## Bijlage 5 - Programma van Eisen

| A. | Algemene eisen |
|---|---|
| A1. | Middels het indienen van een Inschrijving conformeert Inschrijver zich aan het informatiebeveiligingseisen, welke te vinden zijn onder categorie G van dit document. |
| A2. | Inschrijver is verplicht zich bij de uitvoering van haar werkzaamheden te houden aan relevante geldende wet- en regelgeving. |

| B. | Eisen aan het controleteam |
|---|---|
| B1. | Inschrijver stelt een vast controleteam beschikbaar voor het uitvoeren van de jaarrekening controle. Het controleteam bestaat tenminste uit één (1) partner, een senior manager (accountmanager) en een controleleider. |
| B2. | Inschrijver beschikt over gekwalificeerd en deskundig personeel, die over de voor Nuffic benodigde kennis, vaardigheden en of het vermogen beschikken m.b.t. jaarrekeningrecht, WNT, fiscaliteiten, automatisering en regelgeving rondom projectsubsidies |
| B3. | Bij de uitvoering van onderhavige opdracht dient de Inschrijver zowel bij de tussentijdse/interim controle als bij de eindcontrole, zoveel mogelijk hetzelfde team in te zetten, evenals voor de overige beoogde werkzaamheden.<br>Jaarlijkse wijzigingen in het controleteam worden door de Inschrijver zoveel mogelijk voorkomen. Ingeval van personele wisselingen in het vaste controleteam zorgt Inschrijver voor kennisoverdracht, zodat dit geen invloed heeft op de uitvoering van de controle. Bij vervanging van personen binnen het controleteam wordt een minstens gelijkwaardig persoon aangeboden. |
| B4. | Nuffic heeft de mogelijkheid, bij zwaarwegende redenen, om van de Inschrijver te verlangen dat een lid van het controleteam door een andere persoon wordt vervangen. Deze vervanging mag niet leiden tot andere of hogere kosten voor Nuffic. |

| C. | Eisen aan de dienstverlening |
|---|---|
| C1. | De controlewerkzaamheden bestaan uit:<br>• Controle van de jaarstukken<br>• Daaraan voorafgaande interimcontrole<br>• Verklaringen bij subsidieverantwoordingen<br>• Natuurlijke adviesfunctie |
| C2. | De jaarrekeningcontrole is gericht op het uitbrengen van een onafhankelijke controleverklaring omtrent de getrouwheid van de jaarrekening.<br>Bevindingen worden vastgelegd in een accountantsverslag. De jaarrekeningcontrole vindt plaats in maart/begin april. |
| C3. | Tijdens de interimcontrole zal de accountant zich een oordeel vormen over de kwaliteit van de Administratieve Organisatie/Interne Controle, de geautomatiseerde gegevensverwerking en het financiële beheer. Waarderingsvraagstukken en overige items die richting de jaarrekening bijzondere aandacht vragen worden hierbij benoemd. Bevindingen worden vastgelegd in een managementletter.<br>De interimcontrole vindt plaats in oktober/begin november. |
| C4. | Inschrijver is bekend en gaat akkoord met het verrichten van accountantscontrole op programmaverantwoordingen. De diverse subsidievoorwaarden van de programma's bepalen de reikwijdte van de accountantscontroles. Het gaat hierbij om programma's die Nuffic uitvoert in opdracht van het ministerie van Buitenlandse zaken, OCW en de Europese Commissie. Momenteel zijn dit onderstaande programma's. |

| | |
|---|---|
| | Wanneer er tijdens de looptijd van de overeenkomst sprake is van nieuwe programma's, dan vallen deze programma's tevens binnen de scope van de opdracht.<br>▪ SCOPE (doorlopend t/m controlejaar 2028)<br>▪ MSP IIIB (doorlopend t/m controlejaar 2026)<br>▪ Aanbesteding PO/VO/MBO<br>De controlewerkzaamheden voor programmaverantwoordingen worden uitgevoerd door de Inschrijver. |
| C5. | Inschrijver is in staat om incidentele controlewerkzaamheden te verrichten. Hiervoor vraagt Nuffic een separate offerte op. |
| C6. | Jaarlijks - voorafgaand aan de accountantscontrole - stellen Nuffic en Inschrijver een planning vast. Beide partijen wijken niet af van de definitieve opleverdata binnen deze planning en stellen de benodigde capaciteit beschikbaar. In de planning wordt rekening gehouden met de uiterste aanleverdatum van Nuffic's opdrachtgevers (het Ministerie van OCW/DUS-i, het Ministerie van Buitenlandse Zaken en de Europese Commissie) en de vergaderingen van de Audit Commissie. De aanleverdata en de vergaderdata van de Audit Commissie kunnen jaarlijks wijzigen. |

