BIJLAGE 4 – Selectiecriteria voor SOC-diensten

Inleiding

In deze selectiefase toetsen wij uitsluitend organisatie-eigenschappen: governance, borging, compliance, continuïteit en cultuur. Beschrijf per criterium kort en concreet hoe dit bij u is ingericht en onderbouw dit met organisatie brede bewijsstukken (bijvoorbeeld beleid en procedures, certificaten, organogrammen en audit- of managementreviewverslagen). Klantcases of dienst specifieke prestaties vragen wij in deze fase niet.

Bewijsstukken mogen in samengevatte of geanonimiseerde vorm worden aangeleverd. Vertrouwelijke informatie mag worden weggelaten voor zover de strekking aantoonbaar blijft.

Werk uw antwoord per selectiecriterium (SC) uit in een apart documentgedeelte, maximaal één A4 per selectiecriterium. Verwijs bij elk selectiecriterium naar het relevante bewijs (documenttitel, datum en pagina).

Vul daarnaast in Bijlage 5 (beoordelingsmatrix) per selectiecriterium een korte reflectie (max 150 woorden) op uw antwoord in en ken uzelf een score toe op basis van de hieronder aangegeven scores en kwalificaties. Het beoordelingsteam kan uw reflectie en zelfscore gebruiken als hulpmiddel, bijvoorbeeld in geval van onduidelijkheid.

Het beoordelingsteam zal bij het beoordelen van de selectiecriteria (vanzelfsprekend) ook onderstaande puntenverdeling en bijbehorende kwalificaties hanteren. De beoordelaars van het beoordelingsteam bepalen zelfstandig – en iedere beoordelaar voor zich – de score voor de selectiecriteria.

- 2 punten -> uw antwoord op het selectiecriterium kwalificeert als **GOED**. Uw antwoord sluit geheel aan op onze vraag bij het selectiecriterium. Tevens levert u hier geldig en relevant bewijs voor.
- 1 punt -> uw antwoord op het selectiecriterium kwalificeert als **VOLDOENDE**. Uw antwoord sluit deels maar voldoende aan op onze vraag bij het selectiecriterium. Tevens levert u hier geldig en relevant bewijs voor.
- 0 punten -> uw antwoord op het selectiecriterium kwalificeert als **ONVOLDOENDE**. Uw antwoord sluit niet of onvoldoende aan op onze vraag bij het selectiecriterium.
- 0 punten -> **GEEN** geldig bewijs: zonder geldig en relevant bewijs – los van de kwaliteit van uw antwoord – is de score voor het selectiecriterium 0 punten.

Tot slot: de selectiecriteria hebben geen minimumniveau en worden uitsluitend gebruikt voor onderlinge rangschikking van geschikte gegadigden.

SC1. Governance, kwaliteitsmanagement en interne beheersing

Gewone taal (wat we willen weten):
Wie is waarvoor verantwoordelijk en hoe borgt de organisatie kwaliteit en continue verbetering? We zoeken geen verhalen over dienstverlening, maar bewijs dat de basis op orde is. Denk aan duidelijke rollen, periodiek overleg en afspraken die worden nageleefd en getoetst.

Onze vraag (vakterm-niveau):
Beschrijf de organisatie brede governance voor kwaliteit en risicobeheersing, inclusief: rollen/mandaten en besluitvorming (organogram, RACI), periodieke managementreviews, interne auditfunctie, jaarplan en de PDCA-cyclus (planning, uitvoering, evaluatie, verbetermaatregelen). Licht de scope en geldigheid toe (entiteiten/locaties).

Mee te leveren bewijs (voorbeelden):

- Organogram, RACI of mandaatbeschrijvingen; charters voor overleg/gremia
- Kwaliteits- en risicobeleid; interne auditplanning en voorbeeld van een auditrapport
- Verslag van managementreview inclusief besluiten en verbetermaatregelen
- ISO 9001/ISO 20000 of ISAE/SOC-assurance met scope

SC2. Informatiebeveiliging en privacy-compliance (organisatie breed)

Gewone taal (wat we willen weten):
Is beveiliging en privacy aantoonbaar voor de hele organisatie geregeld? Denk aan toegang tot systemen, beheer van wijzigingen en het borgen van privacy door beleid, processen en toezicht.

