Vraagpunten naar aanleiding van de oplegmemo voor de stuurgroep

1. Privacy compliance Vaccinatieregister COVID gaat verder dan enkel informatiebeveiliging van het systeem CIMS .
2. Niet is aangeven wat er met het advies van 5.1.2e is gedaan, dat gezien het verhoogde dreigingsprofiel ten aanzien van het vaccinatieregister er inzicht dient te zijn in hoeverre externe partijen de voor hen bekende openstaande risico's hebben gedicht. De in de concept DPIA geadresseerde privacy risico's zijn niet geadresseerd.
3. CIMS is in de voorgestelde opzet niet BIO compliant (dus ipse facto niet AVG compliant). Niet naleving van de BIO betekent zeker in de huidige context dat RIVM niet alle passende technische en organisatorische maatregelen heeft getroffen om een op de (privacy) risico afgestemd beveiligingsniveau te borgen.
4. De eisen aan het systeem zijn incompleet. Er zijn bijvoorbeeld geen eisen geformuleerd voor de beschikbaarheid, capaciteit en responsetijden, performance. Er lijkt evenmin rekening te zijn gehouden met aan het systeem te stellen aanvullende eisen in verband met het doel van dit systeem. Ook die aspecten zijn niet meegenomen in de risico-analyse.
5. Vanuit privacy oogpunt kan op dit moment niet aan sommige eisen voldaan worden. De eisen voor informatiebeveiliging moeten onder andere gebaseerd zijn op de classificatie van de informatie die verwerkt en opgeslagen wordt. De IB classificatie is nu nog een schuivend paneel. Het minimale niveau zou BBN2 zijn maar er zit ook informatie in de database over diplomaten, NAVO-medewerkers, geprivilegieerden gegevens over gezondheid, unieke identificatienummers etc. Deze gegevens zouden geclassificeerd moeten worden op BBN3 en de vraag is dan welke informatiebeveiligingseisen daaraan gesteld moeten worden en of daaraan in de huidige CIMS-opzet aan voldaan wordt. Vanuit privacy compliance perspectief is BBN 2 + beveiliging geïndiceerd. Hier is bij de IB risicoanalyse geen rekening mee gehouden. Niet aangeven/ aangetoond is op welke wijze rekening is gehouden met het verhoogde dreigingsbeeld.
6. Alle (interne) koppelingen zijn nog niet geïnventariseerd en beschreven. Er is nog geen systeemdecompositie en niet duidelijk is hoe de koppeling met de Azure-beheercloud van Ordina eruit ziet. Ook de koppeling met de invoerkanalen zijn nog niet voldoende uitgeschreven en gedefinieerd.
7. De acceptatiecriteria zijn onvoldoende beschreven en er is nog geen proces ingericht voor het formeel accepteren van het systeem na testen.
8. De Project Start Architectuur (huidige 0.5 versie) is nog niet goedgekeurd en de opmerkingen van diverse personen is nog niet verwerkt. Deze PSA zou eerst het formele goedkeuringsproces moeten doorlopen. Als deze niet goedgekeurd is weten we immers niet hoe het systeem opgebouwd is en kan ook niet met zekerheid getest worden of het geheel functioneert zoals het ontwerp aangeeft.
9. Ervan uitgaande dat de verantwoordelijkheid van het RIVM voor de gegevens start op het moment dat deze binnenkomen dan zit daar nu nog een grote blinde vlek. Onduidelijk is of dit CSV-bestanden zijn of dat er een directe applicatiekoppeling met GGD-GHOR komt. Daarover is nog geen besluit genomen. Verder is er nog veel onduidelijkheid over de toegangsbeveiliging van de CSV-bestanden. Ook hoelang deze bewaard blijven, hoe voorkomen kan worden dat er ongeautoriseerde toegang plaatsvindt, etc.
10. Databasebeheerders hebben toegang tot data in de database. Voor dit beheer maken ze gebruik van een groepsaccount dus in principe is dergelijke toegang niet tot personen herleidbaar en daarmee niet voldoet aan de AVG-richtlijnen. Deze toegang wordt ook niet gelogd en er zijn geen afspraken over de beoordeling van de eventuele logfiles. De logging van toegang van systeembeheerders, applicatiebeheerders, functionele beheerders en databasebeheerders moet goed beschreven en vastgelegd zijn. Dit proces of processen zijn nu nog onvoldoende of niet beschreven. Hiermee lopen we gevaar dat we misschien wel logfiles hebben maar ze niet controleren en er niet over rapporteren. We weten zelfs niet of ze volledig zijn. Voor de databasebeheerders zijn we bijvoorbeeld daarin volledig afhankelijk van Ordina. De eisen die we daarvoor aan Ordina stellen staan niet op papier.
11. Het wijzigingsproces (CAB) voor de applicatie is nog niet volledig uitgeschreven en daarmee weet nog niet iedereen wat zijn/haar rol is in dat proces. Er lijkt evenmin voorzien te zijn in de "tijdelijke CAB", zoals

