Handreiking Inkoop ICO

Inkoopeisen Cybersecurity Overheid

November 2021 [versie 2.0 definitief]

ICO Wizard

Titel	Handreiking ICO Wizard
Datum	November 2021
Versie	2.0 Definitief
Opdrachtgever	Voorzitter werkgroep BIO en directeur CIP
Regime	Becommentarieerde praktijk
Auteurs	Ad Reuijl, Yosta Dammen
Reviewers	Versie 1.0: Werkgroep ICO, Elleke Oosterwijk

Versie en status	Datum	Auteur	Distributie	Wijziging
1.0	15/10/2020	Ad Reuijl, Yosta Dammen	Publicatie op CIP.overheid	
1.1	7/12/2020	Yosta Dammen		Toevoegen aanpassingen ICO-Wizard, aanvulling Inkoopproces
1.2	18/1/2021	Elleke Oosterwijk	Yosta	Nieuwe CIP template
1.3	21/1/2021	Elleke/Yosta		Opmerkingen weggewerkt
2.0	25/11/2021	Ad Reuijl		Wijzigingen: Systematiek van aanvullende selecties, procesautomatisering, Privacy, BIO-O-maatregelen

Considerans

CIP-producten steunen op kennis van professionals uit verschillende organisaties actief in het CIP-netwerk, zowel uit de overheid als de markt.

Opmerkingen en aanvullingen kun je melden op cip-overheid.nl/contact.

Inhoudsopgave

1 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, moet ook de verwerving van ICT-middelen via inkopentrajecten en uitbestedingen voldoen aan de veiligheidseisen.

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

1.1 Waarom specifieke cyber security criteria voor leveranciers?

Voor alle overheidsorganisaties geldt de BIO als baseline voor het treffen van beveiligingsmaatregelen. De generieke eisen in de BIO moeten op basis van risicoanalyse in organisatie specifieke maatregelen worden vertaald, zo ook voor in te kopen of uit te besteden ICT-producten en -diensten.

Inkoop richt zich meestal op concrete producten en diensten. Bij het opstellen van de beveiligingseisen bij zo'n product of dienst moeten uit de BIO de relevante controls worden gedestilleerd. Om dat proces te vergemakkelijken zijn specifieke thema's ontwikkeld zoals toegangsbeveiliging, clouddiensten en applicatieontwikkeling. Per thema is bepaald welke BIO-controls relevant zijn. Vervolgens is uitgewerkt welke concrete maatregelen nodig zijn om zo'n thema op BBN2-niveau te beveiligen. Naast de verplichte overheidsmaatregelen uit de BIO en de implementatierichtlijnen uit de ISO 27002 is daarbij tevens dankbaar gebruik gemaakt van maatregelensets bijv. uit de NIST, BSI en SoGP, met aanvullingen daarop vanuit de Pas Toe of Leg Uit lijst van het Forum Standaardisatie, de Richtlijnen van het NCSC en Grip-op-SSD (Secure Software Development). Op deze wijze is per thema een complete set van te treffen maatregelen bepaald die elke organisatie desgewenst, op basis van een gedegen risicoanalyse, nog verder kan aanpassen aan de specifieke lokale omstandigheden. Al deze eisen kunnen worden opgenomen als concrete inkoopeisen in aanbestedingen.

1.2 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 hoofdstukken 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. Daarom is het van belang de rollen in het inkoopproces te bezetten met de mensen die daarvoor in de organisatie verantwoordelijkheid dragen en daarvoor de benodigde IB-kennis hebben.

2 Het inkoopproces, rollen en betrokkenheid bij de Inkoopeisen

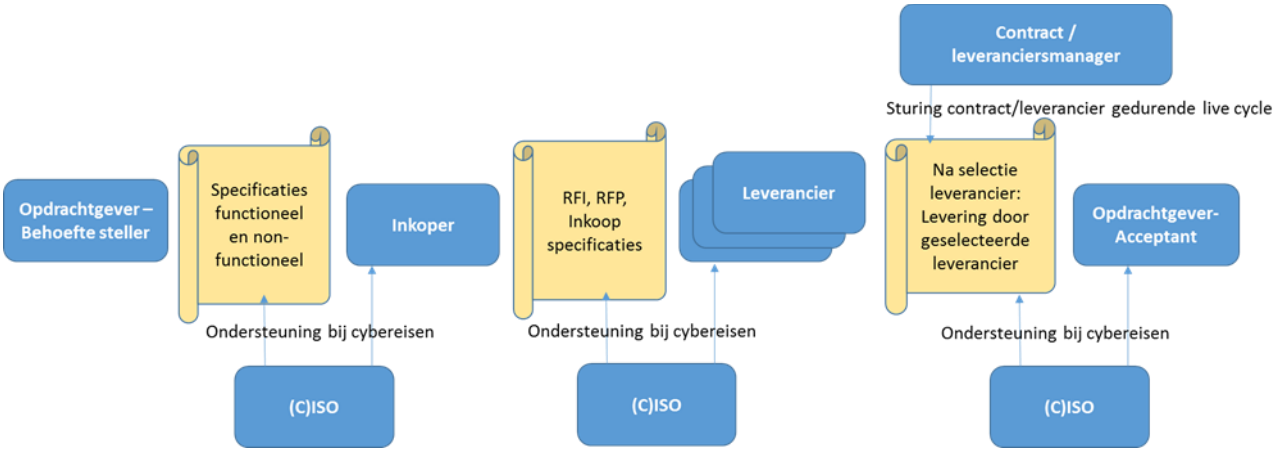
Hieronder volgt een overzicht van de rollen in het inkoopproces en de betrokkenheid bij de eisen. Omdat het stellen van eisen alleen zin heeft wanneer die ook worden nagekomen en getoetst, is gekozen voor een brede processcope, van behoefte tot levering. De duiding van de rollen is zo generiek mogelijk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

