



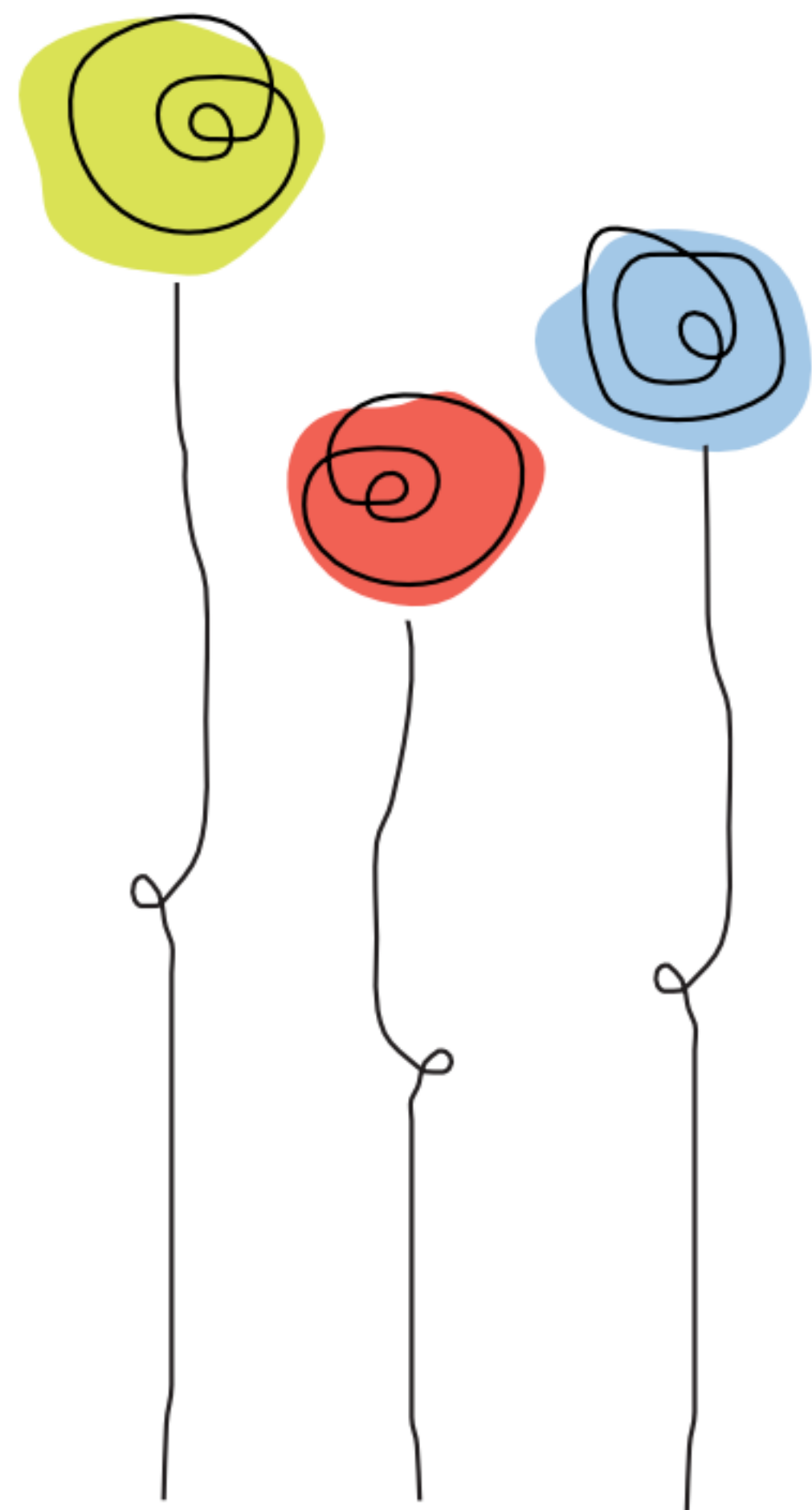
Thinking Security Works

Richard Kranendonk

`richard@thinkingsecurity.works`

`https://www.thinkingsecurity.works`

22 april 2024



human*kind*
KINDEROPVANG EN -ONTWIKKELING

Voorstel Duurzame Informatieveiligheid

22 april 2024

Inhoud

A. Uitgangspunten

1. Onze Visie
2. Onze Rol
3. Situatie Humankind
 - Technische beveiliging
 - Mens en organisatie
 - Uitdagingen voor Humankind

