# Programma Effectieve IV Keten Forensisch Onderzoek

“vertrouwen in de keten”

# Wat komt aan bod

- **Context voor de aanpak**
- **De controls in scope**
- **De keuze voor de MMA, transparantie als basis voor vertrouwen**
- **Uitvoering**

# DE CONTEXT

# Effectieve IV Forensisch Onderzoek: Context

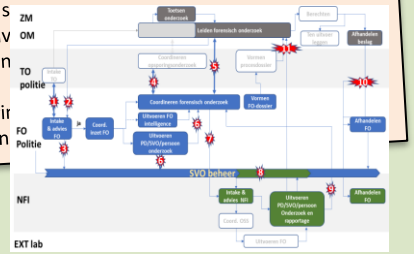


**KETENWENS 1a**

**Als** OM en FO politie **wil ik** bij een opsporingsonderzoek een actueel digitaal gemeenschappelijk forensisch beeld (single point of truth) kunnen raadplegen, waaronder:

1. Alle verrichtte en lopende forensische onderzoeksactiviteiten i.c.m. bijbehorende bevindingen en resultaten;
2. Beschikbare sporendragers en sporen i.c.m. bijbehorende (beslag)status en locatie;
3. Relevante mediabestanden waaronder foto- en video opnames van plaatsen delict of SVO's
4. Relevante onderzoek adv
5. Betrokken contactperson NFI en OM

**teneinde** gezamenlijk sturin onderzoek bij dat opsporin




**November 2018 Visie**

**Januari 2019 Programma**

**December 2019 Onderzoek**

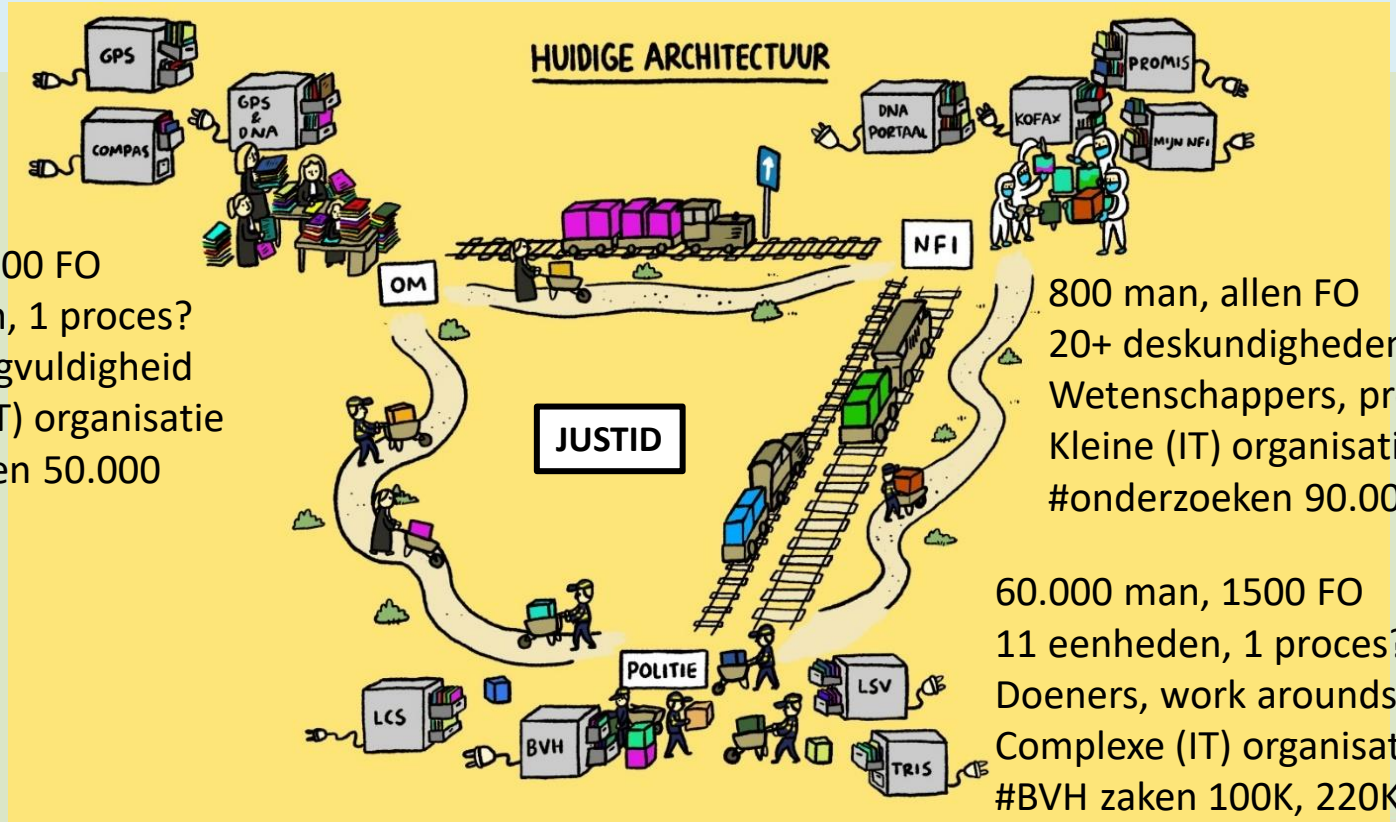
**2020/2021 Analyse (1-4) en Randvoorwaarden**

