Security Governance Proces

7 juni 2023

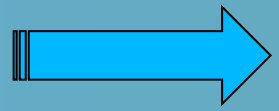
PvIB Platform voor InformatieBeveiliging

HUISHOUDELIJKE MEDEDELINGEN

Telefoon op stil

Badge graag inleveren bij vertrek

Evaluatie graag inleveren via de QR-code



Parkeren is gratis. Een uitrijkaart is niet nodig

Registratie bij binnenkomst en na afloop voor toekennen PE punten
Deze dien je zelf op te voeren (voor o.a. (C)PE punten)

Volgende bijeenkomst: 15 juni – De gevaren van Social Media

PvIB Platform voor InformatieBeveiliging

Programma

Planning	Agenda	Bijdrage
18:30	**Opening** Max Webber	
18:35	**NBility Model** – Netwerkbedrijven Ton van der Knaap,	
19:20	**Meetbare Maatregel Aanpak** (MMA) André Beerten	• NFI, Politie en OM Rutger Gooszen
20:10	Pauze	
20:30	**OpenKAT - en relatie MMA** Brenno de Winter	• Auditors visie op continu auditing Bas van der Linden en Leo Benschop
21:20	Afsluiting, borrel en netwerken	

PvIB Platform voor InformatieBeveiliging

Max Webber

- Cyber Privacy Security Consultant
  - 20+ jaar Ervaring C/ISO rollen

- 2019 Activiteiten Commissie PvIB.

Platform voor InformatieBeveiliging

https://www.edsn.nl/nbility-model/

NBility

NBility en Risk management

Platform voor InformatieBeveiliging

JUNI 2023

NBility – Risk management

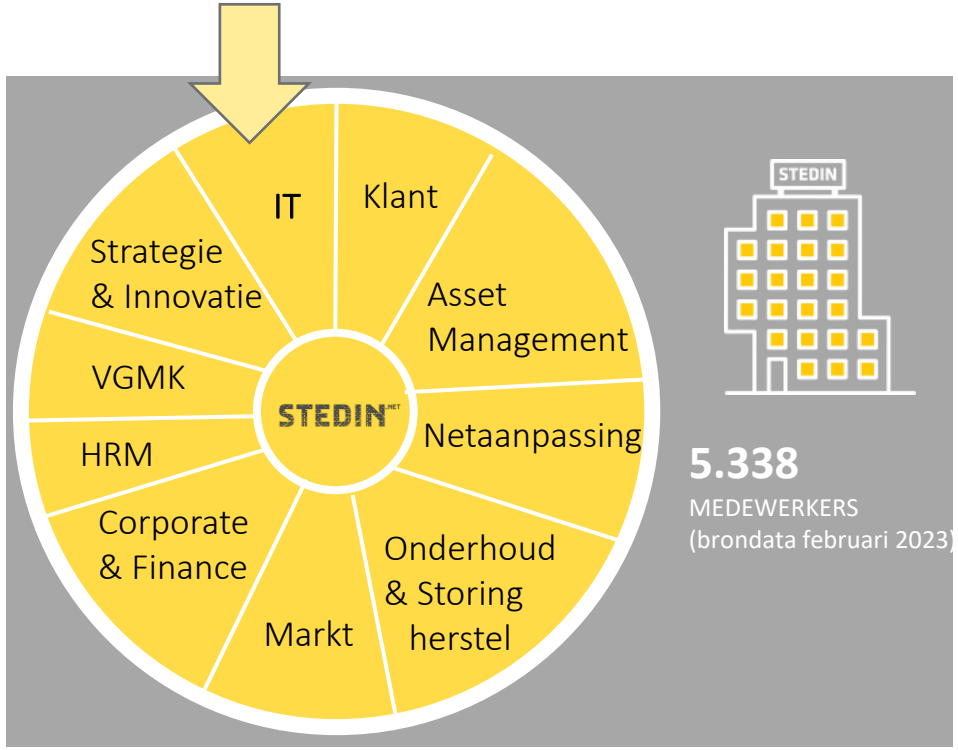
- Introductie
- WAT is een capability
- HOE ziet NBility eruit
- WAAROM NBility
- Usecase: risk management

1. WAT
2. HOE
3. WAAROM
4. VERDIEPING

Wie is Ton van der Knaap

- 2019 – Currently
  - Enterprise architect within Stedin
- 2006–2019
  - Enterprise architect within KPN
- 2000-2006
  - Process consultant within KPN - International Voice
- 1991-2000
  - Consultant Process control within PricewaterhouseCoopers – Global Risk Management Solutions

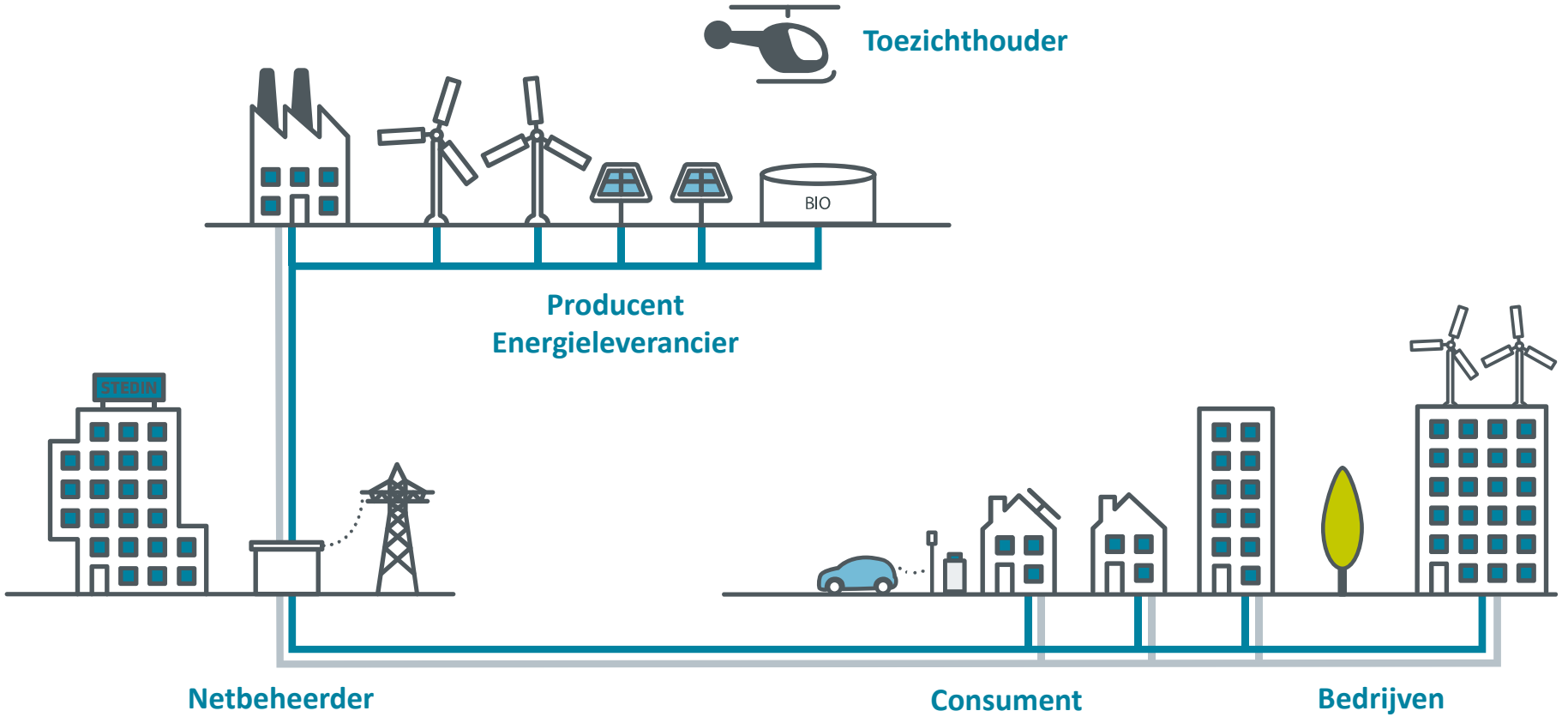
- Education
  - Business Economics; Erasmus University Rotterdam
  - Chartered Accountant; Erasmus University Rotterdam



ton.vanderknaap@stedin.net

De energiemarkt

Ons speelveld



Marktpartijen

STEDIN IN CIJFERS

2022

Netto omzet (mld)		Investeringen infrastructuur (mln)	
In 2022	In 2021	In 2022	In 2021
€1,32	€1,27	€712	€687

Elektriciteit

2.359.911
Aansluitingen elektriciteit

20.746 GWh
Getransporteerde hoeveelheid elektriciteit

22 MIN
Gemiddelde uitvalduur elektriciteit

58.250 KM
Elektriciteitskabel (omtrek aarde is ca. 40.000 km)

Gas

2.100.134
Aansluitingen gas

81%
van onze klanten deden eenvoudig zaken met ons.

3.782 MLN M³
Getransporteerde hoeveelheid gas

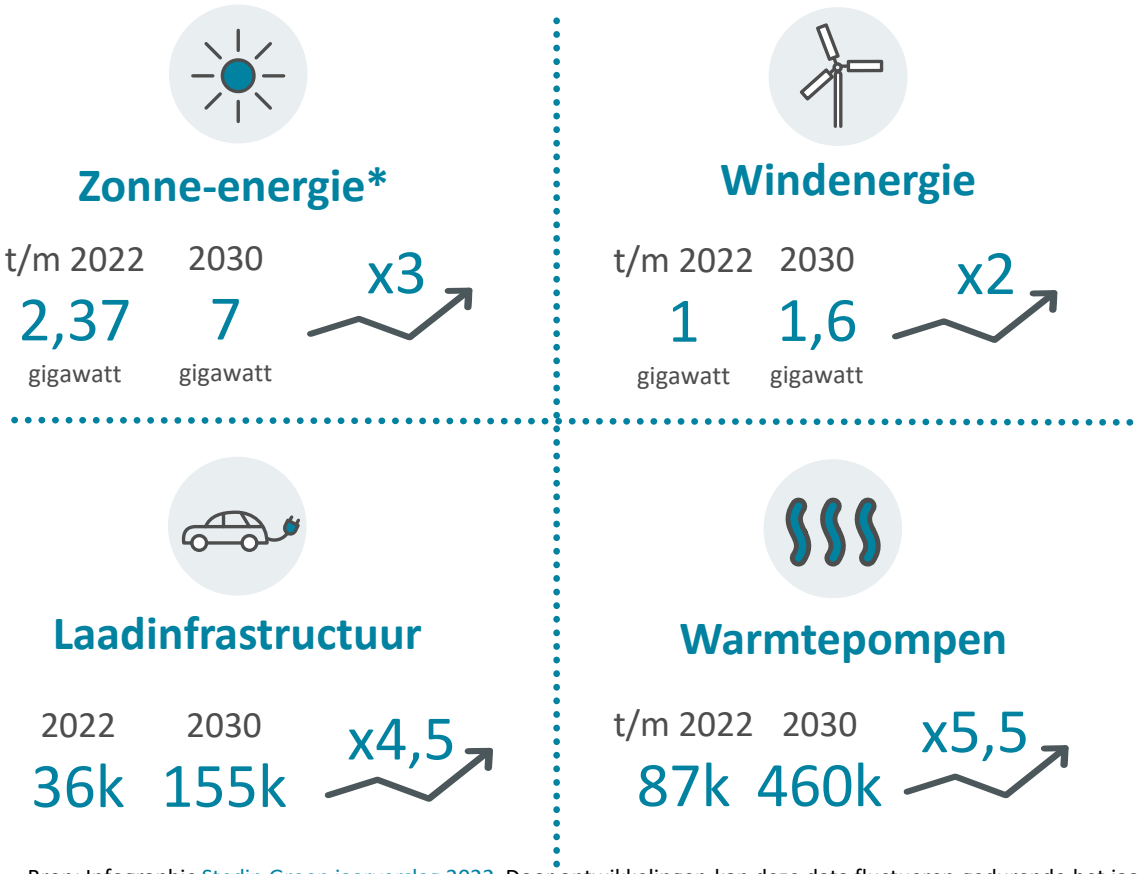
50 SEC
Gemiddelde uitvalduur gas

28.145 KM
Gasleidingen (omtrek aarde is ca. 40.000 km)

WE STAAN VOOR DE GROOTSTE UITDAGING OOIT!

De energietransitie

- Door de energietransitie verduurzaamt de energieproductie in hoog tempo.
- Het elektriciteitsverbruik neemt toe: we gebruiken meer elektriciteit voor het verwarmen van gebouwen, voor elektrisch rijden en voor elektrificatie in de industrie.
- Iedereen in ons verzorgingsgebied toegang geven tot duurzame energie; dát is de maatschappelijke opdracht van Stedin Groep.
- We richten daarom al onze aandacht op het mogelijk maken van de energietransitie.

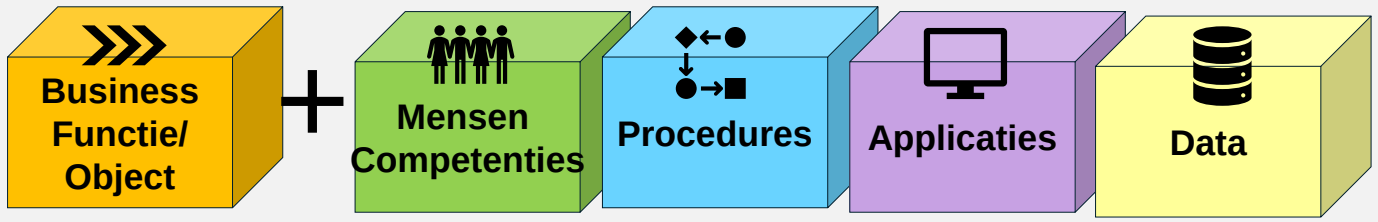


Bron: Infographic Stedin Groep jaarverslag 2022. Door ontwikkelingen kan deze data fluctueren gedurende het jaar.
* Zon op dak

STEDIN GROEP

Business capabilities: best practice voor besturen organisatie inrichting in veranderende omgeving

Business capability – WAT een organisatie kan:
beschrijft de business **functionaliteit/object**
en ondersteunt het **managen** van de **middelen** die ervoor nodig zijn.



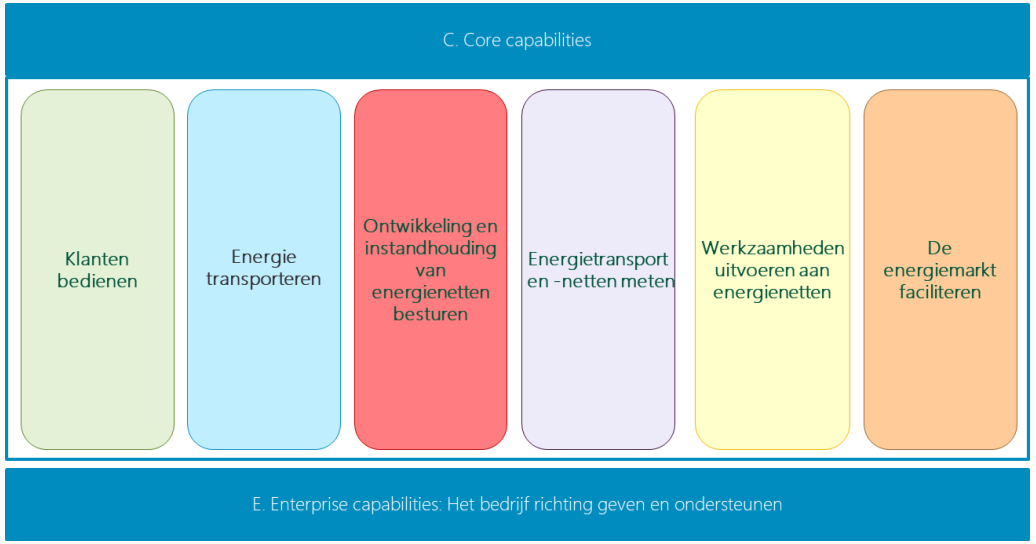
Een Business capability **model**
toont alle business capabilities in **samenhang**
die een organisatie nodig heeft om **succesvol** te zijn

Business Capabilities zijn:

- ✓ Stabiel in de tijd, ze beschrijven WAT een organisatie doet, niet HOE
- ✓ Niet afhankelijk van wie processen uitvoert en hoe deze worden uitgevoerd
- ✓ Minder politiek dan organisatie structuren
- ✓ Onafhankelijk van systeem implementaties
- ✓ Makkelijk herkenbaar voor iedereen binnen en buiten het bedrijf

NBility is het Business Capability model voor Netbeheerders

Netbeheerder Business capabILITY



NBility – Een gemeenschappelijke taal voor sneller veranderen

NBility model ontwikkeld met collega netbeheerders

Van wie
Voor wie

Netbeheer Nederland

Met wie

STEDIN.NET

alliander

ENEXIS GROEP

TenneT Taking power further

gasunie

NBility model versie 2.1 gepubliceerd (Ned+Eng).