| **D. Eisen aan de communicatie** | |
|---|---|
| D1. | Evaluatiemomenten zijn onderdeel van de accountantscontrole. Inschrijver plant jaarlijks een overleg in, waarbij de vaste contactpersoon van Nuffic en de controleleider bij elkaar komen om de dienstverlening (op operationeel niveau) te evalueren. |
| D2. | De jaarlijkse evaluatie dient ondersteund te worden door managementinformatie waarin de door de inschrijver bestede uren inzichtelijk zijn, afgezet tegen de geplande uren en gesplitst naar functiecategorieën. Tevens dient eventueel meerwerk naar tijdbesteding en inhoudelijke achtergrond onderbouwd te zijn. |
| D3. | Inschrijver beschikt over een beveiligde digitale omgeving voor het aanleveren van de voor de controle benodigde documenten en stelt deze beschikbaar aan Nuffic. |
| D4. | Ingeval dreigende overschrijding van het overeengekomen honorarium informeert de Inschrijver Nuffic hierover terstond. |
| D5. | De controleleider is verantwoordelijk voor de uitvoering van de dienstverlening en daarnaast het aanspreekpunt voor Nuffic. De controleleider is tijdens kantooruren (09:00 uur - 17:00 uur) beschikbaar voor vragen. Het contact met Nuffic verloopt uitsluitend via de door Nuffic aangegeven contactpersonen. |
| D6. | Uiterlijk 1 maand voor aanvang van de controlewerkzaamheden verstuurt Inschrijver een overzicht met daarop alle documenten die door Nuffic moeten worden aangeleverd voor de controle. |
| D7. | Het concept accountantsverslag wordt door de Inschrijver in principe in april aangeleverd en de concept managementletter in november, tenzij hierover in overleg tussen Inschrijver en Nuffic afwijkende afspraken worden gemaakt. |
| D8. | De managementletter wordt in conceptvorm - na voorafgaand hoor en wederhoor tussen o.a. de controleleider, de senior financieel medewerkers, de teamleider F&C en de manager bedrijfsvoering - voorgelegd aan de audit commissie en aansluitend aan de directeur-bestuurder, respectievelijk het MT. |
| D9. | Indien Nuffic dit wenst, zal Inschrijver in de vorm van minimaal de partner deelnemen aan vergaderingen van toezichthoudende organen. |
| D10. | Inschrijver zal eventueel te verrichten correcties in de concept jaarrekening tijdens het controletraject direct kenbaar maken. |

| E. | Eisen aan de (informatie-)beveiliging van de portal |
|---|---|
| E1. | Inschrijver garandeert dat zij de vertrouwelijkheid van Nuffic data beschermt. De informatie van Nuffic wordt conform de Privacy wetgeving opgeslagen en behandeld. Nuffic gegevens mogen niet voor andere doeleinden gebruikt worden zonder toestemming van Nuffic. |
| E2. | Voor toegangsautorisatie tot de portal gebruikt Inschrijver multi-factor-authenticatie. |
| E3. | De minimum wachtwoordlengte is 8 tekens en het wachtwoord dient een combinatie te zijn van tenminste drie van de volgende categorieën: hoofdletters, kleine letters, cijfers, symbolen. |
| E4. | Informatie over technische kwetsbaarheden van de portal behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden te worden geëvalueerd en passende maatregelen te worden genomen om het risico dat ermee samenhangt aan te pakken. |
| E5. | De portal van de Inschrijver wordt jaarlijks gecontroleerd op technische naleving van beveiligingsnormen en risico's ten aanzien van de feitelijke veiligheid. Dit kan bijvoorbeeld door (geautomatiseerde) kwetsbaarheidsanalyses of penetratietesten. |
| E6. | Security incidenten en inbreuken op de privacy worden zo spoedig mogelijk en tenminste op de dag van ontdekking aan de Security Officer van Nuffic én aan de contactpersoon van Inschrijver bij Nuffic gemeld (en bij diens afwezigheid aan de Manager Bedrijfsvoering). Op verzoek van Nuffic worden relevante logs beschikbaar gesteld. In geval van een (vermoed) informatiebeveiligingsincident is de bewaartermijn van de gelogde incidentinformatie minimaal drie jaar. Nuffic wordt geïnformeerd over welke maatregelen Opdrachtnemer treft en nog gaat treffen. |

