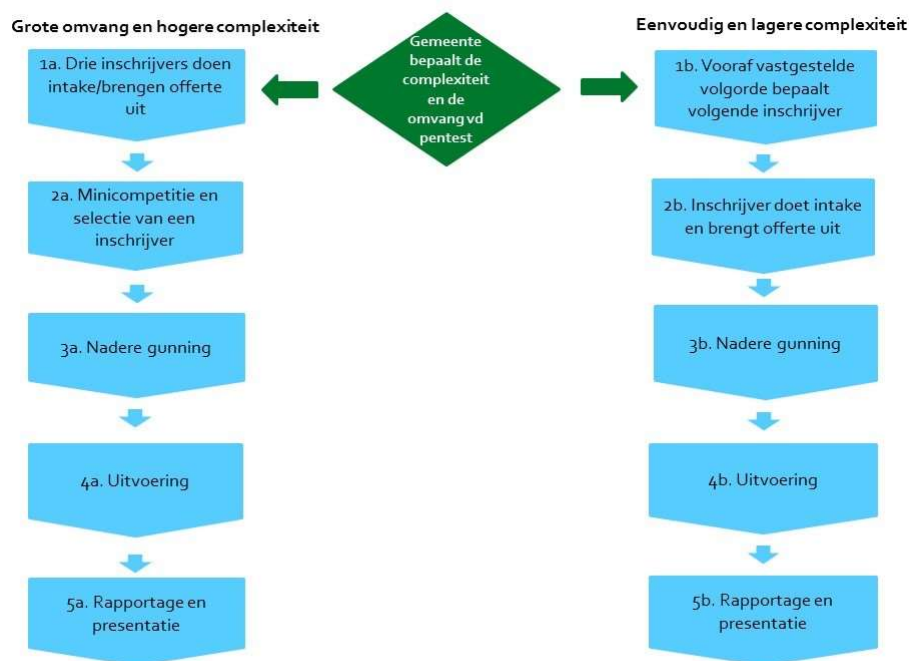


Bijlage 9 - Procedure van gunning Nadere Opdrachten voor Pen- en hacktesting

De in deze Bijlage beschreven procedure moet worden beschouwd als een eis of een uitvoeringsvoorwaarde. Indien Inschrijver hieraan niet kan voldoen, wordt deze uitgesloten van verdere deelname aan de aanbestedingsprocedure. Inschrijver dient in de aanbestedingsbrief te bevestigen dat hij volledig voldoet aan hetgeen hier beschreven. Dit laat onverlet dat Inschrijver ook akkoord gaat met het overige zoals beschreven in deze aanbestedingsleidraad, inclusief Bijlagen.

De Gemeente wil dat iedere Nadere Opdracht voor een penetratietest, afhankelijk van de omvang en complexiteit van de test, volgens een vaste procedure loopt. Binnen deze procedure is er sprake van gunning van de Nadere Opdracht¹ via een vooraf vastgestelde volgorde (per toerbeurt) of via een minicompetitie. Het gunningsproces ziet er als volgt uit:



¹ Let op! Dit is niet de gunning van de Raamovereenkomst. Deze is beschreven in de aanbestedingsleidraad.

1 Intake

De gunning van iedere Nadere Opdracht start met een aanvraag en een intake gesprek. De intake zal uiterlijk op de vijfde (5^e) werkdag na de aanvraag van de Gemeente plaatsvinden.² De leverancier brengt hier geen separate kosten voor in rekening.

Tijdens de intake wordt in samenspraak met de leverancier(s) vastgesteld wat de scope, diepgang en planning van de penetratietest zal zijn.

De Gemeente realiseert zich dat de kans om het maximum aantal kwetsbaarheden met samenhangende risico's te vinden, zo groot mogelijk is wanneer er zoveel mogelijk tijd, expertise en geld in een test wordt geïnvesteerd. De Gemeente zoekt hier naar een balans tussen investering (scope, gevraagde inspanning) en resultaat (aantal en type kwetsbaarheden). De Gemeente wil daarom dat de leverancier tijdens de intake hierover adviseert.

2 Inhoud Nadere Offerte

De Nadere Offerte is time boxed (vaste tijd, vaste prijs) gespecificeerd en omvat alle gevraagde werkzaamheden, inclusief de rapportage en eventueel de presentatie³, maar uitgezonderd een eventuele hertest. De Nadere Offerte bevat in ieder geval de volgende informatie:

- 1) Het doel van de penetratietest:
 - a) de onderzoeksvraag
 - b) de wijze waarop de leverancier voor de betreffende penetratietest een balans heeft gezocht tussen investering en resultaat, zoals toegelicht in de vorige paragraaf 1 ('Intake').
- 2) De scope van het onderzoek:
 - a) de te onderzoeken objecten (applicaties en/of systemen en/of netwerk componenten);
 - b) technische gegevens (IP adressen en URL's);
 - c) aantallen databases;
 - d) mogelijke complexiteiten en speciale aandachtspunten zoals bijv. een code review;
 - e) onderdelen die expliciet niet worden getoetst;
 - f) welke omgeving(en) het betreft (ontwikkeling, test, acceptatie, productie);
 - g) of de relevante onderdelen van de Logius norm (bij DigiD) getoetst dienen te worden;
 - h) of het een hertest betreft op basis van resultaten van een eerdere penetratietest;
 - i) gebruik van eventuele kwetsbaarheden op de betreffende omgeving.
- 3) Plan van aanpak:
 - a) testplan en gebruikte methode;
 - b) de locatie van uitvoering van de penetratietest (intern of extern);
 - c) testmethode ('niveau van voorkennis') black-, grey- of whitebox;
 - d) de namen van medewerkers die de test zullen uitvoeren en een onderbouwing van de door de Gemeente gestelde eisen aan de medewerkers bijv. m.b.v. hun CV's;
 - e) eventuele risico's;
 - f) de door de Gemeente gewenste uitvoerdatum of data;
 - g) doorlooptijden, deadlines en de tijden waarop de werkzaamheden worden uitgevoerd;
 - h) een uiterste datum voor de oplevering van het rapport;
 - i) overzicht, inclusief planning van de benodigde inzet van medewerkers van de Gemeente.

² Deze termijn start op de eerste werkdag nadat de Gemeente de aanvraag bij de leverancier heeft ingediend.

³ Een presentatie hoeft enkel plaats te vinden bij grote en complexe adviezen en onderzoeken

- 4) Werkafspraken (zoals afgestemd tijdens de intake):
 - a) wat de leverancier moet doen als er een kritieke kwetsbaarheid wordt gevonden (testen stoppen, rapporteren, of doorgaan);
 - b) momenten waarop er niet getest mag worden;
 - c) voor de complexere en grotere opdrachten, het soort presentatie(s) en de doelgroep;
 - d) of de test dusdanig moet worden uitgevoerd dat detectie van de test (en escalatie via een incident response proces) zoveel mogelijk vermeden wordt;
 - e) communicatie: de frequentie van tussentijds voortgangsoverleg;
 - f) eventuele randvoorwaarden tijdens de uitvoering;
- 5) De investering (prijs) op basis van het benodigde aantal dagen/dagdelen.

Na ontvangst van de door de Gemeente getekende Nadere Offerte is de leverancier in staat om binnen 5 werkdagen te starten met het uitvoeren van de penetratietest, tenzij op verzoek van de Gemeente een datum eerder of verder in de toekomst is overeengekomen.

3 Gunning Nadere Opdracht op basis van vooraf vastgestelde volgorde (toerbeurt)

Indien het een niet-complexe penetratietest betreft, een test van geringe omvang, of een test die met spoed moet worden uitgevoerd (binnen drie werkdagen), dit ter beoordeling van de Gemeente, zal de Gemeente per toerbeurt, in een vaste volgorde aan een leverancier vragen om een intake uit te voeren en een offerte op te stellen. De volgorde wordt bepaald door de Eindscore Economisch Meest Voordelige Inschrijving (zie aanbestedingsleidraad), waarbij de leverancier met de hoogste eindscore, de eerste opdracht krijgt gegund, dan de nummer twee en tenslotte nummer drie, gevolgd door de nummer 1, etc.

De leveranciers hebben een leveringsverplichting. Indien blijkt dat een leverancier gedurende een periode van 3 maanden op minder dan 70% van de aanvragen een aanbieding doet, of te laat reageert op de intake of het indienen van de offerte, dan is de Gemeente gerechtigd om de Overeenkomst te ontbinden. Hiervoor is geen ingebrekestelling noodzakelijk.

4 Gunning Nadere Opdracht op basis van minicompetitie

Indien het een penetratietest van grote omvang en/of hogere complexiteit betreft, dit ter beoordeling van de Gemeente, wordt een minicompetitie tussen de drie leveranciers gestart. De drie leveranciers worden uitgenodigd voor een intake en worden op basis daarvan gevraagd een offerte, inclusief een plan van aanpak op te stellen. Op basis van onderstaand model gunt de Gemeente de Nadere Opdracht.

Criteria minicompetitie	Maximale score	Uitvraag
Kwaliteit van de Offerte, incl. het plan van aanpak	70 punten	Intakeformulier /offerte
Prijs	30 punten	Op basis van aantal in te zetten dagdelen

Per Nadere Opdracht kan de Gemeente eisen stellen aan de uitvoering.

5 Eisen aan Nadere Opdrachten

Per Nadere Opdracht kan de Gemeente eisen stellen aan de medewerkers van de leverancier die de Opdracht gaan uitvoeren. Het betreft dan bijvoorbeeld (niet limitatief) eisen aan de screening van de medewerkers (zoals VOG) en opleiding en ervaring van de medewerkers. De Gemeente kan

eisen stellen aan de wijze waarop de leverancier dit dient aan te tonen, bijvoorbeeld in de vorm van de CV's van uitvoerend personeel.

Ook kan de Gemeente per Nadere Opdracht een uiterste opleverdatum voor de resultaten van de test stellen (oplevering van de definitieve eindrapportage).