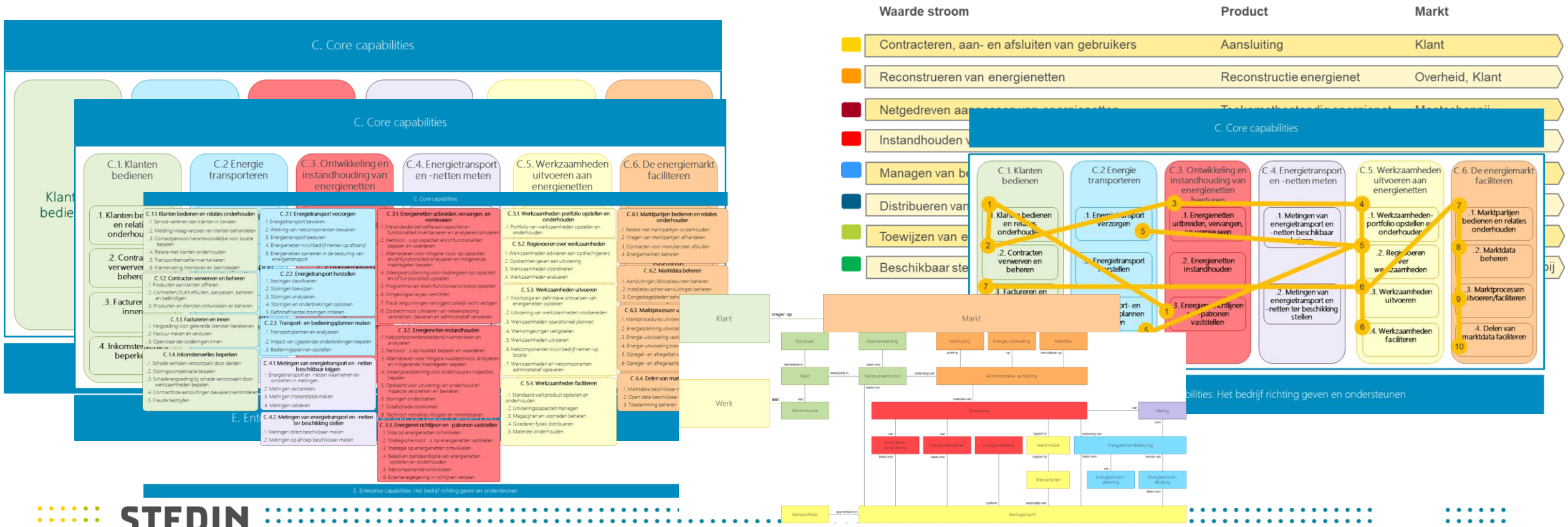
Veel ontwikkelingen tegelijkertijd, noemer ontbreekt

Samen want veel (toekomstige) ontwikkelingen in sector verband

NBility model: Capabilities, Waardestromen en Bedrijfsobjecten

Referentiemodel voor een netbeheerder

- NBility Capabilities en Bedrijfsobjecten op 3 detailniveaus
- Waardestromen en Capabilities per Waardestroom



NBility geeft inzicht en overzicht bij change & run

Elkaar **sneller begrijpen** en daardoor sneller veranderen

Ontwerpkeuzes om de juiste ontkoppelingen (applicatie**grenzen**) en juiste

Informatiebeveiliging – risico analyse (BIV classificaties en BCM analyses) sneller /consistenter opstellen.

Organisatie vormgeven en **verantwoordelijkheden** expliciet maken zowel binnen de

Impact van nieuwe/veranderende wetgeving analyseren.

Nieuwe mensen inwerken in wat de Netbeheerder doet.

Keuzes in ver

Besturen en vergelijken van procesprestaties/KPI's binnen en buiten Stedin:

Veranderingen plotten om te voorkomen dat je met 8 personen de badkamer staat te verbouwen of te implementeren

Esperanto geen succes, waarom NBility wel?

MET ELKAAR WILLEN EN GAAN GEBRUIKEN

Ofta lingvo akcelas ŝanĝo

Esperanto: Een gemeenschappelijke taal versnelt veranderen

Usecase – Risk management

- Risk management:
  - een capability in het model
  - een interne waardestroom
- Capability model: een hulpmiddel voor risk management
  - Inzicht en overzicht: relatie Waardestroom - Capability – Object – Applicatie => scoping
  - Eigenaarschap / business owners achterhalen
  - Organiseren van het werk
    - Wie doet wat / monitoring
    - Prioriteitstelling
  - Heat map voor risico’s / bottlenecks /incidenten

https://www.edsn.nl/nbility-model/

- NBility Introductiepresentatie
- NBility model presentatie en excel
- Opname NBility webinar
- Frequently asked questions
- Engelstalige versie van NBility

- https://www.edsn.nl/nbility-model/

Bijlagen

Business capabilities

Niveau 1

C. Core capabilities

- Klanten bedienen
- Energie transporteren
- Ontwikkeling en instandhouding van energienetten besturen
- Energietransport en -netten meten
- Werkzaamheden uitvoeren aan energienetten
- De energiemarkt faciliteren

E. Enterprise capabilities: Het bedrijf richting geven en ondersteunen

Business capabilities

Niveau 2 Core Capabilities

2. HOE

C. Core capabilities

C.1. Klanten bedienen	C.2 Energie transporteren	C.3. Ontwikkeling en instandhouding van energienetten besturen	C.4. Energietransport en -netten meten	C.5. Werkzaamheden uitvoeren aan energienetten	C.6. De energiemarkt faciliteren
.1. Klanten bedienen en relaties onderhouden	.1. Energietransport verzorgen	.1. Energienetten uitbreiden, vervangen, en vernieuwen	.1. Metingen van energietransport en -netten beschikbaar krijgen	.1. Werkzaamheden-portfolio opstellen en onderhouden	.1. Marktpartijen bedienen en relaties onderhouden
.2. Contracten verwerven en beheren	.2. Energietransport herstellen	.2. Energienetten instandhouden	.2. Metingen van energietransport en -netten ter beschikking stellen	.2. Regievoeren over werkzaamheden	.2. Marktdata beheren
.3. Factureren en innen	.3. Transport- en bedieningsplannen maken	.3. Energienetrichtlijnen en -patronen vaststellen		.3. Werkzaamheden uitvoeren	.3. Marktprocessen uitvoeren/faciliteren
.4. Inkomstenverlies beperken				.4. Werkzaamheden faciliteren	.4. Delen van marktdata faciliteren

E. Enterprise capabilities: Het bedrijf richting geven en ondersteunen

NBility

Business capabilities

Niveau 3 Core Capabilities

2. HOE

C. Core capabilities

C.1.1. Klanten bedienen en relaties onderhouden
..1. Service verlenen aan klanten in kanalen
..2. Melding/vraag/verzoek van klanten behandelen
..3. Contactpersoon/verantwoordelijke voor locatie bepalen
..4. Relatie met klanten onderhouden
..5. Transportbehoefte inventariseren
..6 Klantervaring monitoren en beïnvloeden

C.1.2. Contracten verwerven en beheren
..1. Producten aan klanten offreren
..2. Contracten/SLA's afsluiten, aanpassen, beheren en beëindigen
..3. Producten en diensten ontwikkelen en beheren

C.1.3. Factureren en innen
..1. Vergoeding voor geleverde diensten berekenen
..2. Factuur maken en versturen
..3. Openstaande vorderingen innen

C.1.4. Inkomstenverlies beperken
..1. Schade verhalen veroorzaakt door derden
..2. Storingscompensatie bepalen
..3. Schadevergoeding bij schade veroorzaakt door werkzaamheden bepalen
..4. Contractloze aansluitingen bewaken/verminderen
..5. Fraude bestrijden

C.2.1. Energietransport verzorgen
..1. Energietransport bewaken
..2. Werking van netcomponenten bewaken
..3. Energietransport besturen
..4. Energienetten in/uitbedrijf nemen op afstand
..5. Energienetten opnemen in de besturing van energietransport

C.2.2. Energietransport herstellen
..1. Storingen classificeren
..2. Storingen toewijzen
..3. Storingen analyseren
..4. Storingen en onderbrekingen oplossen
..5. Definitief herstel storingen initiëren

C.2.3. Transport- en bedieningsplannen maken
..1. Transport plannen en analyseren
..2. Impact van (geplande) onderbrekingen bepalen
..3. Bedieningsplannen opstellen

C.4.1. Metingen van energietransport en -netten beschikbaar krijgen
..1. Energietransport en -netten waarnemen en omzetten in metingen
..2. Metingen verzamelen
..3. Metingen interpretabel maken
..4. Metingen valideren

C.4.2. Metingen van energietransport en -netten ter beschikking stellen
..1. Metingen direct beschikbaar maken
..2. Metingen op afroep beschikbaar maken

C.3.1. Energienetten uitbreiden, vervangen, en vernieuwen
..1. (Veranderde) behoefte aan capaciteit en functionaliteit inventariseren en analyseren/simuleren
..2. Netrisico' s op capaciteit en/of functionaliteit bepalen en waarderen
..3. Alternatieven voor mitigatie risico op capaciteit en/of functionaliteit analyseren en mitigerende maatregelen bepalen
..4. (Meerjaren)planning voor maatregelen op capaciteit en/of functionaliteit opstellen
..5. Programma van eisen/functioneel ontwerp opstellen
..6. Omgevingsanalyses verrichten
..7. Tracé vergunningen verkrijgen/zakelijk recht vestigen
..8. Opdracht voor uitvoeren van netaanpassing verstrekken, bewaken en administratief verwerken

C.3.2. Energienetten instandhouden
..1. Net(componenten)toestand inventariseren en analyseren
..2. Netrisico' s op kwaliteit bepalen en waarderen
..3. Alternatieven voor mitigatie kwaliteitsrisico analyseren en mitigerende maatregelen bepalen
..4. (Meer)jarenplanning voor onderhoud en inspecties bepalen
..5. Opdracht voor uitvoering van onderhoud en inspectie verstrekken en bewaken
..6. Storingen onderzoeken
..7. Graafschade voorkomen
..8 Technisch netverlies inkopen en minimaliseren

C.3.3. Energienet richtlijnen en -patronen vaststellen
..1. Visie op energienetten ontwikkelen
..2. Strategische risico' s op energienetten vaststellen
..3. Strategie op energienetten ontwikkelen
..4. Beleid en standaardisatie van energienetten opstellen en onderhouden
..5. Netcomponenten ontwikkelen
..6. Externe regelgeving in richtlijnen vertalen

C.5.1. Werkzaamheden-portfolio opstellen en onderhouden
..1. Portfolio van werkzaamheden opstellen en onderhouden

C.5.2. Regievoeren over werkzaamheden
..1. Werkzaamheden adviseren aan opdrachtgevers
..2. Opdrachten geven aan uitvoering
..3. Werkzaamheden coördineren
..4. Werkzaamheden evalueren

C.5.3. Werkzaamheden uitvoeren
..1. Voorlopige en definitieve ontwerpen van energienetten opstellen
..2. Uitvoering van werkzaamheden voorbereiden
..3. Werkzaamheden operationeel plannen
..4. Werkomgevingen veiligstellen
..5. Werkzaamheden uitvoeren
..6. Netcomponenten in/uit bedrijf nemen op locatie
..7. Werkzaamheden en netcomponenten administratief opleveren

C.5.4. Werkzaamheden faciliteren
..1. Standaard werkproduct opstellen en onderhouden
..2. Uitvoeringscapaciteit managen
..3. Magazijnen en voorraden beheren
..4. Goederen fysiek distribueren
..5. Materieel onderhouden

C.6.1. Marktpartijen bedienen en relaties onderhouden
..1. Relatie met marktpartijen onderhouden
..2. Vragen van marktpartijen afhandelen
..3. Contracten voor markdiensten afsluiten
..4. Energiemarkten beheren

C.6.2. Marktdata beheren
..1. Aansluitingen/allocatiepunten beheren
..2. Installaties achter aansluitingen beheren
..3. Congestiegebieden beheren

C.6.3. Marktprocessen uitvoeren/faciliteren
..1. Marktprocedures uitvoeren
..2. Energieplanning uitwisselen
..3. Energie-uitwisseling vaststellen
..4. Energie-uitwisseling toewijzen aan marktpartijen
..5. Opregel- en afregelbehoefte communiceren
..6. Opregel- en afregelaanbod beheren

C.6.4. Delen van marktdata faciliteren
..1. Marktdata beschikbaar maken voor partijen
..2. Open data beschikbaar maken voor derden
..3. Toestemming beheren

E. Enterprise capabilities: Het bedrijf richting geven en ondersteunen

Business capabilities per domein

Enterprise capabilities: Het bedrijf richting geven en ondersteunen – Niveau’ s 1 en 2

C. Core capabilities

E. Enterprise capabilities: Het bedrijf richting geven en ondersteunen

E..1. Bedrijfsrichting opstellen en besturen

- .1. Strategie ontwikkelen en bewaken
- .2. Met Stakeholders in overeenstemming komen
- .3. Transformatie van bedrijfsinrichting besturen
- .4. Bedrijfscontinuïteit en compliance borgen

E.2. Processen en data ontwikkelen en beheren

- .1. Processen besturen
- .2. Data besturen

E.3. Medewerkers werven en inzetbaar houden

- .1. Medewerkers strategie en -plannen opstellen en besturen
- .2. Medewerkers in- en uitstromen
- .3. Medewerkers behouden
- .4. Medewerkers ontwikkelen

E.4. Digitale producten ontwikkelen en beheren

- .1. Digitaal product strategie en -portfolio ontwikkelen en beheren
- .2. Digitale producten realiseren
- .3. Digitale producten leveren
- .4. Digitale producten exploiteren

E.5. Goederen en diensten verkrijgen

- .1. Goederen- en dienstenstrategie en -plannen opstellen en besturen
- .2. Contracten met leveranciers afsluiten en bewaken

E.6. Kantoorgebouwen beheren en faciliteiten beschikbaar stellen

- .1. Gebouwen beheren
- .2. Faciliteiten beschikbaarstellen

E.7. Financiën verkrijgen en beheren

- .1. Financiële strategie en -plannen opstellen, bewaken en rapporteren
- .2. Vermogen en liquiditeiten beheren
- .3. Transacties financieel verwerken en standen beheren

NBility

Business capabilities per domein

Enterprise capabilities: Het bedrijf richting geven en ondersteunen – Niveau 3

C. Core capabilities

E. Enterprise capabilities: Het bedrijf richting geven en ondersteunen

E.1.1. Strategie ontwikkelen en bewaken
..1. Externe en interne analyses uitvoeren
..2. Positionering bepalen en het merk definiëren
..3. Strategie bepalen
..4. Bedrijfsplannen opstellen
..5. Bedrijfsprestaties bewaken

E.1.2. Met Stakeholders in overeenstemming komen
..1. Stakeholderrelatie onderhouden
..2. Wet- en regelgeving bewaken en beïnvloeden
..3. Sectorsamenwerking ontwikkelen
..4. Externe verantwoording afleggen

E.1.3. Transformatie van bedrijfsinrichting besturen
..1. Enterprisearchitectuur definiëren
..2. Veranderportfolio opstellen en bewaken
..3. Veranderportfolio items besturen
..4. Onderzoek en innovaties realiseren

E.1.4. Bedrijfscontinuïteit en compliance borgen
..1. Strategische risico's inventariseren en bewaken
..2. Informatiebeveiliging borgen
..3. Privacy borgen
..4. Bedrijfscontinuïteit borgen
..5. Veiligheid, gezondheid, milieu en kwaliteit borgen
..6. Juridische zaken besturen en bewaken
..7. Crisissen beheersen

E.2.1. Processen besturen
..1. Processen definiëren en verbeteren
..2. Processen orkestreren

E.2.2. Data besturen
..1. Data definiëren en beheren
..2. Datakwaliteit borgen
..3. Data ontsluiten
..4. Data-analysemodellen opstellen en beheren
..5. Data duurzaam bewaren

E.3.1. Medewerkers strategie en -plannen opstellen en besturen
..1. Medewerkersstrategie opstellen en besturen
..2. Medewerkersplannen opstellen en besturen
..3. Organisatie inrichten en optimaliseren

E.3.2. Medewerkers in- en uitstromen
..1. Medewerkers werven en selecteren
..2. Medewerkers aannemen
..4. Medewerkers laten uittreden

