centrum informatiebeveiliging
en privacybescherming

Handreiking SPINK

Informatieveiligheid geborgd in contracten

April 2020 [v1.1]

Titel	Handreiking SPINK (Security Proof INKopen) Informatieveiligheid geborgd in contracten
Opdrachtgever	Centrum Informatiebeveiliging en Privacybescherming
Status	Versie 1.1 * Becommentarieerde praktijk
Auteurs en reviewers	Jeroen Gaiser (Rijkswaterstaat), Willem Blom (Supply Value) Update versie 1.1 CIP
Bijdrage van	met medewerking van de leden van de Werkgroep Uniformering inkoopprocessen (zie Colofon)
Datum	april 2020
Filenaam	202004 Handreiking SPINK

Considerans

Met het doel informatie-uitwisseling en kennisdeling te bevorderen wil CIP onder andere 'good practices' ter beschikking stellen. Dit kunnen praktijkvoorbeelden zijn, handreikingen voor beleid, beschrijvingen van de stand van zaken in bepaalde ontwikkelingen, en dergelijke. De herkomst is van oorsprong een reflectie op een onderwerp door mensen uit de CIP-netwerk, maar het kunnen ook notities zijn uit de praktijk van de CIP-organisaties die zonder verder commentaar worden gepubliceerd. De kern is dat de bijdragen altijd zijn gebaseerd op de expertise van de opstellers en deelnemende reviewers en/of het idee dat wat in één organisatie goed werkt, ook voor andere organisaties nuttig kan zijn. Soms is het resultaat dus de uitkomst van een groepsproces en in andere gevallen wordt iets 'as is' ter kennisneming of overname aangeboden. CIP heeft categorieën geformuleerd waarmee reikwijdte, intentie, status en/of draagvlak van CIP-publicaties wordt aangegeven. Een nadere uitleg hiervan staat op www.cip-overheid.nl.

De CIP-documenten hebben geen ander doel dan kennisoverdracht en reflecteren niet noodzakelijk de opvattingen van alle contribuanten, CIP-deelnemers en/of alle CIP-partijen. Publicatie vindt plaats op zowel de openbare website www.cip-overheid.nl als de besloten community site cip.pleio.nl.

Voorwoord

Wanneer de overheid marktpartijen contracteert voor de levering van digitale diensten wordt regelmatig het volledige eisenpakket waaraan de overheid moet voldoen opgelegd aan de leveranciers. Dit eisenpakket zal echter slechts voor een beperkt deel gelden en beïnvloedbaar zijn voor leveranciers. Voor dit dilemma is een werkwijze ontwikkeld waarin opdrachtgevers binnen de overheid heldere, toetsbare en op maat gesneden criteria kunnen opnemen en borgen in bestaande contractprocessen. Dit maakt contractteksten in hoge mate voorspelbaar en herbruikbaar in nieuwe aanbestedingen. Dat is winst voor zowel opdrachtgevers als leveranciers.

Colofon

Versie 1.0 van dit stuk is gepubliceerd op 15 april 2018. Het is het product van Werkgroep Uniformering inkoopprocessen, waaraan de volgende mensen hebben meegewerkt:

Keyvan Ajamlou	Rijkswaterstaat
Patrick van den Berg	Rijkswaterstaat
Willem Blom	Supply Value
Leonie Bos	IUC-Noord
Jeroen Gaiser	Rijkswaterstaat
Remco Gulickx	ICTU
Donald Heertje	Rijksoverheid
Ad Kint	CIP
Gijs Koolen	ACM
Ralf Koops	Rijksoverheid
Eveline van Petten	Ministerie van Binnenlandse Zaken
Tady Slebioda	CIP
Gerrit Tijman op Smeijers	UWV
Jaap Visser	Rijkswaterstaat

Managementsamenvatting

De overheid heeft de ambitie om vooruitstrevend en efficiënt ICT in te zetten om burgers en bedrijfsleven zo optimaal mogelijk te ondersteunen. Spil in deze strategie is publiek-private interactie bij het leveren van adequate oplossingen. Informatiebeveiliging (IB) is onlosmakelijk verbonden met het leveren van deze ondersteunende (digitale) diensten. Binnen overheids-organisaties zijn kaders zoals de BIO opgesteld om de IB op een juist niveau te borgen.

Als de overheid aan marktpartijen vraagt om digitale diensten te ontwikkelen, zijn deze kaders niet zonder meer op te leggen. Ze moeten vertaald worden naar de specifieke uitbestedings-vraag die voorligt.

Voor dit dilemma is een werkwijze ontwikkeld waarin opdrachtgevers binnen de overheid heldere en toetsbare criteria kunnen opleveren die meegenomen kunnen worden in bestaande contractprocessen: de handreiking Security Proof Inkopen (SPINK). Deze werkwijze maakt het mogelijk om de kloof tussen IB en contractmanagement te overbruggen door IB kwaliteitsaspecten te vertalen in contracttermen. Deze handreiking is aangevuld met de 'Wizard SPINK', waarmee een gemakkelijke manier wordt geboden om de werkwijze toe te passen.

Deze werkwijze maakt het ook mogelijk om IB uniform en herhaalbaar uit te besteden. Hierdoor wordt het uitbestedingsproces gestroomlijnd en wint het aan consistentie en transparantie. Binnen de organisatie is hiermee een gestandaardiseerde werkwijze mogelijk, waardoor gelijksoortige uitvragen gebruik kunnen maken van de data van eerdere trajecten.

Dit document legt een breed gedragen basispakket van eisen voor, waaraan een organisatie haar eigen specifieke eisen kan toevoegen. Deze basis zorgt voor een 'vliegende start'. Juiste implementatie van deze werkwijze leidt er toe dat de kwaliteit van uitvragen op het aspect IB vergroot wordt, terwijl de kosten afnemen naarmate de methode meer wordt ingezet.

De doelgroep voor dit document omvat zowel aanbestedende diensten (inkopers, contractmanagers, IB-functionarissen) als marktpartijen (de leveranciers). Binnen aanbestedende diensten is deze werkwijze geschikt voor zowel rijksoverheidsdiensten als gemeentes maar deze kan ook voor opdrachtgevers buiten de overheid zijn nut hebben.

De toegevoegde waarde van deze werkwijze bestaat uit 5 pijlers, die voordelen opleveren voor zowel de opdrachtgever als de opdrachtnemer:

- Uniformering van de werkwijze tussen verschillende organisaties;
- Voorspelbaar & goed opdrachtgeverschap;
- Herleidbaarheid eisen;
- Sturing op IB-beheersdoelen;
- Mogelijkheid tot herhaling.

Inhoudsopgave

1 Inleiding

Dit document heeft als hoofddoelgroep medewerkers die verantwoordelijk zijn voor informatiebeveiliging, contractmanagement en inkoop. Secundaire doelgroepen zijn mensen verantwoordelijk voor audits en andere betrokken partijen bij uitbestedingen en informatiebeveiliging (IB). Het doel van deze handreiking is de inpassing en toepassing van de generieke werkwijze voor informatiebeveiliging in contracten. Dit document behandelt eerst een terugblik over hoe deze werkwijze tot stand is gekomen.

Na de beschrijving van de aanleiding wordt het totstandkomingsproces van dit product toegelicht. Hierin wordt behandeld hoe de werkwijze van Rijkswaterstaat is veralgemeniseerd tot een voor iedereen bruikbare handreiking en wizard. In 2.3.4 wordt de SPINK-werkwijze toegelicht. We besluiten met een voorbeeld van het toepassen van deze werkwijze.

1.1 Begrippen en rollen

Hieronder volgt een lijst met een toelichting op begrippen die in dit document een rol spelen. De processen zijn uiteraard per organisatie verschillend en er moet per organisatie dan ook bekeken worden door wie deze worden ingevuld.

Term	**Uitleg**
Bestek	De complete set aan inkoopdocumenten die worden meegegeven bij een aanbesteding.
Aanbesteding	Het proces van specificeren, selecteren en contracteren van het uitbestede product of dienst.
Eisen	De eisen zijn minimum specificaties die zijn gesteld door de aanbestedende dienst. Dit zijn minimum eisen waaraan voldaan moet worden.
Algemene Voorwaarden	Voorwaarden die van toepassing zijn op de overeenkomst zoals ARBIT, ARVODI of algemene inkoopvoorwaarden.
VSP	Vraag Specificatie Proces. Alle eisen die betrekking hebben op de processen.
VSE	Vraag Specificatie Eisen. Alle eisen die betrekking hebben op de systemen.
Kader & Richtlijnen	Een set aan regels waarbinnen gehandeld moet worden.
AD	Aanbestedende Dienst. Dit is een dienst die verplicht is tot het houden van aanbestedingen en is veelal een (semi)publieke organisatie.
BIO-eis	Een control die genoemd wordt binnen de BIO.
ISO	De Internationale Organisatie voor Standaardisatie. Deze organisatie heeft meerdere standaarden ontworpen. Alle standaarden door de ISO worden aangeduid met ISO-*nummer*. In dit document zal vooral worden verwezen naar de ISO-27001 en 27002, de standaard voor informatiebeveiliging.

