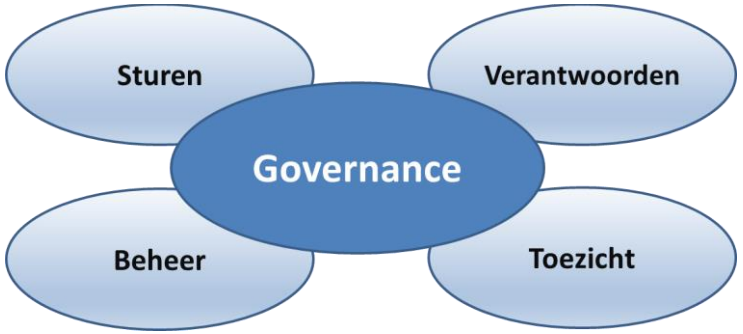
Activiteiten governance



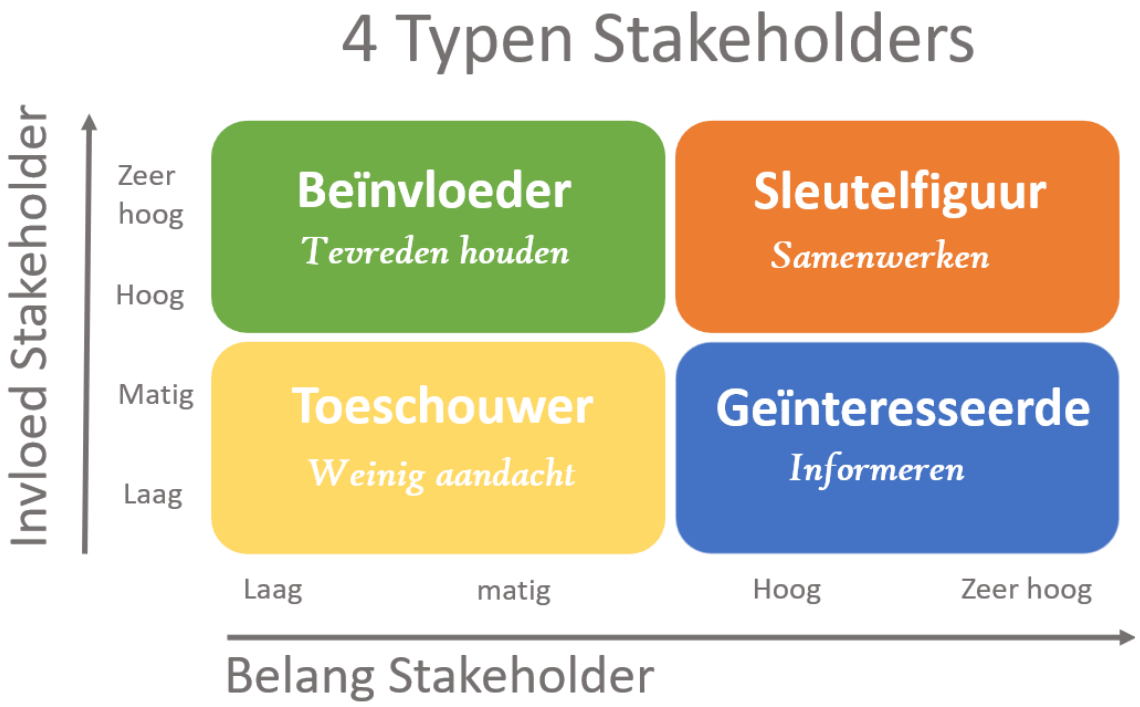
Sectie van BIO 2019

Gebaseerd op de ISO/IEC 27002:2013 RASCI matrix

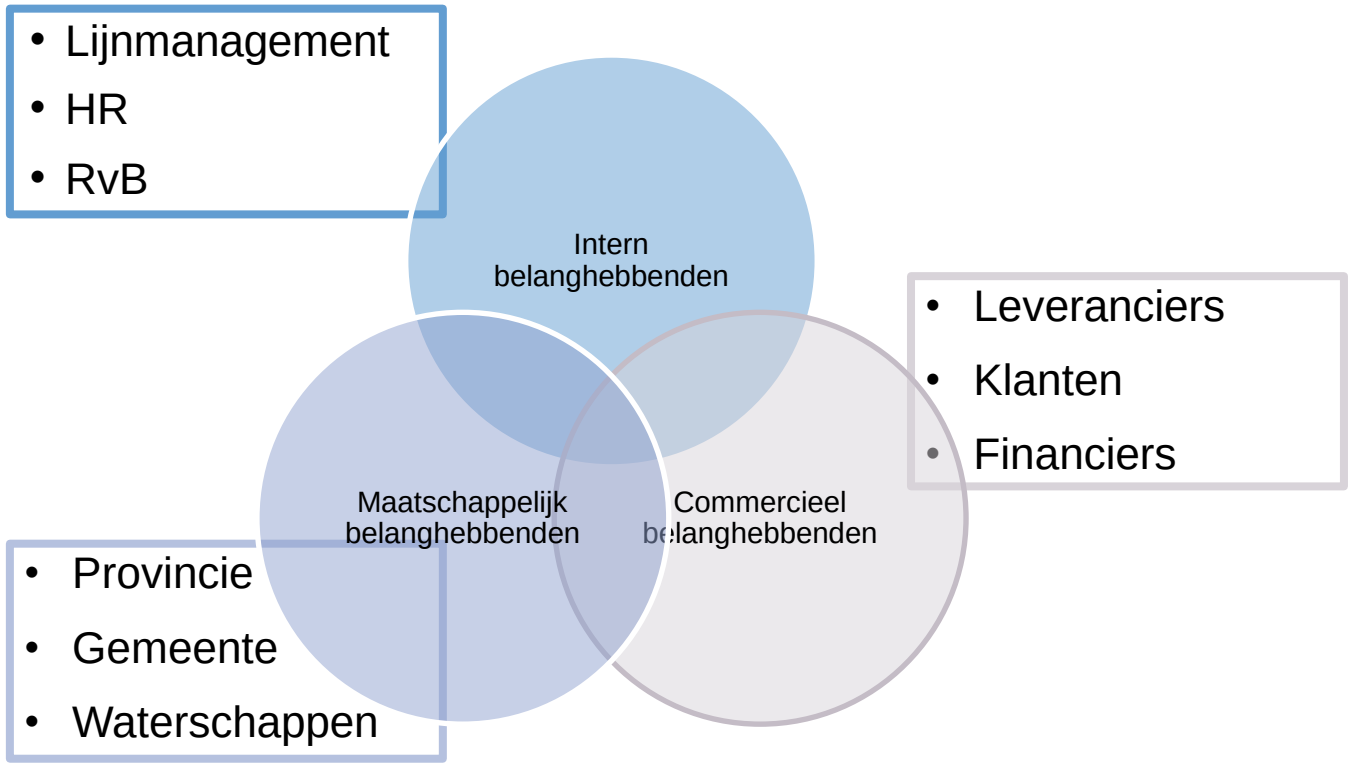
R = Responsible
A = Accountable
S = Supportive
C = Consulted
I = Informed

		Informatie / systeem eigenaren	Personeel	Directeur	MT	CISO	Lijnmanager 1
05	**Informatiebeveiligingsbeleid**						
05.1.1	Beleidsregels voor informatiebeveiliging	C	I	A	C	R	
05.1.2	Beoordeling van het informatiebeveiligingsbeleid	C		A	S	S	
06	**Organiseren van informatiebeveiliging**						
06.1.1	Rollen en verantwoordelijkheden bij informatiebeveiliging	A	I		R	C	
06.1.2	Scheiding van taken	A	I		C	C	
06.1.3	Contact met overheidsinstanties	A			C	S	
06.1.5	Informatiebeveiliging in projectbeheer	A			C	S	
06.2.1	Beleid voor mobiele apparatuur	A	I		C	S	
06.2.2	Telewerken	A	I		R	C	