E.3.3. Medewerkers behouden
..1. Medewerkerrelatie onderhouden
..2. Medewerkers (her)plaatsen
..3. Medewerkers belonen
..4. Medewerkersverzuim begeleiden
..5. Medewerkerstijd verantwoorden

E.3.4. Medewerkers ontwikkelen
..1. Medewerkersprestatie evalueren
..1. Medewerkers opleiden en certificeren
..2. Medewerkers duurzame inzetbaar houden

E.4.1. Digitale productstrategie en – portfolio ontwikkelen en beheren
..1. Digitale productstrategie ontwikkelen en besturen
..2. Digitale productenportfolio beheren

E.4.2. Digitale producten realiseren
..1. Digitale producten creëren, aanpassen en verwijderen
..2. Digitale producten testen

E.4.3. Digitale producten leveren
..1. Digitale producten uitrollen en opleveren
..2. Digitale producten beschikbaar stellen

E.4.4. Digitale producten exploiteren
..1. Gebruik digitale producten ondersteunen
..2. Werking digitale producten zeker stellen

E.5.1. Goederen- en dienstenstrategie en -plannen opstellen en besturen
..1. Goederen- en dienstenstrategie opstellen
..2. Goederen- en dienstenplannen en besturen

E.5.2. Contracten met leveranciers afsluiten en bewaken
..1. Inkoopleveranciersrelatie onderhouden
..2. Goederen en diensten contracteren en/of bestellen
..3. Naleving van contracten bewaken

E.6.1. Gebouwen beheren
..1. Gebouwenstrategie en -plannen opstellen en besturen
..2. Gebouwen verkrijgen, verbouwen en afstoten
..3. Gebouwen onderhouden

E.6.2. Faciliteiten beschikbaarstellen
..1. Gebouwinstallaties beheren
..2. Gebouwen schoonhouden
..3. Ruimtes beschikbaarstellen
..4. Voedsel en drank beschikbaarstellen
..5. Veiligheid kantoorgebouwen borgen
..6. Goederenafhandeling verzorgen

E.7.1 Financiële strategie en -plannen opstellen, bewaken en rapporteren
..1. Financiële strategie opstellen
..2. Financiën plannen
..3. Financiële informatie verstrekken en adviseren
..4. Financiële verantwoording afleggen

E.7.2. Vermogen en liquiditeiten beheren
..1. Schulden beheren
..2. Waarde van activa beheren
..3. Banktegoeden beheren
..4. Vorderingen beheren
..5. Verplichtingen beheren

E.7.3. Financiële transacties verwerken en standen beheren
..1. Financiële transacties verwerken
..2. Financiële standen beheren
..3. Financiële beheermaatregelen uitvoeren

Waarde stromen

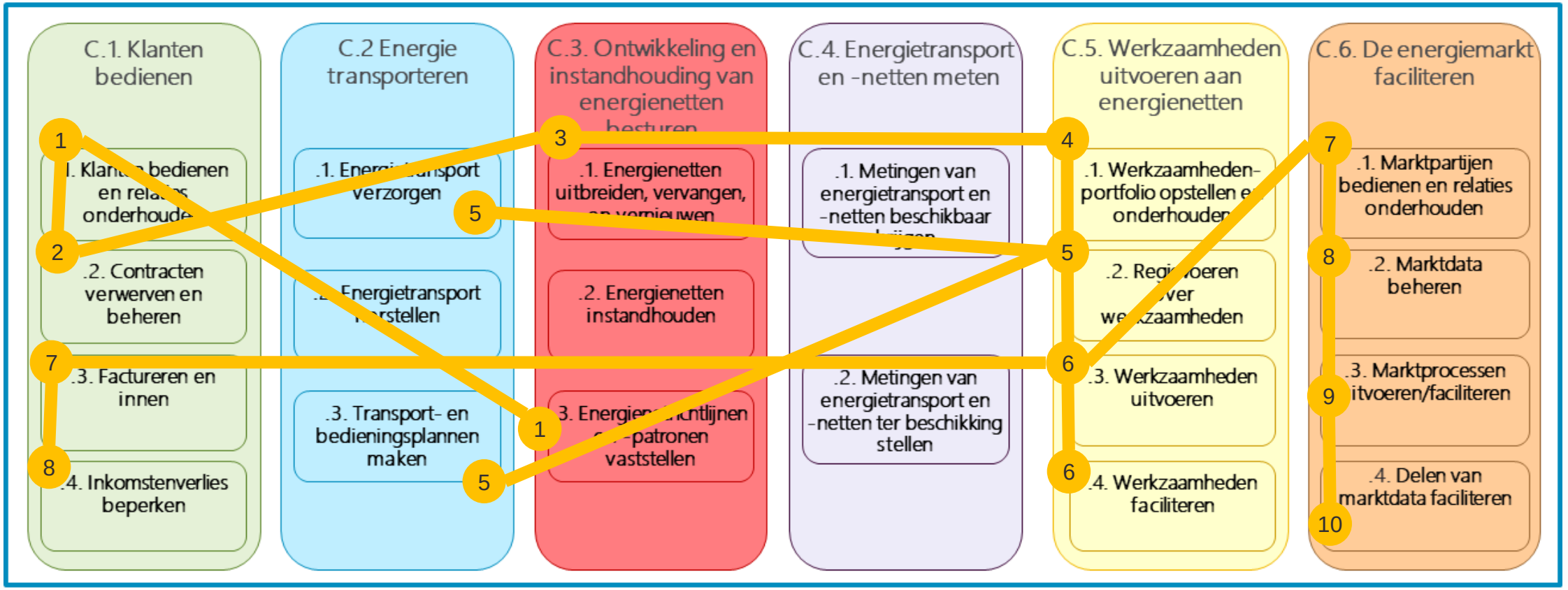
Waarde stromen, Producten en Markten

waardestroom	Product	Markt
Contracteren, aan- en afsluiten van gebruikers	Aansluiting	Klant
Reconstrueren van energienetten	Reconstructie energienet	Overheid, Klant
Netgedreven aanpassen van energienetten	Toekomstbestendig energienet	Maatschappij
Instandhouden van energienetten (onderhoud+storingherstel)	Betrouwbaar energienet	Maatschappij, Klant
Managen van beschikbare energienetcapaciteit (near real time)	Transportcapaciteit	Maatschappij
Transporteren van energie (real time)	Afgeleverde energie	Klant
Toewijzen van energie-uitwisseling	Toegewezen energie-uitwisseling	Marktpartij
Beschikbaar stellen van netbeheerdata	Netbeheerdata	Marktpartij, Maatschappij

Business capabilities per waardestroom

P.A. Contracteren, aan-en afsluiten gebruikers

C. Core capabilities

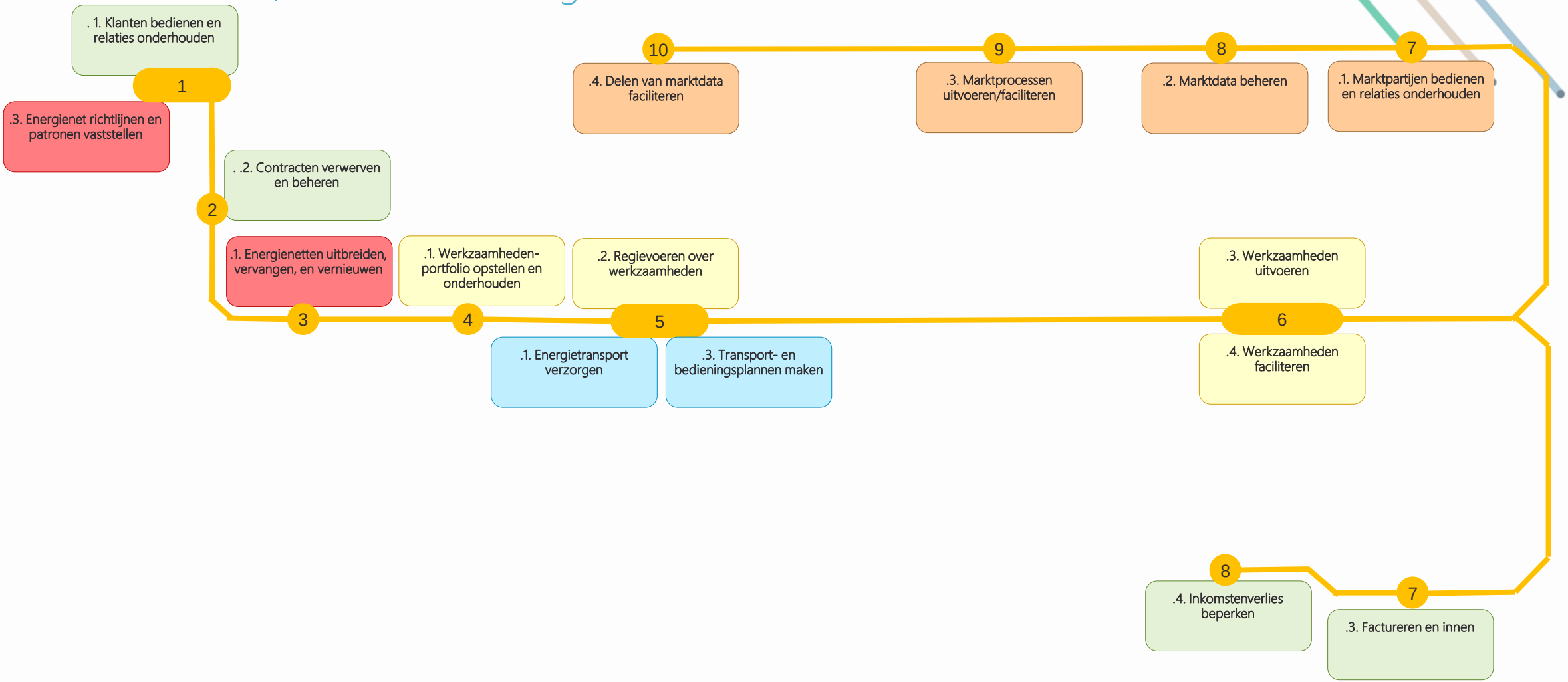


E. Enterprise capabilities: Het bedrijf richting geven en ondersteunen

Business capabilities per waardestroom

P.A. Contracteren, aan-en afsluiten gebruikers

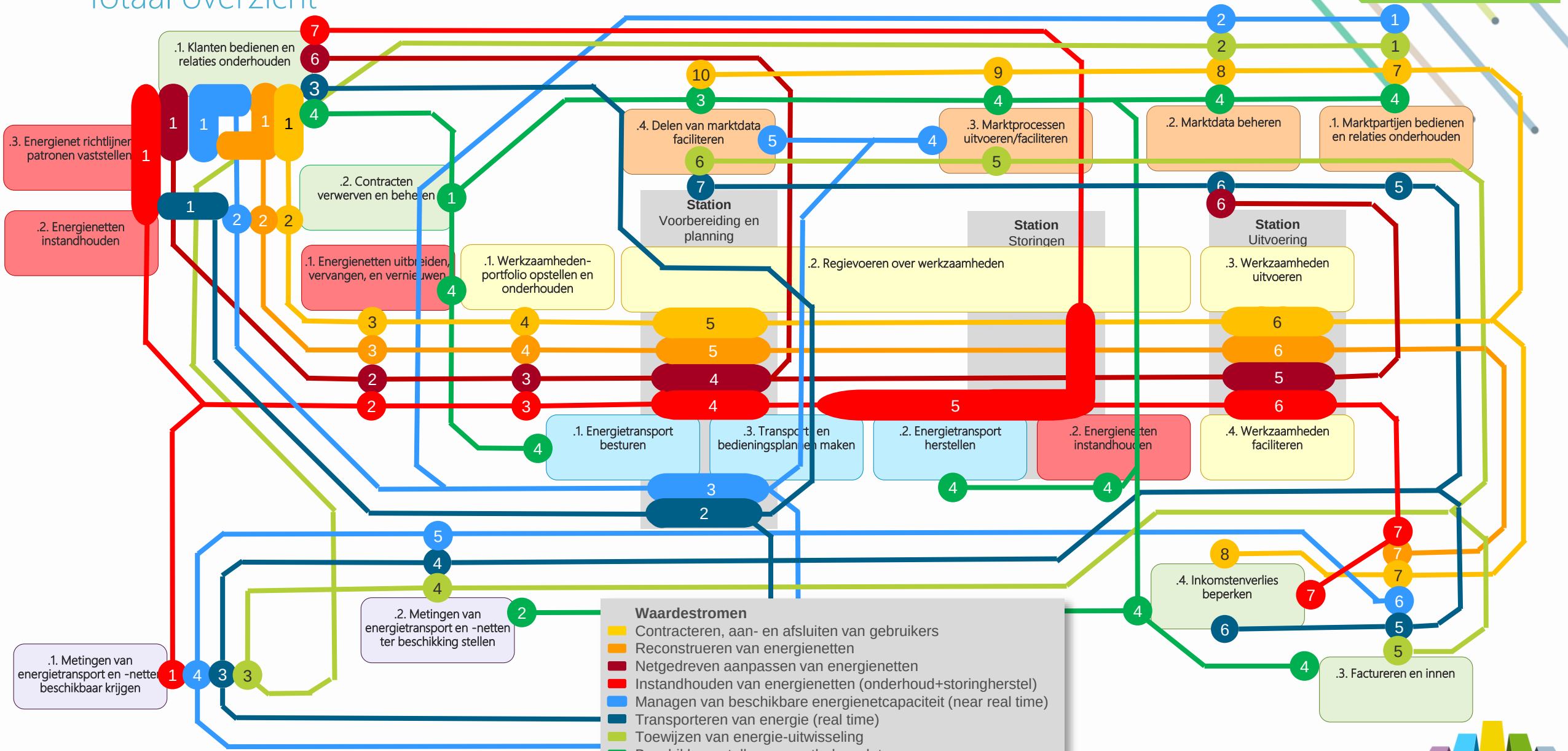
2. HOE



Business capabilities per waardestroom

Totaal overzicht

2. HOE



Interne (secundaire) waardestromen

Waardestromen en Producten

	Waardestroom	Product
I.A.	Bepalen en bewaken strategie en plannen	Business Strategie, Business Plan en Rapportage
I.B.	Veranderen bedrijfsinrichting	Bedrijfsinrichting
I.C.	Borgen bedrijfscontinuïteit en compliance	Compliant organisatie
I.D.	Beschikbaar maken en houden van inzetbare medewerkers	Inzetbare medewerkers (incl. fysieke en digitale werkplek)
I.E.	Realiseren van informatievoorziening	Uitgevoerd proces en/of beschikbare data
I.F.	Beschikbaar maken en stellen goederen en diensten	Beschikbare goederen en diensten
I.G.	Beschikbaar maken en stellen financiële assets en informatie	Beschikbare financiële assets en informatie

Interne waardestroom

I.B. Veranderen bedrijfsinrichting

1 C.1.2 Producten en diensten ontwikkelen en beheren
1 C.3.3 Energienetrichtlijnen en -patronen vaststellen

C. Core capabilities

E. Enterprise capabilities: Het bedrijf richting geven en ondersteunen

E..1. Bedrijfsrichting opstellen en besturen
- .1. Strategie ontwikkelen en bewaken
- .2. Met Stakeholders in overeenstemming komen
- .3. Transformatie van bedrijfsinrichting besturen
- .4. Bedrijfscontinuïteit en compliance borgen

E.2. Processen en data ontwikkelen en beheren
- . Processen besturen
- .2. Data besturen

E.3. Medewerkers werven en inzetbaar houden
- .1. Medewerkers strategie en -plannen opstellen en besturen
- .2. Medewerkers in- en uitstromen
- .3. Medewerkers behouden
- .4. Medewerkers ontwikkelen

E.4. Digitale producten ontwikkelen en beheren
- .1. Digitaal product strategie en -portfolio ontwikkelen en beheren
- 2. Digitale producten realiseren
- 3. Digitale producten leveren
- 4. Digitale producten exploiteren

E.5. Goederen en diensten verkrijgen
- .1. Goederen- en dienstenstrategie en -plannen opstellen en besturen
- .2. Contracten met leveranciers afsluiten en bewaken