Contractmanagement	Alle activiteiten die door de Opdrachtgever in zowel de contractvoorbereiding als contractrealisatie worden uitgevoerd en die erop gericht zijn om zeker te stellen dat de eisen uit het contract (de overeenkomst) worden nagekomen en dat de risico's voor de opdrachtgever aantoonbaar beheerst worden.
Inkoop	Tijdens het inkoopproces stelt de verantwoordelijke medewerker inkoopdocumenten op en wordt het aanbestedingstraject begeleid. Eventueel verzorgt de proceseigenaar ook de contractuele zaken in het proces. Indien er een aparte juridische afdeling is binnen inkoop kan dit ook worden uitbesteed.
Project management	De verantwoordelijke voor het project management is de verantwoordelijke voor het aan te besteden product/dienst. Deze persoon is eindverantwoordelijke voor het hele traject en zorgt voor de samenwerking tussen de verschillende organisatieonderdelen.
IB	De verantwoordelijke voor IB geeft advies over de informatie beveiligingseisen voor het aan te kopen product/dienst. Hij zal de kwetsbaarheden en risico's duidelijk maken voor het product/dienst en verstrekt het advies al dan niet met verplichte betrokkenheid aan het project / de beheerorganisatie.

2 Het ontstaan en nut van generieke werkwijze IB in contracten

Dit hoofdstuk behandelt de ervaringen om IB in contracten te borgen en de noodzaak om hier een werkwijze in te hanteren. Dit hoofdstuk heeft tot doel om de aanleiding inzichtelijk te maken, zodat helder wordt hoe deze werkwijze inpasbaar is in uw organisatie. Door het doel helder te maken, is de logica van de werkwijze beter te begrijpen en is het inpassen van de werkwijze in de organisatie overzichtelijker.

2.1 Historie van de vraag

Alle overheidslagen hanteren de BIO als baseline voor de inrichting van hun informatiebeveiliging. Deze baseline is afgeleid van de ISO 27002 standaard en bevat zeer veel controls.
Bij uitbestedingen zien we in hoofdzaak de volgende varianten:

1. In de uitbesteding wordt aangegeven dat 'er aan de BIO moet worden voldaan';
2. In de uitbesteding wordt aangegeven dat de te leveren dienst 'ISO compliant', moet zijn;
3. In de uitbesteding wordt een lijst aangegeven van controls die geïmplementeerd moeten worden.

De varianten 1 en 2 zijn makkelijk als tekst op te nemen, maar zijn erg onduidelijk over de daadwerkelijke invulling van de controls. Er is niet duidelijk welke controls op welk deel van de te leveren dienst van toepassing zijn en wat de criteria zijn wanneer iets 'goed' is. Daarnaast bevat variant 1 controls die specifiek zijn voor de betreffende organisatie en onmogelijk door een

opdrachtnemer in de private sector door te voeren zijn, nog los van de vraag of ze überhaupt zinvol zijn als vraag aan de opdrachtnemer. Een voorbeeld hiervan is dat een opdrachtgever voorschrijft hoe de IB organisatie eruit moet zien van de opdrachtnemer.

Scenario 3 heeft als voordeel dat duidelijk is welke controls nodig zijn, maar er is dan nog steeds niet helder gesteld wanneer een control 'juist' is ingevuld. Daarnaast is deze methode erg arbeidsintensief voor de opdrachtgever en garandeert niet dat bij nieuwe dreigingen of kwetsbaarheden de controls nog steeds dekkend zijn voor het risico.

Samengevat: voor het scherpstellen van de vraag aan de opdrachtnemer en het meetbaar maken van het antwoord van die opdrachtnemer, is een baseline (de BIO) niet het goede middel.
Voor de drie genoemde varianten geldt dat het taalgebruik in de IB modellen ongeschikt is voor juridisch bindende documenten.

2.2 **De oplossing van Rijkswaterstaat**

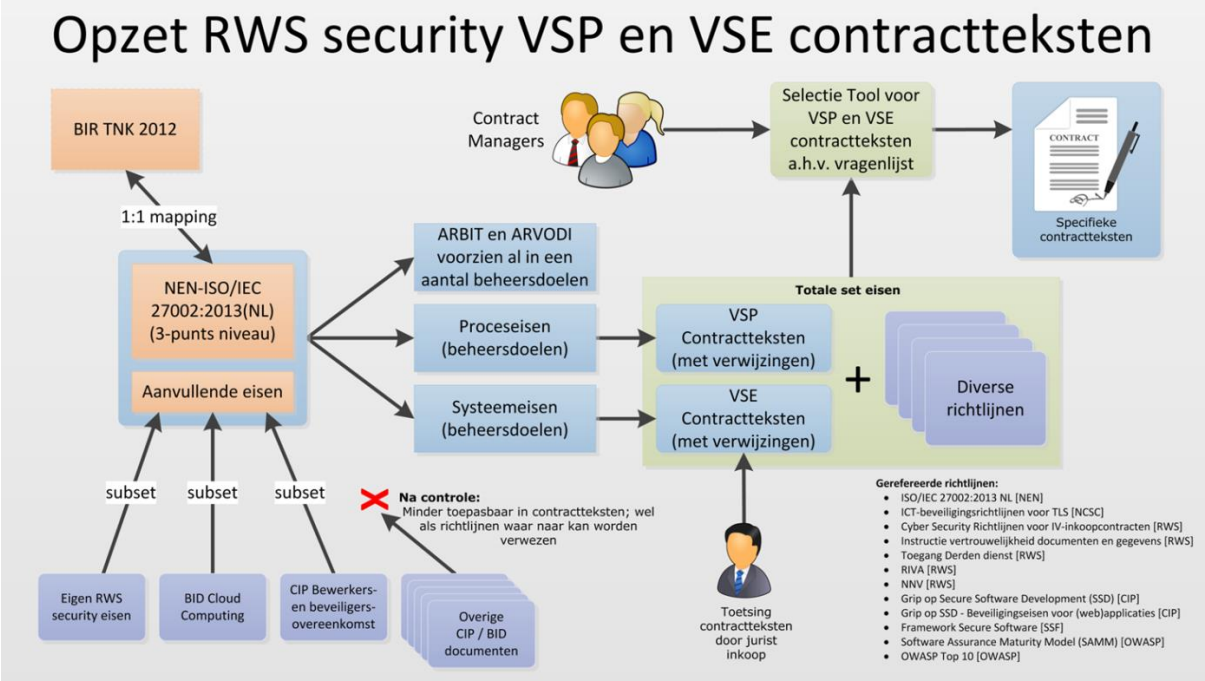
Bij Rijkswaterstaat is voor deze uitdaging binnen het Industriële Automatiseringsdomein (IA) een werkwijze gekozen om IB criteria te vertalen in contractteksten. De IA-markt kent IB-kaders zoals ISO niet. Het was daarom essentieel om deze helder en gespecificeerd uit te vragen. Deze werkwijze, weergegeven in figuur 1, is erg succesvol en is daarom ook vertaald zodat deze tevens toegepast kan worden voor standaard IV-diensten.

Een belangrijk verschil met de klassieke manier van uitvragen, is dat de IB eisen worden gebracht als *beheersdoelen*. Deze manier van uitvragen is noodzakelijk door de lange looptijden van contracten in de IA markt (>10 jaar), waardoor dynamische onderwerpen, zoals IB, toekomstbestendig moeten worden geformuleerd. Door te beschrijven welke risico's moeten worden gemitigeerd, wordt de juiste beveiliging van informatie beter geborgd dan door concrete controls te noemen.

In de eerste stap is vastgesteld welke set eisen voor Rijkswaterstaat de baseline vormt (zie figuur 1), en welke documenten er zijn om richting te geven aan hoe de controls moeten worden ingericht. Daarna is bepaald in welke mate de ARBIT (Algemene Rijksvoorwaarden Bij IT-overeenkomsten) en ARVODI (Algemene Rijksvoorwaarden Voor het Verstrekken van Opdrachten tot het verrichten van Diensten), die al standaard gelden bij aanbestedingen, redundantie kent met verzamelde eisen in stap 1. Aangezien deze eisen al geborgd zijn, zijn deze eisen niet opgenomen in de VSP/VSE. Het is ook mogelijk om de GIBIT (Gemeentelijk Inkoopvoorwaarden Bij IT) te gebruiken binnen gemeentelijke aanbestedingen. Deze is op een paar punten anders dan de ARBIT maar dit zal geen noemenswaardige problemen geven.

Hieronder zijn de eisen opgesplitst in proceseisen en techniek eisen. De proceseisen zijn geborgd in de Vraag Specificatie Proces (VSP) en de technische eisen in de Vraag Specificatie Eisen (VSE). In deze VSP/VSE wordt verwezen naar specifieke richtlijnen die SMART maken welke criteria er zijn voor een beheersdoel.