B. Plan van Aanpak

- I. Randvoorwaarden scheppen
- II. Structuur aanbrengen
- III. Capaciteiten ontwikkelen
- IV. Borging

C. Planning en investering

Onze Visie

De Menselijke Maat

Menselijke creativiteit en autonomie zijn essentieel voor het functioneren van een organisatie

Beveiligingsmaatregelen moeten werkbaar zijn

Veiligheid is een zaak van *alle* medewerkers, niet alleen van IT & FG

Met vrijheid komt verantwoordelijkheid

Veiligheid is een proces van voortdurende verbetering

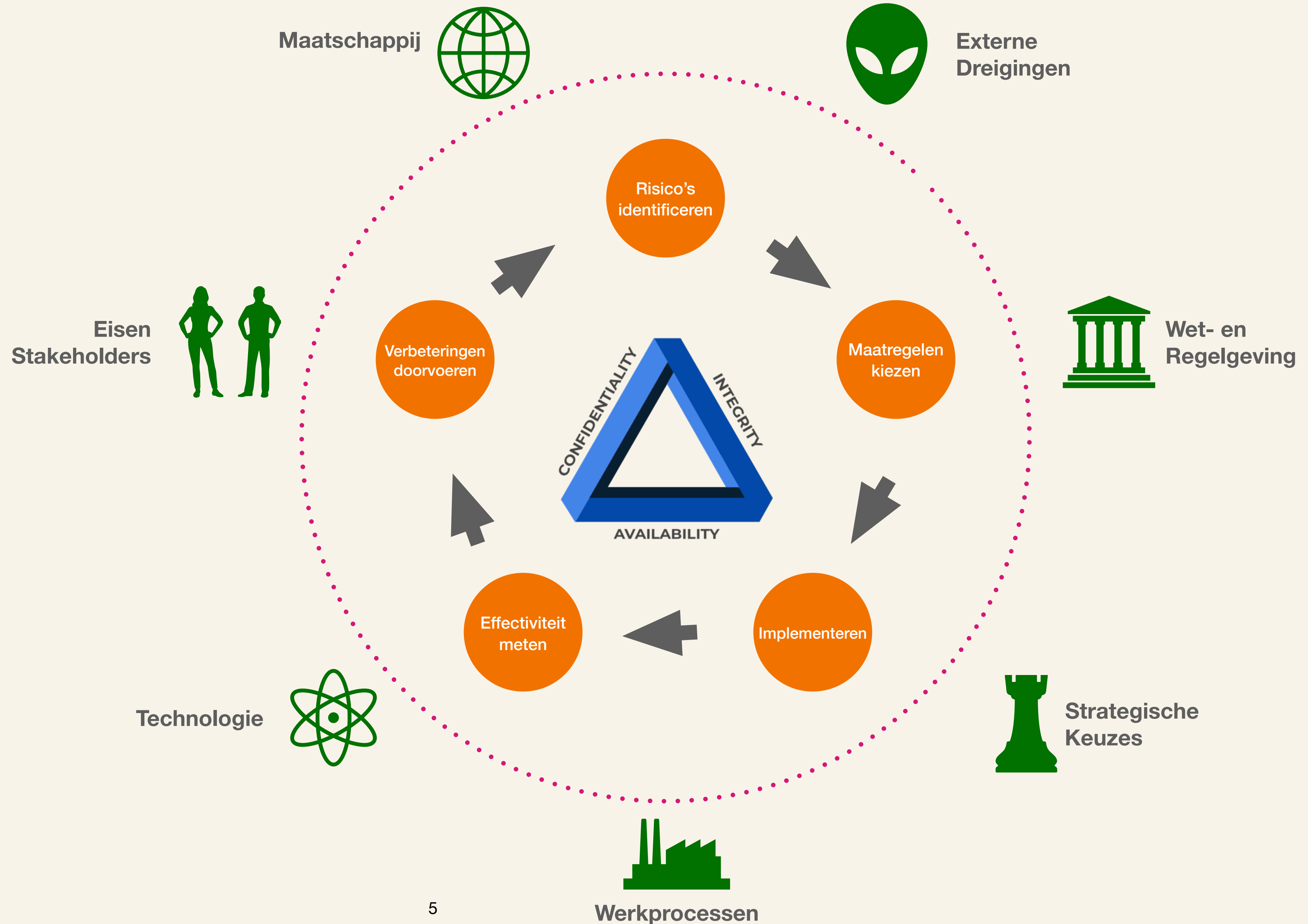
Dat proces heeft goede sturing nodig



Veiligheid is een proces

van continue
verbetering

in een voortdurend
veranderende
omgeving



Onze Rol

- Onafhankelijk adviseur
- Procesbegeleider
- Regievoerder



Stock Photo – onze adviseurs zijn echte mensen.