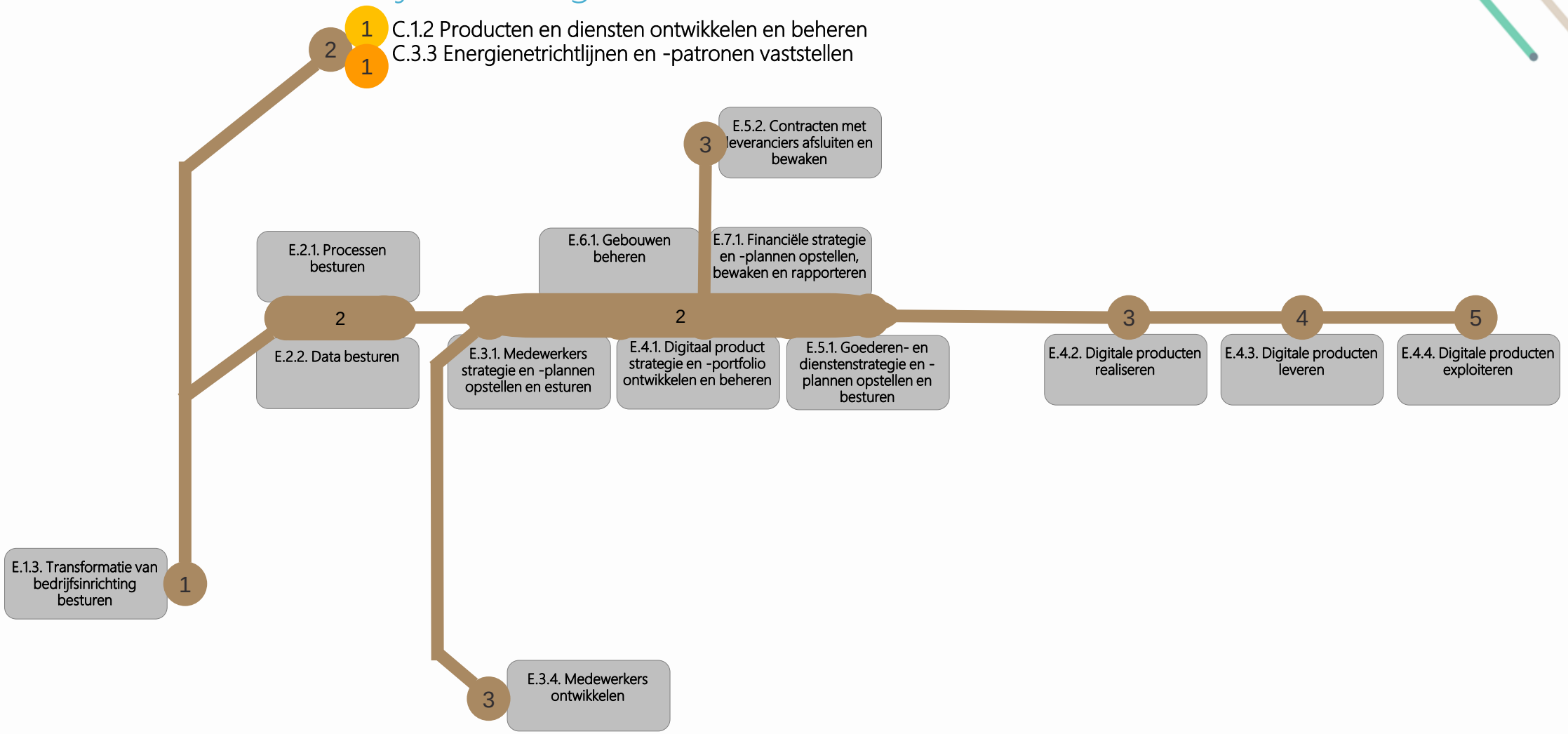
E.6. Kantoorgebouwen beheren en faciliteiten beschikbaar stellen
- . Gebouwen beheren
- .2. Faciliteiten beschibaarstellen

E.7. Financiën verkrijgen en beheren
- . Financiële strategie en -plannen opstellen, bewaken en rapporteren
- .2. Vermogen en liquiditeiten beheren
- .3. Transacties financieel verwerken en standen beheren

NBility

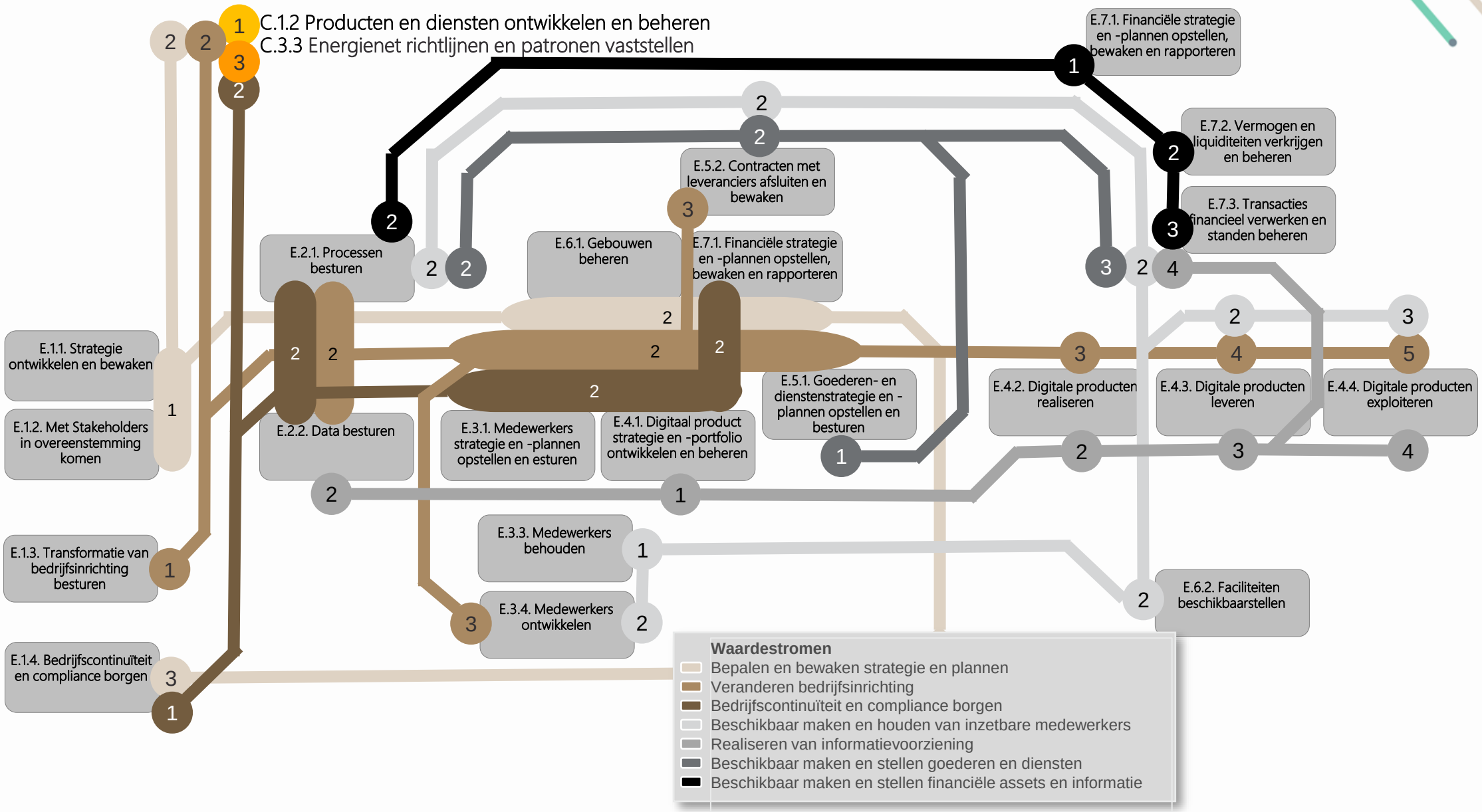
Interne waardestroom

I.B. Veranderen bedrijfsinrichting

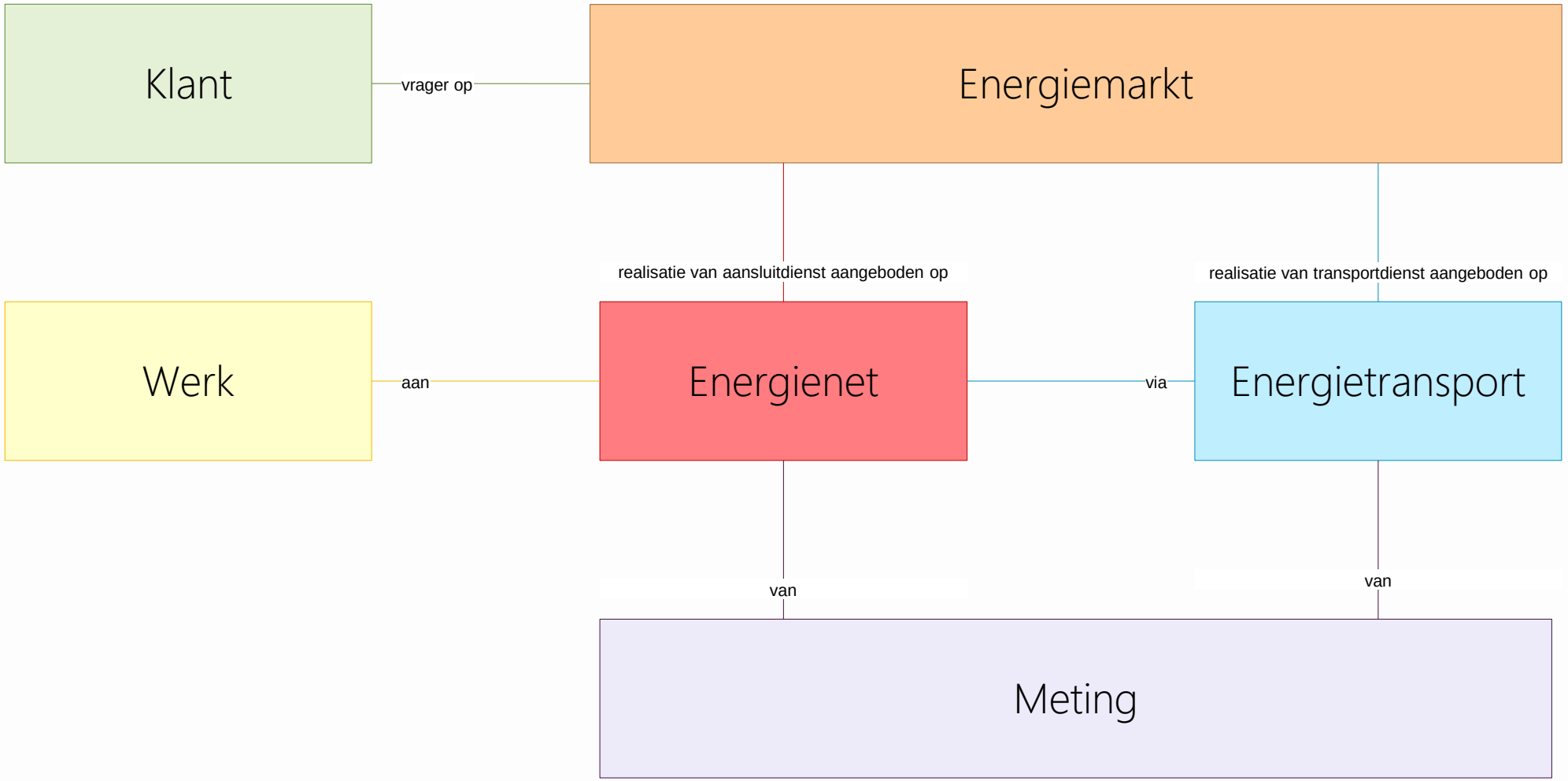


Interne waardestroom

Veranderen bedrijfs- en productiefactoren inrichting



Bedrijfsobjecten
Niveau 1



Bedrijfsobjecten
Alle niveaus

Klant

Klant
- Klant

Klantinteractie
- Klantaanvraag
- Transportbehoefte
- Klantcontactmoment
- Klantnotificatie
- Klantervaring
- Klantzaak

Klantovereenkomst
- Klantofferte
- Klantovereenkomst
- Product

Klantverrekening
- Klantfactuur

Energietransport

Transportbesturing
- Energietransport
- Bedieningssituatie
- Bedieningshandeling
- Opregel- of afregelactie
- Netcomponentprestatie

Transportafwijking
- Storing

Transportplanning
- Transportberekening
- Bedieningsplan
- Niet-beschikbaarheid
- Onderbreking

Energienet

Energienet
- Netcomponent
- Netfunctie
- Netcomponentconfiguratie
- Omgevingsanalyse
- Zakelijk recht of tracévergunning

Netverandering
- Functioneel ontwerp
- Netberekening
- Capaciteitsknelpunt
- Netaanpassingsopdracht
- Investeringsplan

Netkwaliteit
- Netcomponentconditie
- Kwaliteitsknelpunt
- Onderhouds- of inspectieplan
- Onderhouds- of inspectieopdracht
- Graafbericht

Netbeleid
- Technische bedrijfsstandaard

Meting

Meting
- Meting

Werk

Werkportfolio

Werkopdracht
- Werkopdracht

Werkactiviteit
- Voorlopig of definitief ontwerp
- Werkplan
- Medewerkerinzet
- Werkactiviteit

Werkmiddel
- Standaardwerkproduct
- Uitvoeringscapaciteit
- Materiaal
- Werkmiddel
- Goederenbeweging
- Uitvoeringsvergunning

Energiemarkt

Marktpartij
- Marktpartij
- Marktzaak
- Energiemarkt
- Marktovereenkomst

Aansluiting
- Aansluiting
- Aansluitlocatie
- Installatie
- Congestiegebied

Marktproces
- Marktverzoek
- Energieprogramma of prognose
- Energie-uitwisseling
- Opregel- of afregelbehoefte
- Opregel- of afregelaanbod

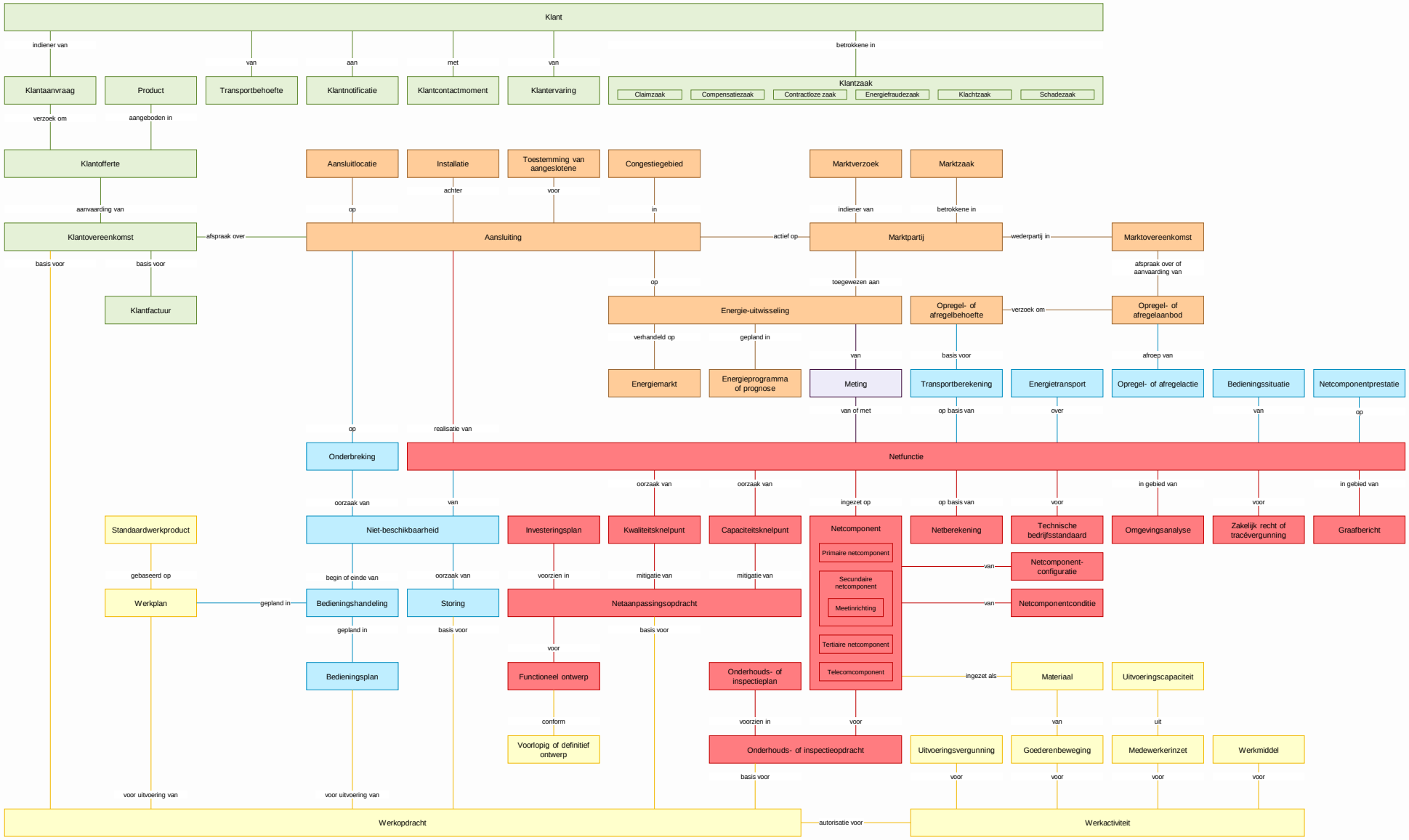
Marktdataverstrekking
- Toestemming van aangeslotene

NBility

Bedrijfsobjecten
Niveau 3

Relaties zijn te lezen in natuurlijke taal door lidwoorden en een vervoeging van ‘(kan) zijn’ in te voegen. Bijvoorbeeld:
- Een klant kan de indiener zijn van een klantaanvraag
- Een klantaanvraag is een verzoek om een klantofferte
- Enzovoort

Alleen de belangrijkste relaties zijn weergegeven.