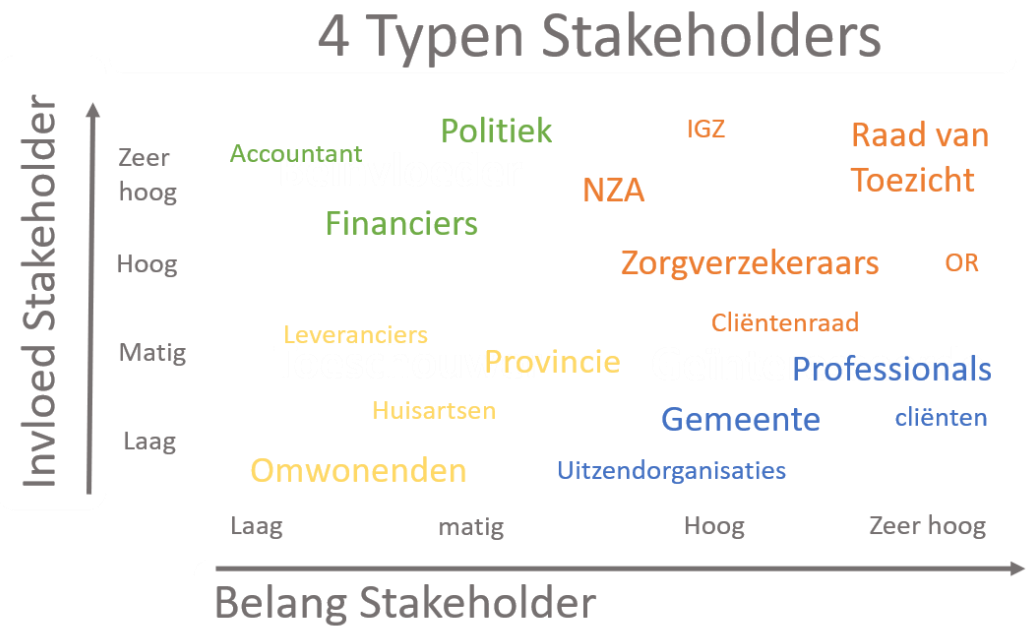
Typen stakeholders



Stap 1: Identificeren van stakeholders



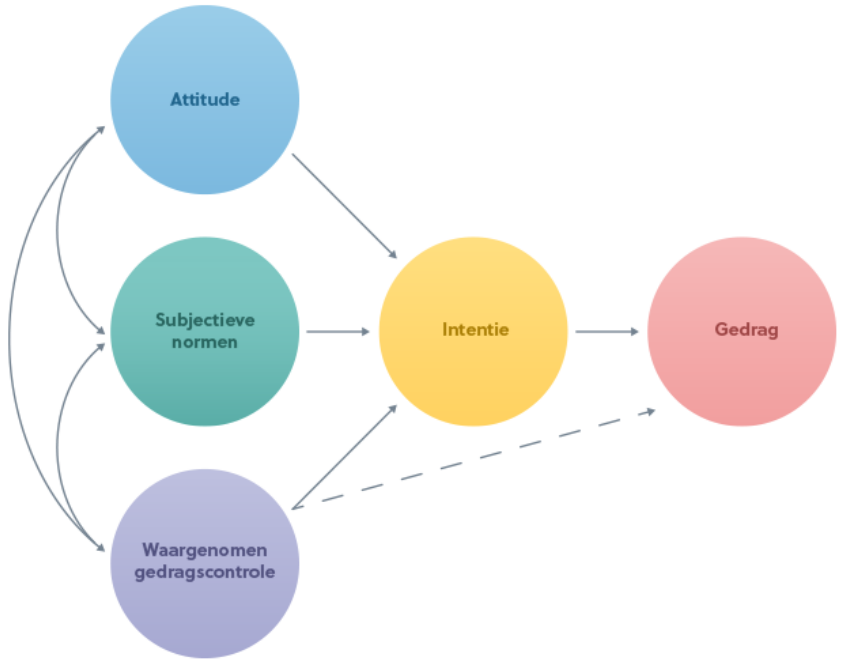
Stap 2: Typeren van stakeholders

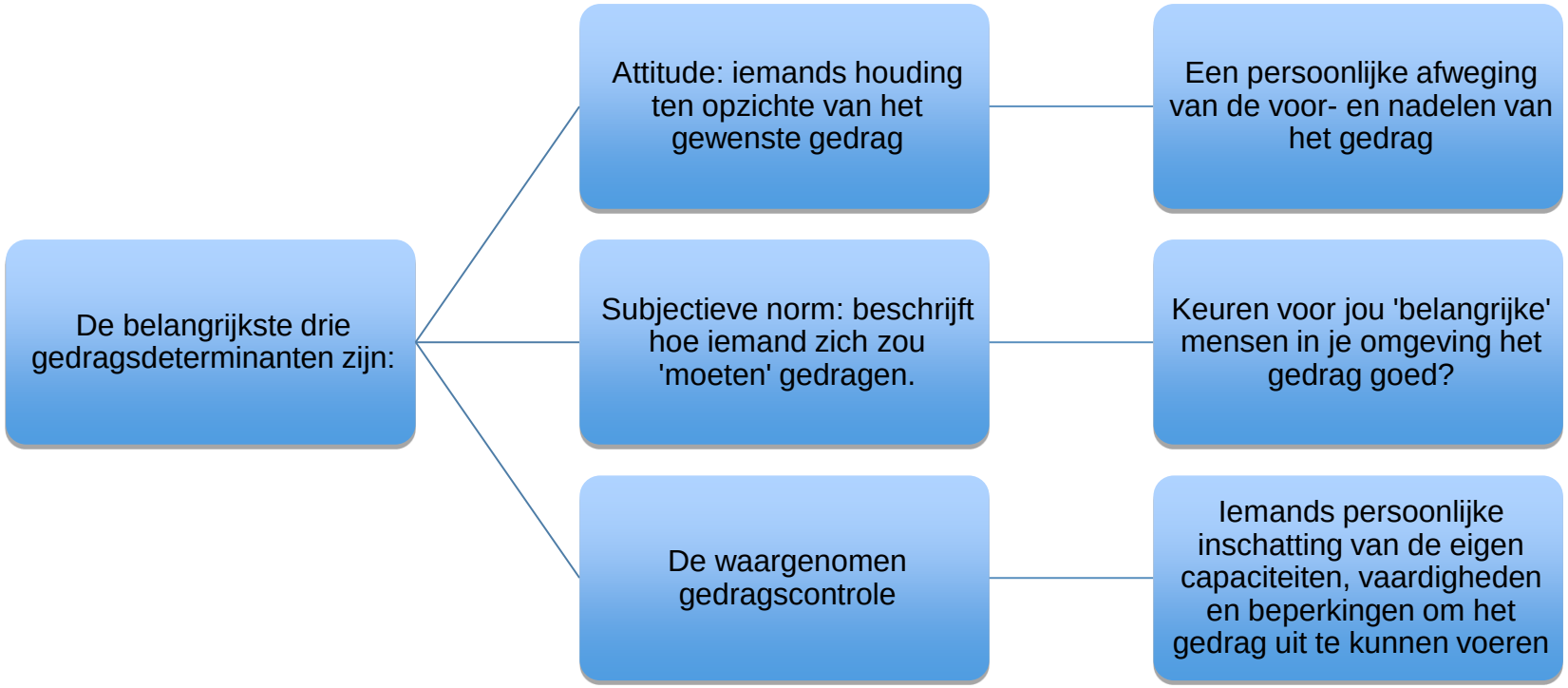


Voorbeeld zorgorganisatie

Stap 3: Stakeholder- Strategieën bepalen

1. Beïnvloeder → Tevreden houden
2. Sleutelfiguur → Samenwerken
3. Toeschouwer → Weinig aandacht
4. Geïnteresseerde → Informeren


Attitude
Subjectieve normen
Waargenomen gedragscontrole
Intentie
Gedrag


De belangrijkste drie gedragsdeterminanten zijn:
Attitude: iemands houding ten opzichte van het gewenste gedrag
Een persoonlijke afweging van de voor- en nadelen van het gedrag
Subjectieve norm: beschrijft hoe iemand zich zou 'moeten' gedragen.
Keuren voor jou 'belangrijke' mensen in je omgeving het gedrag goed?
De waargenomen gedragscontrole
Iemands persoonlijke inschatting van de eigen capaciteiten, vaardigheden en beperkingen om het gedrag uit te kunnen voeren

- Attitude is de meest bepalende gedragsdeterminant (onderzoek Radboud Universiteit)
- Alle drie de determinanten leiden tot de intentie om het gedrag te vertonen
- De waargenomen gedragscontrole (kan ik dit?) zet de intentie om in daadwerkelijk gedrag
- Ook belangrijk, zeg maar randvoorwaardelijk, is dat iemand de benodigde kennis en vaardigheden in huis heeft om het gedrag uit te kunnen voeren