Ondersteunend aan deze werkwijze is ook een selectietool gemaakt, die het sneller en eenvoudiger maakt om een relevante selectie te maken voor een specifieke uitvraag uit de complete set VSP/VSE. Deze tool kan gebruikt worden door de contractmanagers om de relevante IB teksten te selecteren.



Figuur 1 Opzet werkwijze Rijkswaterstaat *VSP/VSE. Bron* Rijkswaterstaat

2.3 **Toegevoegde waarde; de Businesscase**

Deze paragraaf beschrijft een vijftal effecten van de werkwijze, die het proces gemakkelijker maken voor zowel de aanbestedende dienst als de opdrachtnemer. Van elk effect wordt aangegeven wat het voordeel is voor de marktpartij en voor de aanbestedende dienst. De voordelen komen het best tot hun recht als er niet enkel wordt opgelegd door de aanbestedende dienst (Angelsaksisch model) maar als de dialoog wordt gevoerd met leveranciers (Rijnlands model).

2.3.1 *Uniformering werkwijze tussen gelijksoortige organisaties*

AD: In Nederland zijn tientallen Aanbestedende Diensten (AD'en) die alle IT-gerelateerde inkopen doen. Deze AD'en hebben verschillende manieren van werken en selecteren vaak zonder duidelijke systematiek welke eisen wel of niet van toepassing zijn. Door een uniforme werkwijze te gebruiken is het gemakkelijker om enerzijds te switchen tussen de verschillende AD'en en anderzijds knowhow te verkrijgen van collega's binnen een andere organisatie.

Markt: Ook voor de aanbodzijde is het belangrijk een uniform proces te hebben. Opdrachtnemers kunnen daardoor gemakkelijker zien wat gevraagd wordt en wat de rationaliteit is van bepaalde eisen. Het is voor opdrachtnemers ook gemakkelijker om niet bij elke AD steeds weer nieuwe

teksten te moeten doorlezen, maar op voorhand al duidelijkheid te hebben omtrent de eisen die gesteld kunnen worden.

2.3.2 *Voorspelbaar & goed opdrachtgeverschap, positief beeld naar opdrachtnemers*

AD: Door de in dit document beschreven werkwijze te volgen, is de AD in staat een betere afweging te maken voor de proces- en systeemeisen, die als input dienen bij de strategiebepaling tussen inkoop, IM en de interne opdrachtgever.

Markt: Voorspelbaar en goed opdrachtgeverschap is essentieel voor opdrachtnemers. Opdrachtnemers moeten kunnen verwachten dat er goed is nagedacht over de eisen en wensen. Met het gebruik van een duidelijke en transparante methodiek als deze is het voor opdrachtnemers beter in te schatten of er over eisen is nagedacht.

2.3.3 *Herleidbaarheid eisen/transparantie*

AD: Het is gemakkelijker om contractteksten en beheersdoelen aan te passen indien een bovenliggend eisenkader wordt toegepast, doordat het selectief aanpassen van eisen mogelijk is.

Markt: Door de beschreven systematiek is het voor alle gevraagde proces- en systeemeisen duidelijk wat de achterliggende gedachte is en waarop deze eisen zijn gebaseerd. De AD kan besluiten om de ingevulde tool mee te sturen zodat de Markt de rationale van de opdrachtgevers kan doorgronden.

2.3.4 *Sturen op IB beheersdoelen i.p.v. 'afvinken' framework*

AD: In plaats van het afvinken van een lijst met BIO-eisen stuurt op AD op de beheersdoelen van dit framework. Met deze methodiek kan gestuurd worden op de beheersdoelen en wordt de BIO niet enkel meer gezien als een 'papieren tijger'.

Markt: De leverancier hoeft niet te voldoen aan alle normen binnen de BIO, maar alleen aan de eisen die door de AD zijn gesteld, zoals die van toepassing zijn op deze aanbesteding.

2.3.5 *Herhaalbaar*

AD: Bij een nieuwe uitvraag door de AD kunnen de teksten van overeenkomstige eisen hergebruikt worden. Daarmee wordt aan efficiency gewonnen.

Markt: Aangezien de aanbestedingen uniform zijn opgezet, kan gemakkelijk gecontroleerd worden of wordt voldaan aan de eisen. Er hoeft niet bij elke aanbesteding gekeken te worden waaraan de contractteksten refereren, aangezien deze bekend en uniform zijn. Daardoor kan makkelijker geconstateerd worden of de aangeboden producten aan alle eisen voldoen.

3 Totstandkoming generieke werkwijze

Dit hoofdstuk beschrijft hoe de werkwijze van Rijkswaterstaat gegeneraliseerd is tot een breder toepasbare methode.

3.1 Rijkswaterstaat context

In de VSP/VSE zijn Rijkswaterstaat -specifieke kaders en eisen opgenomen, overigens met uitzondering van het deel dat al in de ARBIT/ARVODI geborgd is. De Rijkswaterstaat werkwijze is gepresenteerd op de CIP Practitioner Community (PRACO) van 3 maart 2017. De aanwezige deelnemers achtten het instrument geschikt voor breder gebruik, waarop CIP de uitdaging heeft opgenomen om de werkwijze te generaliseren en breed te ontsluiten.

3.2 Werkgroep

Binnen het CIP-netwerk werd een brede werkgroep geformeerd en met deze klus belast. Grofweg heeft de werkgroep de volgende fasen doorlopen:

1. Vaststellen van het op te leveren product en het doornemen van de Rijkswaterstaat methodiek;
2. Het ontdoen van de methode van Rijkswaterstaat -specifieke zaken, waarbij ook de relevantie van de verschillende eisen werd getoetst;
3. Reviewronde op de contractteksten en de tooling;
4. Toets en review bij de bredere groep van PraCo-leden;
5. Vaststelling van het opgeleverde document en uitrol in de CIP community.

Na elke werkgroep-sessie werden acties uitgevoerd en documenten opgesteld. Deze acties werden steeds uitgevoerd door meerdere leden binnen de werkgroep van verschillende organisaties, waarbij ook de achterban werd ingeschakeld voor specifieke onderwerpen zoals juridische teksten.

3.3 Generalisatie

In het proces van generalisatie zijn de teksten ontdaan van specifieke Rijkswaterstaat -namen, termen, etc. en vervangen door algemene begrippen, generieke functietitels ed.

Specifieke aanvullende Rijkswaterstaat -eisen zijn verwijderd. In plaats daarvan is een werkwijze opgesteld voor het toevoegen van organisatie-specifieke aanvullende eisen. Ieder organisatie kan dus eigen eisen toevoegen aan de lijst.

4 Implementatie en werkwijze VSP/VSE

Dit hoofdstuk gaat in op de implementatie van de werkwijze. Hiervoor wordt eerst toegelicht hoe de werkwijze in twee fasen kan worden toegepast. Daarna wordt aangegeven hoe aanvullende eisen ten opzichte van de basisset kunnen worden toegevoegd. Daarna wordt het Excel sheet, het hulpmiddel dat de methode ondersteunt, besproken en wordt afgesloten met een korte beschrijving van de rollen die betrokken zijn bij deze werkwijze.

4.1 Toepassing VSP/VSE

Elke organisatie heeft eigen processen, een eigen cultuur en omgang met haar leveranciers. Het is dan ook belangrijk om de werkwijze in te bedden in de eigen processen. Bij het borgen van IB-eisen in externe dienstverlening, spelen twee expertises een belangrijke rol: contractmanagement en informatiebeveiliging. De werkwijze zorgt ervoor dat deze twee partijen op een wederzijds begrijpelijke manier kunnen samenwerken.

Het is de bedoeling dat de werkwijze in gezamenlijkheid wordt toegepast, waardoor beide partijen elkaar beter herkennen en ondersteunen in het inkoopproces. Het is aan te bevelen deze werkwijze eerst in één of meerdere pilots toe te passen, zodat ervaring kan worden opgedaan en onvolkomenheden in de implementatie kunnen worden gladgestreken. Het is belangrijk in deze pilots ook open te staan voor de feedback van leveranciers.