2.1 Inkoopprocessen en security-eisen

De term 'Inkoopprocessen' wordt in deze handreiking gehanteerd in de meest ruime zin van het woord. Daarvoor zijn twee redenen:

1. Het toepassen van de ICO-Wizard is mogelijk en zinvol in een breed scala van verwervingsvarianten, bijvoorbeeld:
    - Europese aanbestedingen van mantels, van specifieke producten, van diensten, van projecten, etc;
    - Minicompetities binnen mantels;
    - Inkopen/offerteaanvragen, bijv. met driepartijen-offertes of direct naar één partij;
    - Uitbestedingen aan Shares Service Centra;
    - Opdrachten binnen de eigen organisatie, bijv. van producteigenaar aan ontwikkelafdeling.
2. De ICO-Wizard is in elk soort verwervingsproces toepasbaar, ongeacht de precieze inrichting van het inkoopproces in de specifieke organisatie. Organisaties kunnen binnen hun eigen proces het gebruik van de Wizard inbedden. Wel is van belang dat de juiste rollen betrokken zijn in het inkoopproces. Vandaar dat we hier de nadruk leggen op die rollen.

Onderstaande afbelding geeft schematisch het verband van de verschillende rollen weer. In de praktijk zullen er meer betrokkenen zijn, bijv. juristen, auditors, andere specialisten en interne stakeholders. Het gaat hier echter niet om een uitputtende beschrijving van het inkoopproces. De focus ligt hier nadrukkelijk op enkele basisrollen die van cruciaal belang zijn bij het stellen van informatieveiligheidseisen en derhalve te maken hebben met het inzetten van de ICO-Wizard.



Afbeelding 1: Bij het stellen van informatiebeveiligingseisen (Cybereisen) betrokken rollen in het inkoopproces

2.2 Rol opdrachtgever-behoeftesteller

De opdrachtgever-behoeftesteller kan zijn een businessverantwoordelijke, productmanager, informatiemanager etc. De opdrachtgever is verantwoordelijk voor het informatiesysteem waarbinnen de via inkoop te verwerven producten en/of 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. De veiligheidseisen zijn standaard voor ieder 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

De inkoper 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 het resultaatrapport uit de ICO-Wizard 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 en toets, de realisatie van de beveiligingsmaatregelen wordt bevestigd door de leverancier. 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- of leveranciersmanager

In veel organisaties is de rol van contract- of leveranciersmanager 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 (kunnen) 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.

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

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

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

2.7 Rol (C)ISO

De CISO (Chief Information Security Officer) heeft binnen het inkoopproces de rol van adviseur/ondersteuner op het terrein van informatiebeveiliging. Al naar gelang de behoeftesteller en/of inkoper meer of minder kennis heeft van dit aandachtsgebied zal die ondersteuning van minder of meer belang zijn, waarbij wel aangetekend wordt dat de CISO zijn verantwoordelijkheid moet kunnen nemen in alle hoeken van de organisatie. Ook in die van de inkoopprocessen.

3 Inkooponderdelen

Binnen de ICO-Wizard zijn beveiligingseisen geclusterd naar inkooponderdeel samen gebracht. Per inkooponderdeel wordt een toelichting gegeven op de inhoud van het onderdeel, 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 een 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 of de dienst.

