Handreiking Inkoop ICO

(Inkoopeisen Cybersecurity Overheid)

Versie 0.99-2

25 maart 2020

Inhoudsopgave

1.0 Inleiding en Leeswijzer

De steeds toenemende digitalisering en daarin meekomende risico's op diefstal en misbruik van gegevens maakt het noodzakelijk om voortdurend te blijven werken aan informatieveiligheid. De overheid hanteert daarbij als gezamenlijk kader de Baseline Informatiebeveiliging Overheid (BIO). Naast maatregelen die de organisaties zelf betreffen, moeten ook inkopen en uitbestedingen voldoen aan veiligheidseisen.

De overheid kan met haar inkoopbeleid de vraag naar digitaal veilige ICT-producten en diensten stimuleren. In de eerste plaats omdat zij zelf veilig moet zijn. Maar ook kan zij als belangrijke gebruiker van ICT-diensten bredere impact creëren. Door cyber security criteria op te nemen in het inkoopbeleid moeten leveranciers van de overheid voldoen aan deze eisen. Hierdoor ontstaat een prikkel voor aanbieders om digitaal veilige producten op de markt te brengen. De overheid wil op deze wijze nadrukkelijk het goede voorbeeld geven.

Waarom specifieke cyber security criteria voor leveranciers?

De BIO is gericht op overheidsorganisaties. Voor eisen die overheidsorganisaties aan veilige producten van leveranciers stellen, is de BIO te breed omdat het allerlei facetten bevat die alleen op de processen van de eigen organisatie betrekking hebben. Daarnaast is de BIO te weinig specifiek voor het stellen van scherpe eisen aan de veiligheid op het niveau van ingekochte producten en diensten van leveranciers. De noodzaak om die scherpere eisen te stellen heeft geleid tot verdiepende, naar thema's georiënteerde uitwerkingen die naast de normen uit de BIO dankbaar gebruik maken van normenkaders zoals NIST, BSI en SoGP.

De bij de inkoopeisen gehanteerde documenten (de BIO-thema-uitwerkingen, Grip-op-SSD (Secure Software Development), de Pas Toe of Leg Uit lijst van het Forum Standaardisatie en de Richtlijnen van het NCSC) steunen op input van brede overheidsnetwerken.

Door de genoemde uitwerkingen te hanteren voor eisen aan aanbestedingen en inkopen, ontstaat een aanzienlijk completere en beter valideerbare veiligheidsvraag, dan wanneer alleen de BIO zou worden gebruikt.

Dit document

Dit document beschrijft eerst op hoofdlijnen het proces en de actoren die een rol hebben bij het borgen van de veiligheid van de te verwerven producten en diensten. Aangezien de beveiligingseisen veelal specifiek zijn voor verschillende soorten ICT-middelen, zijn deze toegespitst naar een aantal inkooponderdelen. Daarna volgen korte hoofstukken per inkooponderdeel waarin inhoudelijke duiding wordt gegeven naast de verwijzingen naar de brondocumenten met specifieke beveiligingseisen en instructies voor het samenstellen van de standaardeisenpakketten m.b.v. de bijbehorende 'ICO-Wizard'.

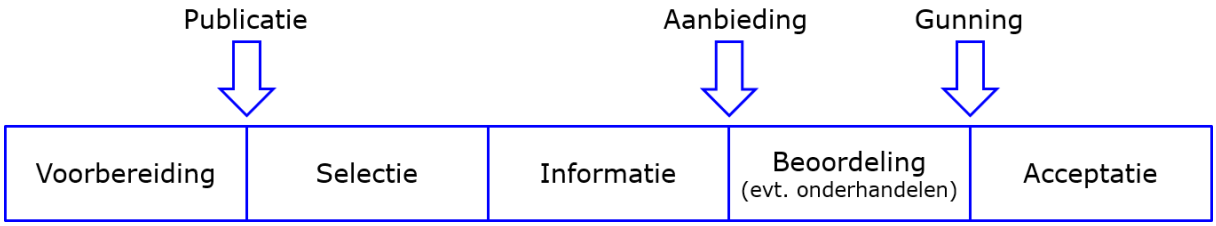
Het toepassen van deze beveiligingseisen in het inkoopproces interfereert niet met de toepassing van de gangbare algemene en specifieke voorwaarden, maar zijn daarop aanvullend.