4.1.1 *Fase I: aanpassen werkwijze aan organisatie*

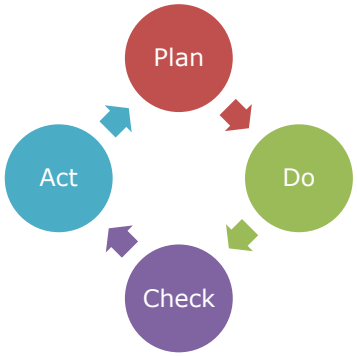
De werkwijze in dit document is een algemene opzet, gebaseerd op de ISO 27001/2. De meeste overheidsorganisaties hebben aanvullende eisen. In 4.2 is omschreven hoe deze aanvullende eisen kunnen worden meegenomen in de werkwijze. Ook kan het zijn dat er richtinggevende documenten zijn voor de invulling van bepaalde eisen. Bijvoorbeeld dat voor de inrichting van encryptie gebruik gemaakt wordt van de whitepaper van het NCSC. Dergelijke specifieke inrichtingscriteria kunnen verwerkt worden in de Excel-sheet die onderdeel is van de werkwijze. De volgende stappen kunnen worden gevolgd voor het toesnijden van de werkwijze op de eigen organisatie:

1. De huidige VSP/VSE zijn gebaseerd op het toepasselijk zijn van inkoopvoorwaarden zoals ARVODI en de ARBIT. Eisen die bijvoorbeeld al geborgd zijn in de ARBIT zijn niet opgenomen in de VSP/VSE, om doublures te voorkomen. Als andere IT inkoopvoorwaarden worden gehanteerd (bijvoorbeeld de GIBIT), is het zaak om het verschil in inkoopvoorwaarden te bepalen en waar nodig de VSP/VSE aan te passen.
2. Bepaal hoe de werkwijze moet worden ingepast in de bestaande processen. Hierbij moet worden gekeken naar het inkoopproces van de organisatie en worden bepaald in welke fase van dat proces de tooling ingezet zal worden (bij strategiebepaling, selectie e.d.). Binnen deze stap moeten de volgende rollen aanhaken: IB, Inkoop en Contractmanagement.
3. Maak de contractteksten specifiek voor de eigen organisatie. Houd er echter rekening mee dat de teksten nog steeds begrijpelijk moeten blijven voor de 'leek' en niet teveel gaan afwijken van de standaard. Dit om de uniformering tussen verschillende organisaties te behouden. Binnen deze stap moeten de volgende rollen aanhaken: IB, Jurist, Inkoop.

4. Selecteer de betreffende IB-richtlijnen die de organisatie wil gebruiken binnen deze methodiek. Geadviseerd wordt om 'open' richtlijnen te gebruiken zoals die van het CIP, NCSC, de rijksoverheid e.d. Deze richtlijnen worden meer gedragen binnen de private sector en worden regelmatig up-to-date gehouden. Deze selectie aan IB-richtlijnen moet uiteindelijk worden toegevoegd in de tooling.
5. Optioneel aanpassen van achterliggende logica zodat deze beter aansluit bij de AD. Dit kan ook gebeuren na een paar keer de tooling gebruikt te hebben, op het moment dus dat er enige ervaring is opgedaan. Binnen deze stap moeten de volgende rollen aanhaken: IB, Inkoop, Contractmanagement.

4.1.2 *Fase II: toepassen van de werkwijze*

Nadat de tool is ingericht voor de AD moet deze worden uitgerold binnen de organisatie. Om de uitrol binnen een organisatie goed te laten verlopen en de methodiek ook blijvend te laten gebruiken binnen de organisatie is het belangrijk om een goede PDCA cyclus in te richten.



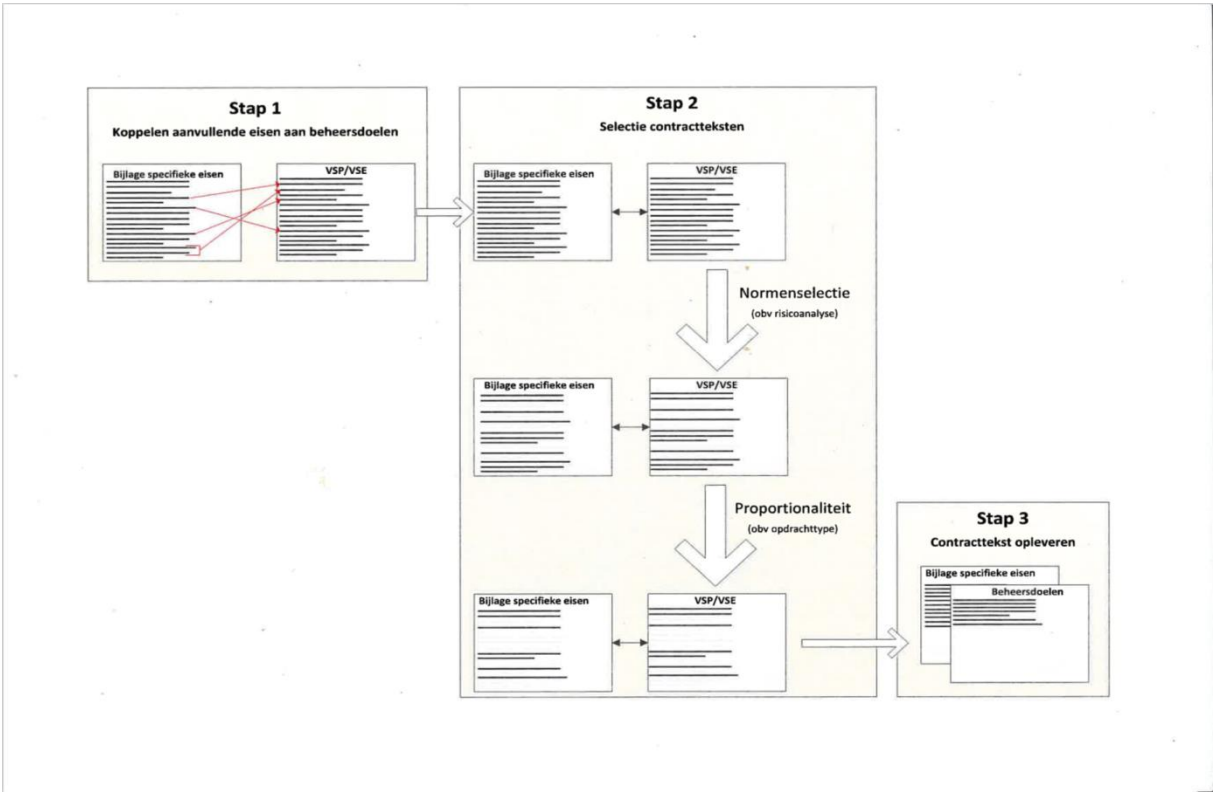
Bij elk gebruik van de tooling waarbij de rationale wordt ingevoerd moet worden geëvalueerd welke eisen wel/niet zijn geselecteerd en afwijken van het advies. Indien bij meerdere aanbestedingen steeds dezelfde afwijkingen plaatsvinden kan de tool herijkt worden zoals beschreven in de methodiek in 4.1.1. In de volgende cycli zullen de gegeven adviezen om een eis te gebruiken steeds beter passen bij de organisatie zelf.

Belangrijk is om bij het gebruik van deze methodiek altijd de gebruikte documenten op te slaan en te bewaren, dit is noodzakelijk voor audits achteraf. Bij elke eis van de BIO moet worden uitgelegd of er voldaan wordt en indien dat niet zo is, waarom niet ('comply or explain'). Als het Excel bestand goed is ingevuld, zal deze methodiek dit verzorgen.

4.2 **Borgen aanvullende eisen**

Aangezien organisaties specifieke, aanvullende eisen kunnen hebben, is een werkwijze opgesteld voor de verwerking daarvan in de werkwijze. Net zoals bij het standaard model zal het eisenpakket worden beoordeeld en wordt gekeken of er overlap is met de reeds bestaande proces- en systeemeisen en met ARBIT/ARVODI.

Nadat het eisenpakket is vergeleken met de reeds gehanteerde eisen moet een ontdubbeling plaatsvinden. Vervolgens worden de aanvullende eisen gekoppeld aan de beheersdoelen en omgevormd naar contractteksten. Deze worden net zoals de aangeleverde teksten in begrijpelijke taal omgezet en met verwijzingen naar diverse richtlijnen om zo actuele veiligheidseisen te hanteren. Vervolgens worden, net als bij de 'algemene' eisen het geval is, de normen geselecteerd met behulp van een risico analyse. Daarna wordt gekeken of de geselecteerde eisen proportioneel zijn en wordt een set aan contractteksten opgeleverd. Het bovenstaande is schematisch weergegeven in figuur 2.



Figuur 2 Opzet werkwijze aanvullende eisen

4.3 **Tooling in Excel**

De beschreven werkwijze wordt ondersteund door een Excel-tool, De Wizard Security Proof Inkopen. (SPINK).

Het eerste tabblad van de tool bevat de vragenlijst die gebruikt wordt als startpunt voor de aanbesteding. Op het tweede en derde tabblad zijn alle proces- en systeemeisen opgenomen waaruit wordt geselecteerd o.b.v. de gemaakte instellingen op het eerste tabblad. Het is van belang de gemaakte selectie met motivatie van de rationale te bewaren voor eventuele audits. Op het 4e tabblad komt de export lijst te staan met alle geselecteerde contractteksten. Deze lijst kan simpel naar een Word-document worden geëxporteerd of in Excel zelf worden uitgeprint. Het laatste tabblad bevat de vertaaltabel waarin de vertalingen tussen de BIO, ISO:27002/2005, ISO:27002/2013, beheersdoelen, contractteksten en rationale staan.

4.4 **Betrokken taakomschrijvingen**

Om deze methodiek tot een goed einde te brengen wordt geadviseerd om de volgende rollen te betrekken.