Onze vraag (vakterm-niveau):
Toon aan dat een organisatiebreed ISMS en privacy-governance effectief werken. Beschrijf: certificering/assurance (bijv. ISO/IEC 27001 met Statement of Applicability), toegangsbeheer (RBAC), beheer van privileged access inclusief logging en periodieke reviews, change- en configuratiemanagement, key management en secrets management en de privacy-rollen en processen (FG/DPO, DPIA, verwerkingsregister, awareness).

Mee te leveren bewijs (voorbeelden):

- ISO/IEC 27001-certificaat en SoA (of gelijkwaardig); eventueel SOC 2/ISAE-rapport
- Beleid en procedures voor RBAC en privileged access; voorbeelden van periodieke access reviews

- Change-/configuratiebeleid en voorbeeld van CAB-notulen of change-registraties
- Privacy-governance: aanstelling FG/DPO, DPIA-procesbeschrijving, verwerkingsregister, trainingsoverzicht

SC3. Dataverantwoordelijkheid, EU/EER-residency en ketenbeheersing

Gewone taal (wat we willen weten):
We willen exact weten waar data zich bevindt, wie erbij kan, welke subverwerkers worden ingezet en hoe u garandeert dat onze data binnen de EU/EER blijft en niet blootstaat aan buiten EU-wetgeving of extraterritoriale risico's. Daarnaast moet worden aangetoond dat u voldoet aan de Europees vastgestelde soevereiniteitsmaatregelen, waaronder de *Sovereignty Effectiveness Assurance Levels (SEAL)* uit het EU Cloud Sovereignty Framework van de Europese Commissie of een gelijkwaardig/vergelijkbaar niveau van borging.

Onze vraag (vakterm-niveau):
Beschrijf hoe uw organisatie EU/EER residentie, dataverantwoordelijkheid en ketenbeheersing borgt. Licht toe:

- waar data wordt verwerkt, opgeslagen en gerepliceerd (EU/EER),
- hoe subverwerkers worden geselecteerd en beheerst,
- hoe u maatregelen heeft ingericht die verwerking binnen de EU/EER waarborgen, risico's op extraterritoriale toegang mitigeren en EU-controle over data en encryptiesleutels borgen, en in hoeverre deze maatregelen aansluiten bij SEAL niveau 2 van het EU Cloud Sovereignty Framework (EC, v1.2.1 – 2025) of een gelijkwaardig niveau van borging. Een formele SEAL-certificering of afgerond SEAL-assessment is niet vereist.
- Hoe u exit/overdrachtsprocedures borgt.

Mee te leveren bewijs (voorbeelden):

- Datastroom- en locatieoverzicht (data mapping) met classificatie en opslaglocaties
- Actueel subverwerkersregister plus due-diligencecriteria en voorbeeld van contractuele waarborgen.
- SEAL assessments of mappings die aantonen welke Sovereignty Objectives en SEAL niveaus worden gehaald.
- Documentatie van maatregelen tegen extraterritoriale toegang (zoals juridische analyses, technische isolatiemaatregelen, splitcontrol, EU only key custody).
- Exit- en dataverwijderingsprocedures inclusief verantwoordelijkheden, termijnen en audit-mogelijkheden.
- Rapportages of audits die uw dataverantwoordelijkheid, ketencontrole en EU/EER residentie aantonen.

SC4. Organisatorische continuïteit, capaciteit en veerkracht

Gewone taal (wat we willen weten):
Kan de organisatie doorwerken bij tegenslag? We kijken naar brede continuïteit: voldoende mensen, vervanging, kennisborging en geteste plannen voor verstoringen.