| F. | Eisen aan de prijs en facturatie |
|---|---|
| F1. | De tarieven dienen in Prijsinvulformulier ingevuld te worden. |
| F2. | Inschrijver offreert een vast tarief voor de jaarrekeningcontrole, welke bestaat uit de interimcontrole en balanscontrole en resulteert jaarlijks in:<br><br>1. De jaarrekeningcontrole, welke bestaat uit de interimcontrole en de balanscontrole, die resulteert jaarlijks in:<br><br>o De controleverklaring;<br><br>o Een managementletter die een weergave vormt van de uitgevoerde interimcontrole. Hierin legt de accountant zijn bevindingen en aanbevelingen vast t.a.v. de kwaliteit van de Administratieve Organisatie/Interne Controle, de geautomatiseerde gegevensverwerking, waarderingsvraagstukken en het financiële beheer;<br>o Het accountantsverslag. Hierin worden de bevindingen n.a.v. de uitgevoerde balanscontrole weergegeven en de opvolging van de belangrijkste gesignaleerde risico's bij de interimcontrole;<br>o Getekend vaststellingsformulier DUS-I;<br>o Periodiek overleg met Nuffic;<br>o Controle van de verkorte jaarrekening in het Engels;<br>o Eventueel aanvullend vereiste rapportages (bijv. rapport van bevindingen).<br><br>2. De controle van financiële verantwoordingen van programma's.<br>3. Natuurlijke adviesfunctie m.b.t. het functioneren en de kwaliteit van de administratieve organisatie/ interne beheersing (AOIB), bijvoorbeeld (maar niet uitsluitend): adviezen op basis van relevante interne en externe ontwikkelingen, adviezen op basis van controlebevindingen, bevindingen op het gebied van IT-omgeving van Nuffic, adviezen die een logisch gevolg zijn van rapportages van Nuffic en adviezen gericht op versterking van de kwaliteit van de bedrijfsvoering. |

| | |
|---|---|
| F3. | Alle geoffreerde bedragen en (uur)tarieven gelden gedurende de gehele looptijd van de Overeenkomst en zijn inclusief alle bijkomende kosten, maar exclusief BTW. Met bijkomende kosten wordt o.a. bedoeld: Salariskosten, overheadkosten (w.o. huisvesting en salariskosten van niet productief personeel, binnenlandse reis- en verblijfskosten (woon-werkverkeer, inclusief reistijd), parkeerkosten, etc. |
| F4. | De opgegeven tarieven zijn vast in de eerste twee (2) jaar na de ingangsdatum van het contract. Vervolgens mogen de geoffreerde tarieven voor de optionele verlengingsperiode éénmaal per jaar, per 1 juli 2027, worden bijgesteld. Hierbij wordt het CBS-prijsindexcijfers voor zakelijke dienstverlening gehanteerd, mits deze niet hoger is dan 4% (de maximale indexering is 4%). |
| F5. | Aanvullende werkzaamheden (meerwerk) zijn binnen deze overeenkomst uitgesloten, tenzij daartoe voorafgaand aan de uitvoering van de werkzaamheden een gemotiveerd schriftelijk voorstel wordt ingediend, waarin de noodzaak van het meerwerk wordt onderbouwd en waarin een specificatie is opgenomen van het in rekening te brengen meerwerk. Meerwerk moet vooraf worden afgestemd en moet vooraf schriftelijk zijn geaccordeerd door de Manager Bedrijfsvoering. Inschrijver signaleert en treedt in overleg met Manager Bedrijfsvoering wanneer budgetoverschrijding dreigt. |
| F6. | Facturatie vindt plaats onder vermelding van het Purchase Order nummer (PO) dat vooraf wordt aangeleverd door Nuffic. |
| F7. | Facturen worden digitaal, in PDF formaat verstuurd aan facturen@nuffic.nl |
| F8. | Facturatie vindt plaats onder vermelding van een specificatie, waarin de aard van de werkzaamheden wordt beschreven. De kosten worden transparant per onderwerp en het type werkzaamheden verantwoord. |
| F9. | Per factuur kan slechts op één Purchase Order nummer gefactureerd worden. |

