ITGC’s efficiënt en effectief inzetten in Horizontaal Toezicht

Grace Ramkisoen

Ernest d’Haens

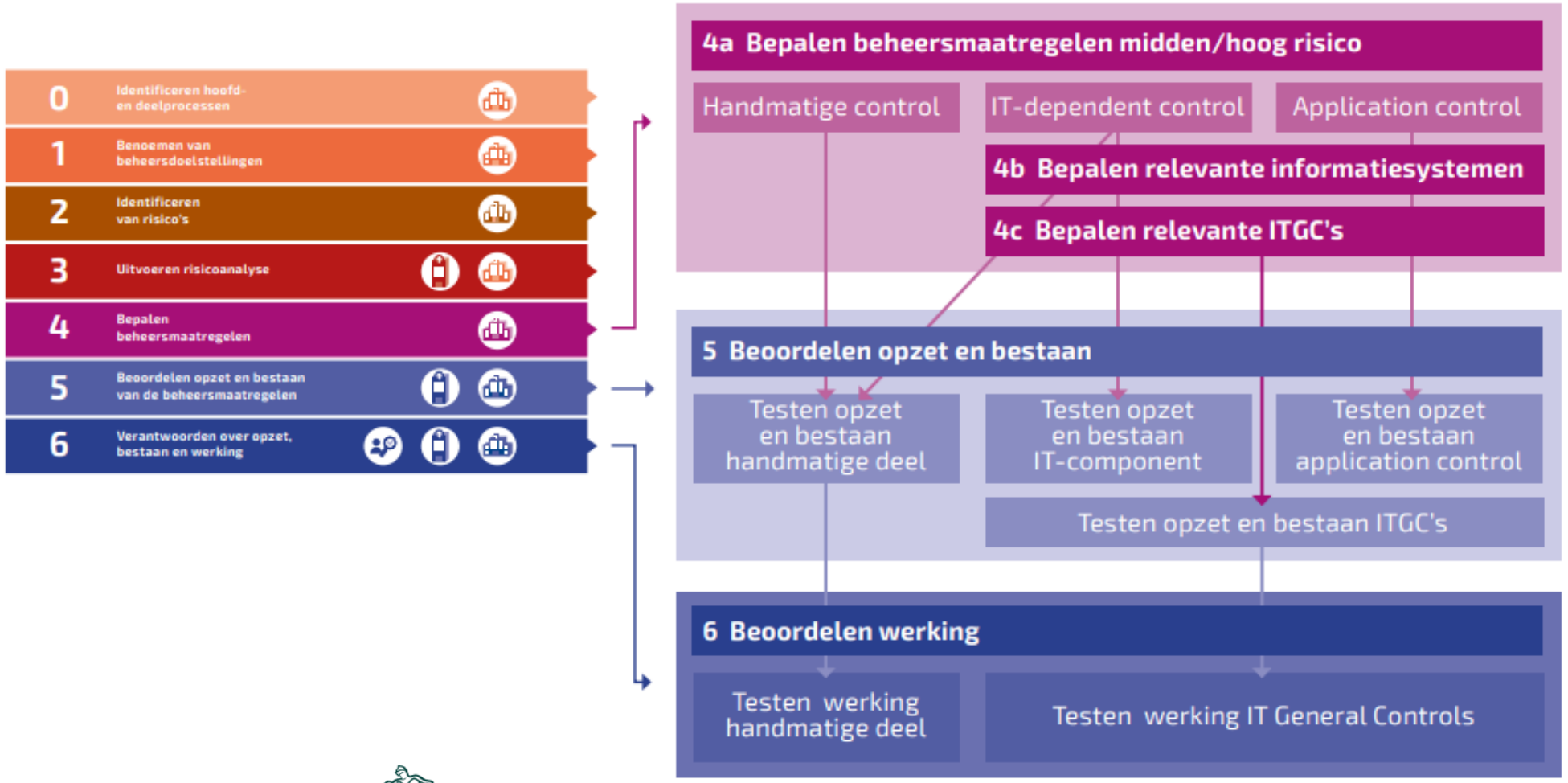
Programma

1. Scoping ITGC binnen – 10 minuten
2. Praktijkvoorbeeld toegangsbeveiliging - Autorisatiematrix EPD theorie + casus – 15 minuten
3. Vertaalslag audit rapport bevinding naar impact op de praktijk van HT inleiding + casus – 10 minuten
4. Periodieke controles, kan het makkelijker – 5 minuten