De Meetbare MaatregelAanpak

André Beerten
CISSP CISM CISA CIPP/E
andre@octopus-IB.nl
06-12727238

OCTOPUS

Wij zijn..

https://bartjoosten01.blogspot.com/2012/03/t-schaap-met-de-5-poten.html

We zijn als martelaren voor de goede zaak

De falende CISO

'Hoe we voortmodderen'

Een niet aflatende stroom berichten in de media vertelt ons dat de beveiliging van informatie te wensen overlaat en dat we de strijd tegen de digitale onveiligheid dreigen te verliezen. Voorkomende incidenten onderstrepen deze claim met hun oplopende frequentie en de ernst van de gebeurtenissen. Hoe komt dit en wat is de rol van informatiebeveiligers, (C)ISO's, hierin? Wij zijn immers de professionals, de mannen en vrouwen met security kennis en de fraaie certificaten. Toch!?

https://www.harryknip e-het-geboortedorp-van-martelaar-perboyre

Maar wat laten dan we achter?

- … dat met ons vertrek in elkaar zakt..
- En onze opvolgers beginnen weer vanaf 0
  - Omdat er weinig gedocumenteerd is
  - Omdat ze een ander idee hebben
  - Omdat niemand anders zijn vinger opsteekt

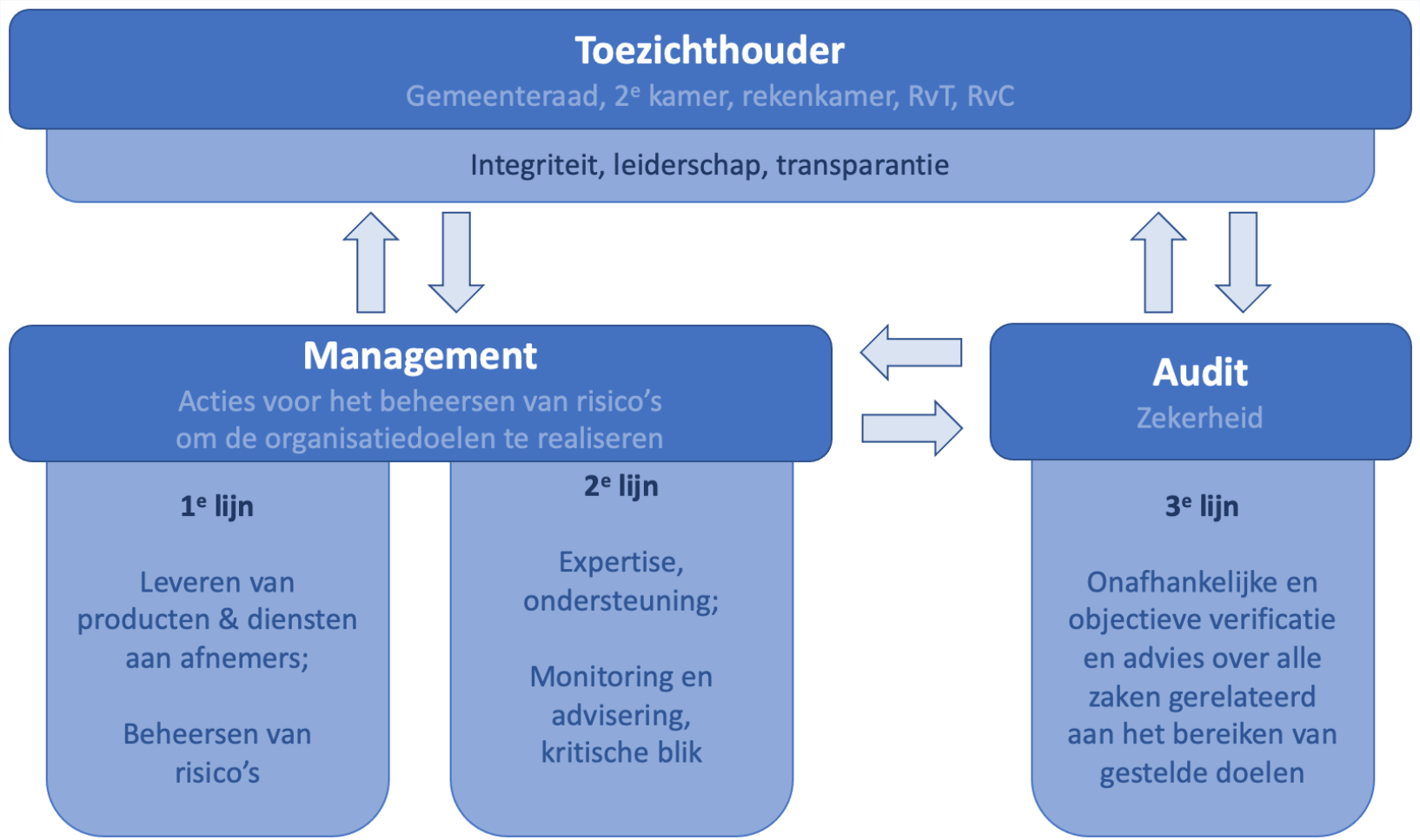
- Ze deden mee zolang wij eraan trokken, de energie erin pompten

Het gaat dus over:

EIGENAARSCHAP

https://www.managementboek.nl/boek/9789492881397/handboek-eigenaarschap-ontwikkelen-bij-anderen-frans-wijngaarden

Eigenaarschap is voor de 1e lijn



Hoe moet dat, eigenaarschap?

Kaderstellen = opdracht & beleid

Faciliteren = methode & middelen

Samenwerken = gesprek

http://utrechtseruimtemakers.nl/van-participatie-naar-eigenaarschap

De opleidingen ..

Mark Hoevers en ik -beide goed opgeleid- hadden (in 2014 al..) een goed gesprek over ons falen

https://www.youtube.com/watch?v=_JmA2ClUvUY

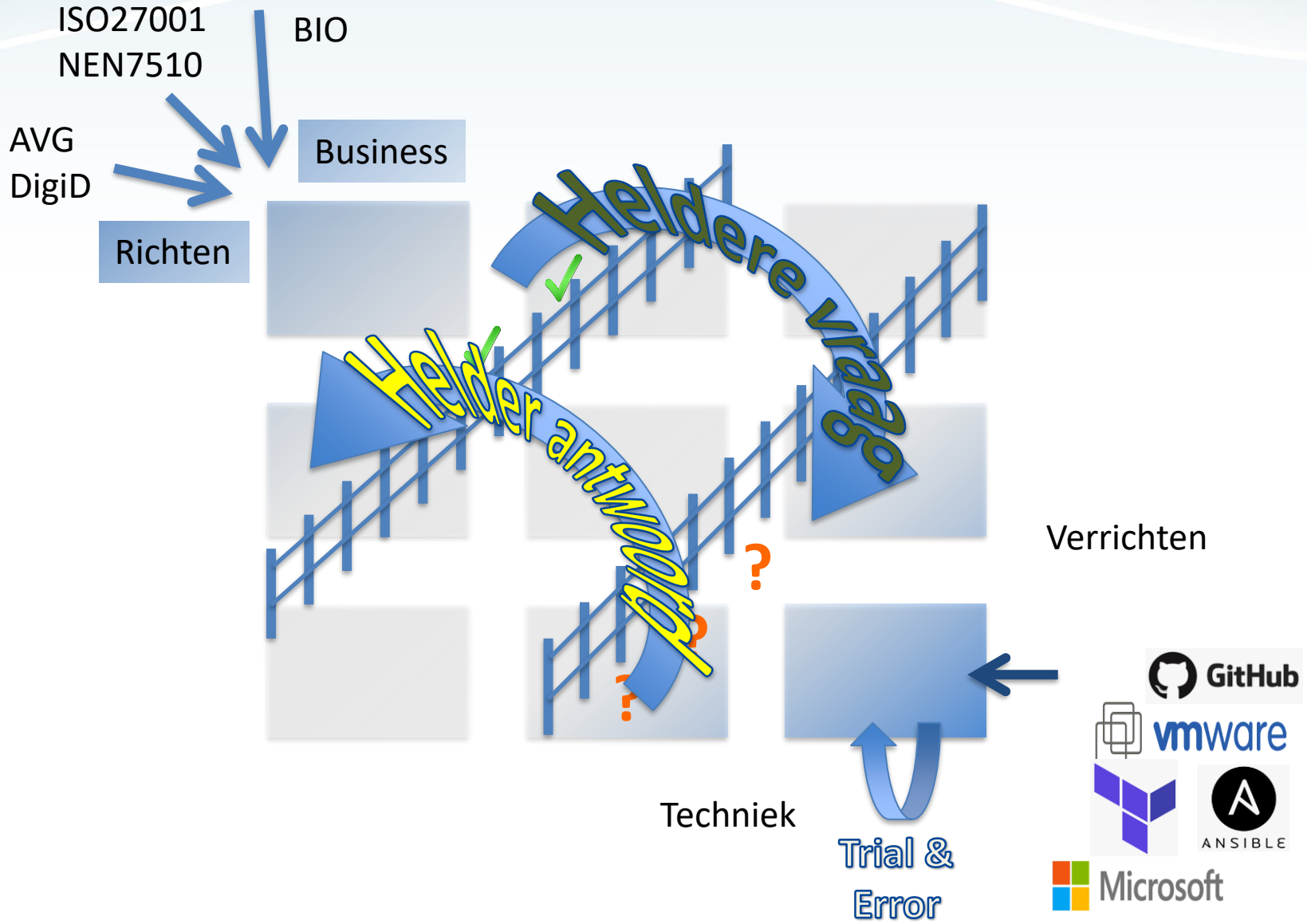
Probleemstelling

- Hoe stuurt het ISMS de implementatie aan en ..
  - Welke hulp kunnen w robleemeigenaar te worden/blijven

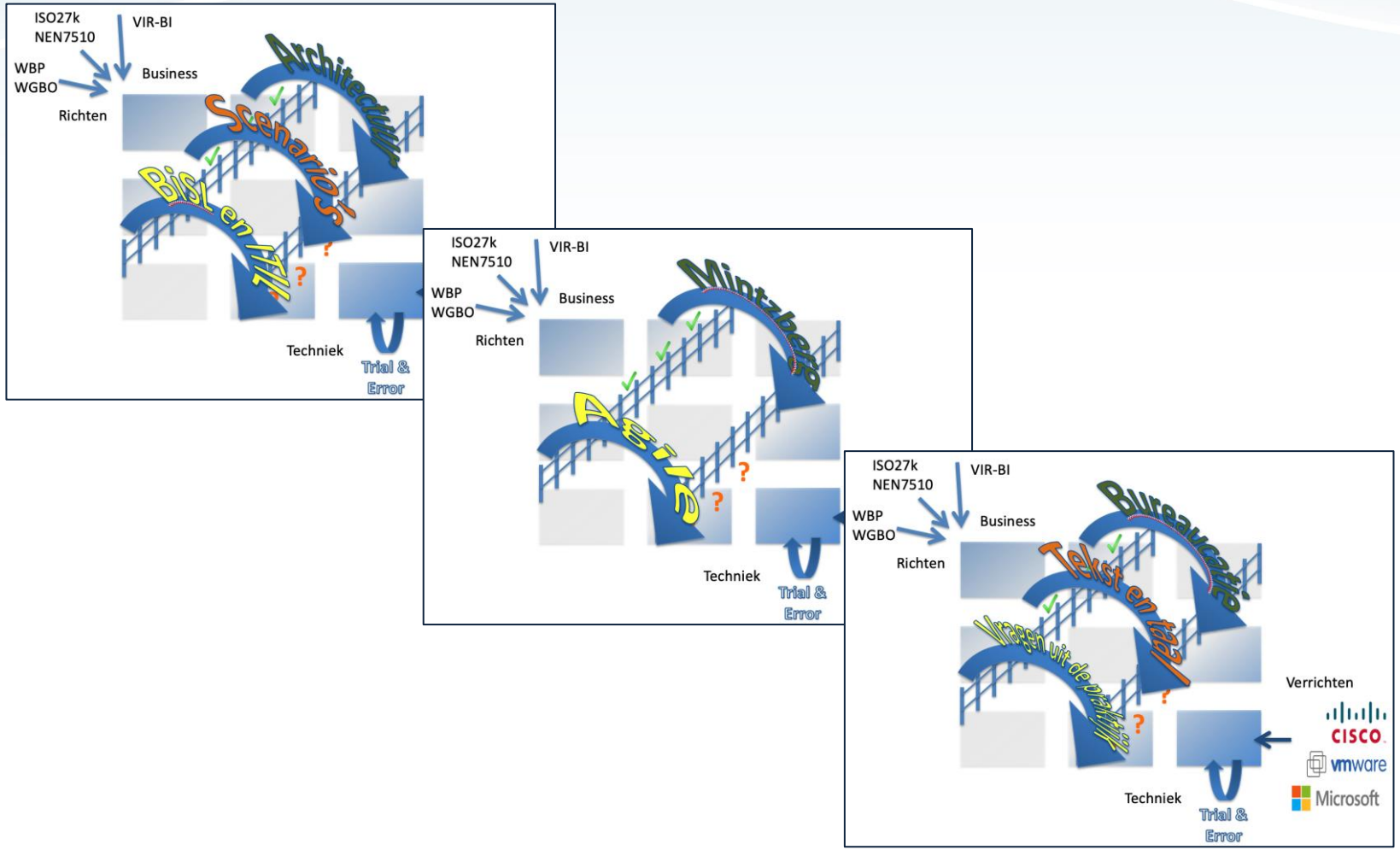
- Hoe ontstaat een betrou
  - Van de kwaliteit & de an de beveiliging
  - Van de nodige verbete
- Zonder dat we dat aan e vragen..!

De implementatiekloof

Beeld: Prof. Maes, 9-vlaks model



Maesbruggen 1-3

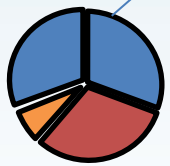


Maesbrug 4: MMA

- De ‘Meetbare MaatregelAanpak’ is een werkmethode voor de ‘control-eigenaar’
  - Analyseren
  - Ontwerpen
  - Documenteren
  - Beoordelen..
  - Én rapporteren over
    - Mate van control (aka volwassenheid)
    - Verbeterplannen
    - Restrisico’s!

Implementeren met de MMA

Start: beschouw de maatregel**scope** met (mogelijk) haar meerdere onderdelen en **verantwoordelijk**en.

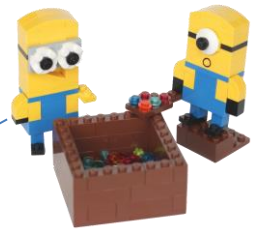


Analyseer de **control-opdracht**:
- Normtekst BIO/NEN/ISO
- Tactisch beleid
- Risicobeeld van je directie
- Opdrachten uit BIA's/DPIA's
- Verwerking-specifieke kaders
- ISO27002- & 27701-suggesties

Analyseer: welke **kennis & competenties** heb je nodig, hoe **werken** die **samen**

Ontwerp de maatregel als cyclisch proces met:
- Preventie (voorkom het risico)
- Detectie (weet of je maatregel werkt)
- Repressie (beperk de schade bij een incident)
- Meetpunten en -methodes (**KPI**)

Documenteer leesbaar & compact



Realiseer:
- Beoordeel volwassenheid
- Plan verbeteracties
- **Publiceer** voor alle belanghebbenden

Voer uit, **meet** doorlopend de effectiviteit (KPI's in proces en techniek)

Rapporteer, analyseer en **verbeter**, meld **restrisico's**

Herhaal!