Situatie Humankind

o.b.v. verstrekte informatie april 2024

Technische Beveiliging

Uitbesteed aan Ilionx

- Humankind is in de basis tevreden over de dienstverlening van Ilionx
- Er is ruimte voor verbetering t.a.v. het pro-actief omgaan met kwetsbaarheden en incidenten
- De SLA's zijn 'dun' en er wordt niet op gestuurd
- De kwaliteit van de technische beveiliging tegen externe dreigingen kan o.b.v. de verstrekte informatie niet afdoende worden vastgesteld

De Menselijke Factor

Omdat 80% van de incidenten is te herleiden naar menselijk handelen

- Er is weinig aandacht voor de menselijke kant van informatieveiligheid: bewustzijn en handelen
- Er is geen proces voor risicomanagement en continue verbetering
- Er is geen informatieveiligheidsbeleid en geen meerjarenplan
- Er is onvoldoende sturing op informatieveiligheid

Uitdagingen voor Humankind

- Opstellen passend beleid en meerjarenplan
- Nemen van werkbare maatregelen o.b.v. actuele en specifieke risico's
- Managen van de leverancier(s)
- Verzekeren actieve betrokkenheid van de organisatie
- Inrichten van de besturing t.a.v. informatieveiligheid

Plan van Aanpak

Voorstel

Fasering

- I. Scheppen Randvoorwaarden
- II. Aanbrengen Structuur
- III. Ontwikkelen Capaciteiten
- IV. Blijvend Sturen op Verbetering

Fase I – Randvoorwaarden scheppen

Check op Basisveiligheid door Onafhankelijke Partij

- Bescherming tegen actuele externe dreigingen
- Verzekering beschikbaarheid:
 - Backups en noodvoorzieningen
 - Calamiteitenplan (o.a. Ransomware)

Fase I – Randvoorwaarden scheppen

Bewustzijn en Buy-in van management

Workshop Sturen op Risico's

- Belang van sturen op verbetering
- Bewustwording van risico's binnen de eigen management scope
- Inzicht in, en sturing op veiligheid en procesvolwassenheid
- Nemen van een actieve verantwoordelijkheid

Fase I – Randvoorwaarden scheppen

Leidende principes en doelen vaststellen

... passend bij de missie, cultuur,
structuur en risicotolerantie van de
organisatie

Fase II – Structuur aanbrengen

- Sturing op informatieveiligheid: eigenaarschap risico's en maatregelen, rolverdeling, managementproces
- Beleid op hoofdlijnen
- Meerjarenplan
- Risico analyse
- Fit/gap analyse t.o.v. referentie-framework
- Implementatieplan maatregelen

Fase III – Capaciteiten ontwikkelen

Wanneer ze nodig zijn, o.b.v. het implementatieplan

- Risicomanagement
- Incident Response
- Leveranciersmanagement
- Sturing op informatieveiligheid
- Helderheid voor toezichthouders