parnassia groep

Sint Maartenskliniek

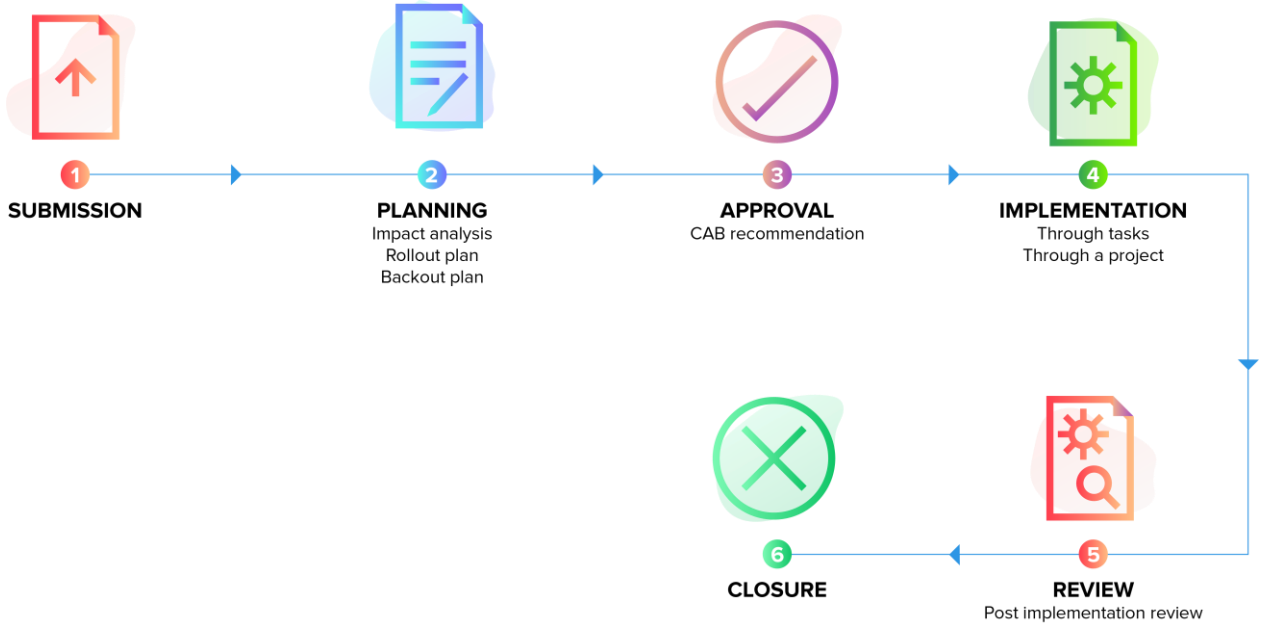
1. Scoping ITGC's binnen HT (1/3)



parnassia groep

Sint Maartenskliniek

1. Scoping ITGC's binnen HT (2/3)



- Logische toegangsbeveiliging
  - Procedure verkrijgen, wijzigen en intrekken toegangsrechten
  - Autorisatiematrix
  - Authenticatiebeleid

- Wijzigingsbeheer
  - Wijzigingsaanvragen geautoriseerd
  - Wijzigingen juist, volledig en tijdig doorgevoerd
  - Bescherming tegen verstoringen

parnassia groep

Sint Maartenskliniek

1. Scoping ITGC’s binnen HT - Assurance verklaringen (3/3)

- ISAE3402 / COS3000
- Beoordeling assurance rapportages
  - Geschiktheid auditor
  - Geschiktheid type assurance rapport
  - Scope van het assurance rapport
  - Toereikendheid periode assurance rapport i.r.t HT verantwoording
  - Uitgevoerde controlewerkzaamheden
  - Oordeel en bevindingen in het assurance rapport
  - Beoordeling impact bevindingen assurance rapportage op de interne beheersmaatregelen HT