4.4.1 *Opdrachtgevers rol*

De opdrachtgever behartigt de belangen van de proceseigenaar en neem de uiteindelijke beslissingen. De opdrachtgever moet enerzijds de methodiek accorderen binnen de organisatie,

vervolgens moet de opdrachtgever deze methodiek ook blijven monitoren op het gebruik en promoten binnen de organisatie.

4.4.2 *Juridische rol*

Bij de inrichting van de methodiek binnen de organisatie moeten juristen aanschuiven om de inrichting goed vast te stellen. De juristen moeten tijdens dit proces zorgdragen voor contractteksten die in lijn zijn van de organisatie en zullen advies geven over specifieke eisen die gelden voor de organisatie.

4.4.3 *Inkoop rol*

De afdeling inkoop zal uiteindelijk de partij zijn die de uitkomst van dit product voornamelijk gebruikt bij de daadwerkelijke aanbesteding. De contractteksten die uit deze methodiek vloeien kunnen worden gebruikt binnen het bestek van de aanbesteding. Daarnaast kan de input die wordt verkregen tijdens een RFI worden gebruikt binnen de PDCA-cyclus om de tooling te verbeteren.

4.4.4 *IB rol*

De medewerkers die verantwoordelijk zijn voor informatiebeveiliging zullen een rol spelen binnen het vaststellen van de beheersdoelen en de achterliggende logica op basis van het risicoprofiel. Daarnaast moet de IB-verantwoordelijke helpen om keuzes te maken voor de richtlijnen die de organisatie wil toepassen. Als laatste is de IB-rol ook verantwoordelijk voor het bijstellen en bepalen van de rationale, mocht deze veranderen.

4.4.5 *Contractmanagement rol*

Contractmanagers moeten uiteindelijk de beheersdoelen gaan monitoren en controleren. Het is belangrijk om bij het inrichten van deze methodiek in de organisatie de contractmanagers mee te nemen en met hen regelmatig de werkbaarheid van de beheersdoelen te evalueren.

5 Voorbeelduitwerking

Om een beter beeld te geven van de methodiek zoals beschreven in de eerdere hoofdstukken is in dit hoofdstuk een voorbeelduitwerking gemaakt voor een cloud based urenregistratiesysteem. In deze uitwerking is het volgende product besteld met de volgende eisen:

Omschrijving: Er is een cloud based urenregistratiesysteem nodig. Er is gekozen om een off-the shelf product te kiezen omdat AD geen maatwerk meer wil aankopen. Er moet wel iets geconfigureerd worden uiteraard bij de leverancier voor de AD en daarnaast is ook een adviesklus gekoppeld aan de levering om alles intern te implementeren en medewerkers de app te laten gebruiken.

Product: Cloudbase gebaseerde uren registratiesoftware (COTS) met advies voor implementatie.

Locatie: Publieke cloud binnen EU grondgebied.

Gebruikers: Alle medewerkers eigen gegevens; Finance, HR voor administratie.

5.1 **Vragenlijst**

Vragenlijst voor selectie van VSP en VSE contracteisen m.b.t. informatiebeveiliging

BELANGRIJK: Dit document bevat alle VSP en VSE uit versie 1.0 van het vastgestelde moederdocument "handleiding VSP-VSE Eisen". Lees alle opmerkingen onderaan deze pagina aandachtig door alvorens met de vragenlijst aan de slag te gaan.

Algemeen	Antwoord
Naam contract:	CIP
Omschrijving:	Uren registratietool
Organisatieonderdeel	HR
Contactpersoon organisatie onderdeel:	Alex
Contactpersoon contractmanagement:	Bernard

#	Vragen m.b.t. supportdiensten en onderhoud	Antw.
1a	Wordt beheer of monitoring op afstand besteld van systemen op het netwerk van aanbestende dienst?	Nee
1b	Wordt beheer of monitoring besteld van systemen rechtstreeks op het netwerk van aanbestedende dienst?	Nee
1c	Worden COTS programmatuurupdates en/of advies besteld, maar worden deze niet door Wederpartij zelf uitgevoerd?	Nee

#	Vragen m.b.t. hosting diensten	Antw.
2	Worden diensten afgenomen waarvan zich systemen buiten het netwerk van aanbestedende dienst bevinden?	Ja

#	Vragen m.b.t. aankoop van apparatuur	Antw.
3	Wordt apparatuur aangekocht als onderdeel van het contract?	Nee

#	Vragen m.b.t. aankoop van programmatuur	Antw.
4a	Wordt COTS programmatuur aangekocht als onderdeel van het contract?	Ja
4b	Wordt customizing van COTS programmatuur aangekocht uit te voeren op locatie(s) van aanbestedende dienst?	Ja
4c	Wordt customizing van COTS programmatuur aangekocht, uit te voeren buiten locatie(s) van aanbestedende dienst?	Nee
4d	Wordt maatwerkprogrammatuur besteld en/of onderhoud hiervan, te ontwikkelen op locatie(s) van aanbestedende di	Nee
4e	Wordt maatwerkprogrammatuur besteld en/of onderhoud hiervan, te ontwikkelen buiten locatie(s) van aanbestedend	Nee

#	Vragen m.b.t. consultancy	Antw.
5a	Worden consultancydiensten aangekocht, uit tevoeren op locatie(s) van aanbestedende dienst?	Ja
5b	Worden consultancydiensten aangekocht, uit te voeren buiten locatie(s) van aanbestedende dienst?	Nee

#	Vragen m.b.t. betrouwbaarheid	Antw.
6a	Is de Prestatie gerelateerd aan een Missie Kritiek Systeem (MKS)?	Nee
6b	Welke mate van vertrouwelijkheid is gewenst m.b.t. de Prestatie?	Hoog
6c	Welke mate van integriteit is gewenst m.b.t. de Prestatie?	Midden
6d	Welke mate van beschikbaarheid is gewenst m.b.t. de Prestatie?	Midden
6e	Worden als onderdeel van de Prestatie persoonsgegevens verwerkt of opgeslagen? Zo ja, zet dan ook handmatig de vertrouwelijkheid op Hoog!	Ja

5.2 **Rationale + Eisen export**

Indien bovenstaande vragenlijst wordt ingevuld komt na het invullen van de rationale een uitgebreide lijst naar voren. In deze lijst zijn alle eisen opgenomen met betrekking tot het proces. Voor de eenvoud is gekozen om alle eisen over te nemen die zijn geadviseerd en geen eisen weg te halen of bij te voegen. Dit zou in de praktijk echter wel kunnen gebeuren bij gegronde redenen. Binnen de teksten staan links de nummers, deze nummers zijn een directe link naar de gerelateerde eis in de ISO:27002.
Er staan ook bepaalde cijfers tussen {}. Dit zijn documenten waarnaar gerefereerd wordt, deze staan in 5.6.

5.3 **VSP Contracteisen**

VSP Eis	Beschrijving
5.1.1	Wederpartij is voor de overeengekomen Prestatie gecertificeerd conform de meest recente versie van de NEN-ISO/IEC 27001 norm of gelijkwaardig, blijft dit voor ten minste de duur van de Overeenkomst en levert hiervan bewijs telkens terstond op eerste verzoek van Opdrachtgever.
6.1.1	Wederpartij dient voor ten minste alle processen genoemd in de Overeenkomst aantoonbaar de verantwoordelijkheden, taken en bevoegdheden op de daartoe geëigende plaatsen binnen de (project)organisatie te beleggen.
6.1.2	Wederpartij dient beleid te hebben voor functiescheiding (mits redelijkerwijs mogelijk) bij het beleggen van uitvoerende, controlerende en beheertaken betrokken bij de Prestatie, en dient dit aantoonbaar operationeel geborgd te hebben in processen.
6.1.5	Wederpartij dient te beschikken over een operationeel geborgd projectbeheerproces voor de Prestatie waarin informatiebeveiliging aantoonbaar geïntegreerd is.
6.2.1	Wederpartij dient een aantoonbaar operationeel geborgd proces te hebben voor versleutelen van gegevens op mobiele apparatuur betrokken bij de Prestatie waarbij rekening wordt gehouden met de classificatie van deze gegevens {4} en actualiteit van de veiligheid van de gebruikte versleutelingsmethoden {3}.
7.1.1	Wederpartij dient een aantoonbaar operationeel geborgd proces te hebben voor de screening van het Personeel dat werkzaamheden verricht: 1. op het gebied van ontwikkelen of herzien van ontwerptekeningen en/of -documenten; 2. ontwikkelen, testen, beheren, installeren, configureren en/of bedienen van programmatuur of apparatuur; 3. in bedienings- of technische ruimtes; 4. aan kabels en leidingen; 5. aan beveiligings- en veiligheidsdocumentatie en -instructies betrokken bij de Prestatie middels ten minste een relevante Verklaring Omtrent Gedrag (VOG), waarbij gedurende de contractperiode een screening nooit ouder mag zijn dan 5 jaar. Hangende de aanvraag van een screening kan