Onze vraag (vakterm-niveau):
Toon aan dat business continuity management (BCM) en workforce zekerheid zijn ingericht en periodiek getest. Beschrijf: BCM-beleid en governance, uitgevoerde BIA's, oefen- en testprogramma en opvolging van leerpunten, capaciteitsplanning (bezetting, piek/ziekte), vervangings- en achtervangprincipes en kennisborging (documentatie/overdracht).

Mee te leveren bewijs (voorbeelden):

- BCM-beleid en governance; samenvatting van BIA's
- Rapporten van oefeningen en tests met logboek van verbeteracties en status
- Capaciteits- en roosterprincipes en achtervang-/vervangingsbeleid
- Voorbeelden van kennisbanken, overdrachtsformats of runbook-structuren

SC5. Integriteit, screening en compliance-cultuur

Gewone taal (wat we willen weten):
We willen werken met een integere organisatie. Dat betekent: (her)screening van medewerkers, duidelijke gedragsregels, functiescheiding waar dat hoort en een veilige meldcultuur.

Onze vraag (vakterm-niveau):
Beschrijf hoe integriteit en naleving structureel zijn geborgd. Neem hierin mee pre- en her-screening (scope, frequentie, dossiervorming), gedragscode en anti-corruptie/COI-regelingen, principes van functiescheiding en autorisatie, beveiligde meldkanalen (speak-up), onderzoek en opvolging van meldingen, en training/awareness met dekking en periodiciteit.

Mee te leveren bewijs (voorbeelden):

- Screeningsbeleid plus voorbeeld van geanonimiseerde screeningsbewijzen of een auditverslag
- Gedragscode, anti-corruptie- en COI-beleid; voorbeeld van COI-registratie of attestatie
- Autorisatie- en functiescheidingsprincipes (beleid/proces); steekproef van autorisatiebeoordelingen
- Speak-up/meldproces, rapportage over meldingen (geanonimiseerd) en opvolging; awareness-statistieken

SC6. Kennisontwikkeling, professionalisering en adaptief vermogen

Gewone taal (wat we willen weten):
De wereld verandert snel. We willen zien dat de organisatie gericht investeert in kennis en een vast proces heeft om nieuwe typen data of technologie gecontroleerd en veilig in te voeren.

Onze vraag (vakterm-niveau):
Geef aan hoe de organisatie leert en innoveert. Beschrijf: L&D-strategie en -budget, opleidings- en certificeringsprogramma's en skill mapping, communities of practice en kennisdeling, en het gestandaardiseerde proces voor intake, risicobeoordeling, besluitvorming en borging bij introductie van nieuwe datatypen en technologieën. Neem voorbeelden van 'lessons learned' op.

Mee te leveren bewijs (voorbeelden):

- L&D-/opleidingsplan, skill matrix en certificeringsoverzichten
- Beschrijving van intake- en risicobeoordelingsproces voor nieuwe data/technologie plus voorbeeld van documentatie
- Voorbeelden van verbeter- of innovatie-initiatieven met evaluaties (post-implementation review)

SC7. Duurzaamheid en maatschappelijk verantwoord ondernemen (MVO)

Gewone taal (wat we willen weten):
We vragen om zicht op beleid en aanpak rond duurzaamheid en MVO, inclusief energiegebruik in IT/hosting en hergebruik of verantwoorde afvoer van hardware.

Onze vraag (vakterm-niveau):
Toon aan dat duurzaamheids- en MVO-doelstellingen zijn vastgesteld, gemonitord en verantwoord. Beschrijf governance, doelen en KPI's, maatregelen voor energie-efficiëntie en e-waste/re-use, en (indien van toepassing) externe assurance of certificering.