  → zijn er bij bevindingen voldoende compenserende maatregelen getroffen

parnassia groep

Sint Maartenskliniek

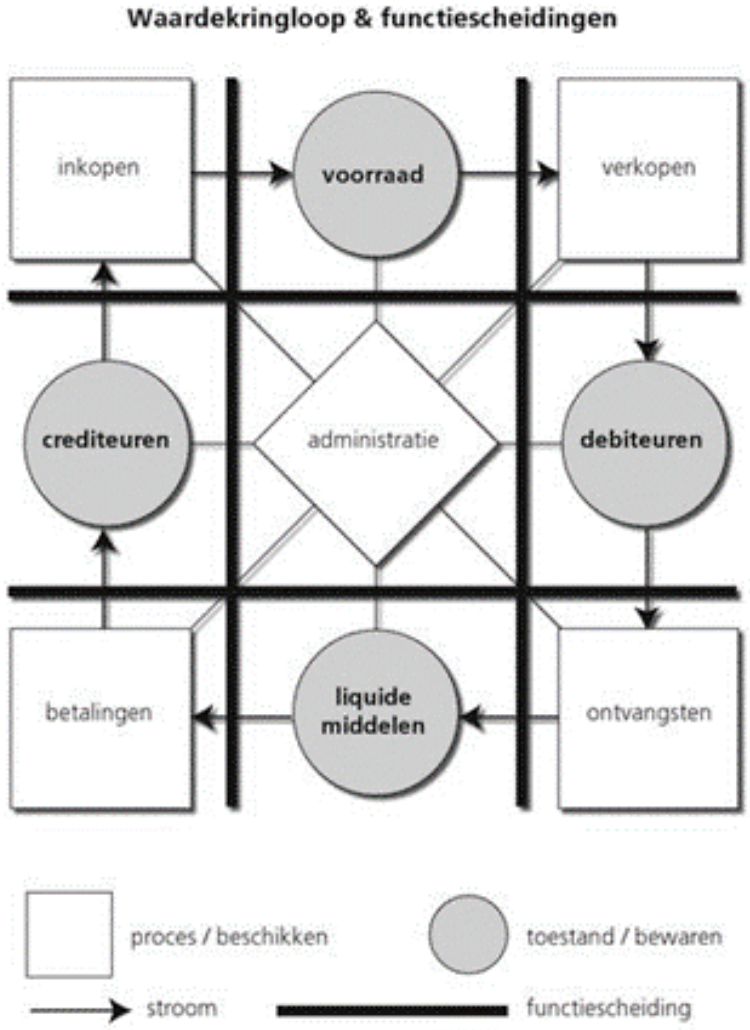
2. toegangsbeveiliging - Autorisatiematrix EPD (1/3)

Basis uitgangspunten autorisatiematrix:

- Functie- en afdeling gebonden
- Sluit aan werkzaamheden (niet meer rechten dan noodzakelijk)
- Sluit aan bij procesafspraken / control framework HT
- Input vanuit meerdere disciplines van belang (zorg/ privacy officer/ AOIC/ etc.)
- Bevat functiescheiding waar wenselijk

Functiescheiding:

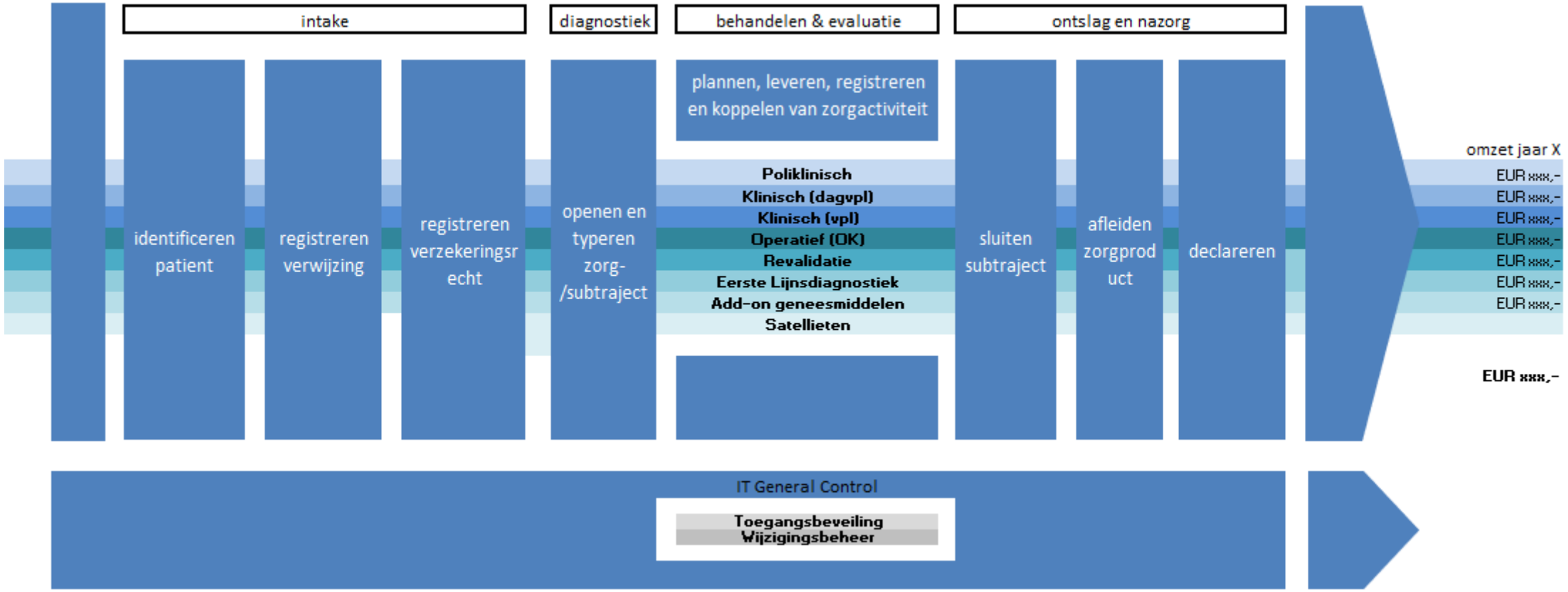
- Primaire functiescheiding
- Secundaire functiescheiding