Voorbeelden van maatregelen

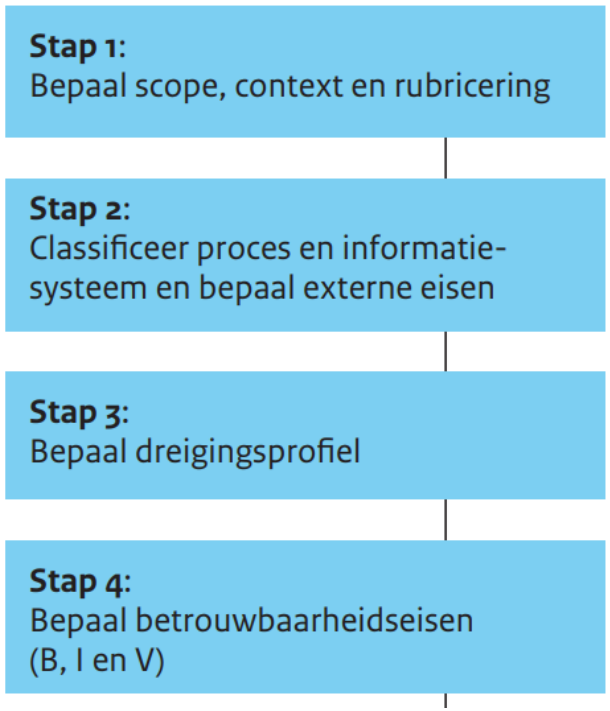
	Organisatorisch	Technisch	Fysiek
Sturend	IB-beleid	Baseline	Verkeerslichten
Afschrikkend	Sanctiebeleid	Juridische voorwaarden	“Pas op voor de hond”
Preventief	Gebruikersregistratie	Authenticatie	Hek
Detectie	Lograpport toegang	IDS, Log monitoring	CCTV
Correctie	Sanctie	Isoleren	Brandblusser
Herstel	Business Continuity plan	Restore van Backup	Restauratie kantoor
Compenserend	Supervisie, logging	Key logger	Verdediging in de diepte

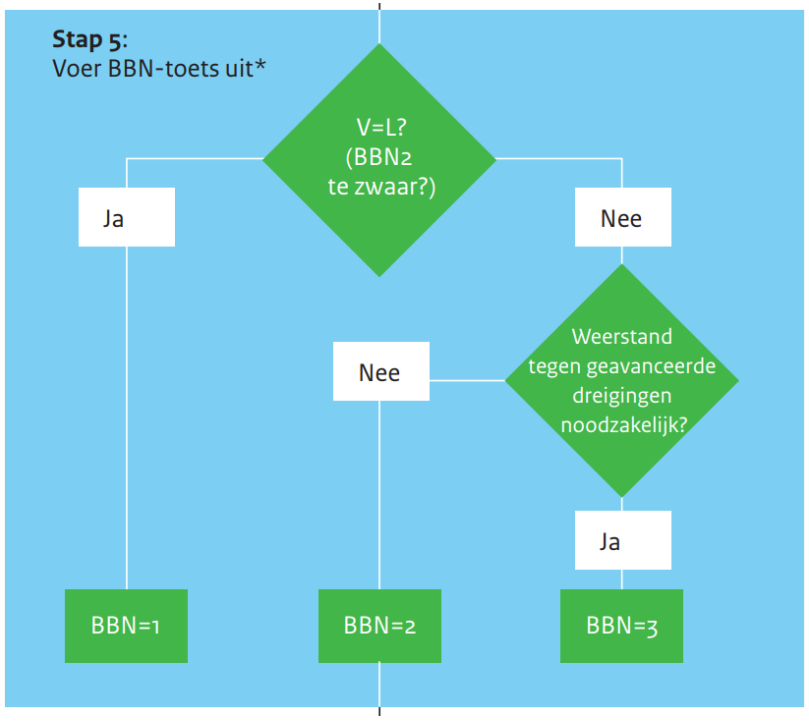
Criteria bij de selectie van maatregelen (1v2)

Is het economisch zinnig?	Kosten/baten van risico en maatregelen
Is het organisatorisch haalbaar?	Hoeveel invloed heeft het op het proces?
Is het commercieel haalbaar?	Draagt het bij aan de bedrijfsvoering?
Is het juridisch verstandig?	Hoe verhoudt het risico of de maatregel zich tot wet- en regelgeving?

