Succes

- Control oftewel risicobeheersing
 - Passend bij de organisatiedoelen
- Óf
 - Lang in dienst blijven
 - Een goed salaris, veel vakantie
 - Een positie met aanzien
 - Geen sores..

12 | **ib** INFORMATIEBEVEILIGING MAGAZINE

Een plek waar voor de betrokkenen bij informatiebeveiliging (en privacy, laten we die vooral niet vergeten) passende informatie vindbaar is noemt 'het Register'. De informatie over informatie en beveiliging die ontbreekt is voor IS-Insappers. En volgens mij ook voor een betrouwbaar beeld van de gevraagde 'passende beveiliging': daar hoort ook alle informatie over opzet-bestaan-werking van beveiliging in thuis, ongeacht de methode en middelen die je hanteert voor beveiliging. Waarom? Omdat de 'business', oftewel de vinagers van beveiliging moeten weten hoe de beveiligers (de control-eigenaren) presteren. De risicovoorwoordelheid ligt immers in de business en niet bij de ondersteunende afdelingen (of zie ik dat anders)? En natuurlijk is zo register handig als de auditor wil weten hoe je de boel beveiligd.

Fundamenteel

- Informatiebeveiliging is een ratio-kwestie
- Conflict ‘tussen hart en hoofd’
 - D. Kahneman
 - Onze ratio gebruiken we graag zo weinig mogelijk, omdat die ‘duur’ en traag is
 - We vertrouwen primair op ‘intuïtie’ & reflexen (emotie)
 - Ons intuïtieve beoordelingsvermogen schiet op veel manieren tekort
 - We beoordelen risico’s veelal verkeerd
- Informatiebeveiliging voelt dus niet ‘fijn’

Wat is je taak?

ISMS-
wolk



Regels & risico's



Organisatie (mens & proces)