parnassia groep

Sint Maartenskliniek

2. toegangsbeveiliging (2/3)
Voorbeeld administratief proces leveren zorg

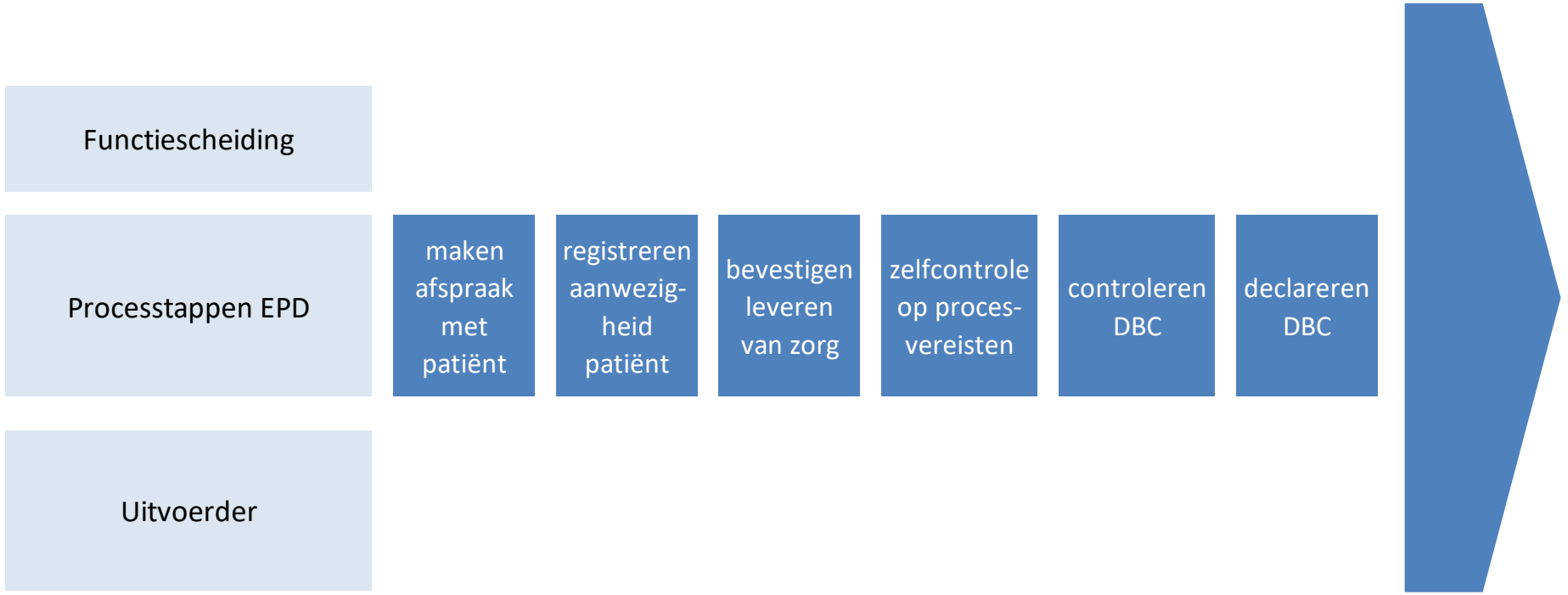


parnassia groep

Sint Maartenskliniek

2. Toegangsbeveiliging (3/3) - functiescheiding autorisatiematrix EPD

voorbeeld functiescheiding EPD leveren zorg



parnassia groep

Sint Maartenskliniek

2. Toegangsbeveiliging (3/3) - functiescheiding autorisatiematrix EPD

voorbeeld functiescheiding EPD leveren zorg

Welke functies wil je gescheiden zien?

parnassia groep

Sint Maartenskliniek

2. Toegangsbeveiliging (3/3) - functiescheiding autorisatiematrix EPD

voorbeeld functiescheiding EPD leveren zorg

parnassia groep

Sint Maartenskliniek

3. Vertaalslag audit rapport naar de praktijk van HT (1/2)

parnassia groep

Sint Maartenskliniek

3. Vertaalslag audit rapport naar de praktijk van HT (2/2)

Casus:

Bevinding: We hebben voor één gebruiker (arts) vastgesteld dat rechten (planrechten) niet conform de autorisatiematrix zijn toegewezen.

1. Wat is de impact hiervan op HT?
2. Kun je compenserende maatregelen bedenken?

parnassia groep

Sint Maartenskliniek

4. Periodieke controles ITGC (1/2)

Periodieke controle – deelwaarnemingen op:

- uitgeven autorisaties (indienst)
- intrekken autorisaties (uitdienst)
- wijzigen autorisaties (functiewijziging)
- beheerrechten
- logging gebruik beheerrechten

Praktijk:

Vaak inefficiënt en foutgevoelig

Gevolg:

Tijdverlies en fouten in procedures

parnassia groep

Sint Maartenskliniek

4. Periodieke controles ITGC (2/2)

De volgende stap:

Continuous monitoring!

parnassia groep

Sint Maartenskliniek

Lessons learned

- ITGC zijn vorm van basis hygiëne. Belangrijk, maar geen ‘garantie voor succes’.
- Kijk vooraf goed naar belang van de verschillende ITGC-onderdelen voor jouw control framework.
- Zoom in op de aspecten die echt impact (kunnen) hebben op HT zoals beheerrechten, basis functiescheiding of functiescheiding waar echt op gesteund wordt in HT, wijzigingen in stamtabellen, configureerbare application controls, etc.
- Vaak wordt er beperkt gesteund op bijvoorbeeld functiescheiding (autorisatiematrix) en vaak zijn er mitigerende maatregelen als gegevensgerichte deelwaarnemingen. Dat maakt het belang van aantoonbaar werkende ITGC, of de impact van bevindingen t.a.v. ITGC voor HT kleiner.
- Kijk ook achteraf, bij een bevinding in de ITGC, goed naar de werkelijke impact voor de HT-verantwoording en eventueel aanwezige mitigerende maatregelen/
- Probeer periodieke controles op de ITGC te automatiseren waar dat efficiënt kan (‘continuous monitoring’).

parnassia groep

Sint Maartenskliniek