Noordbeek

Rijndijk 235
2394 CD Hazerswoude

Telefoon
Fax
Mobiel 5.1.2e

Email 5.1.2e @noordbeek.com

RIVM
5.1.2e
Postbus 1
3720 BA BILTHOVEN

Hazerswoude, 23 december 2020

Betreft: Opdrachtbevestiging voor een Quick Scan BIO op CIMS

Geachte 5.1.2e

U heeft, in overleg met de heer 5.1.2e van het ministerie van VWS, Noordbeek verzocht een voorstel uit te brengen voor het uitvoeren van een quick scan op de informatiebeveiliging van het COVID-vaccinatie Informatie- en Monitoringsysteem (CIMS).

Noordbeek heeft dit voorstel opgesteld in de vorm van een opdrachtbevestiging, welke als volgt is ingedeeld:

1. Achtergrond
2. Opdrachtomschrijving
   2.1. Scope
3. Aanpak
4. Doorlooptijd en tijdsbeslag
5. Rapportage
6. Teamsamenstelling
7. Honorarium
8. Bankrekeningnummer
9. Randvoorwaarden
10. Geldigheidsduur en algemene voorwaarden

1. Achtergrond

RIVM heeft het Information Security Management System (ISMS) en de daarbij vereiste maatregelen geïmplementeerd in overeenstemming met de Baseline Informatiebeveiliging Overheid (BIO).

RIVM bouwt momenteel het COVID-vaccinatie Informatie- en Monitoringsysteem (CIMS).

Het ministerie van VWS heeft RIVM verzocht een onderzoek uit te laten voeren op compliance met de BIO op de Basisbeveiligingsniveaus 2, 2+ en 3 (BBN2, BBN2+ en BBN3) voor CIMS, met als rapportage-deadline het begin van de werkdag op 28 december 2020.

2. Opdrachtomschrijving

Noordbeek heeft opdracht gekregen om een quick scan uit te voeren op compliance met de BIO op diverse Basisbeveiligingsniveaus voor CIMS, inclusief de processen, koppelingen, werkzaamheden van de leverancier en het datacenter.

Noordbeek informeert het RIVM tijdens het onderzoek over de (voorlopige) bevindingen, om te borgen dat de rapportage voor wat betreft vorm en inhoud voldoet aan de informatiebehoefte van de opdrachtgever.

2.1. Scope

De scope betreft de applicatie CIMS, de CIMS-database en de SFTP-server, met hun koppelingen, autorisatiebeheer, en ontwikkel- en beheerprocessen.

Er worden geen werkzaamheden uitgevoerd met betrekking tot de werking van interne beheersingsmaatregelen en wij brengen daarover geen oordeel tot uitdrukking. Tevens worden in het kader van deze audit door ons geen penetratietesten en vulnerability scans uitgevoerd.

De werkzaamheden voor de quick scan worden verricht in overeenstemming met de vaktechnische richtlijnen van onze beroepsorganisatie de Nederlandse Orde van Register IT-Auditors (NOREA).

3. Aanpak

Bij de onderzoeksaanpak wordt doorgevraagd en worden de waarnemingen gevalideerd totdat de gewenste mate van volledigheid van de inventarisatie en inzicht in risico's en kwetsbaarheden is bereikt.

4. Doorlooptijd en tijdsbeslag

Wij kunnen na gunning direct starten met deze opdracht.

Uw planning is:
- Dinsdag 22 december 2020 starten met de voorbereiding van het onderzoek:
- Woensdag 23 en donderdag 24 december 2020 uitvoeren van het onderzoek;
- Zondag 27 december 2020 opleveren van het concept rapport aan RIVM ter review;
- Maandag 28 december 2020 opleveren van het rapport aan het ministerie van VWS.

Wij zetten een team in van twee personen, waarbij de tijdsbesteding per persoon is:
- Voorbereiding: 1 dag;
- Onderzoek: 2 dagen;
- Rapportage: 2 dagen;
- Nazorg en toelichten van de conclusies: 0,5 dag.