Techniek

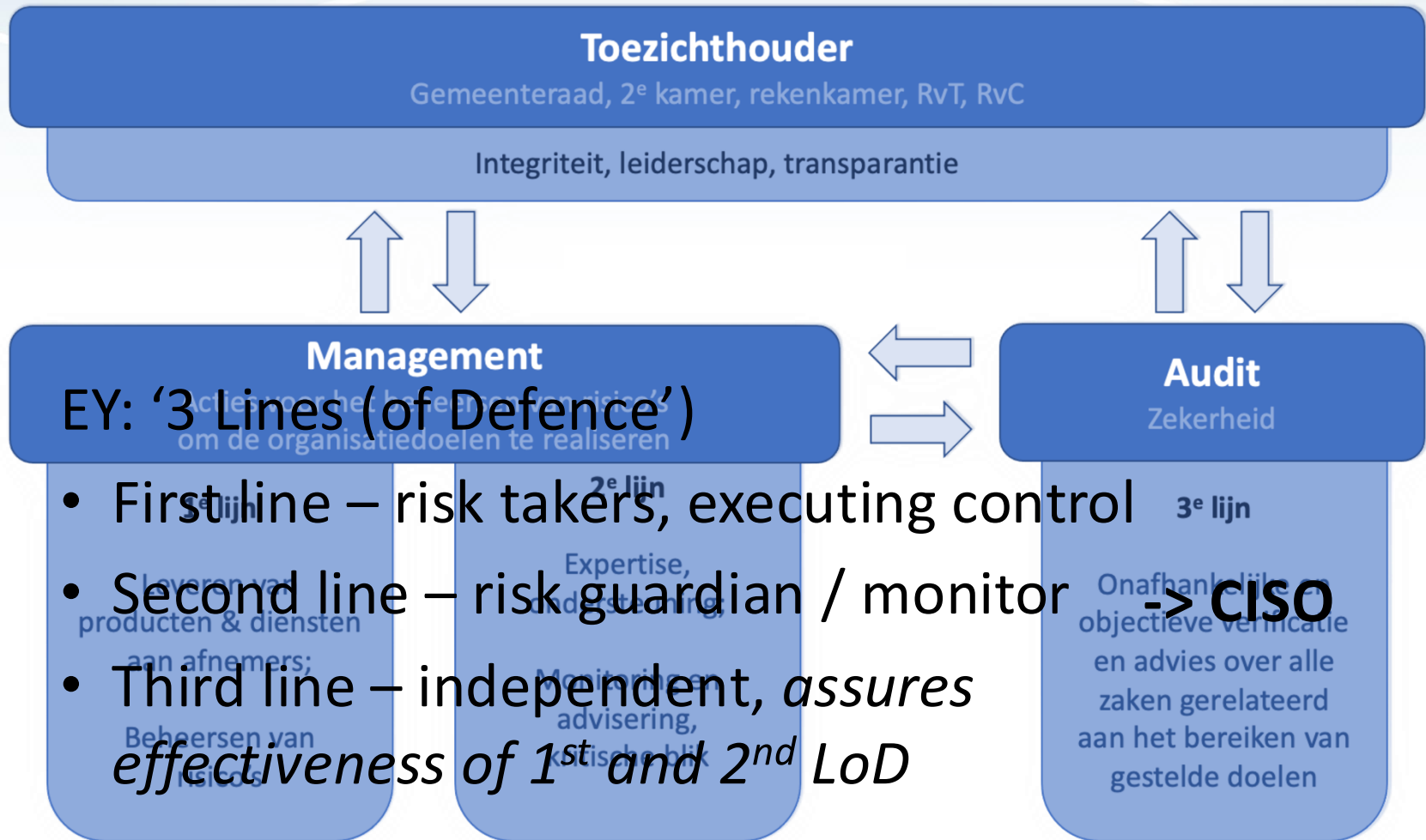
Mintzberg

- Simpele structuur ...
- Machinebureaucratie ...
- Professionele organisatie ...
- Divisiestructuur ...
- Adhocratie / innovatieve organisatie ...
- Zendingsorganisatie ...
- Politieke organisatie ...

Welke bedrijfsstijl (in NL)

- Angelsaksisch = hiërarchisch
 - Ben je verantwoordelijk voor de veiligheid, voor het resultaat
 - Heb je de middelen, mensen en macht
- Rijnlands = consensus
 - Je moet het organiseren, signaleren, besturen
 - 3 lines of defence (eigenaarschap in de **1^e lijn**)
 - Anderen hebben de macht en moeten je rugdekking bieden

Volgens EY 3-lines model



Wat heeft de 2^e lijn nodig om succesvol te zijn?

- Mandaat
- Kennis
- Mensen
- Middelen
- Afstand
- Autonomie
- Antenne

Mandaat

- Om het ISMS in te richten
 - Via beleids- en structuurvoorstellen
- Over de werking te adviseren
- Te rapporteren over
 - Stand van het ISMS
 - Stand van de implementatie van controls
 - (Rest-)risico's
 - Incidenten & kwetsbaarheden

Kennis

- CISSP, CISM, CISA, CRISC etc etc..
- Techniek?
- Vooral: mens & organisatie
 - Cultuur en structuur
 - Verandermanagement
 - Politiek – hoe de hazen lopen
 - Relaties

Mensen

- Waarvoor:
 - Beleid opstellen, bijhouden
 - Beleid interpreteren
 - Nieuwe wetten en regels volgen
 - ISMS bouwen en bewaken
 - Adviseren & apporteren
- En eigenaren voor alle 1^e-lijns activiteiten

- De classificatie van de persoonsgegevens die in deze verwerking w	
- De afspraken over maatregelen en toezicht die we in dit verband he	
Naam eigenaar voor akkoord:	Datum:
Handtekening:	

te' handtekening

Sinterklaas

Middelen

- BIA-methode
- Een implementatie & beoordelingsmethode
 - Neem control-eigenaren bij de hand (maar schrijf niet voor)
 - Wacht niet tot de auditor er iets van vindt, maar denk: MMA
- Leg een éigen RISICOREGISTER aan!
 - Het bedrijfsbrede RR is te grofstoffelijk..

Afstand

- Pas op voor operationele rollen, waar en hoe dan ook, daar heb je geen tijd voor
- Vermijd projecten, voor je het weet ben je
 - Overal bij geweest,
 - En zal het dus wel allemaal OK zijn..
 - Je bent de Excuus-Truus!