Het betreft namelijk veiligheidseisen met een product- of procesinhoudelijk karakter. Vanwege het specifieke en inhoudelijke karakter van de eisen, zijn deze niet altijd direct begrijpelijk voor alle spelers in de keten van inkoop tot acceptatie. Niet iedereen hoeft de teksten echter in detail te kennen.

2.0 Het inkoopproces, rollen en betrokkenheid bij de Inkoopeisen

Hieronder volgt een overzicht van de rollen in het inkoopproces en de betrokkenheid bij de eisen. Omdat het stellen van eisen alleen zin heeft wanneer die ook worden nagekomen en getoetst, is gekozen voor een brede processcope, van behoefte tot levering. De duiding van de rollen is zo generiek mogelijk gehouden om aan te kunnen sluiten op alle overheden.

2.1 Het Inkoopproces



Voorbereiding en plaatsen publicatie
In het voorbereidingsproces lopen per aanbesteding verschillende en uiteenlopende sub-processen. De belangrijkste sub-processen zijn het kiezen van een aanbestedingsprocedure, de samenstelling van het inkoopteam en de beoordelingscommissie, raamovereenkomsten en het vaststellen van de gunningsvoorwaarden. De uitkomst van het voorbereidingsproces is een gedocumenteerde aanbestedingsopdracht welke online kan worden geplaatst en waarop organisaties kunnen inschrijven.

Selectie
Bij het selectieproces worden de gegadigden aan de hand van de uitsluitgronden, minimumgeschiktheidseisen en gunningsvoorwaarden beoordeeld. Bij de selectie van gegadigden zijn drie soorten eisen om hun geschiktheid te toetsen:

- De technische en beroepsbekwaamheid van de gegadigden;
- De beroepsbevoegdheid;
- De financiële en economische draagkracht van een ondernemer.

Informatie
Na de selectie van gegadigden is het noodzakelijk dat er informatie wordt uitgewisseld. Dit kan informatie zijn met betrekking tot het aan te besteden project, maar kan ook informatie zijn zoals de bewijsvoering van de selectiecriteria van een gegadigde. Het organiseren van vragenrondes of inlichtingen vindt ook plaats in dit proces. Tijdens het uitwisselen van informatie moet elke vorm van onderhandeling worden vermeden en staan de vier beginselen van de Europese aanbestedingswetgeving centraal.

Aanbieding
Na de informatie-uitwisseling worden de gegadigden gevraagd een aanbieding te doen voor een vooraf vastgestelde datum. Het aantal te selecteren gegadigden om een aanbieding te doen moet in geval van een niet-openbare procedure minimaal 5 zijn. Bij een concurrentiegerichte dialoog, een mededingingsprocedure met onderhandeling en een procedure van het innovatiepartnerschap is dit aantal minimaal 3.

Beoordeling
In het beoordelingsproces worden alle reacties op aanbiedingen beoordeeld. Als er meerdere aanbiedingen zijn, zijn de gunningscriteria:

- De beste prijs-kwaliteitverhouding (BPKV);
- De laagste kosten berekend op basis van kosteneffectiviteit;
- De laagste prijs.

Acceptatie
Tijdens het acceptatieproces wordt beoordeeld of het aangeboden product voldoet aan de functionele en de niet-functionele eisen. Zie paragraaf 3.3 voor verificatiemethoden.

2.2 Rol Opdrachtgever-behoeftesteller

Dit kan zijn een businessverantwoordelijke, productmanager, Informatie manager etc. De opdrachtgever is verantwoordelijk voor het informatiesysteem waarbinnen de via inkoop te verwerven producten diensten gebruikt zullen worden. De risicoafweging die hij of zij maakt, heeft invloed op de eisen die gesteld moeten worden aan de in te kopen producten en diensten. (Ook de BIO hanteert de risicoanalyse van de businessverantwoordelijke als uitgangspunt).