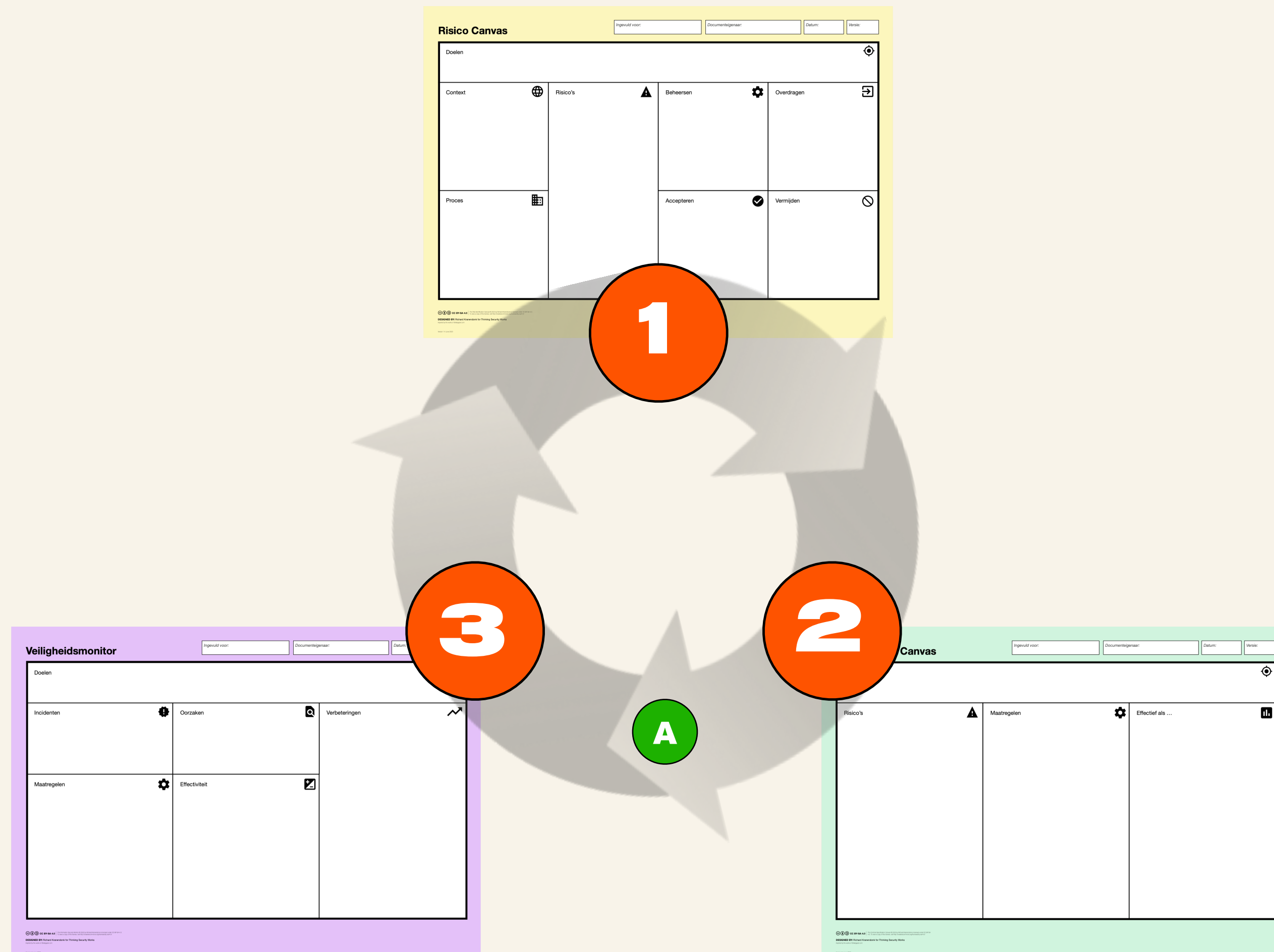
Fase IV – Borging

Blijvend verbeteren

- CISO-as-a-Service:
 - Casus-gerichte advisering aan, en in opdracht van, de informatiemanager (o.a. toepassing van maatregelen en wijzigingen in systeemlandschap)
 - Monitoren van en rapporteren over dienstverlening security (o.a. Ilionx)
 - Actieve advisering m.b.t. relevante ontwikkelingen in de buitenwereld
- Sturing op informatieveiligheid integreren in het managementsysteem van Humankind
- Implementatie PDCA cyclus voor continue verbetering o.b.v. de Canvas Methode voor Informatieveiligheid – sturing op bewustzijn en gedrag

Toelichting Canvas Methode voor Informatieveiligheid

Continue verbetering in een cyclus van drie workshops



1 Workshop Risico's

- ✓ Breng omgeving en proces in kaart
- ✓ Identificeer de Risico's
- ✓ Bepaal Eigenaarschap

2 Workshop Maatregelen

- ✓ Selecteer Maatregelen
- ✓ Definieer Succes

A Afstemmingsoverleg

- ✓ Risico's en maatregelen bespreken met IT manager en CISO
- ✓ Vaststellen maatregelen en actiehouders