Criteria bij de selectie van maatregelen (2v2)

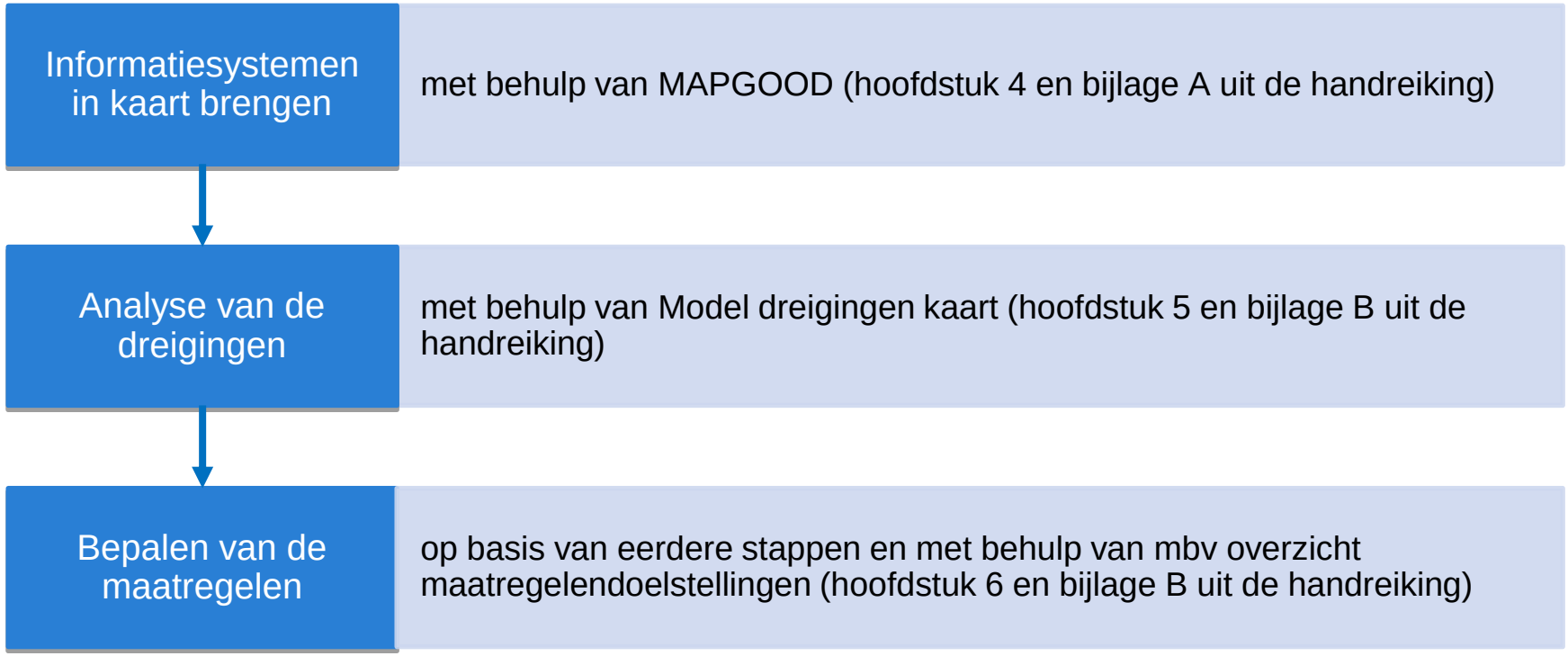
Is er politiek en/of sociaal draagvlak?	Hoe staan management, medewerkers en omgeving er tegenover?
Is het technisch haalbaar?	Wat is er mogelijk? Welke kennis is voorhanden?
Hoe effectief is de maatregel?	Hoeveel restrisico blijft er over? Hoe ga ik straks aantonen dat het resultaat daadwerkelijk aan de behoefte tegemoet komt?


Stap 1:
Bepaal scope, context en rubricering
Stap 2:
Classificeer proces en informatie-systeem en bepaal externe eisen
Stap 3:
Bepaal dreigingsprofiel
Stap 4:
Bepaal betrouwbaarheidseisen (B, I en V)


Stap 5:
Voer BBN-toets uit*
V=L?
(BBN2
te zwaar?)
Ja
Nee
Weerstand
tegen geavanceerde
dreigingen
noodzakelijk?
Nee
Ja
BBN=1
BBN=2
BBN=3