Deze veiligheidseisen worden niet steeds opnieuw bedacht. Ze zijn als standaardeisenpakketten bijeengebracht in dit document en de bijbehorende ICO-Wizard, en geselecteerd op basis van hun relevantie voor het inkoopproces. Ze gelden bij default.

Indien uit de risicoanalyse van de opdrachtgever blijkt dat bepaalde eisen achterwege kunnen blijven, dan wel moeten worden verzwaard, geeft de opdrachtgever dat expliciet per eis aan bij de opdracht tot inkoop.

2.3 Rol Inkoper

Dit is degene die de vraag in de markt uitzet. Dat kan via een aanbesteding, een meer partijen offerte of een onderhandse offerte. De inkoper geeft de op het betreffende inkoopsegment van toepassing zijnde hoofdstukken mee als onderdeel van de eisen. Wanneer de opdrachtgever geen opmerkingen of aanvullingen heeft meegegeven, gaan de toepasselijke eisen in dit document onverkort mee met de aanbesteding of offerteaanvraag tot en met de contractsluiting.

In het proces van gunning zullen over en weer vragen beantwoord moeten worden in het spel tussen de opdrachtgever en inkoper enerzijds en de aanbieders anderzijds. Hierbij zal het nodig zijn beveiligingsexpertise in te schakelen. De beveiligingsexpert zal daartoe ook de onderliggende documenten met de detailbeschrijvingen van de beveiligingseisen hanteren.

De inkoper ziet erop toe dat in de afspraken over acceptatie van de levering, tevens de expliciete acceptatie wordt geregeld van de realisatie van de beveiligingsmaatregelen. Daarnaast zal de inkoper ook afspraken maken over het in stand blijven van de veiligheidsmaatregelen bij nieuwe releases van de producten, waardoor de beveiliging geen eenmalige actie is, maar in een cyclisch proces wordt bewaakt.

2.4 Rol contract-/leveranciersmanager

In veel organisaties is deze rol ingevuld om de voortgang en het nakomen van contracten, SLA's en dergelijke te monitoren. Indien deze rol is ingevuld, zal de contract- of leveranciersmanager in het overleg met de leverancier zorgen dat ook de afgesproken beveiligingseisen

onder de aandacht blijven en worden nagekomen. Ook hierbij zal het soms nodig zijn beveiligingsexpertise in te schakelen. De beveiligingsexpert zal daartoe ook de onderliggende documenten met de detailbeschrijvingen van de beveiligingseisen hanteren.

2.5 Rol Leverancier

De Leverancier realiseert, bouwt en test het nieuwe product, bouwt en test een onderhoudsrelease, past een applicatiepakket aan, levert een standaardpakket, stelt een Clouddienst ter beschikking etc.
De leverancier hanteert de ICO-Wizard met de toepasselijke eisen en gebruikt de gedetailleerde normbeschrijvingen in de onderliggende documenten voor de realisatie van de vereiste beheersingsmaatregelen bij de realisatie van de gewenste functionaliteit.

2.6 Rol Opdrachtgever-Acceptant

Het stellen van eisen in inkoopprocessen is pas effectief als ook geverifieerd wordt of de levering voldoet aan de gestelde eisen. Verschillende vormen van verificatie kunnen sterk uiteenlopen: van directe bewijsvoering zoals acceptatietesten en aanlevering van bewijstukken tot indirecte methoden als audits en verklaringen van derde partijen. Daarnaast is het een keuze - veelal bepaald door de kosten die het met zich meebrengt - welke methodes toegepast zullen worden en of ze in volledigheid worden toegepast dan wel in de vorm van steekproeven. Sommige eisen lenen zich voor directe verificatie methoden, andere (de meeste) juist niet. Dit is dus sterk bepalend voor de te kiezen methode.

De aard van de norm en de kosten zullen dus bepalend zijn voor de vraag hoe verificatie plaatsvindt.

Voor de verificatie zijn de met de ICO-Wizard geselecteerde eisen en hun onderliggende gedetailleerde normbeschrijvingen van belang. Als de opdrachtgever de toetsing in eigen hand houdt, kan het daarbij nodig zijn extra beveiligingsexpertise in te schakelen.