**2022/nu Bouw Fase Realisatie**

POLITIE | Nederlands Forensisch Instituut, Ministerie van Justitie en Veiligheid | OM

Effectieve IV Keten Forensisch Onderzoek

# De ketenpartijen (culturen)




5500 man, 100 FO
11 parketten, 1 proces?
Juristen, zorgvuldigheid
Complexe (IT) organisatie
#onderzoeken 50.000

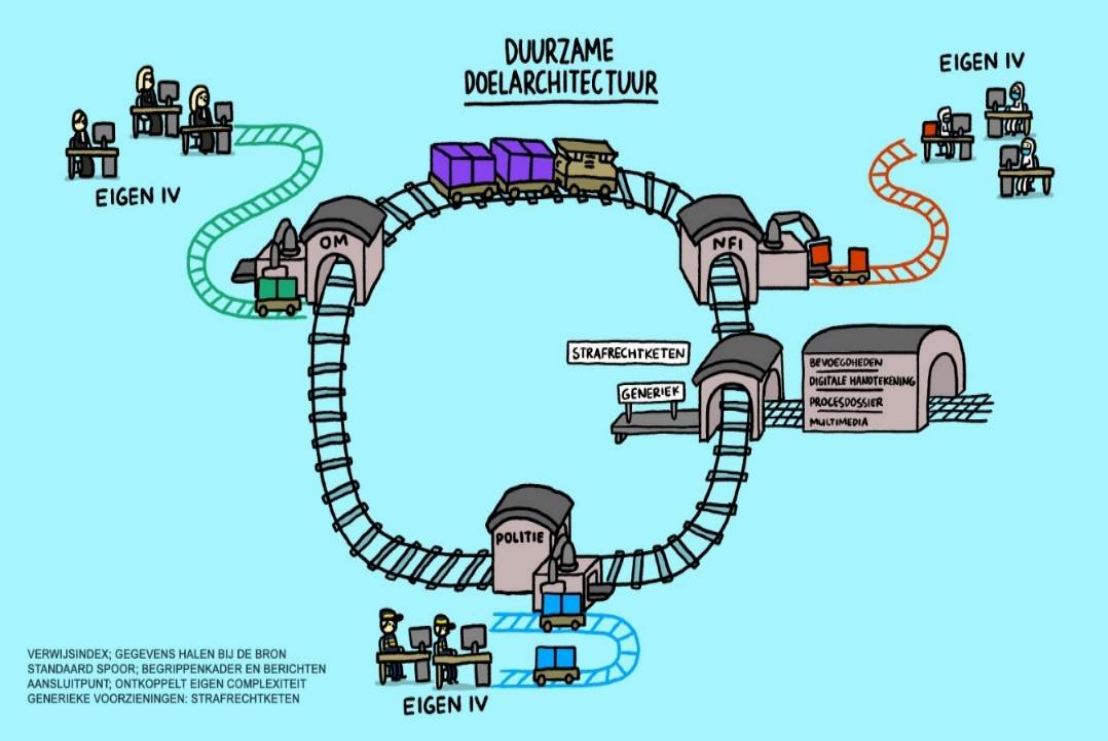
800 man, allen FO
20+ deskundigheden, 1 proces?
Wetenschappers, precies
Kleine (IT) organisatie
#onderzoeken 90.000 (30K DNA)

