

Behoefteprofielen Perceel 2 Informatiebeveiliging

211005

De verwachte soorten opdrachten:

Met verwijzing naar de structuur van het NCSC-document "ICT-Beveiligingsrichtlijnen voor Webapplicaties, RICHTLIJNEN-leesversie", NCSC, september 2015¹:

CIBG	<p>Opdrachten in het beheersingsdomein, en op alle lagen van het uitvoeringsdomein, waar mogelijk uitgesplitst naar de genoemde vier (4) ICT-lagen met bijbehorende richtlijnen. Focus op netwerken/infrastructuur intern is minder groot.</p> <p>Concreet zijn de volgende aandachtsgebieden benoemd:</p> <ul style="list-style-type: none">- Penetratietesten – Black box, Grey box en White box- Fysieke beveiliging (passencontrole, toegang panden, ODC),(niet direct verwacht maar wel in scope)- 7 x 24 Monitoring (vulnerability scan, met centrale incidentmanager)- Awareness; bijvoorbeeld Phishing activiteiten en Social engineering activiteiten, voorlichting en trainingen.- Resultaatverplichte consultancy met uitwerkingen (advisering op informatiebeveiligingsvraagstukken, onderzoek en advies op functiescheiding, toegang echten en inrichting van taken, bevoegdheden en verantwoordelijkheden, review vanuit IB perspectief bij aanbestedingen of ander documentatie, risicoanalyses etc.).
VWS	<p>Het gaat om dienstverlening op het gebied van:</p> <ul style="list-style-type: none">- de organisatie van de informatiebeveiliging;- risicomanagement (risico-analyses);- privacybescherming (DPIA, opstellen Verwerkersovereenkomst etc.);- alle soorten penetratietesten;- code reviews;- kwetsbaarheidsonderzoeken ('vulnerability scans')- audits op daadwerkelijke fysieke beveiliging (gebouw, rekencentrum, gegevensdragers etc.);- tooling (automation, GRC, discovery), zowel regulier (on premise) als cloud (SaaS e.d.);
RIVM	<p>Opdrachten kunnen In principe in alle domeinen verwacht worden.</p>
SSC-ICT	<p>Opdrachten kunnen In principe in alle domeinen verwacht worden. Het zal niet alleen om penetratietesten gaan, maar ook om opdrachten in het kader van beheer en bouw van applicaties, dan wel om niche kennis</p>
SZW	<p>Nadruk ligt voor SZW op het uitvoeringsdomein, met nadruk op de domeinen toegangsvoorzieningsmiddelen en webapplicaties. Het beheersingsdomein is</p>

¹ Zie: [ICT-beveiligingsrichtlijnen voor webapplicaties | Publicatie | Nationaal Cyber Security Centrum \(ncsc.nl\)](#)

	<p>grotendeels het werkveld van SSC-ICT, in afstemming met SZW. Voor SZW ligt de focus in het beheersingsdomein vooral op SAP S/4 omgevingen.</p> <p>Voor de periode van 2022 en verder ligt de focus naar verwachting op:</p> <ul style="list-style-type: none"> - periodieke Pentests, red teaming (o.a. op de webapplicaties van Inspectie SZW en portalen UvB), inclusief initiële test en hertest; - Automated vulnerability scans (optioneel, hangende kosten en mate waarin dit niet door de zittende leverancier wordt geregeld); - Het uitvoeren van IT-audits o.b.v. control framework (bv ADR) (bv met percelen zoals softwaretesting, hardwaretesting, apps, eventueel fysieke pentesten/awareness/social engineering).
OCW/IvhO	<p>De opdrachten in het uitvoeringsdomein kunnen op het gebied van de gebruiker-laag en toegangsvoorziening-laag liggen.</p> <p>OCW zal/kan opdrachten in de markt zetten met betrekking tot:</p> <ol style="list-style-type: none"> a. Het opstellen van beleid (IvhO volgt OCW) b. het uitvoeringsdomein (IvhO denkt naast techniek ook aan mogelijke opdrachten rondom processen en awareness) c. het beheersingsdomein (IvhO denkt naast testen ook aan het verzamelen en registreren van materiaal t.b.v. compliance)
RWS	Nadruk ligt op de KWIV-dimensie 1 BOUWEN en KWIV-dimensie 2 ONTWIKKELEN.
SVB	<p>Verwacht met name opdrachten in het uitvoeringsdomein. Pentesten vinden meestal op dat niveau plaats. Bij verschuiving van het aandachtsgebied naar Cloud, zou het kunnen dat er in het beheersingsdomein zaken gaan landen. Of het noodzakelijk is of er op het beleidsdomein aandacht nodig is, is nog niet bekend. Er spelen ook zaken zoals het hybride-SOC. Ook neemt SVB nu al diensten af m.b.t. “digitale brandweer”, maturity assessments, red-team, etc.</p>