In paragraaf 3.7 zijn verschillende vormen van verificatiemethode(n) beschreven.

2.7 Mantelovereenkomst en specifieke opdrachtovereenkomsten

In het geval van een langdurige samenwerking kunnen partijen hun afspraken vastleggen in een mantelovereenkomst, ook wel genoemd een raamovereenkomst. Dit kan betrekking hebben op verschillende soorten samenwerkingsverbanden, zoals met een softwareontwikkelingsbedrijf, een hostingpartij of een consultancybedrijf. In een mantelovereenkomst staan de algemene afspraken, zoals:

- De verantwoordelijkheden en verplichtingen van partijen;
- Op welke wijze opdrachten worden verleend;
- De facturatie- en betalingsafspraken;
- Afspraken over intellectuele eigendomsrechten;
- Bepalingen over de aansprakelijkheid, looptijd, verlenging etc.

Bij een specifieke opdracht volgt een opdrachtovereenkomst met de specifieke afspraken, zoals een duidelijke omschrijving van de werkzaamheden die dienen te worden uitgevoerd en het product dat moet worden geleverd.

De ICO-Wizard kan worden gebruikt voor het selecteren van de eisen bij de aanbesteding voor een mantelovereenkomst, waarbij bijvoorbeeld de proces-eisen gelden voor de mantelovereenkomst en de product-eisen later in de opdrachtovereenkomst worden ingevuld. Bij het afsluiten van de mantelovereenkomst moet duidelijkheid zijn welke eisen op welke wijze worden meegenomen door de leverancier.

3.0 Beveiligingseisen inkooponderdelen

Per inkooponderdeel wordt een toelichting gegeven op de inhoud van het inkooponderdeel, de context binnen de ICO-Wizard, welke onderliggende stukken ten grondslag hebben gelegen aan het inkooponderdeel en de eventuele specifieke normenkaders die gebruikt zijn.

In de ICO-Wizard worden de eisen die van toepassing zijn op de verschillende inkooponderdelen kort getypeerd. Via de aangevinkte inkooponderdelen verwijzen deze typeringen naar de hiergenoemde onderliggende documenten met gedetailleerde beschrijvingen. In de ICO-Wizard is steeds de samenvatting van de eis weergeven (het wat).

Door selecties te maken die passen bij de karakteristiek van de in te kopen producten en diensten wordt de set van standaardeisen verkregen. De op deze wijze geselecteerde eisen gelden als baseline. Als de opdrachtgever vanuit zijn of haar risicoanalyse geen wijzigingen aangeeft, dan gelden de eisen als uitgangspunt voor de aanbesteding, contractering, acceptatie en levering van het product/de dienst.

3.1 Beveiligingseisen Software

Het begrip software omvat een veelheid van onderwerpen. Als inkooponderdeel behoeft dit nadere onderscheiding. Binnen de ICO Wizard onderscheiden we de volgende onderdelen:

a. Maatwerkapplicaties en applicatiepakketten: Een applicatie kan worden verworven door interne ontwikkeling, uitbesteding of inkoop van een commercieel product, niet zijnde standaard software. Aanvullend wordt hier onder wordt verstaan applicaties voor specifieke toepassing die wel als pakket worden aangeboden (bijv. pakket voor sociale diensten etc.). De Secure Software Development (SSD) beveiligingseisen zijn opgesteld om zowel voor de interne als de externe leverancier van applicatiepakketten te ondersteunen. Wanneer er sprake moet zijn van authenticatie met behulp van DigiD, is toepassing vereist van een specifieke selectie van normen welke worden getoetst door Logius. Deze eisen kunnen geselecteerd worden door het inkooponderdeel DigiD aan te vinken.
b. Mobiele Apps: betreft Applicaties die als 'app' geïnstalleerd kunnen worden en draaien binnen het besturingssysteem van het mobiele apparaat, of als onderdeel van de webpagina meekomen en draaien binnen mobiele browsers. In het normenkader zijn de beveiligingseisen voor 3 soorten apps opgenomen (Webapps: dit zijn applicaties die alleen in een webbrowser draaien, Native apps: draaien binnen het besturingssysteem op het mobiele apparaat, Hybride apps: hybride apps zijn een combinatie van webapps en native apps).
c. Standaardpakketten (ERP, KA-pakketten etc.): de specifieke beveiligingseisen voor deze vorm van software zijn nog in ontwikkeling en worden in de loop van 2020 opgenomen in de ICO Wizard.