Mee te leveren bewijs (voorbeelden):

- ESG-/MVO-beleid, doelstellingen en recente rapportage (bijv. CO_2-footprint of energieverbruik)
- Maatregelen voor energie-efficiëntie (bij IT/hosting) en e-waste/re-use-proces
- (Indien aanwezig) ISO 14001-certificaat of onafhankelijke assurance

SC8. 24×7 monitoring van open-source infrastructuren

Gewone taal (wat we willen weten):
Onze organisatie maakt intensief gebruik van een breed open-source ecosysteem. We zoeken daarom een dienstverlener die aantoonbaar in staat is om open source infrastructuren, platformen en security-componenten professioneel en 24×7 te monitoren, analyseren en ondersteunen. Het gaat hierbij niet om één specifieke technologie, maar om het vermogen om complexe, heterogene OSS-omgevingen structureel te operationaliseren binnen een SOC.

Onze vraag (vakterm-niveau):
Gezien het OSS-karakter van de omgeving is ervaring met 24×7 OSS-monitoring een kritische succesfactor. Toon aan de hand van ten minste één referentie aan dat uw SOC ervaring heeft met het ondersteunen van open-source infrastructuren en platformen binnen een 24×7 detectie- en responsoperatie. Beschrijf hoe de dienstverlening bij de referent is ingericht en ga daarbij in op de onderstaande aspecten. De genoemde OSS-componenten zijn indicatief en niet limitatief, beoordeeld wordt in hoeverre de referentie de relevante ervaring en volwassenheid van uw SOC aantoont:

• Welke typen OSS-componenten bij de referent worden ondersteund (voor zover van toepassing), zoals bijvoorbeeld: hypervisors, networking (DNS, DHCP, load balancing), proxy's en gateways, VPN, IAM/IAP, observability (logging, metrics, tracing), Infrastructure as Code (IaC), service discovery, API-gateways, open-source databases, repositories/artifact registries, secrets management, configuration management, data orchestration en analytics.
• Hoe OSS-telemetrie (logs, metrics, traces) wordt verzameld, genormaliseerd en gebruikt voor detectie, correlatie en triage.
• Hoe continuïteit van OSS-expertise is geborgd (o.a. 24×7 bezetting, achtervang, documentatie en specialistische expertise).
• Hoe OSS-kennis en vaardigheden worden onderhouden (bijv. skill-matrices, opleidingen, certificering en kennisdeling).
• Hoe nieuwe OSS-technologieën worden geonboard, getest en geïntegreerd in het reguliere SOC-proces.

Mee te leveren bewijs (voorbeelden):

De gegadigde levert relevant en beknopt bewijs dat betrekking heeft op de opgegeven referentie. Onderstaande opsomming is indicatief en niet limitatief. Gegadigde kan volstaan met een selectie van stukken die gezamenlijk de gevraagde ervaring en organisatorische volwassenheid aantonen. Gelijkwaardige vormen van bewijs worden geaccepteerd.

• Overzicht van typen open-sourcecomponenten die bij de referent worden ondersteund.
• Skill-matrix en opleidings- en/of certificeringsaanpak gericht op OSS-technologieën.

• Procesbeschrijving voor onboarding, normalisatie en integratie van OSS-telemetrie.
• Voorbeeld(en) van detectieregels, correlatielogica of playbooks gebaseerd op OSS-telemetrie.
• Voorbeeld(en) van rapportages of dashboards waarin OSS-platformen zijn opgenomen.
• Beschrijving of documentatie waaruit 24×7 monitoring en achtervang voor OSS-bronnen blijkt.
• Voorbeeld van de onboarding van een nieuw OSS-component (bijv. registratie, test, change en evaluatie).

Beoordeling van SC8 vindt plaats op basis van de mate waarin de referentie de relevante ervaring, diepgang en organisatorische volwassenheid van de SOC-dienstverlening aantoont.

Weging van de selectiecriteria

De weging wordt uitgedrukt in een factor die vermenigvuldigd wordt met de score. Een factor 8 geeft aan dat het betreffende selectiecriterium 8x zwaarder weegt dan een selectiecriterium met een weging factor 1.

SC1 - factor 1
SC2 - factor 1
SC3 - factor 3
SC4 - factor 2
SC5 - factor 1
SC6 - factor 2
SC7 - factor 1
SC8 - factor 8