BIO/N

Versie / datu

Opdracht

BIO -controlt
- *De voll*

BIO overheid
- *De ma*

1. Doel

Doel
- *Is er ee*

Scope (bereik
- *Is er ee*
- *Welke*

2. Veran

- *Is (dee*
- *Docum*

3. Kennis

- *Is het b*
- *Docum*

4. Samen

- *Is afste*
- *Docum*

5. Instru

- *Ken je*
- *Verwe*
- *Welke*
- *Docum*

6. Maatregel-opzet

Werking van de control op hoofdlijnen. Verwijs zoveel voor details naar (proces-) ontwerpdocumenten etc.
Documentatie: …

Preventie (voorkomt het risico)
- *Is de opdr*

Detectie (merkt
- *Zijn er mee*

Repres
-

Correct
-

MMA C

Maatregel-bestaan

7. Middelen-toewijzing

- *Zijn er middelen (mensen, apparaten, software, diensten) aangewezen voor een goede*

Discussion

Enter your comment. Wiki syntax is allowed:

AB: lekker zeg, elk bewijs, documentatie ontbreekt → vette onvoldoende! Ik stel voor eerst maar eens iemand te zoeken die écht verantwoordelijk wil zijn en die zorgt voor geld en aandacht..

Save | Preview

Bijlage: verbeterpunten

-

Bijlage: (rest-)risico's

-

Maatregel-be

7. Middeler

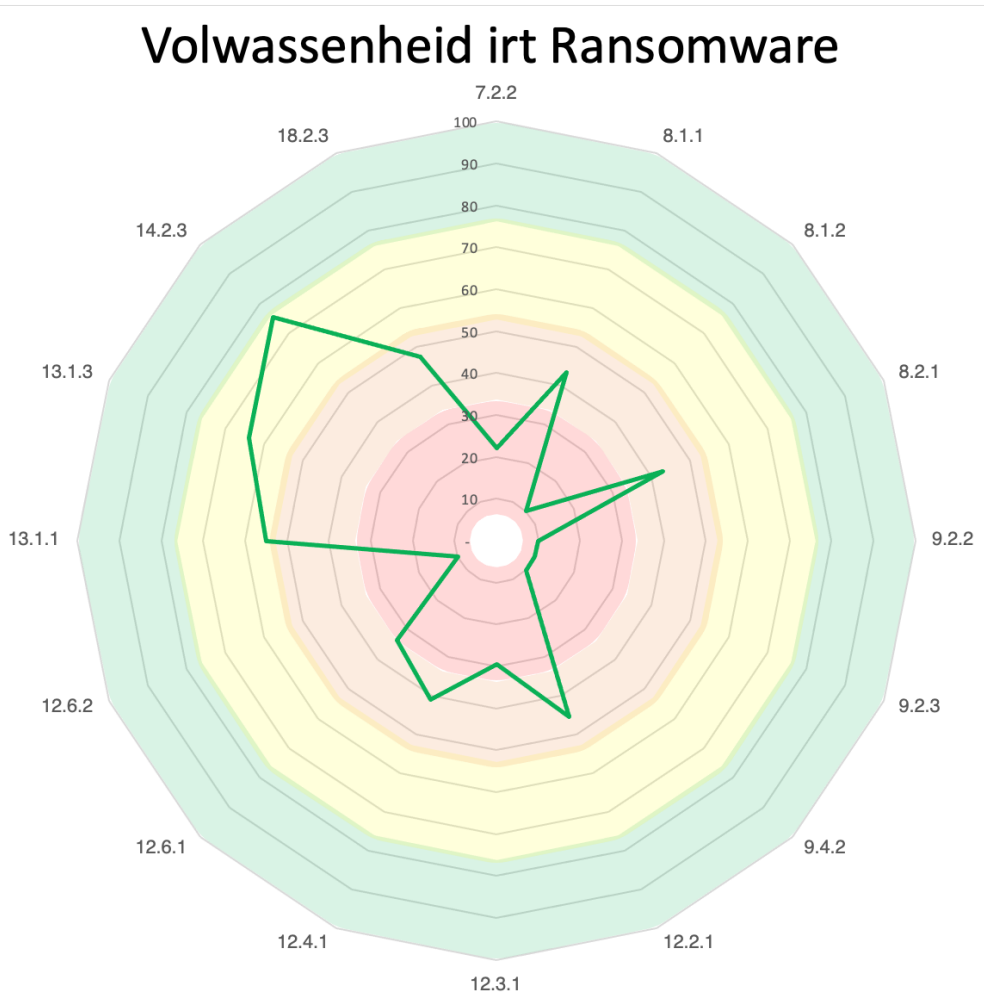
- *Zijn er middelen (mensen, apparaten, software, diensten) aangewezen voor een goede uitvoering?*

Control beoordelen per control

Beheren van speciale toegangsrechten		
9.2.3 - Het toewijzen en gebruik van speciale toegangsrechten moeten worden beperkt en beheerst.		
Doel & Scope	FO-module-middelen wel in beeld, overige scope niet volledig	f
Verantwoordelijkheden	Niet duidelijk belegd	n
Competentie	Schieten tekort	l
Samenwerking	Geen, alleen incidenteel, ad hoc	p
Opdracht	Niet goed noch gestructureerd	p
Ontwerp (met KPI's)	Preventie: onvoldoende fijnmazig en op mappen, dus risicovol Detectie: beperkt Repressie: mogelijk, door CISO	p
Realisatie met middelen	Onduidelijk of het voldoet	p
Middelengebruik	Onwaarschijnlijk	l
Meten & Rapporteren	Nee	n
Bijsturen	Nee	n
	Documenten / bewijslast	**42**
	Geen	

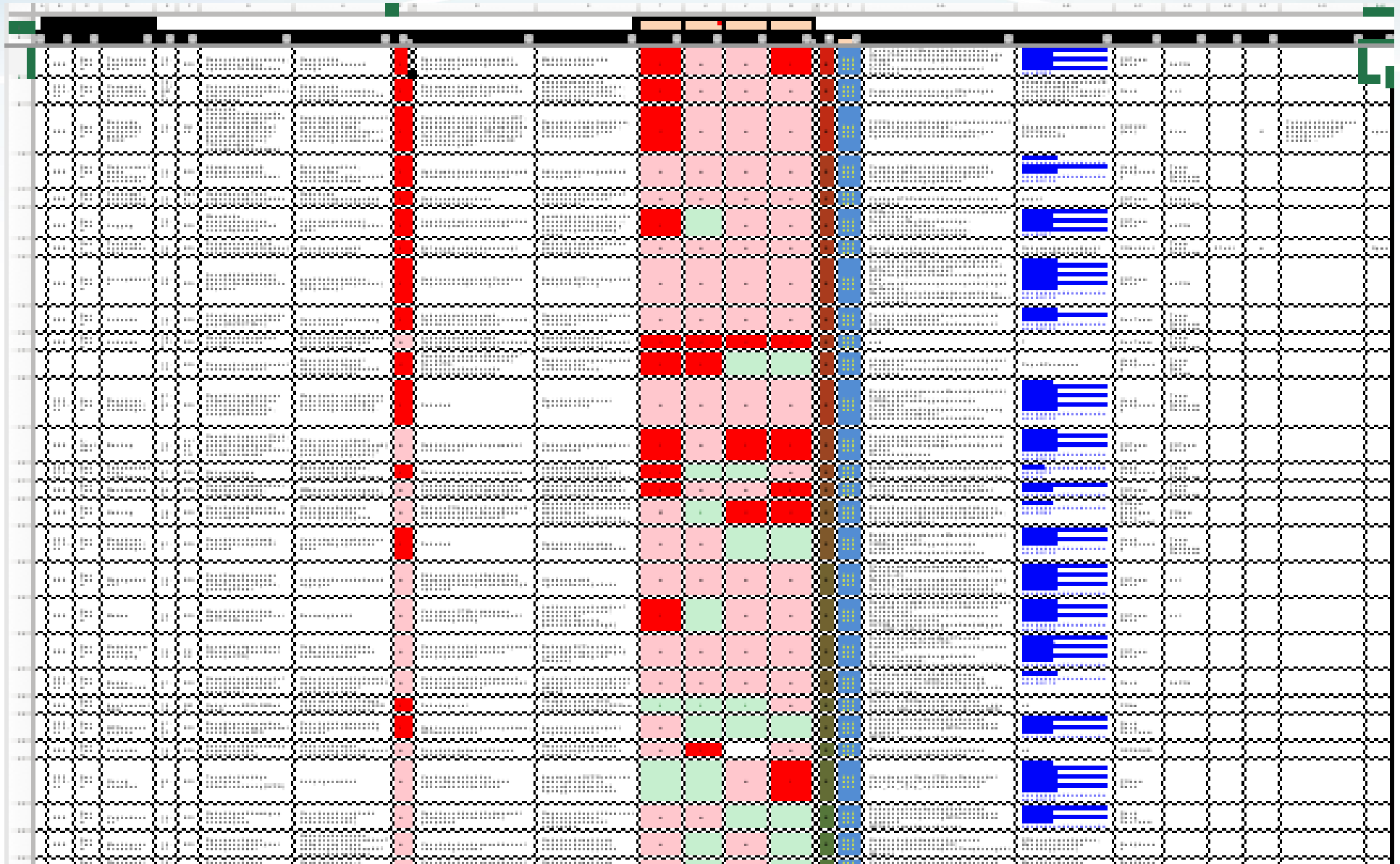
Relevant rapporteren

	BIO	Controls
	6.2.2	Telewerken
12	7.2.2	Bewustzijn,
15	8.1.1	Inventarisei
16	8.1.2	Eigendom v
19	8.2.1	Classificerer
28	9.2.2	Gebruikers t
29	9.2.3	Beheren vai
35	9.4.2	Beveiligde ir
60	12.2.1	Beheersmaa
61	12.3.1	Backup
62	12.4.1	Gebeurtenis
67	12.6.1	Beheer van
68	12.6.2	Beperkinger
70	13.1.1	Beheersmaa
72	13.1.3	Scheiding in
85	14.2.3	Technische
116	18.2.3	beoordeling



	BIO	Ransomware
	32	√
	22	√
	44	√
ging.	10	√
	43	√
	10	√
	10	√
	10	√
	46	√
	30	√
	41	√
	34	√
	10	√
	55	√
	64	√
egels	76	√
	48	√

Urgentie rapporteren



Verbeterpotentieel rapporteren

Restrisico in de huidige situatie
Mogelijkheid van beschikbaarheids-, integriteits- en vertrouwelijkheids-incidenten. Oorzaak slechte beheersing van de wijzigingen, mogelijkheden voor omzeilen van informele afspraken, ontbreken van sanctiemogelijkheden.
Controleverlies in wijzigingensproces. Oorzaak combinatie van groot personeelsverloop en ontbrekende documentatie.

Verbeteracties:

https:/[redacted]atlassian.net/browse/BIO-2

Actie	Jira Ticket
Acceptatie- en productie-omgevingen beter scheiden scheiden (ABX/Ansible tower, door [redacted]	https://[redacted].atlassian.net/browse/S2-471
Push zonder code review onmogelijk maken	https://[redacted].atlassian.net/browse/S2-472
Goedkeuringsprocedure A→P formaliseren, inclusief security checks (openvas, Molecule)	https://[redacted].atlassian.net/browse/S2-473
Changelog-inspecties organiseren & opvolging afwijkingen middels incidentproce	https://[redacted].atlassian.net/browse/S2-474
[redacted]isicoinput eisen in user stories (verplicht 'haakje' opnemen) Een [redacted] moet dus aanwezig zijn	https://[redacted].atlassian.net/browse/S2-475
Directe toegang op infra (bypass van Ansible en terraform / werken vnaf de desktop) striktbeperken (alleen met OK van [redacted]	https://[redacted].atlassian.net/browse/S2-476
Verantwoordelijkheid, met mandaat en leesbare/beschikbare documentatie (werkprocessen en checklists) organiseren.	https://[redacted].atlassian.net/browse/S2-477
Werken met checklists in de review-fase (vòòr het besluit A→P)	https://[redacted].atlassian.net/browse/S2-478
Wijzigingen alleen accepteren als deze via Jira zijn geregistreerd	https://[redacted].atlassian.net/browse/S2-479

Dualiteit

- EIGENAARSCHAP
  - Van informatieverwerkingen/bedrijfsprocessen en systemen en dús van risico's
  - Van controls en dus van beveiliging, passend en effectief
- GESPREK
  - klant en leverancier van veiligheid, gesprek over risico's en maatregelen, over de implementatiekloof heen
- En de CISO is de gespreksleider

Voordelen (1)

- Plan –
  - Ontdekken & ontwerpen van wat al goed werkt
  - Met de middelen en in de stijl van de organisatie
- Do
  - Beveiligen als een continuproces
  - Met preventie, detectie, repressie en KPI
- Check & act
  - Beoordelen en verbeteren
  - Op basis van consensus 1e en 2e lijn

Voordelen (2)

- Direct betrokken verantwoordelijke zijn de informatiebron
- Niet de mening van de auditor/toezichthouder telt, maar die van de 1e lijn / control-eigenaar → claim-based auditing
- Inhoud-agnostisch gesprek dus geen ‘strijd’ over inhoud, maar een gesprek

Nadelen

- Ambachtelijke, arbeidsintensieve 1e doorgang (enkele uren per control)
- Leerproces: niet praten over wat je doet, maar hoe je dat ‘doen’ *beheerst* → ‘control’

Voorwaarden

- Stel kaders
  - Eigenaarschap voor elke control (naam en rugnummer) met opdracht om met de MMA te werken
  - Formuleer tactisch beleid voor heel de norm (het ‘waarom’ en het ‘wat’)
  - Vraag om onderbouwde rapportages door de 1e lijn
- Faciliteer
  - Reik de MMA aan, zorg voor opleiding en kaders
- Werk samen!
  - Voer een gesprek over élke control (en neem de tijd!)

En nu de praktijk

- Concept ontwikkeld 2017
  - Hoogheemraadschappen (HHR & HHSK)
  - Antonius ziekenhuis Sneek (certificatie NEN7510)
  - 2020 directie OI & S (Datapunt) Amsterdam
  - 2021 heel Amsterdam, VWS RDO (afd Covid), veiligheidsregio Noord-Holland noord
  - 2022 Belastingdienst, Dijklander ziekenhuis, Politie-OM-NFI (forensische keten)
  - 2023 Maxima Medisch centrum . . .