Gedetailleerde informatie over de eisen op de het gebied van software zijn opgenomen in de volgende documenten:

- Secure Software Development (SSD) Eisen aan (Web-)applicaties. Zie link: https://www.cip-overheid.nl/category/producten/secure-software/#grip-op-ssd-de-normen
- Secure Software Development (SSD) Eisen aan mobiele applicaties. Zie link: https://www.cip-overheid.nl/category/producten/secure-software/#grip-op-ssd-de-normen-voor-mobiele-apps
- BIO-Thema-uitwerking Applicatie. Zie link: https://www.cip-overheid.nl/category/producten/bio/#applicatieontwikkeling
- Beveiligingsrichtlijnen WEB-applicaties. Zie link: https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties

3.2 Beveiligingseisen Serverplatform

Het inkooponderdeel Serverplatform beperkt tot de basis functionaliteit en algemene onderwerpen die gerelateerd zijn aan serverplatforms. Het betreft componenten als server-hardware, virtualisatietechnologie en besturingssysteem (OS). Naast de betreffende normen vanuit de BIO wordt hier ook gebruik gemaakt van andere Best Practices als: SoGP en NIST.

Gedetailleerde informatie over de eisen op de het gebied van Serverplatform zijn opgenomen in het volgende document. Zie link:

https://www.cip-overheid.nl/category/producten/bio/#serverplatform

3.3 Beveiligingseisen Communicatievoorzieningen

Het inkooponderdeel Communicatievoorzieningen betreft een aantal verschillende type soorten communicatievoorzieningen:

a. Openbare diensten zoals: Instant messaging en sociale media.
b. Elektronische berichten – informatie opgenomen in elektronische berichten (inhoud).
c. Informatietransport - het transporteren van informatie via allerlei communicatiefaciliteiten, zoals: email, telefoon, fax video (inhoud).
d. Netwerkdiensten - het leveren van aansluitingen, zoals: firewalls, gateways, detectiesystemen en technieken voor te beveiligen netwerkdiensten, zoals authenticatie, netwerk (infrastructuur) - dit betreft de fysieke en logische verbindingen.

Naast de betreffende beveiligingseisen vanuit de BIO worden onder dit inkooponderdeel de specifiek van toepassing zijnde beveiligingseisen van andere baselines, zoals de BSI, de NIST en SoGP.

Gedetailleerde informatie over de eisen op de het gebied van Communicatievoorzieningen zijn opgenomen in het volgende document. Zie link:

https://www.cip-overheid.nl/category/producten/bio/#communicatievoorzieningen

3.4 Beveiligingseisen Huisvesting IV

Het inkoop onderdeel Huisvesting IV omvat met name de eisen die gesteld moeten worden aan de fysieke bescherming van de apparatuur, die gebruikt wordt voor verwerking, transport en opslag van data. Betreft de traditionele huisvesting waarbij het rekencentrum is ondergebracht binnen één fysieke locatie en die gerelateerd zijn aan terreinen, gebouwen, ruimten en middelen.

Gedetailleerde informatie over de eisen op de het gebied van Huisvesting IV zijn opgenomen in het volgende document. Zie link:

https://www.cip-overheid.nl/category/producten/bio/#huisvesting-informatievoorziening

3.5 Beveiligingseisen Toegangsbeveiliging

Het inkooponderdeel Toegangsbeveiliging omvat het geheel aan richtlijnen, procedures en beheersingsprocessen, systemen en faciliteiten die noodzakelijk zijn voor het verschaffen van toegang tot informatiesystemen, besturingssystemen, netwerken, mobiele devices en telewerken van een organisatie.

Gedetailleerde informatie over de eisen op de het gebied van Toegangsbeveiliging zijn opgenomen in het volgende document. Zie link:

https://www.cip-overheid.nl/category/producten/bio/#toegangsbeveiliging.