door 5.1.2e geadviseerd.

12. De scope van de risicoanalyse (RA) is beperkt tot het bestaan en die beperking is ook opgenomen in de RA. Bij de besprekingen van afgelopen dagen is men zich er niet van bewust geweest dat er een beperking is van deze RA. Er is alleen naar het systeem gekeken en niet naar processen, er is niet naar werking van bestaande processen gekeken, er is niet naar beleidsuitgangspunten gekeken. Men heeft de RA als een complete RA beschouwd in de besprekingen en nooit gekeken naar noodzakelijke aanvullingen. Privacy risico's zijn in de analyse niet meegenomen (wel is aangeduid welke IB maatregelen impact op privacy kunnen hebben). De informatiebeveiligingsrisico's zijn (nog) niet vertaald naar privacy risico's.
13. Er wordt het gehele systeem CIMS niet cf BIO en AVG gelogd. Gevolg is dat je bij een inbreuk op de beveiliging* niet kunt uitsluiten dat die inbreuk tot een onrechtmatige verwerking heeft geleid. En dient die inbreuk dus te worden beschouwd als een datalek. (*Een inbreuk op de beveiliging van persoonsgegevens moet ruim worden geduid. Het is niet van belang of passende technische of organisatorische maatregel zijn getroffen. Een datalek kan zich in beide situaties voordoen)
14. Door het gebruik van een legacy systeem wordt ook het risico op onvolledige of geen documentatie groter. We weten op dit moment de status van de documentatie niet en hebben daarmee ook onvoldoende inzicht in de technische implementatie van de applicatie.
15. Er wordt zowel door de applicatiebeheerder (Ordina) blijkbaar gezorgd voor een back-up en door technisch beheer (Campus). Er zijn geen specifieke eisen gesteld en er is geen afstemming over wie nu wat back-upt. Daarmee wordt recovery in geval van calamiteiten lastig. Vraag is of dit afgestemd en getest wordt voordat de applicatie operationeel wordt.
16. 5.1.2h
17. Er is nog geen test ingepland om de back-up te testen door een recovery uit te voeren. Ook zijn er nog geen beschrijvingen van dit proces om dit periodiek te doen. Dit moet afgestemd worden met Ordina.
18. Beleid en procedures voor het verlenen, wijzigingen en verwijderen van speciale toegangsrechten ontbreken. Onbekend is hoe de toegangsrechten procedure bij Ordina verloopt en of het RIVM daarmee akkoord is. Binnen RIVM is ook niet aantoonbaar dat het huidige proces van het verlenen, wijzigen en verwijderen van speciale toegangsrechten werkt en volledig is.
19. Maatregelen zijn (nog) niet compleet en (helemaal) op werking getoetst.

Conclusie 20.12.2020 : de verwerking met de mitigerende maatregelen nog een hoog risico oplevert.

Advies

- De (imago) schade die hiervan het gevolg kan zijn, mee te wegen in de besluitvorming.
- Om in navolging van het tussenadvies van 5.1.2e in dit geval te overwegen, de toezichthoudende autoriteit voorafgaand aan de livegang te raadplegen.

21.12.2020

5.1.2e

5.1.2e