| **G. Informatiebeveiligingseisen** | |
|---|---|
| G1. | Dienstverleners ondertekenden een geheimhoudings-verklaring en/of zijn contractueel gebonden aan een geheimhoudingsbepaling |
| G2. | Informatiesystemen waarop Nuffic informatie is of was opgeslagen dienen op zorgvuldige wijze te worden geschoond van rest data volgens algemeen gebruikelijke standaarden voor datavernietiging (Secure Erase). Minimaal dient de data twee keer overschreven te worden met vaste data, één keer met random data en er dient daarna geverifieerd te worden of de overschrijving gelukt is.<br><br>Gegevens(dragers) worden vernietigd zodra het niet meer noodzakelijk is gegevens voor een gerechtvaardigd doeleinde te bewaren. |
| G3. | Alle accounts waarmee toegang tot systemen van Nuffic of systemen met data van Nuffic via het internet, dienen voorzien te zijn van twee-factor authenticatie. Onder gebruikers wordt binnen deze norm verstaan: Nuffic medewerkers, ingehuurde medewerkers, medewerkers van partijen waarmee Nuffic samenwerkt, medewerkers van leveranciers.<br><br>Bij meer dan 10 gebruikers is aansluiten op de AzureAD van Nuffic (en gebruik van Single Sign On) verplicht.<br><br>Alle beheerder- en andere accounts met verhoogde privileges van systemen met toegang tot Nuffic data dienen altijd voorzien te zijn van twee-factor authenticatie. |

| | |
|---|---|
| G4. | Het wachtwoordbeleid wordt geautomatiseerd afgedwongen via de Nuffic Single Sign on oplossing. Indien deze niet wordt gebruikt dienen onderstaande eisen ingevuld te worden m.b.t. wachtwoorden<br>- minimaal 8 tekens<br>- levensduur van maximaal 90 dagen<br>- de twintig laatst gebruikte wachtwoorden mogen niet worden hergebruikt<br>- het wachtwoord dient tekens te bevatten uit minimaal drie van de onderstaande categorieën: hoofletters, kleine letters, cijfers, symbolen, unicode tekens, gebruikersnaam mag geen onderdeel zijn van het wachtwoord.<br>- het aantal mislukte aanmeldpogingen voordat een account geblokkeerd wordt is 3<br><br>Deze eis is van toepassing op gebruikers zoals gedefinieerd in norm 9.4.2 en voor alle klantgroepen. |
| G5. | Er dient versleuteling voor authenticatie, van data transport en opslag te worden toegepast.<br><br>Er mogen enkel cryptografische technieken worden gebruikt die algemeen als veilig zijn beschouwd. Nuffic hanteert hierbij de adviezen van het NCSC-NL als standaard.<br>Webapplicaties mogen geen http only, SSL2.0, SSL3.0 en/of TLS 1.0 verkeer toe te staan.<br>Webapplicaties dienen wel TLS 1.2 connecties of hoger toe te staan.<br><br>Certificaten dienen als veilig te worden beschouwd door de bekende browsers (Edge, Firefox, Chrome, Safari).<br>Alle Nuffic websites dienen een score van minimaal 98% te behalen (en te behouden) via de test op internet.nl<br><br>Het gebruik van self signed certificaten voor communicatie met derden, en voor digitaal ondertekenen van documenten is niet toegestaan. |
| G6. | Logging van alle toegang (inclusief verwijderen en aanpassen) van de data en systemen die worden gebruikt bij het voldoen van dit contract dient beschikbaar te zijn in een bij Nuffic bekende locatie of aangeleverd te kunnen worden (na goedkeuring) voor een periode van minimaal 3 maanden. |
| G7. | Logfiles bevatten minimaal de gebeurtenis, het van en naar IP-adres, waar mogelijk gebruikersnamen, datum, tijd en ondernomen acties. |
| G8. | Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld |
| G9. | Email mag niet gebruikt worden voor het verzenden van gevoelige/bijzondere of grote hoeveelheden data.<br><br>Het verzenden van e-mail dient te versturen via de Exchange omgeving van Nuffic. |
| G10. | Opdrachtnemer moet kunnen aantonen dat zij minimaal voldoen aan ISO 27001/2. Dit kan aangetoond worden middels certificering of een ISAE 3000 (of vergelijkbare) verklaring.<br>Indien de opdrachtnemer geen certificaat kan aantonen dan dient opdrachtnemer middels andere documentatie kunnen aantonen dat de geïmplementeerde maatregelen minimaal conform ISO 27001/2 zijn. |
| G11. | Met opdrachtnemers die als verwerker voor of namens Nuffic persoonsgegevens verwerken, worden verwerkersovereenkomsten gesloten waarin alle wettelijk vereiste afspraken zijn vastgesteld. |