3.6 Beveiligingseisen Clouddiensten

Het inkooponderdeel Clouddiensten omvat een overzicht van de uitwerking van Clouddiensten vanuit de optiek van CSC (Cloud Service Consumer). De toepassing van Cloudcomputing is een omgeving waarbinnen leveranciers functionaliteit of diensten in de vorm van een technologische blackbox aanbieden, wat betekent dat clouddiensten gekozen worden op basis van een vooraf vastgestelde 'diensten menu kaart'. In het algemeen onderscheid men drie soorten IT-Clouds:

a. Private Cloud (met een dedicated infrastructuur): De IT-voorzieningen zijn ingericht voor één klant.
b. Private/Shared Cloud (met een geheel of gedeeltelijk gedeelde infrastructuur): De IT-voorzieningen zijn toegankelijk voor één klant en delen om kosten te besparen de onderliggende infrastructuur met andere klanten (bijvoorbeeld de opslag en het netwerk).
c. Public Cloud: De IT-voorzieningen zijn toegankelijk via het Internet. De voorzieningen worden meestal gedeeld met andere klanten.

De meest bekende soorten Clouddiensten zijn:
- Software as a Service (SaaS): bij SaaS staat de applicatie volledig onder controle van de dienstverlener.
- Platform as a Service (PaaS): bij PaaS worden de platformen en de infrastructuur beheerd door de CSP en niet de applicaties.
- Infrastructure as a Service (IaaS): Bij IaaS wordt alleen de infrastructuur beheerd door de CSP en niet de applicaties en de platformen.

Gedetailleerde informatie over de eisen op de het gebied van Clouddiensten zijn opgenomen in het volgende document. Zie link:

https://www.cip-overheid.nl/productcategorie%c3%abn-en-worshops/producten/bio-en-uitwerkingen/#Cloud

3.7 Verificatiemethode(n)

Het stellen van eisen in inkoopprocessen is pas effectief als ook geverifieerd wordt of de levering voldoet aan de gestelde eisen. Verschillende vormen van verificatie kunnen sterk uiteenlopen: van directe bewijsvoering zoals acceptatietesten en aanlevering van bewijstukken tot indirecte methoden als audits en verklaringen van derde partijen. Daarnaast is het een keuze - veelal bepaald door de kosten die het met zich meebrengt - welke methodes toegepast zullen worden en of ze in volledigheid worden toegepast dan wel in de vorm van steekproeven. Sommige eisen lenen zich voor directe verificatie methoden, andere (de meeste) juist niet. Dit is dus sterk bepalend voor de te kiezen methode.

De aard van de norm en de kosten zullen dus bepalend zijn voor de vraag hoe verificatie plaatsvindt.

Om toch een handvat aan te reiken is in de kolom 'Verificatiemethode(n) aangegeven welke methoden mogelijk zouden zijn bij de desbetreffende eis. Waar van toepassing zijn meerdere mogelijkheden weergeven.

De geadviseerde methoden zijn:

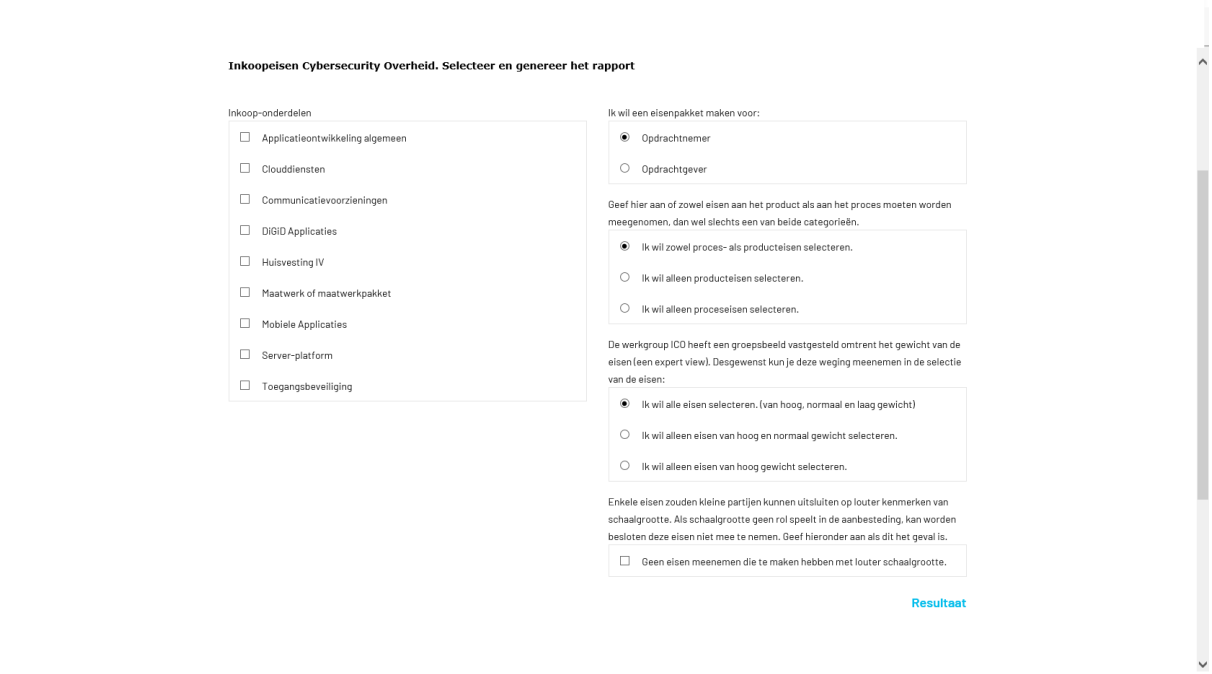
Verificatiemethode	Toelichting
Interne controle	Komt voor bij eisen die voor de opdrachtgever zelf zijn, dan wel mede voor hem.
Overleg bewijsstukken	Komt voor bij opdrachtnemer-eisen waarbij sprake is van geheel of gedeeltelijke toets baarheid op basis van documenten die in de eis al verondersteld zijn.
Testen	Komt voor bij opdrachtnemer-eisen die op geleverd materiaal zien dat toetsbaar is in een testproces. Er is geen onderscheid gemaakt tussen verschillende vormen van testen, maar met name moet gedacht worden aan acceptatietesten en pentesten.
Verklaring (derde partij)	Komt voor bij opdrachtnemer-eisen die niet of slechts deels te verifiëren zijn met voorgaande methoden. 'Verklaring' betekent hier een verklaring van een derde partij waarin de desbetreffende eis is meegenomen. Vormen kunnen zijn: audits en TPM-achtige verklaringen.
Internet.nl	Komt voor bij eisen waarop ook aanvullingen van toepassing zijn uit de Pas-Toe-of-Leg-Uit-lijst van het Forum Standaardisatie. Met internet.nl kan direct getoetst worden of deze aanvulling in werking is.

4.0 Instructie gebruik ICO-Wizard

De ICO-Wizard bevat een uitgebreid pakket van informatiebeveiligingseisen die een rol spelen bij aanbestedingen en inkopen. Met behulp van selectievelden kunnen eisenpakketten worden geselecteerd die passen bij specifieke inkoopsegmenten of combinaties daarvan, en kunnen nadere verfijningen daarop worden toegepast.

4.1 Samenstellen standaardeisenpakket

Afhankelijk van de soort inkoop wordt een eisenpakket samengesteld. Bij inkopen die onderdelen bevatten uit meerdere inkoop(sub)segmenten, wordt het eisenpakket samengesteld uit de eisen die op deze (sub)segmenten betrekking hebben.