	worden volstaan met een eigen verklaring van betreffende persoon gedurende een periode van maximaal zes weken gerekend vanaf de startdatum van deze persoon bij de Prestatie, welke niet verlengd kan worden.
7.2.2a	Wederpartij dient aantoonbaar operationeel geborgd te hebben dat Personeel een opleiding en -training op het gebied van beveiligingsbewustzijn heeft ontvangen passend bij de aard van de uit te voeren werkzaamheden, alsmede jaarlijkse bijscholing krijgt, waarin ten minste ook persoonlijke verantwoordelijkheid en specifieke beveiligingskaders van Opdrachtgever ter sprake komen.
7.2.2b	Wederpartij dient aantoonbaar operationeel geborgd te hebben dat Personeel, verantwoordelijk voor het testen van informatiesystemen betrokken bij de Prestatie, beschikken over actuele en gespecialiseerde kennis, ervaring en opleiding met betrekking tot het testen van de beveiliging hiervan.
7.3.1	Wederpartij dient een aantoonbaar operationeel geborgd proces te hebben voor het definiëren van verantwoordelijkheden en taken met betrekking tot informatiebeveiliging voor de Prestatie en dient naar het Personeel te communiceren dat: 1. deze van kracht blijven na beëindiging of wijziging van het dienstverband; 2. deze ten uitvoer moeten worden gebracht.
8.1.1a	Wederpartij dient aantoonbaar operationeel geborgd te hebben dat van alle informatiesystemen betrokken bij de Prestatie, een inventaris is opgesteld in een Content Management Database (CMDB), zodat deze effectief kan worden gebruikt voor een effectief Configuration Management (CM) ITIL proces, en dat deze CMDB actueel wordt gehouden.
VSP 8.1.1b	Wederpartij dient op verzoek van Opdrachtgever de gegevens vermeld in de Content Management Database (CMDB) over informatiesystemen die ontsloten zijn via de infrastructuur van Opdrachtgever, over te dragen.
VSP 8.2.1	Wederpartij dient aantoonbaar operationeel geborgd te hebben dat alle informatie betrokken bij de Prestatie is geclassificeerd in overeenstemming met het classificatieschema {4} van Opdrachtgever en dat de hierbij behorende beveiligingsmaatregelen worden nageleefd.
VSP 8.3.x	Wederpartij dient over operationeel geborgde processen te beschikken voor het veilig verwijderen van media, transport van media en het beheer van verwijderbare media, betrokken bij de Prestatie, in overeenstemming met het classificatieschema {4} van Opdrachtgever.
VSP 9.1.1	Wederpartij dient te zorgen voor een operationeel geborgde procedure voor het verschaffen van fysieke dan wel logische toegang tot informatieverwerkende faciliteiten, inclusief de uitgifte en inname van accounts en autorisaties, en een actuele registratie hiervan.
VSP 9.2.x	Wederpartij dient minimaal jaarlijks zowel de fysieke als logische toegangsrechten tot informatieverwerkende faciliteiten van het Personeel te beoordelen en te actualiseren via een operationeel geborgd en formeel proces

	en levert hiervan bewijs telkens terstond op eerste verzoek van Opdrachtgever.
VSP 9.3.1	Wederpartij dient van het Personeel te eisen dat het zich houdt aan het Beleid voor wachtwoordgebruik {1} van Opdrachtgever bij het gebruiken van authenticatiegegevens gerelateerd aan de Prestatie.
VSP 9.4.4	Wederpartij dient een aantoonbaar operationeel geborgd proces te hebben voor het controleren van het gebruik van systeemhulpmiddelen, die in staat zijn om beheersmaatregelen te omzeilen voor informatiesystemen betrokken bij de Prestatie.
VSP 9.4.5	Wederpartij dient aantoonbaar operationeel geborgd te hebben dat uitsluitend Personeel die daartoe specifiek bevoegd is, toegang heeft tot de Broncode van informatiesystemen betrokken bij de Prestatie.
VSP 10.1.x	Indien Wederpartij contractueel of wettelijk verplicht is tot de inzet van cryptografie ter bescherming van gegevens betrokken bij de Prestatie, dient Wederpartij voor het gebruik van deze cryptografische beheersmaatregelen over beleid en operationeel geborgde processen te beschikken ter waarborging van gegevens en het gebruik en de bescherming daarvan. Dit beleid en deze processen betreffen ook de levensduur van de maatregelen en daarbij behorende cryptografische sleutels. Dit beleid en deze processen worden strikt nageleefd en de Wederpartij levert hiervan bewijs telkens terstond op eerste verzoek van Opdrachtgever.
VSP 11.1.1	Wederpartij dient fysieke beveiligingszones te hebben gedefinieerd en in gebruik te hebben om gebieden te beschermen, die gevoelige of essentiële informatie en informatieverwerkende faciliteiten bevatten, met betrekking tot de Prestatie. Telkens terstond op eerste verzoek informeert Wederpartij Opdrachtgever over alle relevante aspecten van deze beveiligingszones, zodat Opdrachtgever de kwaliteit daarvan kan beoordelen.
VSP 11.1.5	Wederpartij toont, telkens terstond op eerste verzoek van Opdrachtgever, aan operationeel geborgde procedures te hebben voor het werken in beveiligde gebieden, zoals bedoeld in eis 11.1.1.
VSP 11.2.7	Wederpartij toont, telkens terstond op eerste verzoek van Opdrachtgever, aan te beschikken over en te werken volgens een operationeel geborgd proces voor het vernietigen van data op media bij afvoeren of vervangen van (delen van) informatiesystemen die deze media bevatten en betrokken zijn bij de Prestatie.
VSP 11.2.8	Wederpartij toont, telkens terstond op eerste verzoek van Opdrachtgever, aan te beschikken over en te werken volgens operationeel geborgde procedures voor de bescherming van onbeheerde informatiesystemen, die betrokken zijn bij de Prestatie.
VSP 12.1.1	Wederpartij toont, telkens terstond op eerste verzoek van Opdrachtgever, aan te beschikken over en te werken volgens operationeel geborgde bedieningsprocedures die nodig zijn voor de Prestatie en deze beschikbaar te stellen aan het Personeel en, indien van toepassing de medewerkers van Opdrachtgever.

VSP 12.2.1	Wederpartij toont, telkens terstond op eerste verzoek van Opdrachtgever, aan te beschikken over en te werken volgens operationeel geborgde processen voor bescherming tegen malware op informatiesystemen betrokken bij de Prestatie, waarbij ten minste aandacht wordt besteed aan preventie, detectie, communicatie en herstel.
VSP 12.3.1a	Wederpartij toont, telkens terstond op eerste verzoek van Opdrachtgever, aan te beschikken over en te werken volgens een operationeel geborgd proces voor het minimaal dagelijks maken van back-ups van alle informatie en programmatuur in gebruik voor de Prestatie.
VSP 12.3.1b	Wederpartij dient het recovery proces dat deel uitmaakt van het back-upproces van alle informatie en programmatuur in gebruik voor de Prestatie, minimaal jaarlijks te testen en naar Opdrachtgever te communiceren over de uitkomst hiervan.
VSP 12.4.1	Wederpartij toont, telkens terstond op eerste verzoek van Opdrachtgever, aan te beschikken over en te werken volgens een operationeel geborgd proces voor het voldoende periodiek beoordelen van logbestanden van informatiesystemen betrokken bij de Prestatie, waarbij het interval tussen twee beoordelingen nooit meer mag bedragen dan één maand.
VSP 12.4.3	Wederpartij dient een aantoonbaar operationeel geborgd proces te hebben voor het maandelijks beoordelen van activiteiten van systeembeheerders en -operators op informatiesystemen betrokken bij de Prestatie, die zijn vastgelegd in logbestanden.
VSP 12.4.CC-21	Wederpartij dient logbestanden van informatiesystemen betrokken bij de Prestatie minimaal drie maanden (en bij een vermoed incident minimaal 3 jaar) beschikbaar te houden tenzij met Opdrachtgever een andere bewaartermijn is overeengekomen, en dient, telkens terstond op eerste verzoek van Opdrachtgever, deze afschriften van deze logbestanden ter inzage te overhandigen aan Opdrachtgever.
VSP 12.6.1	Wederpartij dient voor informatiebeveiliging minimaal jaarlijks een risicoanalyse en risicoafweging conform NEN-ISO/IEC 27005 of gelijkwaardig te maken en passende maatregelen te treffen. Telkens terstond op eerste verzoek verstrekt Wederpartij aan Opdrachtgever de informatie die Opdrachtgever nodig heeft om zich van de naleving van deze verplichting te vergewissen.
VSP 13.1.1	Wederpartij toont, telkens terstond op eerste verzoek van Opdrachtgever, aan te beschikken over en te werken volgens operationeel geborgde processen voor beheer en beheersing van netwerken betrokken bij de Prestatie om informatie in informatiesystemen te beschermen, waarbij ten minste aandacht wordt besteed aan onderstaande aspecten: - Management of network security - Technical vulnerability management - Identification and authentication - Network audit logging and monitoring - Intrusion detection and prevention - Protection against malicious code