Autonomie

- Je bent er **niet** om de organisatie 'door de audit' te krijgen
 - Daarvoor een mooi plaatje te tonen
 - Of bewijzen aan te slepen
- Je bent er **wél** om het ISMS te laten draaien en daarvoor
 - Het nodige te doen
 - 'objectief' te rapporteren

Antenne

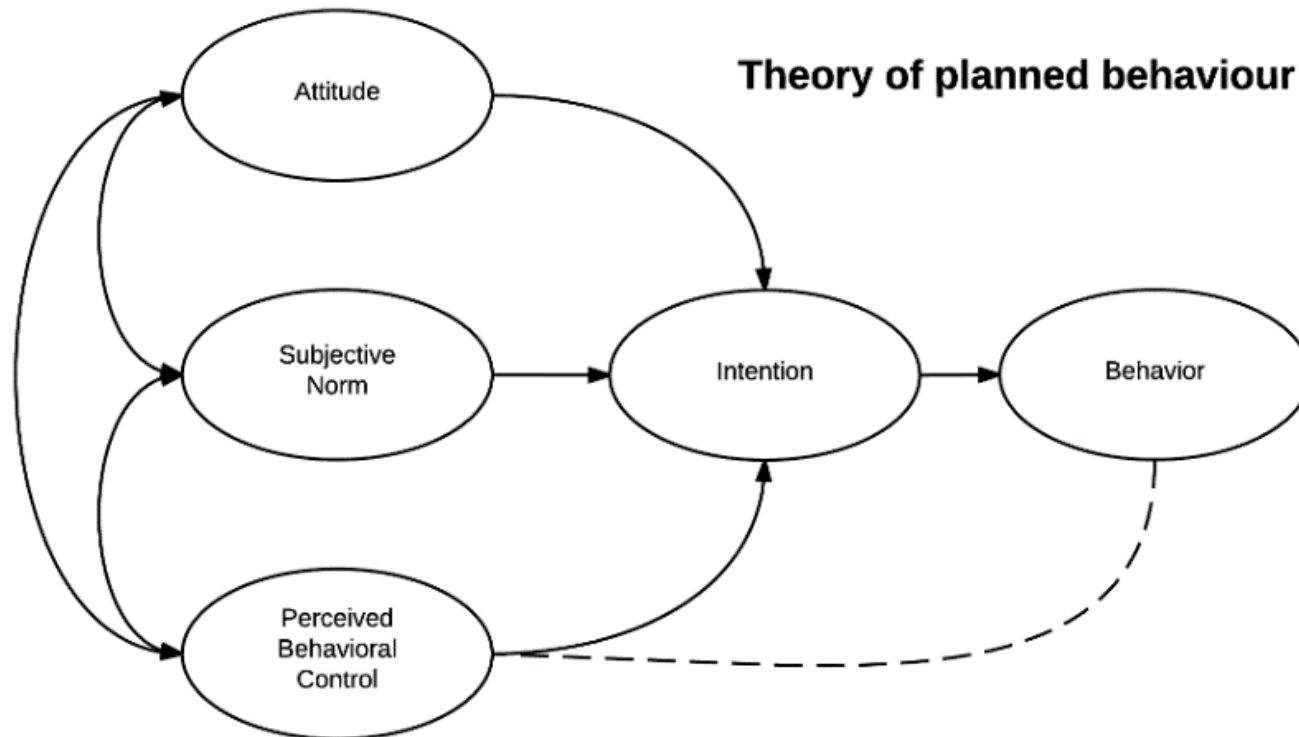
- .. Voor wat de het bestuur écht van je vraagt
 - En of dat een redelijk verzoek is
- .. Voor wat je zélf in die situatie nodig hebt
 - Om overeind te blijven
 - Om effectief te zijn

Talenten

- Schrijven (doelgroep, omvang, actief)
- Presenteren (doelgroep, lijf en taal)
- Reflecteren (hoe word ik gezien)
- Luisteren (wat wordt er écht bedoeld)
- Kijken (hoe 'lopen de hazen')
- Analyseren ..

En als het bestuur nou niet wil?