| | |
|---|---|
| G12. | Nuffic moet de mogelijkheid krijgen om, indien nodig geacht, een audit te doen of uit te laten voeren op alle vereisten zoals vermeld in de overeenkomst.<br><br>Bevindingen vanuit audits waaruit niet naleving van de in de overeenkomst opgenomen eisen voor informatiebeveiliging & privacy blijkt dienen onmiddellijk of binnen een met Nuffic afgestemde termijn te worden verholpen. |
| G13. | Nuffic moet de mogelijkheid krijgen om, indien nodig geacht, een audit te doen of uit te laten voeren op alle vereisten zoals vermeld in de overeenkomst.<br><br>Bevindingen vanuit audits waaruit niet naleving van de in de overeenkomst opgenomen eisen voor informatiebeveiliging & privacy blijkt dienen onmiddellijk of binnen een met Nuffic afgestemde termijn te worden verholpen. |
| G14. | Nuffic moet de mogelijkheid krijgen om, indien nodig geacht, een audit te doen of uit te laten voeren op alle vereisten zoals vermeld in de overeenkomst.<br><br>Bevindingen vanuit audits waaruit niet naleving van de in de overeenkomst opgenomen eisen voor informatiebeveiliging & privacy blijkt dienen onmiddellijk of binnen een met Nuffic afgestemde termijn te worden verholpen. |
| G15. | Andere partijen dan onderdeel van de overeenkomst zullen geen data of toegang tot systemen met data van Nuffic ontvangen van de dienstverlener, tenzij hier expliciet en schriftelijke toestemming voor is verkregen vanuit de Information Security Officer van Nuffic. |
| G16. | Indien het de dienstverlener wordt toegestaan om aan derden informatie door te geven dan dient de dienstverlener alle vereisten op gebied van informatiebeveiliging & privacy zoals opgenomen in de overeenkomst vast te leggen in contractueel overeengekomen afspraken met deze derde partij(en). De eerste dienstverlener blijft verantwoordelijk en aansprakelijk voor de juiste naleving van de uitvoering van de contractuele afspraken. |
| G17. | Nuffic moet, in aanvulling op de mogelijkheid een audit uit te (laten) voeren, in staat worden gesteld om gedurende of na informatiebeveiligingsincidenten controles uit te voeren op de naleving van de in de overeenkomst genoemde vereisten. |
| G18. | Het niet voldoen aan de in de overeenkomst opgenomen eisen voor informatiebeveiliging & privacy kan leiden tot beëindiging van het contract. |
| G19. | Leverancier dient Nuffic proactief te informeren over wijzigingen in de organisatie die de dienstverlening gaan raken of ontdekte risico's die de dienstverlening kunnen beïnvloeden.<br><br>Contractueel wordt met leveranciers overeengekomen dat ze ons op van hun belangrijke wijzigingen in hun bedrijfsvoering op de hoogte brengen. |
| G20. | Ieder informatiebeveiligingsincident, data lek of vermoedelijk incident gerelateerd aan de vertrouwelijkheid, integriteit of beschikbaarheid VAN NUFFIC DATA/DIENSTVERLENING zal direct en zonder onnodige vertraging en altijd binnen 24 uur gemeld worden aan de information security officer van Nuffic via (securityofficer@nuffic.nl) |
| G21. | De opdrachtnemer neemt in alle redelijkheid maatregelen om de integriteit en beschikbaarheid van de data te garanderen. De hersteltijd bij calamiteiten is maximaal een week. De opdrachtnemer moet op enige wijze aan Nuffic aantoonbaar kunnen maken dat dit is geborgd en periodiek wordt geverifieerd en geëvalueerd. |
| G22. | Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving. |