Wij verwachten een totale tijdsbesteding van 88 uur.

5. Rapportage

Voor de rapportage hanteert Noordbeek het formaat van ISAE 4401, namelijk een rapport van feitelijke bevindingen. Deze rapportage wordt eerst in concept aan u als opdrachtgever voorgelegd. Nadat dit concept met u is besproken zal de rapportage definitief worden gemaakt.

De waarnemingen en conclusies worden uitgewerkt conform de Code of Ethics en voorschriften van de NOREA voor de Richtlijn 4401.

6. Teamsamenstelling

De uitvoering van de werkzaamheden wordt verzorgd door de heren:
- 5.1.2e
- 5.1.2e

De eindverantwoordelijkheid voor de uitvoering van de opdracht berust bij ondergetekende, directeur van Noordbeek.

Namens het RIVM treedt de heer 5.1.2e op als contactpersoon voor deze opdracht.

7. Honorarium

Voor het door ons voorgestelde team hanteren wij een gemiddeld uurtarief van 5.1.2b inclusief reis- en verblijfskosten binnen Nederland en exclusief 21% BTW. Er worden geen andere kosten dan het uurtarief in rekening gebracht.

Wij verwachten dat de werkzaamheden van Noordbeek voor dit onderzoek in totaal 88 uur in beslag zullen nemen.

Het totale honorarium van Noordbeek bedraagt 5.1.2b inclusief reis- en verblijfskosten in Nederland en exclusief 21% BTW. Dit bedrag is een maximum bedrag en kan als fixed price worden beschouwd.

Wij factureren na afloop van de werkzaamheden, na uw accordering van onze prestatie.

8. Bankrekeningnummer

De betaling van onze facturen kan verlopen via onze Rabo-rekening met IBAN-nummer NL89 RABO 0364 2373 33, ten name van Noordbeek B.V. te Hazerswoude.

9. Randvoorwaarden

Alle teamleden van Noordbeek beschikken over recente VOG's (aspecten 11, 12, 13 en 41) voor het omgaan met gevoelige informatie.

Noordbeek borgt de vertrouwelijkheid van de waarnemingen, documentatie, aantekeningen en rapportage. Het (concept) rapport wordt enkel gedeeld met de opdrachtgever en eventueel door hem aangewezenen.

Ten behoeve van een efficiënte en effectieve uitvoering van onze werkzaamheden is het van belang dat de bij deze opdracht te betrekken of te interviewen medewerkers tijdens het verloop van de werkzaamheden beschikbaar zijn en de benodigde documentatie en locaties voor ons toegankelijk zijn.

De schatting van het tijdsbeslag is gebaseerd op de uitvoering van de overeengekomen ondersteuning, de tijdige ontvangst van de benodigde informatie en de medewerking van de diverse betrokkenen in de periode van onderzoek. In geval van een wezenlijke verandering in de opdracht of van moeilijkheden bij het verkrijgen van informatie die redelijkerwijs niet konden worden voorzien en die aanvullende werkzaamheden veroorzaken, zullen wij tijdig met u overleggen.

De quick scan betreft een assurance-opdracht met een beperkte mate van zekerheid, conform Richtlijn 4401. Wij voeren een eigen risicoanalyse uit om vast te stellen met welke diepgang wij de door RIVM gerealiseerde beheersmaatregelen moeten beoordelen.

10. Geldigheidsduur en algemene voorwaarden

Deze opdrachtbevestiging heeft een geldigheidsduur van vier weken gerekend vanaf de datum van ondertekening door Noordbeek.

Wij accepteren de inkoopvoorwaarden van RIVM.

Ten slotte

Mocht u nog vragen hebben, aarzelt u dan niet contact met ons op te nemen. Als u zich in deze opdrachtbevestiging kunt vinden, verzoeken wij u ons een getekend exemplaar of een inkooporder te doen toekomen.

Met vriendelijke groet,

5.1.2e

5.1.2e

Voor akkoord,
Bilthoven, d.d.

5.1.2e