60.000 man, 1500 FO
11 eenheden, 1 proces?
Doeners, work arounds
Complexe (IT) organisatie
#BVH zaken 100K, 220K items

Rutger Gooszens

# DE CONTROLS

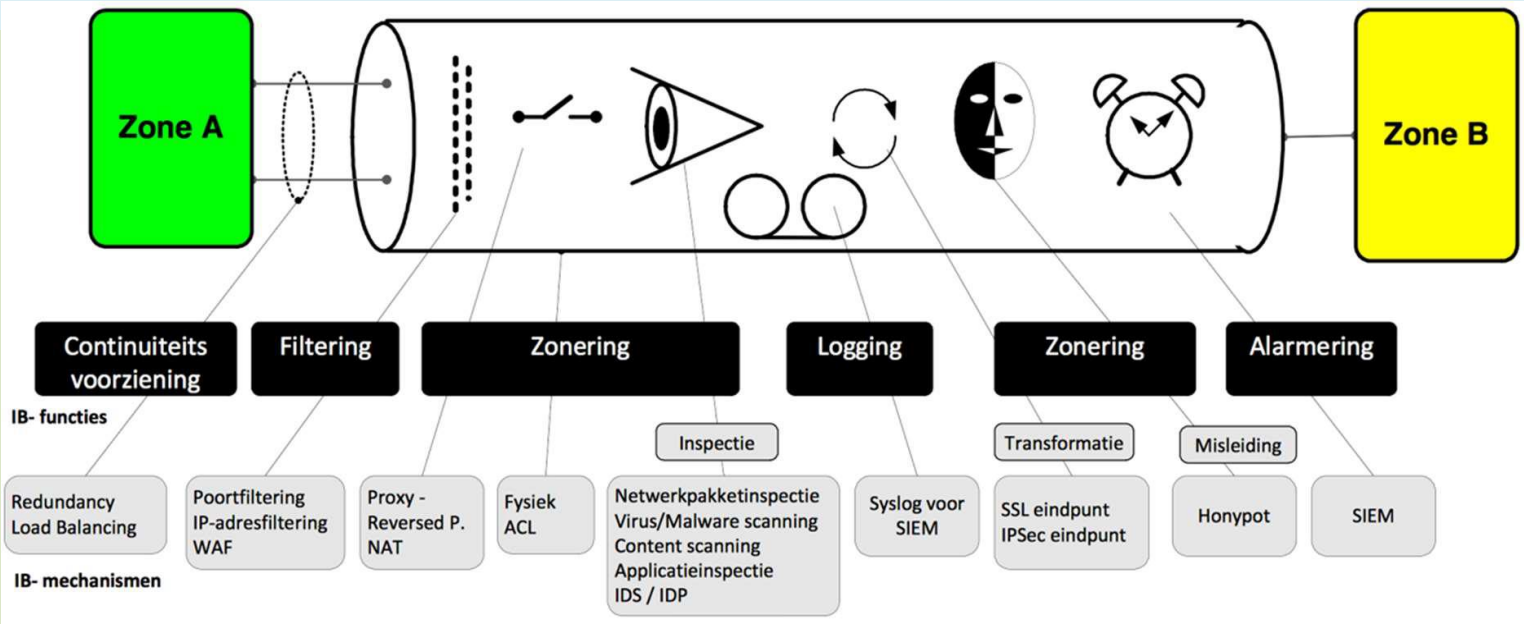
# De gewenste situatie: ontkoppelen door dienst oriëntatie




- Lean werkproces
- Gegevens digitaal uitwisselen via standaard KIC (EBMS berichten en REST/API)
- Eigen IV ontkoppelen van keten IV (afspraken en standaarden)

- Eigen IB domein en ketendomein (wat delen we?)