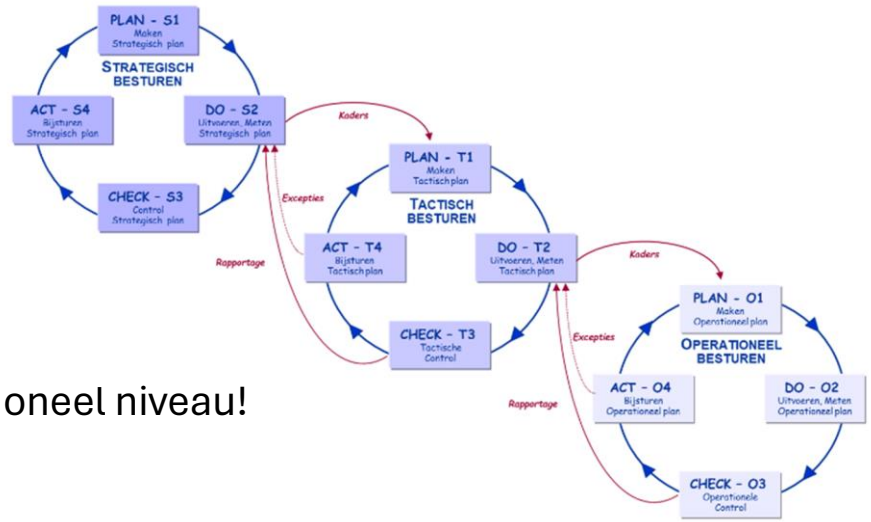
	Stap 1 Informatiesysteem in kaart brengen	Stap 2: Analyse dreigingen	Stap 3: Bepalen maatregeldoelstellingen
Voorbereiding	Analist 4 uur Systeemeigenaar 20 minuten	Analist 6 uur	Analist 10 – 12 uur
Interview / Sessie	Analist 4 uur Systeemeigenaar 4 uur (eventueel technisch en functioneel beheer erbij)	Analist 4 uur Systeemeigenaar 4 uur	Analist 2 uur Systeemeigenaar 2 uur
Uitwerking	Analist 4 uur	Analist 8 uur	Analist 14 uur
Voorbereiding	Analist 4 uur Systeemeigenaar 20 minuten	Analist 6 uur	Analist 10 tot 12 uur

Stappen


Informatiesystemen in kaart brengen
met behulp van MAPGOOD (hoofdstuk 4 en bijlage A uit de handreiking)
Analyse van de dreigingen
met behulp van Model dreigingen kaart (hoofdstuk 5 en bijlage B uit de handreiking)
Bepalen van de maatregelen
op basis van eerdere stappen en met behulp van mbv overzicht maatregelendoelstellingen (hoofdstuk 6 en bijlage B uit de handreiking)

Stel je eerst een aantal vragen:

- Wat wil ik bereiken?
- Hoe meet ik of ik het bereikt heb?
- Hoe ga ik om met afwijkingen?
- Wat en wie heb ik daar bij nodig?



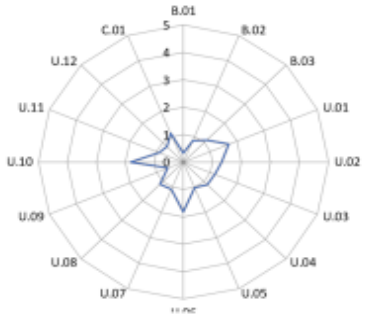
Stel die vragen op strategisch, tactisch en operationeel niveau!

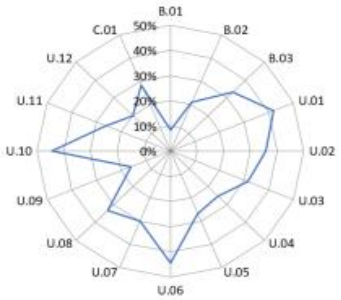
En leg de verbinding tussen die drie niveaus