De mogelijke eisen aan zowel de medewerkers als aan de uiterste opleverdatum zal de Gemeente tijdens de intake aan de leveranciers kenbaar maken.

Beide hiervoor genoemde eisen zijn knock-out criteria. Indien de Offerte en de aangeboden medewerkers hieraan niet voldoen komt de leverancier niet in aanmerking voor de gunning van de betreffende Nadere Opdracht.

6 Beoordeling kwaliteit Nadere Offerte, inclusief Plan van Aanpak

De Nadere Offerte, inclusief plan van aanpak dient ten minste de informatie als genoemd in paragraaf 2 te bevatten. De beoordeling van de kwaliteit van de uitwerking van de Nadere Offerte wordt getoetst op basis van de volgende aspecten:

- de mate waarin de offerte/plan van aanpak duidelijk en concreet is;
- de mate waarin offerte/plan van aanpak onderbouwd is;
- de mate waarin offerte/plan van aanpak antwoord geeft op de aanvraag van de Gemeente;
- de mate waarin offerte/plan van aanpak leesbaar en begrijpelijk is voor management én technici.

Per aspect kunnen maximaal 2 punten worden behaald: 0 punten als de offerte niet voldoet aan het betreffende aspect, 1 punt als de offerte gedeeltelijk voldoet en 2 punten als de offerte (vrijwel) geheel voldoet. Deze score zal worden vermenigvuldigd met 70/8 om tot de maximale score van 70 punten te komen.

7 Prijs Nadere Offerte

De prijs van de Nadere Offerte is gebaseerd op het aantal dagdelen dat de leverancier nodig heeft om de Nadere Opdracht uit te voeren vermenigvuldigd met het door leverancier aangeboden dagtarief. De prijs voor een dagdeel is de helft van het dagtarief.

De prijs wordt omgerekend naar een score, waarbij de leverancier met het laagste tarief de maximale score 30 krijgt. Inschrijvers met een hogere prijs krijgen een lagere score, waarbij Inschrijvers met een prijs die anderhalf keer zo hoog is als de laagste prijs nul (0) punten scoren. Prijzen hoger dan anderhalf keer de laagste prijs scoren ook nul punten. De score wordt berekend met onderstaande formule:

Score = MaximaleScore – MaximaleScore * 1,5log (prijs / Laagste prijs)

- MaximaleScore = 30 punten.

Voorbeeld 1. De prijs is de laagste prijs.

- Score = 30 – 30 * 1,5log (laagste prijs / laagste prijs) =
30 – 30 * 1,5log (1) = 30 punten

Voorbeeld 2. De prijs is 1,25 keer de laagste prijs.

- Score = 30 – 30 * 1,5log (1,25 * laagste prijs / laagste prijs) =
30 – 30 * 1,5log (1,25) = 13,5 punten

Voorbeeld 3. De prijs is anderhalf keer zo hoog als de laagste prijs.

- $\text{Score} = 30 - 30 * 1,5 \log(1,5 * \text{laagste prijs} / \text{laagste prijs}) = 30 - 30 * 1,5 \log(1,5) = 0 \text{ punten}$

8 Gunning Nadere Opdracht voor hertest

Op basis van de resultaten van een penetratietest kan de Gemeente constateren dat het niveau van beveiliging onvoldoende is en maatregelen treffen om risico's te minimaliseren. Na implementatie van de maatregelen kan de Gemeente de leverancier die de initiële penetratietest heeft uitgevoerd vragen om een hertest uit te voeren. Hiermee beoogt de Gemeente uitsluitel te krijgen of de maatregelen doeltreffend zijn doorgevoerd en of de risico's tot een volgens de Gemeente acceptabel niveau zijn verminderd.

Een hertest wordt gezien als een 'normale' penetratietest, waarbij voor gunning echter geen minicompetitie wordt uitgevoerd of wordt gekozen voor een volgende leverancier. Ook de hertest start met een intake en het indienen van een Offerte, inclusief plan van aanpak. Veelal zal de Gemeente aan de leverancier vragen om een hertest uit te voeren op een selectie van de eerder door de leverancier gevonden kwetsbaarheden.

9 Vrijwaringsverklaring

De Gemeente verwacht van leverancier(s) dat er door medewerkers van leverancier professioneel en deskundig wordt gehandeld tijdens het uitvoeren van Pen- en hacktesting om verstoringen van de dienstverlening van de Gemeente te voorkomen. Desondanks realiseert de Gemeente zich dat een penetratietest altijd een risico met zich mee brengt en dat er toch een onverwachte verstoring kan optreden.

Leverancier levert bij het indienen van iedere Nadere Offerte een vrijwaringsverklaring in voor het uitvoeren van de betreffende penetratietest met daarin beschreven de risico's die het uitvoeren van de gevraagde penetratietest met zich meebrengt en dat bij ondertekening de Gemeente leverancier vrijwaart van eventuele gevolgschade veroorzaakt door het uitvoeren van de penetratietest.

[einde]