3.1 Beveiligingseisen Software

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

1. 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 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 de interne als de externe leverancier van applicatiepakketten te ondersteunen. Wanneer 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.
2. Mobiele Apps: Dit 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: dit zijn applicaties de draaien binnen het besturingssysteem op het mobiele apparaat; Hybride apps: dit zijn applicaties die een combinatie van webapps en native apps zijn).
3. Standaardpakketten (ERP, KA-pakketten etc.): de specifieke beveiligingseisen voor deze vorm van software zijn nog in ontwikkeling en worden in de loop van 2021 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
- Secure Software Development (SSD) Eisen aan mobiele applicaties
- BIO-Thema-uitwerking Applicatieontwikkeling
- Beveiligingsrichtlijnen WEB-applicaties
- Softwarepakketten.

3.2 Beveiligingseisen Serverplatform

Het inkooponderdeel Serverplatform beperkt zich 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 aanvullend gebruik gemaakt van andere Best Practices als: SoGP en NIST.

De gedetailleerde informatie over de eisen op het gebied van dit thema zijn opgenomen in het document Serverplatform.

3.3 Beveiligingseisen Communicatievoorzieningen

Het inkooponderdeel Communicatievoorzieningen betreft een aantal verschillende soorten

1. Openbare diensten zoals: instant messaging en sociale media;
2. Elektronische berichten: informatie opgenomen in elektronische berichten (inhoud);
3. Informatietransport: het transporteren van informatie via allerlei communicatiefaciliteiten, zoals email, telefoon, video (inhoud);
4. Netwerkdiensten: het leveren van aansluitingen, zoals firewalls, gateways, detectiesystemen. En technieken voor te beveiligen netwerkdiensten, zoals authenticatie, netwerk (infrastructuur). Het betreft zowel de fysieke als 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 gebruikt.

Gedetailleerde informatie over de eisen op het gebied van dit thema zijn opgenomen in het document 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. Het 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 het gebied van dit thema zijn opgenomen in het document Huisvesting Informatievoorzieningen.

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 het gebied van dit thema zijn opgenomen in het document 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 black-box

aanbieden, wat betekent dat clouddiensten gekozen worden op basis van een vooraf vastgestelde 'diensten menukaart'. In het algemeen onderscheid men drie soorten IT-Clouds:

1. Private Cloud (met een dedicated infrastructuur): De IT-voorzieningen zijn ingericht voor één klant.
2. 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).
3. 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 (Cloud Service Provider) 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 het gebied van dit thema zijn opgenomen in het document Clouddiensten.

3.7 Beveiligingseisen Procesautomatisering

Het inkooponderdeel Procesautomatisering omvat proces- en systeemeisen die gesteld moeten worden bij de aanschaf van zogenaamde Industrial Control Systems, industriële objecten waarbij digitale componenten en aansturing een rol speelt. Het binnen de Watersector overeengekomen kader CSIR (Cybersecurity Implementatierichtlijn Objecten) is als basis gehanteerd voor deze eisen. CSIR is gebaseerd op IEC62443 en heeft relaties met de BIO. Het kader en daarmee dit inkooponderdeel in ICO is ook toepasbaar buiten de Watersector waar procesautomatisering een rol speelt. Gedetailleerde informatie over de eisen op het gebied van dit thema zijn opgenomen in het document CSIR.

3.8 Algemene eisen Ketenpartners

Naast de inkoop-specifieke selectiemogelijkheden kan het voorkomen dat buiten de specifieke eisen het toch ook in algemene zin nodig is dat de leverancier zich richt naar de BIO als geheel. Dit geldt vooral bij langdurige uitbestedingsrelaties. De leverancier maakt dan als het ware onderdeel uit van de keten van dienstverlening van de uitbestedende overheidsorganisatie. Het onderdeel 'Algemeen Ketenpartners' bevat enkele algemene eisen die opgelegd kunnen worden in het geval hiervan sprake is.

Als de keuze voor aanvullende privacy-eisen wordt gemaakt (zie beschrijving hoofdstuk 4), levert de selectie op Algemeen Ketenpartners ook nog een set van algemene privacy-eisen op.

NB. De keuze voor Algemeen Ketenpartners komt niet in de plaats voor de specifieke inkooponderdelen, maar zijn een toevoeging voor de hier beschreven ketenpartnerrelaties.

4 Supplementen op inkooponderdelen

Naast de basisselectie op de onderdelen in hoofdstuk 3, biedt ICO ook de mogelijkheid aanvullende eisen te selecteren bij de gekozen inkooponderdelen. Op dit moment beperkt zich dat tot Privacy-aanvullingen, maar in de toekomst kunnen naar verwachting ook de ABDO-eisen van het ministerie van Defensie worden toegevoegd, met keuzen op verschillende te beschermen niveaus.