2 Workshop Effectiviteit

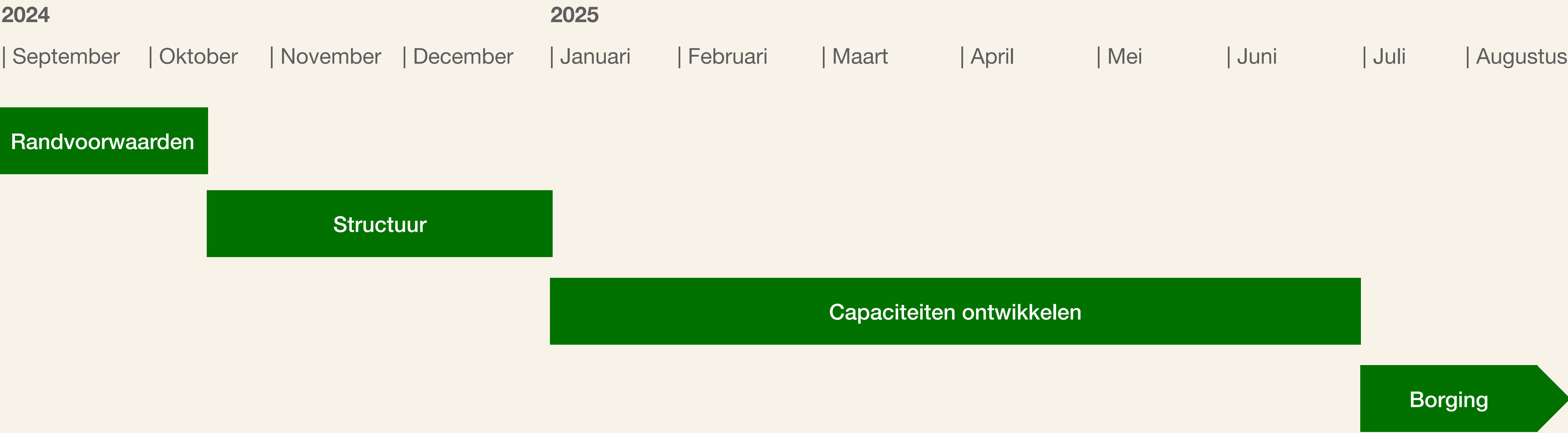
- ✓ Bespreek Incidenten
- ✓ Rapporteer over Effectiviteit
- ✓ Identificeer Verbeteringen

Planning en investering

Voorstel

Planning

Voorstel



Investering

Deliverables per Fase	Dagen	Tarief	Investering
Fase I. Randvoorwaarden			
Check op Basisveiligheid onafhankelijke partij		Stelpost	€ 15,000
Workshop Sturen op Risico's voor Management			€ 1,200
Vaststellen Leidende principes en doelen	1	€ 1,100	€ 1,100
<i>Totaal (ex. Stelpost)</i>			€ 17,300
Fase II. Structuur			
Besturingsmodel	1	€ 1,100	€ 1,100
Informatieveiligheidsbeleid	3	€ 1,100	€ 3,300
Meerjarenplan	1	€ 1,100	€ 1,100
Risico identificatie	3	€ 1,100	€ 3,300
Fit/Gap analyse	2	€ 1,100	€ 2,200
Implementatieplan maatregelen	3	€ 1,100	€ 3,300
<i>Totaal</i>			€ 14,300

Deliverables per Fase	Dagen	Tarief	Investering
Fase III. Capaciteiten	Inschatting – calculatie o.b.v. implementatieplan		
Risicomanagement	4	€ 1,100	€ 4,400
Incident Response plan	3	€ 1,100	€ 3,300
Leveranciersmanagement	3	€ 1,100	€ 3,300
Sturing op informatieveiligheid	4	€ 1,100	€ 4,400
Helderheid voor toezichthouders	1	€ 1,100	€ 1,100
<i>Totaal</i>			€ 16,500
Fase IV. Borging			
CISO-as-a-Service (inschatting per maand, facturatie o.b.v. geleverde inspanning)	4	€ 1,100	€ 4,400
Facilitering Workshops Canvas Methode	Per cyclus per team		€ 3,000
Alternatief: Train-the-Trainer	5 dagen classroom training		€ 12,000