# De controls




+ Toegangsbeveiliging
+ Encryptie transport

# DE MMA ALS METHODE

# Waarom MMA

- 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

# *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/NEN/ISO x.x.x- …

Versie / datum / **eigenaar**

## Opdracht uit de BIO

### BIO -controltekst

- *De volledige controltekst uit de BIO*

### BIO overheidsmaatregelen bij deze control

- *De maatregelen in groen uit de BIO bij deze control*

## 1. Doelen, scope en prestatie

### Doel

- *Is er een toetsbaar te bereiken resultaat voor de control geformuleerd?*

### Scope (bereik)

- *Is er een duidelijke afbakening van het bereik?*
- *Welke verwerkingen/activiteiten vallen buiten bereik?*

### 2. Verantwoordelijkheden

- *Is (deel-)verantwoordelijkheid voor de control opgedragen en geaccepteerd?*
- *Documentatie: …/*

### 3. Kennis & competentie

- *Is het besturende/uitvoerend personeel voorbereid op haar taak?*
- *Documentatie: …*

### 4. Samenwerking en & communicatie

- *Is afstemming tussen betrokkenen in de uitvoering georganiseerd?*
- *Documentatie: …*

### 5. Instructies uit organisatie en omgeving

- *Ken je steeds alle verwerkingen en activiteiten waarvoor deze control geldt?*
- *Verwerk je het 'tactisch' beleid, uitkomsten van BIA's, DPIA's en eisen uit wetten & regels?*
- *Welke suggesties uit de ISO27002 pas je toe, welke niet, waarom niet?*
- *Documentatie: …*

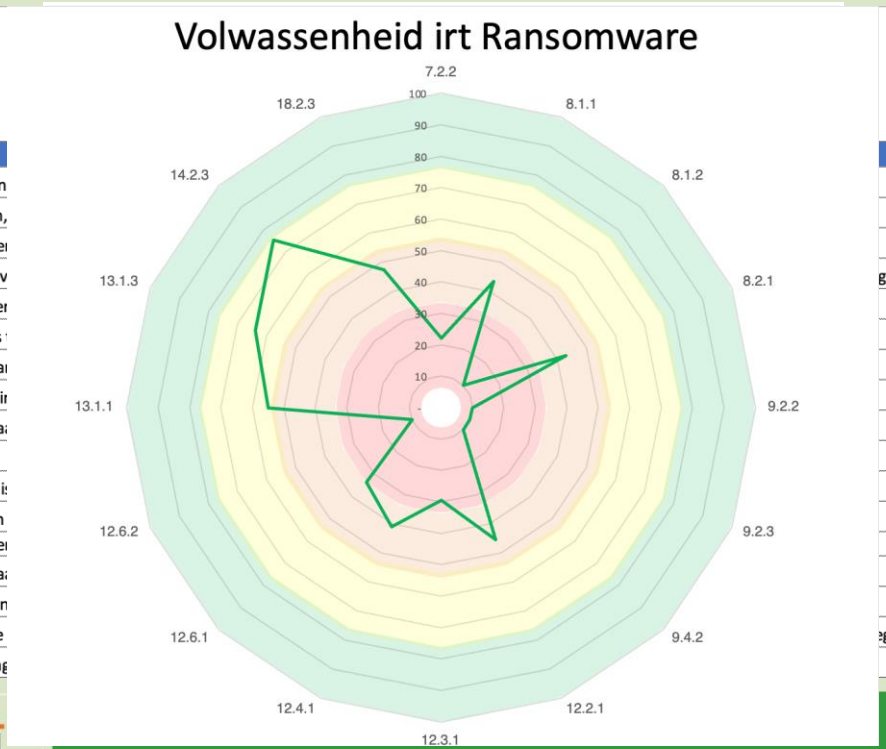
# Control beoordelen per control

| 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<br>Detectie: beperkt<br>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 | |
| | | |
| | | |