Brian Baal: Gemeente Amsterdam

- Project BIO 2021-2022
- 52 directies, ca. 15 ISO’s
- Gemiddeld 38 controls per directie
- Directies met veel autonomie
- Vooraf geen eigenaren/aanspreekpunten bekend
- Beperkte gemeentebrede kaders, beperkte aanwijzingsbevoegdheid

Gemeente Amsterdam

Ervaring met de MMA

- Ontdekking voor de betrokken 1e lijn
  - Directies verklaren
    - Eindelijk duidelijk wat de BIO is en wil
    - Wat implementeren is
    - Hoe de verandering echt vorm kan krijgen
    - Rapporteert over voortgang in de 1e lijn
  - 2e lijn krijgt nieuwe positie
    - Draagt verantwoordelijkheid over
    - Helpt hierna bij het verbeterplan

Gemeente Amsterdam

Rutger Gooszen: Politie-OM-NFI

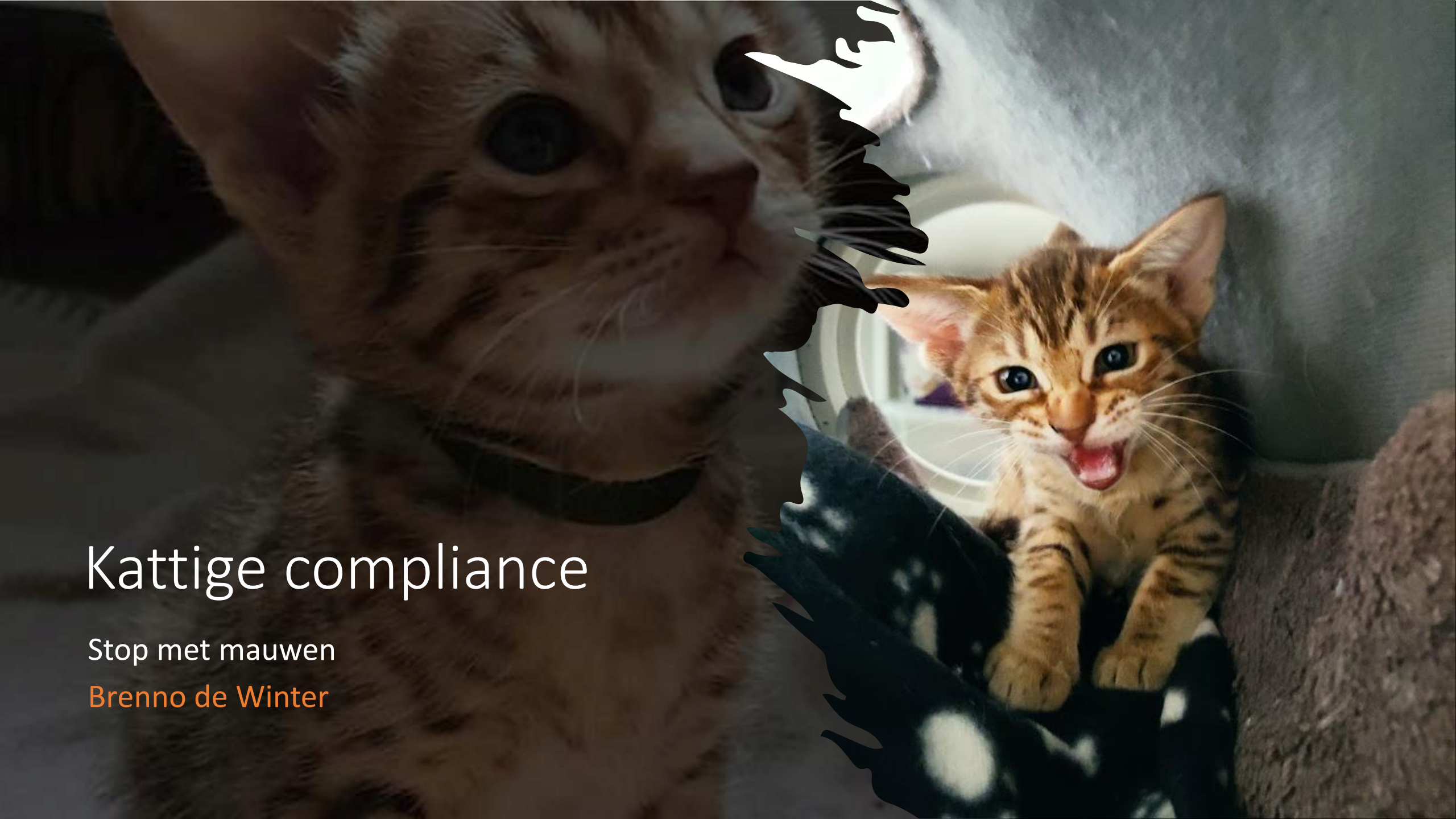
- Project: informatieuitwisseling tussen partijen in de forensische keten
  - We delen informatie maar we willen niet blind vertrouwen
  - Claim ‘we doen de BIO’ is onvoldoende*
  - Elke partij analyseert afgesproken set van controls met de MMA en deelt het eigen oordeel
  - Bij een onvoldoende volgt inhoudelijke bespreking -onder geheimhouding- tussen partijen

VERDONCK KLOOSTER & ASSOCIATES
A HIGHBERG COMPANY

Ervaring met de MMA

- Werkt want
  - Blijft weg bij de inhoud, biedt ruimte aan eigen invulling
  - Laat de verantwoordelijkheid waar die hoort
  - Levert basis voor ‘onderbouwd vertrouwen’
  - Maakt beter rapporteren over veiligheid mogelijk

VERDONCK KLOOSTER & ASSOCIATES
A HIGHBERG COMPANY



Kattige compliance

Stop met mauwen

Brenno de Winter

Brenno de Winter

- Schreef eerste code toen ik 5 jaar oud was
- Hacker
- 15 jaar onderzoeksjournalistiek, Journalist van het Jaar 2011
- Chief Security and Privacy Operations at Ministerie van VWS
- Werk als zelfstandige
- Veel security onderzoek

Vergeet ~~Brenno~~
Ik ben Keiko en vergeet de rest!

UITGELICHT

Dutch Data Forum 2022

Het Dutch Data Forum congres is al vier jaar het fundament voor een datagedreven

COMMUNICATIE / TELECOM 15/05/2023

Training is alles

...music should have a fun and light-hearted tone that complements the lyrics and celebrates the playful nature of cats. Lees ook: **Keiko**'s Kijk: Vertel me niet wat niet mag Neus...

COMMUNICATIE / TELECOM 12/01/2023

5G, Bluetooth en WiFi op Apple-chip: exit Broadcom

...getroffen. Apple wil uiteindelijk alle chips in-house gaan produceren onder de naam Apple Silicon. Lees ook: **Keiko**: Neus voor slechte zaken Knoworries introduceert Teams-bellen op basis van Operator Connect ...

SECURITY 20/12/2022

IT MANAGEMENT 24/10/2022

Hoe het allemaal begon


NOS
npo politiek
LIVE
Afstand
Testen
Licht

Stop met janken

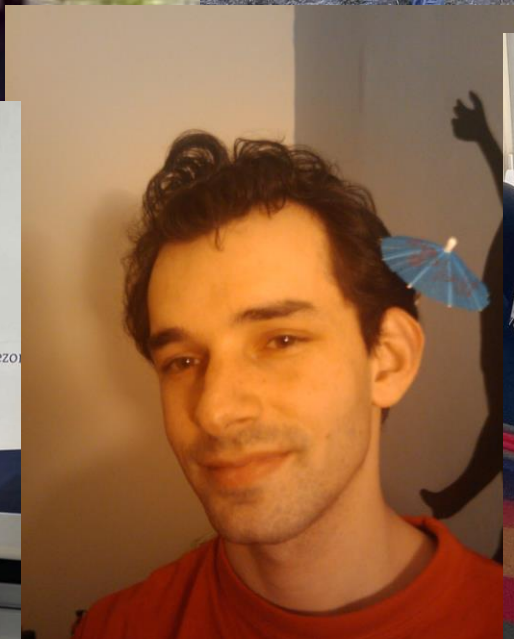







VOOR GROEPS-
IMMUNITEIT
HIER
LIKKEN



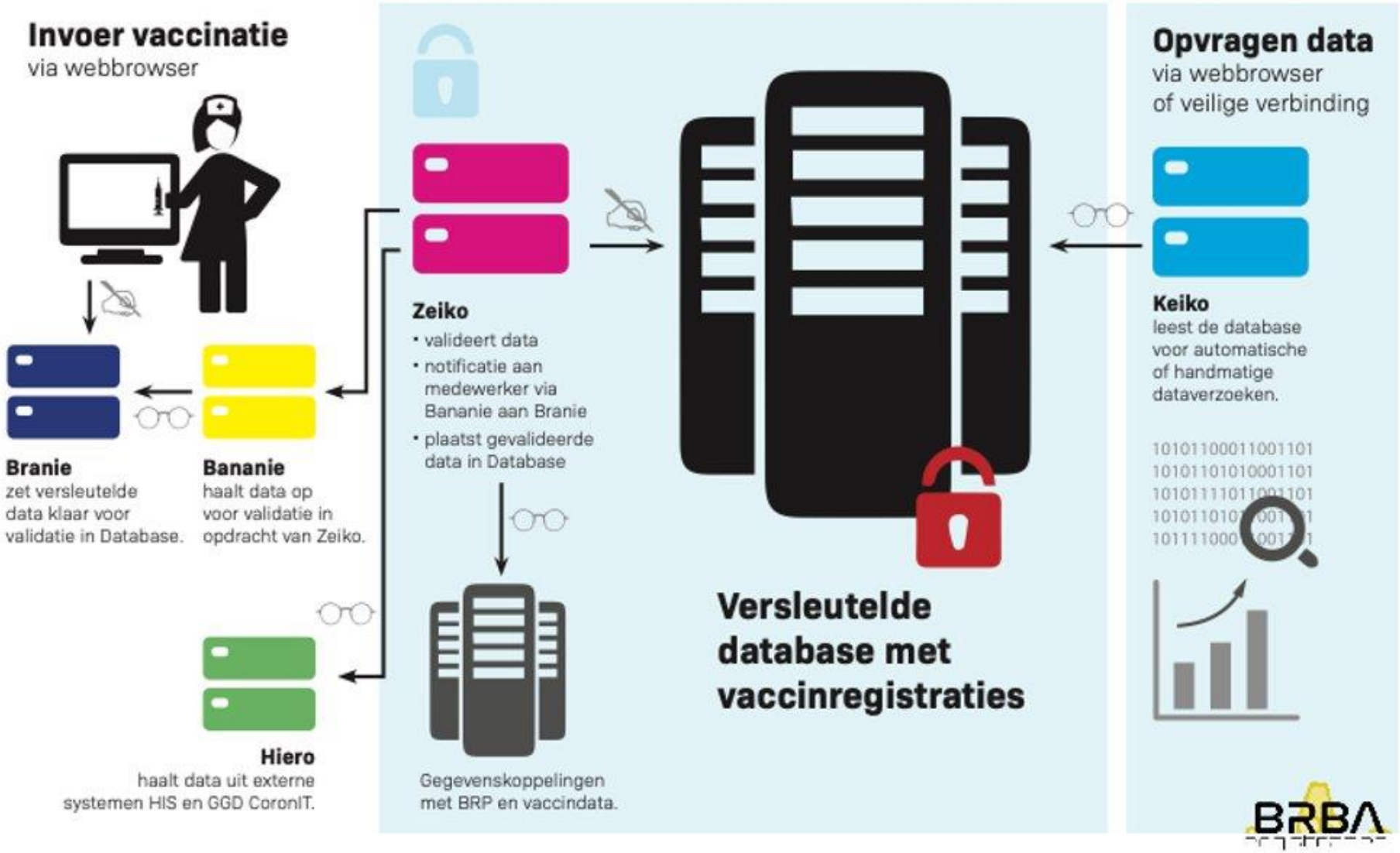

Rijksinstituut voor Volksgezo
en Milieu




ХЕРСОН

Registratie van vaccinaties met *state-of-the-art security*

Rijksoverheid



BRBA

Meer werk dan haalbaar

Veel projecten, klein team:

- EU DCC Sint Maarten
- EU DCC Aruba
- EU DCC Curaçao
- CoronaCheck – EU DCC-system Nederland
- Corona teststraten
- CoronaMelder
- GGD Contact (old school contact tracing)
- Braniebananie (BRBA) - vaccinatiedoorgeefluik
- Ondersteuning naar andere organisaties
- ZKVI – EPD voor vaccinaties
- Handmatige afgifte EU DCC
- Screen voor account toegang
- Fraude bestrijding

- Veel dreigingen:
  - Security by design
  - Privacy design
  - Incidenten
  - Wekelijkse DDoS
  - Fraude
- Diverse standaarden om je aan te houden
- Compliance bewijzen
- Politiek bewijzen dat je de juiste zaken hebt gedaan
- Monitoring
- Vulnerability scanning
- Incidenten onderzoeken
- Risk assessments (FMEA)
- Dreigingsanalyses
- Penetratie tests
- Code reviews

Oude neigingen doorbreken

- Informatiebeveiliging is een vak
  - Dezelfde vraagstukken telkens weer blijven beantwoorden
  - Iedere keer rapporten kloppen in word met vergelijkbare inhoud
  - Rapportages met hard bewijs zijn lastig te vinden
  - Vaak zijn het antwoorden op vragen, niet feiten
  - Technische feiten hebben weinig relatie met normatieve controls
- Positief
  - Er zijn veel tools beschikbaar die feiten kunnen verzamelen
  - Veel tools zijn open source
  - Data is goed te modeleren
  - Repititief werk is goed te automatiseren

Compliance is ...

Bewijzen dat je aan de kaders voldoet

Niet iemand in de ogen kijken

Wie heeft een up-to-date CMDB?

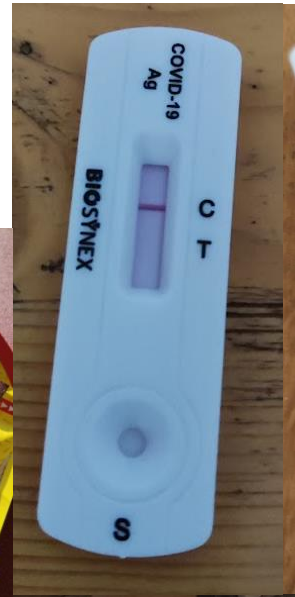
En wie loopt hier onjuistheden te verkondigen?

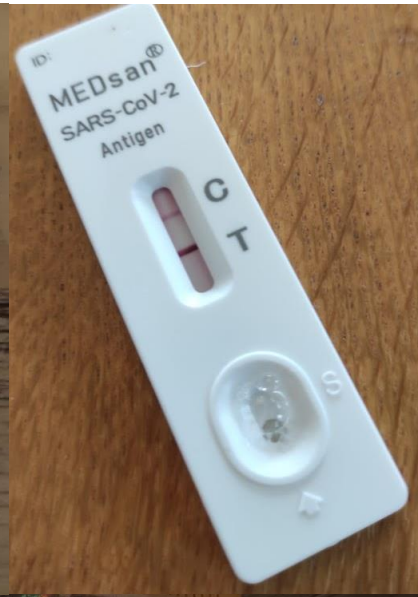
Zoek een speld in de hooiberg

Zoek Franse worstjes in een hooiberg

Zoek een sok in de hooiberg

Feiten in Octopoes ….





Sorteer objecten en plaats ze waar ze horen

- Temporal graph database
  - Objecten zijn feiten
  - Met timestamps wanneer iets voor het eerst is gezien en wanneer het werd verwerkt (gerealiseerd)

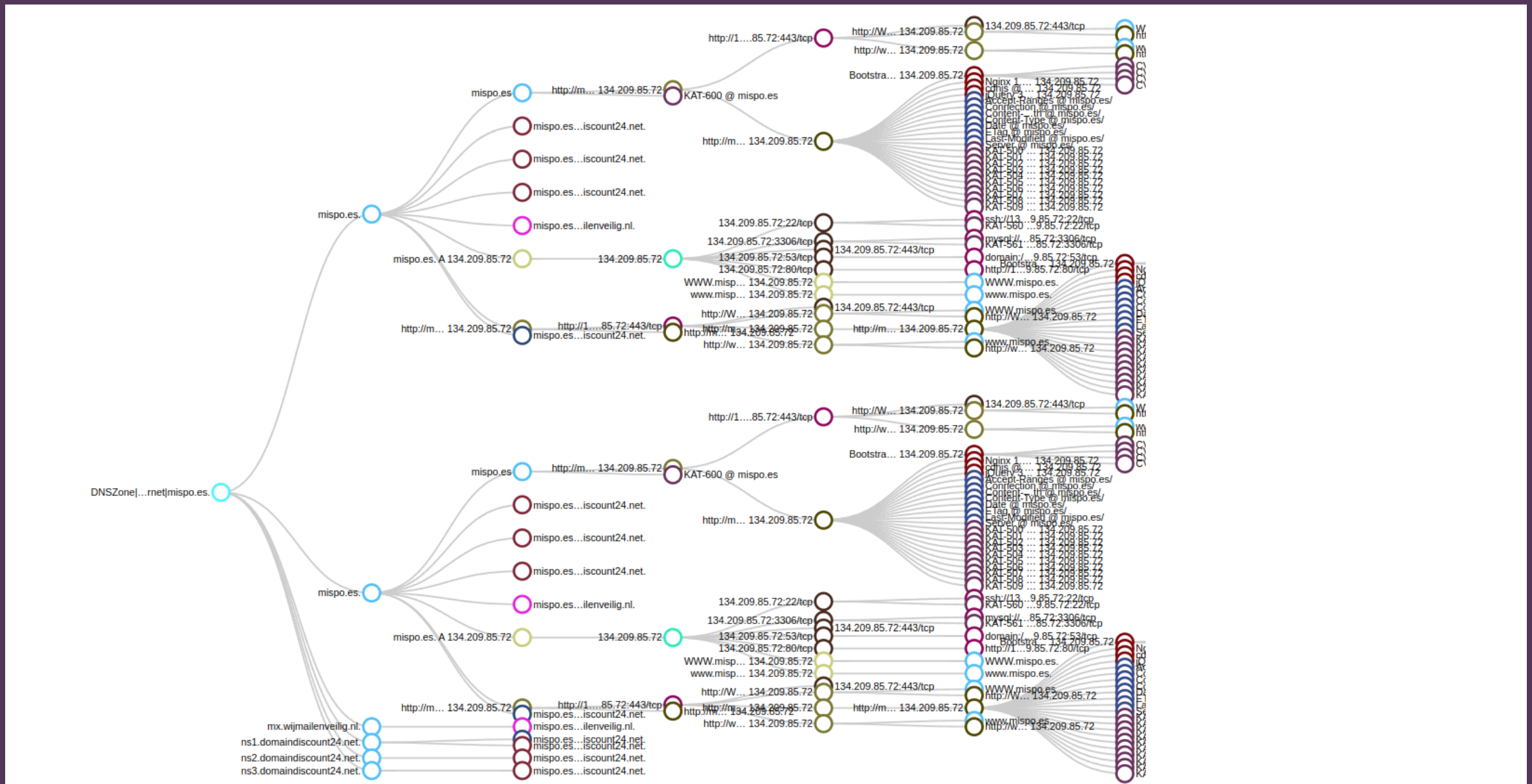
Hoe bewijs je de feiten die je claimt?