(en jij wilt wél)



Ayzen ge-operationaliseerd

Doelgroepen	Attitude = waarden en drijfveren van medewerkers	De norm = 'zo doen wij dat' namens de 'leiding' uit de directe omgeving		Control-perceptie = belang van de eigen rol	Competentie = vaardigheid & middelen
Iedereen		B: ken de huis-gedrag-regels & de <u>privacybeloftes</u> aan de betrokkenen A1: spelvorm, ook tussen sectoren (jury = directie) A2: Zakboekje de sterkste schakel M: fysiek maken en verspreiden Zakboekje F: jaarlijks een spel, met een rol voor de ambassadeurs (zie A3)	B: wees het voorbeeld B: beloon goed gedrag bij je collega's A3: ambassadeurs aanwijzen per sector M: berichten op Plein F: kwartaalbijeenkomsten inrichten voor kennisuitwisseling	B: jij bent een 'verantwoordelijke medewerker' A4: boodschappen van de directie bij instroom & terugkerend bij aanleidingen F: enkele keren per jaar	B: niet klakkeloos klikken B: bij twijfel: vragen! B: weet hoe je classificeert en toegang verleent B: meld datalekken B: etc. A5: <u>phishing-test</u> A6: <u>mystery-man</u> A7: 10 gouden regels F: A5, 6: beide jaarlijks F: A7 bij elke <u>communicatie</u> <u>een</u> verwijzing met linkje
Leidinggevend en eigenaren	Persoonlijke risicoperceptie vanuit de NIS2; - Beoordeling (assessment) van de kandidaten.	- Ken & communiceer je bestuurlijke <u>risk-appetite</u>; - Vertoon voorbeeldgedrag; - Spreek de managers & medewerkers aan op hun gedrag.	- 'Game of <u>threats</u>'; - Intervisie met 'opinion leaders' in de sector.	Leiderschaps-training: - Cultuurverandering begint aan de top: 'De vis rot het eerst aan de kop'.	- Wees de bestuurder die de ISO je vraagt te zijn met - planning & control, - stuurgroep; - Opleiding 'Eigenaarschap hoe doe ik dat?' - Selectietraining nieuwe medewerkers



Er dreigt Frustratie

(Latijn: *frustrari*) is de emotionele toestand van iemand die belemmerd wordt zijn verwachtingen, behoeften of doel te verwezenlijken. In tegenstelling tot depressie, een langdurige negatieve stemming, is frustratie meestal een tijdelijk gevoel.

- Frustratietolerantie gaat over jouw vermogen om problemen, tegenslagen, teleurstellingen en onvervulde behoeften aan te pakken. Hoe reageer je constructief en kalm wanneer dingen anders gaan dan je zou willen? Hoe ga je om met negatieve veranderingen? Hoe ga je om met situaties waarin jouw invloed nihil is, terwijl je toch graag die invloed zou willen hebben?
- <https://nl.wikipedia.org/wiki/Frustratie>

Hoge tolerantie?

Hoge tolerantie? Je laat je niet zomaar gek maken. Je hebt geleerd los te laten, te aanvaarden en te accepteren dat het niet altijd gaat zoals jij wenst.

- Je ploetert moedig voort, en blijft alert op de signalen van je lichaam!

Lage tolerantie?

- Je zit in zak en as en hebt meteen het gevoel dat de wereld vergaat.
 - Je verliest je [zelfbeheersing](#) en wordt enorm boos.
 - Je handelt impulsief.
 - Je vermijdt moeilijke situaties en steekt je hoofd in het zand.
 - Je stikt nog in zelfmedelijden als je niet oppast en kruipt in de slachtofferrol.
 - Je gaat jezelf veroordelen en hebt harde zelfkritiek.
 - Je beschuldigt voortdurend anderen.
 - Je raakt uit verbinding en communiceert niet meer constructief.
 - Je gaat [vechten, bevriezen of vluchten](#).
-
- <https://www.desteven.nl/carriere/loopbaan/organisatiefrustratie>

Doe iets!

Sta op en laat je niet langer gevangenhouden door werkfrustratie.

Neem de controle over je leven en maak keuzes die jouw geluk en welzijn bevorderen.

- <https://www.desteven.nl/carriere/loopbaan/organisatiefrustratie>