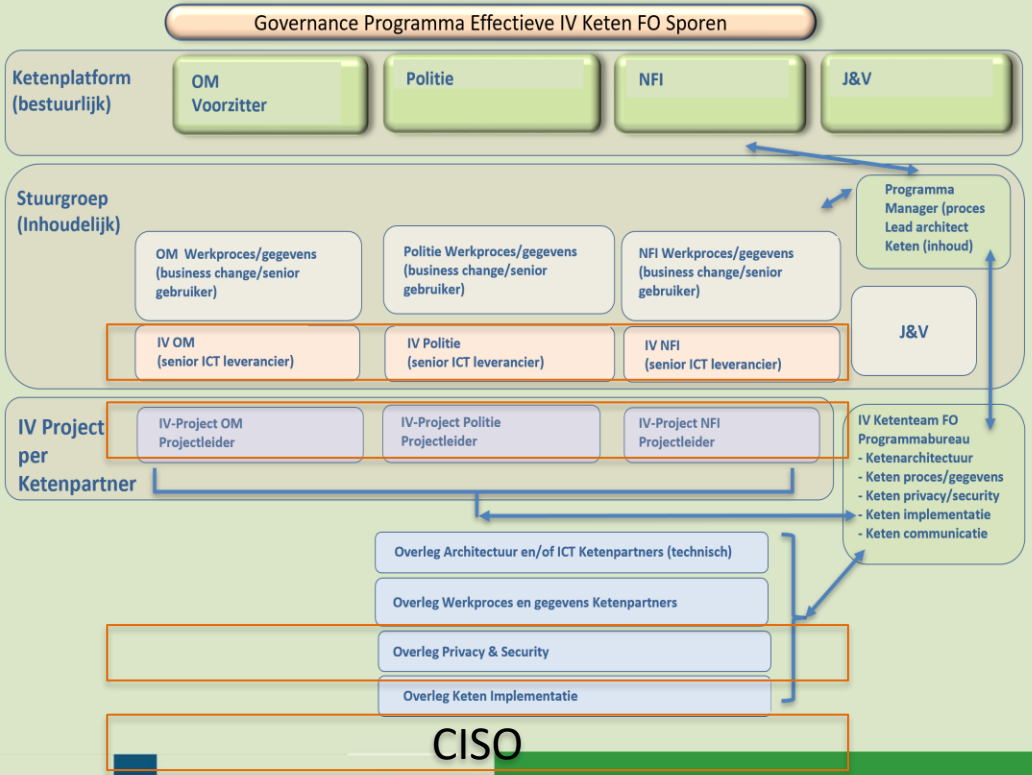
# Relevant rapporteren

| | 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 |
| 29 | 9.2.3 | Beheren va |
| 35 | 9.4.2 | Beveiligde i |
| 60 | 12.2.1 | Beheersma |
| 61 | 12.3.1 | Backup |
| 62 | 12.4.1 | Gebeurtenis |
| 67 | 12.6.1 | Beheer van |
| 68 | 12.6.2 | Beperkinge |
| 70 | 13.1.1 | Beheersma |
| 72 | 13.1.3 | Scheiding in |
| 85 | 14.2.3 | Technische |
| 116 | 18.2.3 | beoordeling |




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

# Trust sessie vanuit de governance




- IV lid stuurgroep (accountable)
- CISO (advies)
- Projectleider (responsible)
- Beveiligingsadviseur Overleg (uitvoering MMA)

# ERVARINGEN

# Voor en tegen

**Voor**

- Eigenaar wordt aangesproken op de claim
- Dialoog
- Geen waardeoordeel/audit maar een continue verbetering

**Tegen**

- Arbeidsintensief
- Eenduidige invulling vergt centrale begeleiding (anders appels en peren)
- Leerproces: niet praten over wat je doet, maar hoe je dat ‘doen’ *beheerst* → ‘control

# Q&A