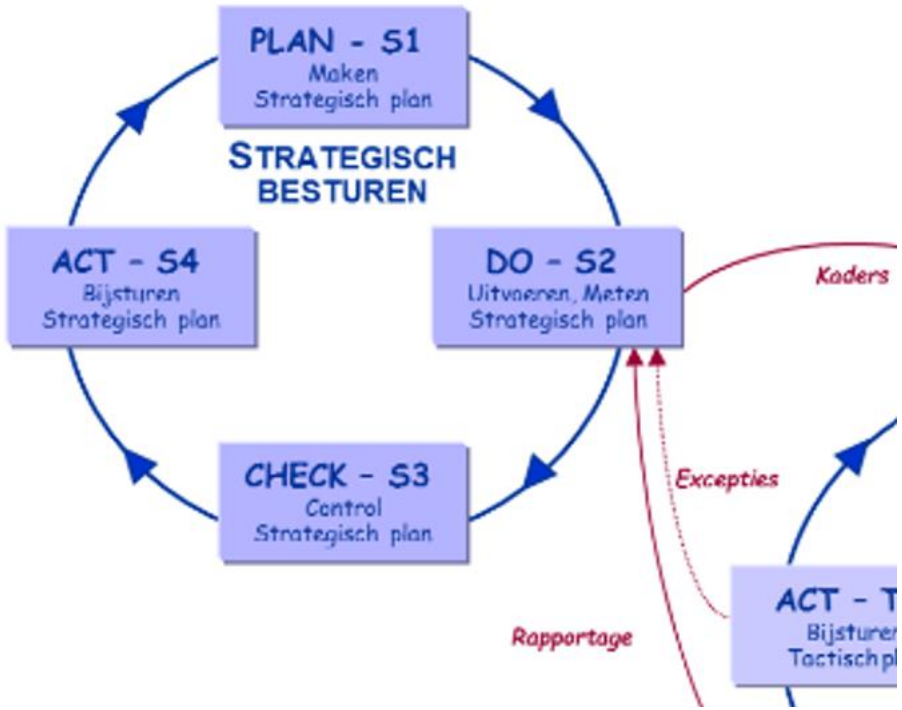
Dat zijn de interfaces die je in beeld moet krijgen

Om uiteindelijk een plan van aanpak te kunnen maken

Maatregelen implementeren strategisch niveau

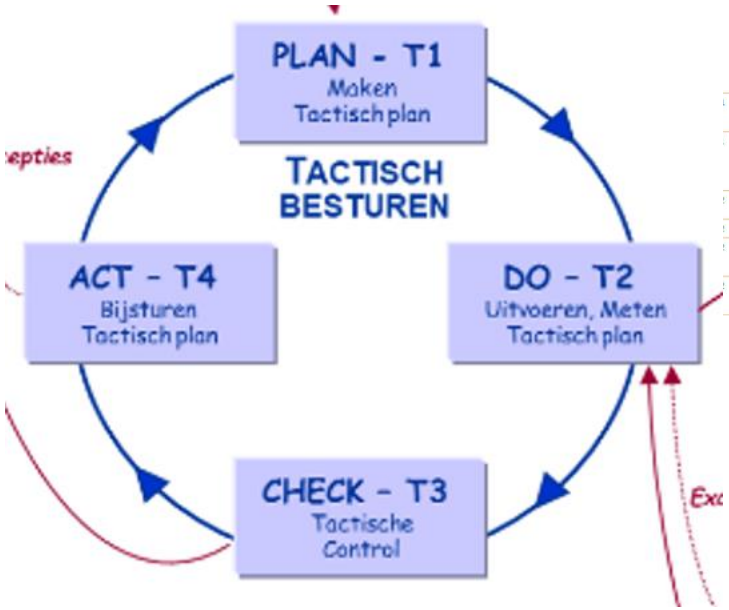






BIO Versie 1

Maatregelen implementeren tactisch niveau



BIO Versie 1

Systeem voor wachtwoordbeheer Systemen voor wachtwoordbeheer behoren interactief te zijn en sterke wachtwoorden te waarborgen.	Dienstenleverancier
Als er geen gebruik wordt gemaakt van two-factor authenticatie, is de wachtwoordlengte minimaal 8 posities en complex van samenstelling. Vanaf een wachtwoordlengte van 20 posities vervalt de complexiteitseis. Het aantal foutieve inlogpogingen is maximaal 10. De tijdsduur dat een account wordt geblokkeerd na overschrijding van het aantal keer foutief inloggen, is vastgelegd.	
In situaties waar geen two-factor authenticatie mogelijk is, wordt minimaal halfjaarlijks het wachtwoord vernieuwd (zie ook 9.4.2.1).	
De eisen aan wachtwoorden moeten geautomatiseerd worden afgedwongen.	
Initiële wachtwoorden en wachtwoorden die gereset zijn, hebben een maximale geldigheidsduur van een werkdag en moeten bij het eerste gebruik worden gewijzigd.	
Wachtwoorden die voldoen aan het wachtwoordbeleid, hebben een maximale geldigheidsduur van een jaar. Daar waar het beleid niet toepasbaar is, geldt een maximale geldigheidsduur van zes maanden.	

Security Information & Event Management