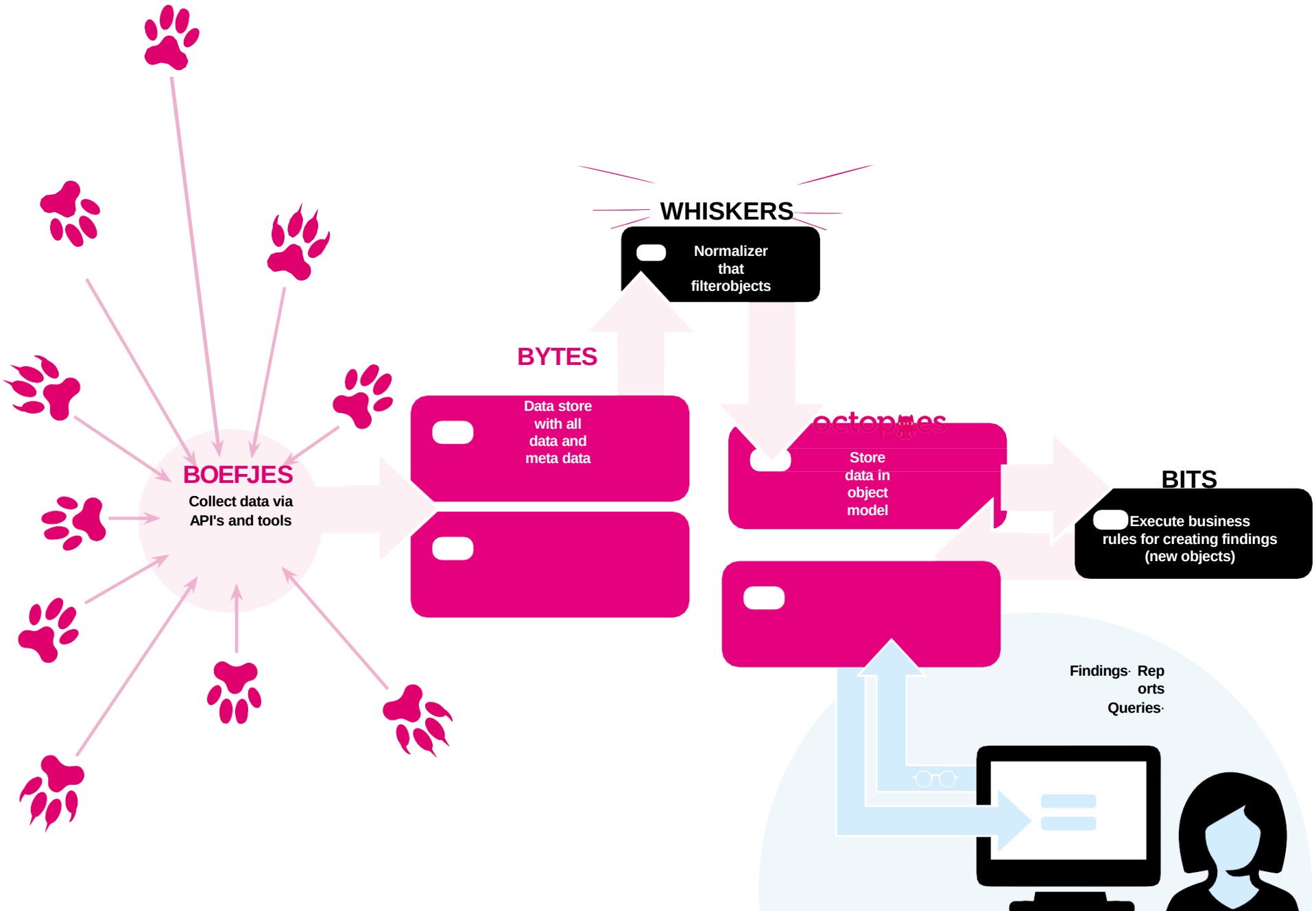
Bij iedere stap:

- Maak je onweerlegbaar bewijs
- Hashen waar het kan
- Hashes worden extern gesigned

Jezelf hoef je niet te overtuigen,

Overtuigen doe je bij iemand anders


DNSZone|…rnet|mispo.es.
mispo.es.
mispo.es
http://m… 134.209.85.72
KAT-600 @ mispo.es
http://1….85.72:443/tcp
http://W… 134.209.85.72
http://w… 134.209.85.72
134.209.85.72:443/tcp
Bootstra… 134.209.85.72
Nginx 1.… 134.209.85.72
http://m… 134.209.85.72
mispo.es…iscount24.net.
mispo.es…ilenveilig.nl.
mispo.es. A 134.209.85.72
134.209.85.72
134.209.85.72:22/tcp
134.209.85.72:3306/tcp
134.209.85.72:53/tcp
134.209.85.72:80/tcp
WWW.misp… 134.209.85.72
www.misp… 134.209.85.72
http://W… 134.209.85.72
http://w… 134.209.85.72
134.209.85.72:443/tcp
http://1….85.72:443/tcp
http://m… 134.209.85.72
mx.wijmailenveilig.nl.
ns1.domaindiscount24.net.
ns2.domaindiscount24.net.
ns3.domaindiscount24.net.


WHISKERS
Normalizer that filterobjects
BYTES
Data store with all data and meta data
BOEFJES
Collect data via API's and tools
octopuses
Store data in object model
BITS
Execute business rules for creating findings (new objects)
Findings· Rep orts
Queries·

Nmap
Scans all 65000 ports behind an IP

See details Install & scan

Nmap250
Scans the 250 most popular ports behind an IP

See details Install & scan

SecurityHeaderDetection
Scans for missing HTML headers

See details Install & scan

CheckIfWebsite
Find websites behind a hostname

See details Install & scan

Nmap
Scans all 65000 ports behind an IP

Nmap250
Scans the 250 most popular ports behind an IP

SecurityHeaderDetection
Scans for missing HTML headers

DnsRecord
Collects all DNS records of a hostname

Let's talk compliance now

Uitgangspunt

OPZET

BESTAAN

WERKING

Octopoes 3.0 (hacking in progress)

- Technische feiten
- JSON-gebaseerd model
  - Het JSON-model in de graph stoppen
  - Maakt namespacing mogelijk
  - Juist standaard op juiste moment toepassen
- Standaarden (frameworks)
  - Versie en geldig meewegen
  - Kijken naar toekomstige controls
  - Reconstrueren compliance in verleden
- Compliance toen en nu

Hoe bewijs je de feiten die je claimt?

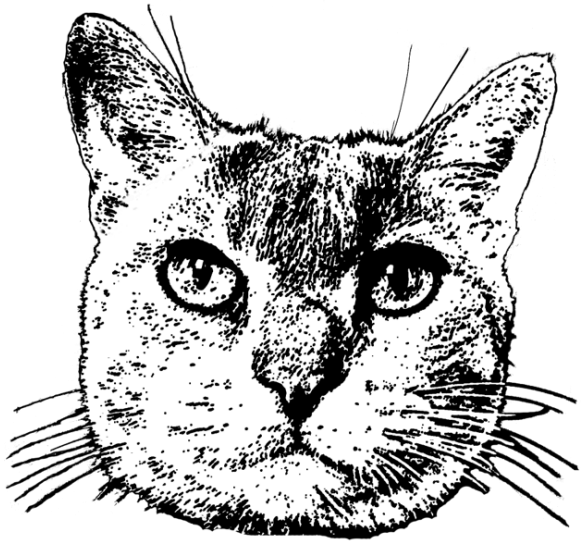
Bij iedere stap:

- Maak je onweerlegbaar bewijs
- Hashen waar het kan
- Hashes worden extern gesigned

Jezelf hoef je niet te overtuigen,

Overtuigen doe je bij iemand anders

OpenKAT is een reeks projecten



- Momenteel in OpenKAT
  - Bits – Business rule engine
  - Boefjes – API-infrastructuur
  - Bytes – Forensische documenten opslag
  - Maya – Documentatie
  - Mula - Scheduler
  - Octopoes – Temporal graph database
  - Whiskers - Normalizers
- Coming soon
  - Calvin – SIEM-tooling/Network monitoring
  - Otis – Signing tool

We are open! Doe mee!

- Openkat.nl
- Meedoen@openkat.nl

- Brenno de Winter
  - +31653536508
  - brenno@dewinter.com
  - @brenno

Vragen? Bijvoorbeeld

- Hoe ga je om met standaarden met gedeeltelijk dezelfde controls?
- Wat doe je op dit moment met AI?
- Sommige controls bestaat alleen uit documentatie. Hoe ga je daarmee om?
- Gaat Keiko wel eens op vakantie?
- Waar staat OpenKAT over 10 jaar?
- Waarom heb je een slide met comic sans?
- Wordt de auditor nu overbodig?







Continual auditing met OpenKAT

Auditor-tooling voor de moderne wereld

Over Cynalytics

Open Source Compliance

Opgericht in 2023 door auditoren en IT specialisten
(Reinoud van Leeuwen, Bas van der Linden, Leo Benschop)

Focus op inzicht in compliance:

OpenKAT is de basis,
de business rules zijn voor de klant.

Wat doet een auditor?

Auditoren verzamelen informatie, correleren en analyseren deze en rapporteren daar over. Ze vergelijken de bestaande met de gewenste situatie.

Daarmee helpen ze organisaties bij het verkrijgen van inzicht in de beheersing van de eigen processen.

Dat werkt alleen als de auditor inzicht heeft in wat er speelt.
Wat zijn de risico's? Waar gaat het mis?

Wat doet OpenKAT?

OpenKAT verzamelt, correleert, analyseert en rapporteert, op continue basis.

Op basis van vastgestelde KPI's kan OpenKAT informatie verzamelen en analyseren. De gegevens worden onweerlegbaar vastgelegd, voorzien van een tijdstempel.

Rapportages geven inzicht in de mate van beheersing: *Wordt er voldaan aan de KPI's?*

De uitdaging van de auditor

We stellen telkens hogere eisen aan de auditor:

- We hebben meer (meer devices, meer processen, meer productie)
- We willen meer en sneller (continu gedetailleerd inzicht)

We willen *nu* weten of onze processen voldoende beheerst worden, zodat we tijdig kunnen bijsturen.

De huidige manier van auditeren (sampling, evalueren, rapporteren) past telkens minder goed.

Enkele voorbeelden van deze uitdagingen

Auditoren moeten toetsen: Evidence van werkzaamheden verzamelen en beoordelen. Herhalende processen echter leveren veel werk op.

- Neem de flow van een virtuele server: Van aanvraag via oplevering tot factuur. Deze flow moet kloppen en onweerlegbaar aantoonbaar zijn.
- Neem de flow van een kwetsbaarheid in software: Van detectie via rapportage tot oplossing. Is dit pad onweerlegbaar aantoonbaar correct en op tijd afgelegd?

Auditoren en OpenKAT

Hoe maakt OpenKAT het auditeren efficiënter en effectiever?

Zoals eerder gemeld:

Op basis van vastgestelde KPI's kan OpenKAT informatie verzamelen, analyseren en rapporteren.

En niet zomaar:

- Verzamelde informatie kan niet tussentijds aangepast (juistheid)
- Het is geschikt per gewenst interval (tijdigheid)
- Kan niet worden verwijderd (volledigheid)

OpenKAT voor de auditor

OpenKAT staat de auditor toe om systeemgericht te toetsen.

Dat is nogal wat: Audits worden effectiever en efficiënter, net als de rapportage: de proceseigenaar heeft continu inzicht in de beheersing van de eigen processen, en beter inzicht in de mate van risicobeheersing.

Bijsturen wanneer nodig, niet na presentatie van tekortkomingen: het wordt een continu proces.

Waar staan we nu?

OpenKAT biedt nu de basis voor systeemgericht toetsen op technische controls:

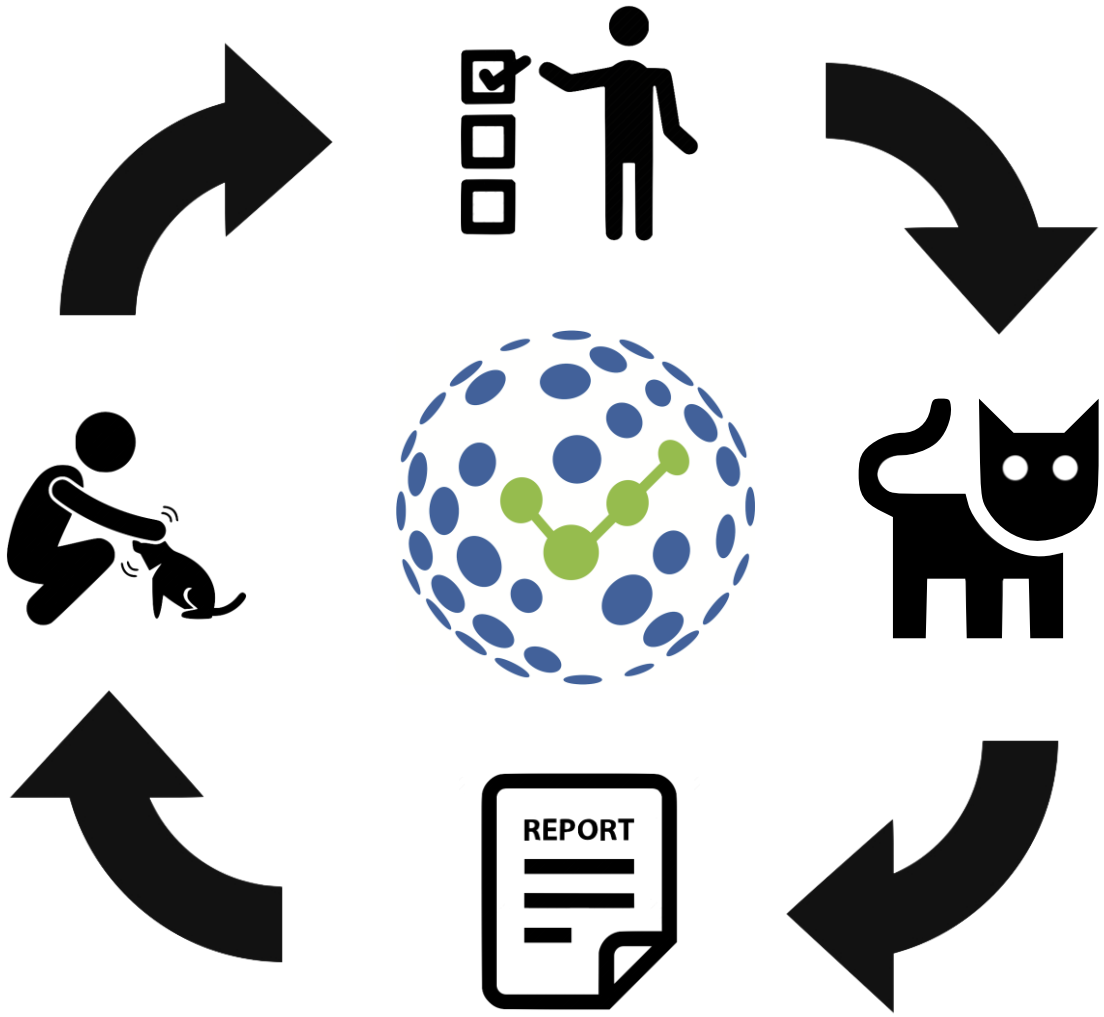
- Kwetsbaarheden, systeemwijzigingen en diverse infrastructuur-instellingen kunnen nu automatisch continu worden getoetst.
- Het waarderen van de ernst en de opvolging wordt in business rules gestopt.
- Daar komen rapportages uit.

De volgende stappen?

- Auditeren as a Service?
- Meer boefjes: niet alleen technisch, meer integratie met bedrijfsprocessen
- Continu inzicht met OpenKAT, slimme business rules en duidelijke stuurinformatie gericht op de risico's van het bedrijfsproces
- De Deming Circle sluitend maken (bijvoorbeeld middels KPI's op basis van MMA)

Waar hebben jullie behoefte aan?

Onze visie



Deming 2.0:

Stap 1: Bepaal KPI’s

Stap 2: Activeer KAT

Stap 3: Krijg rapport

Stap 4: ~~Profit~~ Aai KAT

Ten slotte

Vragen?

Bedankt

Succes met uw Security Governance Inrichting.

PvIB Platform voor InformatieBeveiliging