4.1.1 Invulvelden

1. Inkoop-onderdelen: vul hier in voor welke inkoopsegmenten je beveiligingseisen wilt selecteren. Meerdere combinaties zijn mogelijk. Wanneer je meer wilt weten over het betreffende inkooponderdeel kun je de handreiking Inkoop ICO gebruiken. Hierin wordt per inkooponderdeel context en inhoud geschetst.
2. Eisenpakket voor opdrachtnemer of opdrachtgever: de Wizard is primair bedoeld om eisen aan de (producten/diensten van) de leverancier te stellen. Bijna altijd zijn er ook op de BIO gebaseerde informatiebeveiligingseisen voor jezelf van kracht. Deze kun je apart selecteren via het selectieveld opdrachtgever.
3. Proces en/of producteisen: de Wizard gaat er standaard vanuit dat zowel proces- als producteisen van toepassing zijn. Je kunt afhankelijk van je inkoop impactanalyse expliciet kiezen voor een van de twee. Producteisen zijn met name van belang wanneer het gaat om eisen t.b.v. specifieke producten of oplevering van bijvoorbeeld een softwarepakket. Proceseisen zijn met name van belang wanneer het gaat om eisen t.b.v. mantels, waarbij producten (nog) niet aan de orde zijn.
4. Prioriteit van de eisen: de Wizard selecteert standaard alle prioriteiten die door de brede interbestuurlijke werkgroep als 'expert view' aan de betreffende eis zijn gegeven. Je kunt afhankelijk van je inkoop impactanalyse een andere prioriteitselectie maken.
5. Schaalgrootte: enkele beveiligingseisen zouden kleine partijen louter op kenmerken van schaalgrootte kunnen uitsluiten. Als schaalgrootte geen rol speelt in het inkoopproces kan besloten worden deze eisen niet mee te nemen. Je kunt in die situatie het selectieveld aanvinken.

4.1.2 Resultaat

Als je op de knop resultaat drukt, krijg je de informatie beveiligingseisen te zien die op basis van jouw selectie van toepassing zijn. Bovenaan zie je hoeveel eisen je geselecteerd hebt. Wanneer je een ongeldige combinatie van selectie eisen hebt gemaakt, krijg je geen resultaat terug. Wanneer je op basis van het resultaat een wijziging in de selectie wil maken, vink dan de betreffende selectievelden aan en druk opnieuw op resultaat. Je krijgt nu de nieuwe selectie te zien.

4.1.3 Rapport opmaken

Nadat je het resultaat hebt opgevraagd, verschijnt er een knop 'Rapport opmaken'. Als je op de knop rapport opmaken drukt, wordt er automatisch een Word-export aangemaakt. Het rapport kun je bijvoegen bij de documentatie die je naar de leverancier stuurt in het kader van het inkooptraject.

In dit document kun je op de 1ste pagina je eigen logo toevoegen en de velden "Samengesteld door', 'Organisatie' en een vrij tekstveld invullen. De datum waarop het rapport is opgemaakt wordt automatisch gegenereerd.

Op de 3de pagina vind je een blok terug met de door jouw ingegeven criteria en het aantal eisen dat gegenereerd is. Daarnaast vind je hier de links naar de vindplaatsen van alle normenkaders. Deze zijn in de eerste plaats bedoeld voor de leverancier. Ze bevatten namelijk de uitwerking van de eisen die in het rapport staan. Bij de toets op de uiteindelijke levering dienen ze als achtergrond voor auditers en testers.

Vanaf de 4de pagina worden alle eisen apart in blokken weergegeven. In deze blokken zijn de volgende zaken opgenomen:

- De referentiecode van de norm gebaseerd op de BIO en aanvullende normenkaders.
- Het referentie document behorende bij het geselecteerde inkooponderdeel.
- Het BBN-niveau uit de BIO (meestal 2).
- Relevante standaard PToLU-lijst Forum Standaardisatie: Wanneer op de betreffende beveiligingslijst een standaard uit de lijst van toepassing is, wordt deze hier getoond.
- Samenvatting van de eis: een beknopte omschrijving van de eis. Voor eventuele aanvullende informatie kun je het betreffende brondocument benaderen via de hyperlinks op de 3de pagina.
- Suggesties voor verificatiemethoden: betreft een advisering op welke wijze je kunt toetsen bij de leverancier of aan de eis is voldaan.
- Toelichting: Je hebt bij de toelichting de gelegenheid om aanvullende opmerkingen met betrekking tot de eis te maken, die je op basis van de inkoop impactanalyse of op verzoek van de behoefte steller wil toevoegen.