- Cryptographic based services
- Business continuity management

VSP 13.1.2	Wederpartij dient beveiligingsmechanismen, dienstverleningsniveaus en beheerseisen voor alle diensten betrokken bij de Prestatie opgenomen te hebben in een Service Level Agreement (SLA) met Opdrachtgever met ten minste aandacht voor de beveiligingsaspecten beschikbaarheid, melden van incidenten, doorvoeren van wijzigingen en escalatie.
VSP 13.2.1	Wederpartij toont, telkens terstond op eerste verzoek van Opdrachtgever, aan te beschikken over en te werken volgens operationeel geborgde beleidsregels, procedures en beheersmaatregelen te hebben ter bescherming van het informatietransport betrokken bij de Prestatie, dat via alle soorten communicatiefaciliteiten verloopt.
VSP 14.1.1	Wederpartij dient gedurende de hele levenscyclus beveiliging integraal onderdeel te maken van het proces voor ontwikkeling en onderhoud van informatiesystemen. In het geval van programmatuur dienen hiertoe minimaal de maatregelen geïmplementeerd te worden genoemd in het CIP document Grip op SSD - Beveiligingseisen voor (web)applicaties {10}.
VSP 14.2.x	Wederpartij dient informatiebeveiliging aantoonbaar operationeel geborgd te hebben in de processen die deel uitmaken van de ontwikkelingslevenscyclus van informatiesystemen betrokken bij de Prestatie en toont, telkens terstond op eerste verzoek van Opdrachtgever, aan te beschikken over en te werken volgens de Richtlijn beveiliging bij ontwikkelen {15}.
VSP 14.3.1	Wederpartij dient testgegevens betrokken bij de Prestatie, aantoonbaar zorgvuldig te kiezen, beschermen, controleren, en vernietigen na gebruik. Wederpartij toont, telkens terstond op eerste verzoek van Opdrachtgever, de naleving van deze verplichting aan.
VSP 15.2.1	Wederpartij dient testgegevens betrokken bij de Prestatie, aantoonbaar zorgvuldig te kiezen, beschermen, controleren, en vernietigen na gebruik. Wederpartij toont, telkens terstond op eerste verzoek van Opdrachtgever, de naleving van deze verplichting aan.
VSP 16.1.x	Wederpartij dient over een operationeel geborgd proces te beschikken voor de registratie, rapportage en afhandeling van informatiebeveiligingsincidenten die aansluit op het incidentmanagementproces van Opdrachtgever waarbij ten minste de eisen worden geïmplementeerd uit de Richtlijn voor informatiebeveiligingsincidenten {16}. Ten minste maandelijks dient over deze informatiebeveiligingsincidenten gerapporteerd te worden richting Opdrachtgever.
VSP 17.1.2	Wederpartij dient aantoonbaar te beschikken over een continuïteitsplan voor het handhaven van de Prestatie in ongunstige situaties, waarin ook de continuïteit van de informatiebeveiliging is gewaarborgd.
VSP 18.1.3	Wederpartij dient aantoonbaar operationeel geborgde procedures te hebben voor het beschermen tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave, van registraties op informatiesystemen

	betrokken bij de Prestatie, in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen.
VSP 18.1.CC-09	Gegevens of programmatuur van Opdrachtgever, inclusief daarin aanwezige of door deze gegenereerde gegevens waaronder metadata, die zich bevinden op informatiesystemen van Wederpartij, zijn en blijven ten alle tijden eigendom van Opdrachtgever. Gegevens die door Opdrachtgever aan Wederpartij zijn verstrekt, mag Wederpartij alleen gebruiken voor het doel waarvoor deze zijn verstrekt. Wederpartij treft maatregelen, onder meer in de vorm van afscherming, ter voorkoming van kennisneming en afwijkend gebruik door zijn Personeel.
VSP 18.1.CC-10	Wederpartij toont, telkens terstond op eerste verzoek van Opdrachtgever, aan operationeel geborgde processen te hebben voor het vernietigen van gegevens of programmatuur van Opdrachtgever op apparatuur en alle back-up media van Opdrachtgever. Zowel tussentijds als na contractbeëindiging om welke reden of door welke oorzaak dan ook, is Opdrachtgever bevoegd aan Wederpartij opdracht te geven tot overdracht aan Opdrachtgever of onmiddellijke vernietiging van de gegevens.
VSP 18.1.CC-12	Wanneer gegevens van Opdrachtgever zich bevinden op informatiesystemen van Wederpartij, dient bij contractbeëindiging tussen deze beide partijen, de Wederpartij assistentie te leveren bij de overdracht van deze informatie naar de nieuwe leverancier of terug naar Opdrachtgever, indien Opdrachtgever hierom verzoekt. Tenzij dit naar maatstaven van redelijkheid en billijkheid onaanvaardbaar zou zijn, worden de kosten van de assistentie geacht te zijn verdisconteerd in de door Wederpartij voor zijn Prestaties ontvangen vergoedingen, hoe ook genoemd.
VSP 18.1.CC-14	Wanneer gegevens of programmatuur van Opdrachtgever zich bevinden op informatiesystemen van Wederpartij, dient Wederpartij telkens op eerste verzoek van Opdrachtgever aan te geven waar ter wereld deze informatiesystemen zich bevinden. Indien deze zich buiten de EU bevinden, mag dit uitsluitend in landen waar een passend niveau van gegevensbescherming wordt geboden; welke landen dit zijn, is bepaald door de Europese Commissie.
VSP 18.2.1	Wederpartij dient tenminste jaarlijks een audit uit te voeren naar de opzet, bestaan en werking van de maatregelen op het gebied van de informatiebeveiliging gemeld in het contract met Opdrachtgever, en deze Opdrachtgever te rapporteren over de bevindingen en voorgenomen verbetermaatregelen.
VSP 18.2.2	Wederpartij dient aantoonbaar operationeel geborgde processen te hebben voor het periodiek beoordelen van de naleving van beleidsregels, normen en andere eisen betreffende beveiliging door Personeel betrokken bij de Prestatie.
VSP 18.2.3	Wederpartij dient aantoonbaar operationeel geborgde processen te hebben voor het periodiek beoordelen van de naleving van technische beleidsregels, normen en andere eisen betreffende beveiliging bij informatiesystemen betrokken bij de Prestatie.

5.4 **VSE contracteisen**

VSE Eis	Beschrijving
VSE 6.1.2	Informatiesystemen betrokken bij de Prestatie moeten zijn ingericht met een autorisatiemodel. OPMERKING: Indien de Prestatie uitsluitend bestaat uit de aankoop van informatiesystemen moet deze tekst worden geïnterpreteerd als het standaard beschikken over de functionaliteit de eis te kunnen implementeren.
VSE 6.2.1	Mobiele apparatuur in gebruik door Personeel moet gegevens gerelateerd aan de Prestatie versleuteld opslaan conform de classificatie van deze gegevens {4} middels cryptografische toepassingen waarbij uitsluitend algoritmes en instellingen worden gebruikt met de duiding goed uit de meest actuele versie van het NCSC document Richtlijnen voor Transport Layer Security (TLS) {3}.
VSE 9.1.2	Informatiesystemen betrokken bij de Prestatie bevatten uitsluitend standaard voor programmatuur noodzakelijke functionele accounts of accounts die zijn aangeleverd door het vigerende autorisatieproces.
VSE 9.4.1	Accounts op informatiesystemen betrokken bij de Prestatie beschikken uitsluitend over toegangsrechten gekoppeld aan rollen toegekend via het vigerende autorisatieproces.
VSE 9.4.2	Informatiesystemen betrokken bij de Prestatie beschikken over een beveiligde inlogprocedure conform de richtlijn voor logische toegangsbeveiliging {6} van Opdrachtgever. OPMERKING: Indien de Prestatie uitsluitend bestaat uit de aankoop van informatiesystemen moet deze tekst worden geïnterpreteerd als het standaard beschikken over de functionaliteit de eis te kunnen implementeren.
VSE 9.4.3	Informatiesystemen betrokken bij de Prestatie beschikken over wachtwoordbeheervoorzieningen die het gebruik van sterke wachtwoorden afdwingen die ten minste voldoen aan het Beleid voor wachtwoordgebruik {1} van Opdrachtgever. OPMERKING: Indien de Prestatie uitsluitend bestaat uit de aankoop van informatiesystemen moet deze tekst worden geïnterpreteerd als het standaard beschikken over de functionaliteit de eis te kunnen implementeren.
VSE 11.1.x	Informatieverwerkende faciliteiten betrokken bij de Prestatie zijn fysiek ten minste beveiligd volgens de Richtlijn voor fysieke beveiliging {17} van Opdrachtgever.
VSE 11.2.x	Informatiesystemen betrokken bij de Prestatie zijn beschermd tegen verlies, schade, diefstal, compromittering of onderbreking, waarbij ten minste de eisen worden geïmplementeerd uit de Richtlijn voor fysieke beveiliging {17} van Opdrachtgever.
VSE 12.1.4	Wederpartij dient ontwikkel-, test-, productie- en, indien besteld, educatieve omgevingen aantoonbaar gescheiden (logisch, dan wel fysiek) te hebben voor alle informatiesystemen betrokken bij de Prestatie. Scheiding houdt in dat al het noodzakelijke geregeld moet worden om interferentie tussen de omgevingen te voorkomen en dat de betrouwbaarheid van de productiesystemen gewaarborgd is. De acceptatie- en educatieve

