Scope IT-audit n.a.v. toezegging aan TK

"GGD GHOR Nederland en ik geven samen opdracht tot een externe audit van beide systemen over 6 weken. Deze audit gaat na of de adviezen zijn opgevolgd, in hoeverre de aangekondigde maatregelen daadwerkelijk zijn getroffen en wat de resterende risico's zijn." (Kamerbrief 2 februari 2021)."

Aandachtspunt:

- Volgordelijktijd van beslissen; er is nog niet besloten welke applicatie HPZone gaat vervangen. Daardoor is omvang van audit nu nog niet te bepalen. Wel kunnen we de audit zoveel als mogelijk klaarzetten met de HIS maar vraag is of we toezegging aan TK tijdig gestand kunnen doen.
- Boodschap nu aan TK: Audit staat klaar en de Minister wacht op GGDén totdat ze besluit nemen over vervanging systeem HPZone(lite).
- VRAAG: In welke fase zit de besluitvorming qua advisering aan de DPG-raad? RDO heeft een concept-brief van GGD GHOR gezien dat ze dit lijken te willen.

  Aanvullende vragen:
  Zodra er gekozen wordt, zal de leverancier van de software aan moeten geven wanneer het systeem an sich en het implementatieproces geaudit kunnen worden. Daarna kunnen pas omvang en details van audit bepaald worden.

  Wanneer weten we wel dat er geaudit kan worden?: Zodra de GGDén een besluit nemen. Vooralsnog lijkt doorontwikkeling van GGD Contact de meest voor de hand liggende keuze.

  Wat is daarvoor nodig?: Voor de doorontwikkeling van GGD contact wordt niet gewacht tot een besluit. De te nemen stappen zijn al in kaart gebracht en er is al gestart met de daadwerkelijke doorontwikkeling van GGD Contact vanuit VWS(VWS is de software-ontwikkelaar). Hiervoor wordt hetzelfde proces gevolgd als bij de Coronamelder.

  Aanleiding audit

  Onderwerp van de audit is het extern laten toetsen van beide systemen (CoronIT en HPZone) en of de GGD'en en GGD GHOR NL met behulp van VWS de juiste aanpak hebben gekozen en de juiste analyse daaraan vooraf is gegaan.

Analyse

- Gezien het feit dat er twee analyses bekend zijn (risicoanalyse en KPMG assessment); hebben de GGD'en en GGD GHOR een volledig beeld van de technische, juridische, processen en andere problemen (waaronder problemen met een culturele component) die spelen bij de systemen van de GGD?
  - Toetsing aan NEN-normeringen (7510, 7512, 7513)
  - Toetsing baseline informatiebeveiliging (ISO 27001)
  - Toetsing juridische onderbouwing (privacy)
  - Toetsing codereview
  - Toetsing werkproces (waaronder organisatie)
  - Toetsing gebruiksvriendelijkheid
  - Toetsing principes dataminimalisatie, privacy-by-design, etc.
  - Toetsing interoperabiliteit
  - Toetsing privacykaders:
    - GGD GHOR - Privacy by design
    - Instellen van implementatie-organisatie die privacy by design ook in de praktijk brengt zoals het is ontworpen
    - AVG en UAVG

- Dataversleuteling in de database (data encrypted at rest); (sleutels bewaard in veilige datakluis (HSM))
- Uitgebreide broncodereview (experts die programmacode controleren)
- Pentesten (Genormeerde pentest conform geldende standaarden)
- Awareness training voor de gebruiker

Aanpak

- Is de huidige aanpak de juiste aanpak om zo snel en zo zorgvuldig mogelijk de juiste maatregelen te nemen om risico's op het gebied van privacy, databeveiliging, datazekerheid, opschaalbaarheid en toekomstbestendigheid te mitigeren in beide ICT-systemen van GGD GHOR?
- En is de aanpak met het beoogde resultaat gebruiksvriendelijk voor de gebruiker van de systemen?

Randvoorwaarde
Randvoorwaarde eindresultaat; Als er geaudit wordt, dan moet volledig omschreven zijn wat er is geaudit en niet alleen de interne bevindingen.

Publiek of voor intern gebruik (rekening houdend met eventueel misbruik van informatie):

In principe deelbaar met de Tweede Kamer, tenzij anders gecategoriseerd door NCSC.

Kanttekening: GGD'en zijn eigenaar (GGD GHOR is coördinator). Wat willen zij?

Gevraagde kwaliteiten aan IT-auditor?

Welke specifieke kennis heeft de IT-auditor nodig??

Bijv. specifieke kennis kan betrekking hebben op bepaalde applicaties, tools (zoals data-analyse) of technische infrastructuur (zoals lokaal netwerk, internet, cloud).