	omgevingen dienen representatief te zijn voor de productieomgeving, zodanig dat de test- dan wel oefenresultaten het gedrag van de functionaliteit in de productieomgeving weerspiegelen.
VSE 12.2.1	Informatiesystemen betrokken bij de Prestatie zijn voorzien van detectieve en preventieve maatregelen tegen malware.
VSE 12.3.1	Informatiesystemen betrokken bij de Prestatie beschikken over voorzieningen om back-ups te kunnen maken van alle hier op aanwezige informatie en programmatuur. Indien informatiesystemen zich bevinden op de infrastructuur van de Opdrachtgever, moet dit kunnen gebeuren naar de centrale back-up voorziening van de Opdrachtgever.
VSE 12.4.x	Informatiesystemen betrokken bij de Prestatie leggen gebeurtenissen vast waarbij ten minste wordt voldaan aan de eisen genoemd in de Richtlijn voor logging {18} van de Opdrachtgever. OPMERKING: Indien de Prestatie uitsluitend bestaat uit de aankoop van informatiesystemen moet deze tekst worden geïnterpreteerd als het standaard beschikken over de functionaliteit de eis te kunnen implementeren.
VSE 13.1.3	Groepen van informatiesystemen en gebruikers betrokken bij de Prestatie zijn op basis van functie, rol en/of classificatie in logische of fysieke netwerkdomeinen gescheiden volgens een zoneringsmodel. Voor informatiesystemen geplaatst in de infrastructuur van Opdrachtgever, dient hiervoor een PSA aangehouden te worden die is goedgekeurd door een solution architect van Opdrachtgever.
VSE 13.2.3	Informatiesystemen betrokken bij de Prestatie die gebruik maken van elektronische berichten met daarin gegevens waarvan de vertrouwelijkheid en/of integriteit moet worden gewaarborgd, dienen hiervoor versleuteling en/of hashing te gebruiken waarbij de gehanteerde onderliggende algoritmes en instellingen uitsluitend de duiding goed mogen hebben in de meest actuele versie van het NCSC document Richtlijnen voor Transport Layer Security (TLS) {3}. OPMERKING: Indien de Prestatie uitsluitend bestaat uit de aankoop van informatiesystemen moet deze tekst worden geïnterpreteerd als het standaard beschikken over de functionaliteit de eis te kunnen implementeren.
VSE 14.1.1	In de programmatuur die deel uitmaakt van informatiesystemen betrokken bij de Prestatie zijn minimaal de maatregelen geïmplementeerd genoemd in het CIP document Grip op SSD - Beveiligingseisen voor (web)applicaties {10}. OPMERKING: Indien de Prestatie uitsluitend bestaat uit de aankoop van informatiesystemen moet deze tekst worden geïnterpreteerd als het standaard beschikken over de functionaliteit om de eis te kunnen implementeren.

VSE 14.1.2	Informatiesystemen betrokken bij de Prestatie die informatie uitwisselen via openbare netwerken moeten hiervoor te allen tijde versleutelde protocollen gebruiken waarbij de gehanteerde onderliggende encryptiealgoritmes en instellingen uitsluitend de duiding goed mogen hebben in de meest actuele versie van het NCSC document Richtlijnen voor Transport Layer Security (TLS) {3}. OPMERKING: Indien de Prestatie uitsluitend bestaat uit de aankoop van informatiesystemen moet deze tekst worden geïnterpreteerd als het standaard beschikken over de functionaliteit de eis te kunnen implementeren.
VSE 14.1.3	Informatiesystemen betrokken bij de Prestatie die deel uitmaken van een keten, moeten afhankelijk van de classificatie van de uitgewisselde gegevens, te allen tijde de integriteit dan wel vertrouwelijkheid van deze gegevens waarborgen middels hashing dan wel versleuteling, waarbij de gehanteerde onderliggende encryptiealgoritmes en instellingen uitsluitend de duiding goed mogen hebben in de meest actuele versie van het NCSC document Richtlijnen voor Transport Layer Security (TLS) {3}. OPMERKING: Indien de Prestatie uitsluitend bestaat uit de aankoop van informatiesystemen moet deze tekst worden geïnterpreteerd als het standaard beschikken over de functionaliteit de eis te kunnen implementeren.
VSE 14.2.8a	Informatiesystemen betrokken bij de Prestatie zijn aantoonbaar getest op kwetsbaarheden middels gangbare testmethodieken voordat deze in productie worden genomen. In het geval van programmatuur omvat de gehanteerde testmethodiek ten minste de OWASP Top-10 {13}.
VSE 14.2.8b	Alle bekende kwetsbaarheden op informatiesystemen betrokken bij de Prestatie zijn verholpen voordat deze informatiesystemen in productie worden genomen.
VSE 14.2.9a	Informatiesystemen betrokken bij de Prestatie dienen een acceptatietest te hebben ondergaan op alle in dit contract vermelde systeemeisen voordat deze systemen in productie worden genomen.
VSE 14.2.9b	Informatiesystemen betrokken bij de Prestatie dienen niet in productie genomen te worden voordat alle bevindingen uit de acceptatietest zijn verholpen.
VSE 18.1.5	Informatiesystemen betrokken bij de Prestatie beschermen informatie door middel van cryptografische maatregelen indien relevante overeenkomsten/wet- en regelgeving dit voorschrijven. Hierbij mogen uitsluitend algoritmes worden toegepast aangeduid als goed in de meest actuele versie van het NCSC document ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) {3}. OPMERKING: Indien de Prestatie uitsluitend bestaat uit de aankoop van informatiesystemen moet deze tekst worden geïnterpreteerd als het standaard beschikken over de functionaliteit de eis te kunnen implementeren.

5.5 **Maatregelen i.v.m. persoonsgegevens**

	Als onderdeel van de Prestatie worden persoonsgegevens verwerkt of opgeslagen. Om deze reden moet dit worden aangemeld bij de Privacy Officer van AD. Deze persoon kan vaststellen of een Privacy Impact Assessment (PIA) moet worden uitgevoerd en kan tevens additionele beveiligingseisen opleggen. Dit is een wettelijke verplichting! Deze eisen komen dus nog boven de hier gemelde eisen, die enkel zijn gebaseerd op de BIO.

5.6 **Gerefereerde documenten**

De onderstaande documenten zijn gegenereerd uit de tooling. In dit voorbeeld zijn de documenten geselecteerd voor. Als algemene tools kunnen bijvoorbeeld IB-richtlijnen worden gekozen van organisaties Rijkswaterstaat als: CIP, NCSC, NCTV, SSC-ICT en uiteraard de eigen organisatie. In de tooling zal een aantal kernwoorden worden geplaatst waarmee goede IB-richtlijnen gezocht kunnen worden.

Ref. #	Document
{1}	Rijkswaterstaat Security Centre, " Rijkswaterstaat Cyber Security Richtlijnen voor IV-inkoopcontracten", hoofdstuk "Beleid voor wachtwoordgebruik"
{3}	Nationaal Cyber Security Center (NCSC), "ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)", URL: "https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html"
{4}	Rijkswaterstaat Security Centre, " Rijkswaterstaat Cyber Security Richtlijnen voor IV-inkoopcontracten", hoofdstuk "Beleid voor gegevensclassificatie"
{6}	Rijkswaterstaat Security Centre, " Rijkswaterstaat Cyber Security Richtlijnen voor IV-inkoopcontracten", hoofdstuk "Systeemrichtlijn voor logische toegangsbeveiliging"
{10}	Centrum Informatiebeveiliging en Privacy (CIP), "Grip op SSD - Beveiligingseisen voor (web)applicaties", URL: "http://www.cip-overheid.nl/wp-content/uploads/2014/10/Grip-op-SSD-Beveiligingseisen-v2_0.pdf"
{13}	Open Web Application Security Project (OWASP), "OWASP Top 10", URL: "https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project"
{15}	Rijkswaterstaat Security Centre, " Rijkswaterstaat Cyber Security Richtlijnen voor IV-inkoopcontracten", hoofdstuk "Richtlijnen voor beveiligen bij ontwikkelen"
{16}	Rijkswaterstaat Security Centre, " Rijkswaterstaat Cyber Security Richtlijnen voor IV-inkoopcontracten", hoofdstuk "Procesrichtlijn voor informatiebeveiligingsincidenten"
{17}	Rijkswaterstaat Security Centre, " Rijkswaterstaat Cyber Security Richtlijnen voor IV-inkoopcontracten", hoofdstuk "Systeemrichtlijn voor fysieke beveiliging"
{18}	Rijkswaterstaat Security Centre, " Rijkswaterstaat Cyber Security Richtlijnen voor IV-inkoopcontracten", hoofdstuk "Systeemrichtlijn voor logging"