4.1 Privacy-supplementen

Naar aanleiding van de motie Kröger in februari 2021 is ICO uitgebreid met eisen die zijn ontleend aan Privacy-by-design principes en aan de AVG. Ze zijn toegevoegd als supplementen op een aantal inkooponderdelen. Het betreft aanvullingen, aangezien een deel van de eisen binnen de bestaande inkooponderdelen ook al privacybeschermende effecten hebben. De aanvullende eisen worden alleen meegenomen in de output indien de gebruiker expliciet daarvoor kiest. De privacy-aanvullingen zijn gebundeld in één document. Gedetailleerde informatie over deze eisen is opgenomen in het document Privacy-supplementen BIO-Thema-uitwerkingen.

4.2 Verwacht in de nabije toekomst: ABDO

Nog niet gerealiseerd.

5 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.

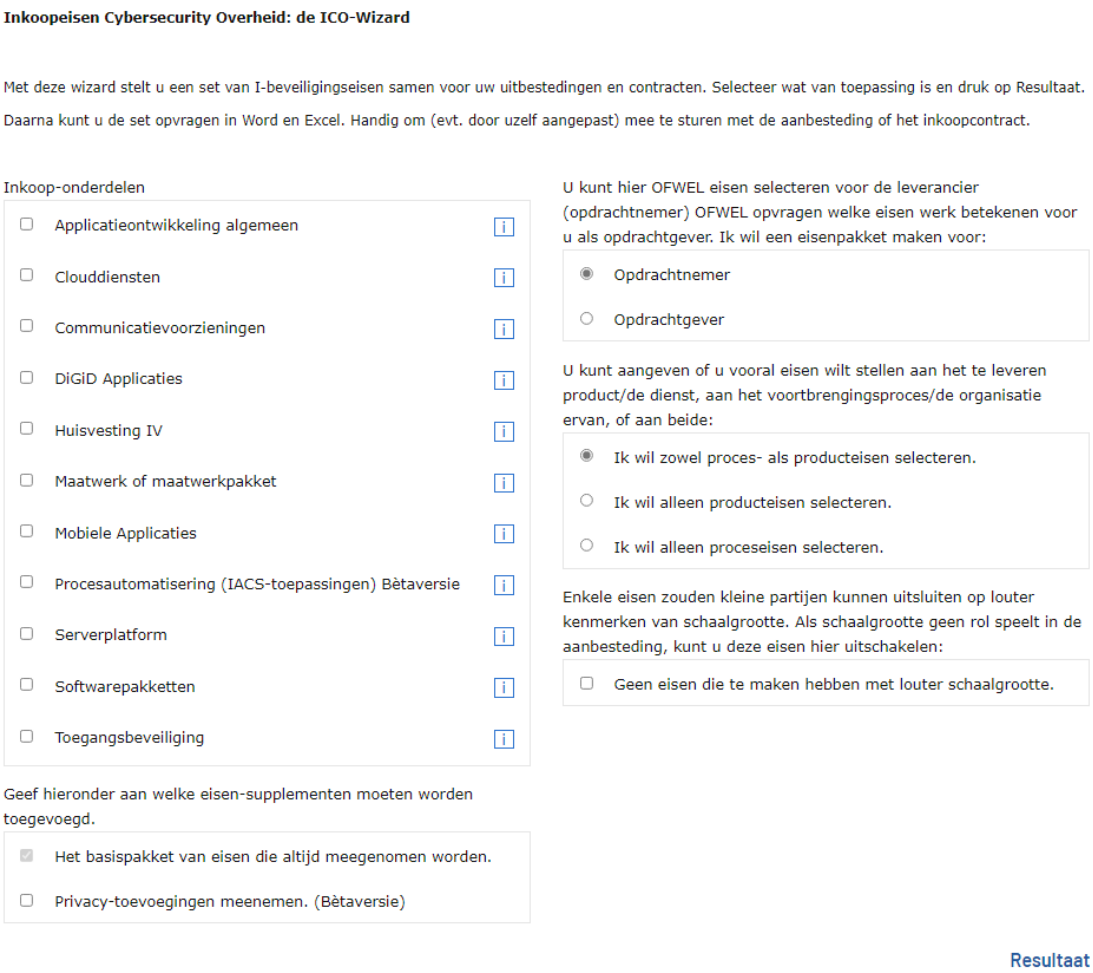
De geadviseerde methoden zijn:

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 toetsbaarheid op basis van documenten die in de eis al verondersteld zijn.
Testen	Komt voor bij opdrachtnemer-eisen waarbij sprake is van op geleverd materiaal (software) en de geleverde functionaliteiten getoetst moeten worden 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.

6 Toepassing van de 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.

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



Afbeelding 2: schermprint van de Wizard.

Ga naar [ICO Wizard - bio-overheid] voor de direct bruikbare wizard.

6.1 Selectiemogelijkheden

Inkooponderdelen

De voornaamste selecties staan op de linkerhelft van de pagina. Dit betreft de inkooponderdelen. Vul hier in voor welke inkoopsegmenten je beveiligingseisen wilt selecteren. Meerdere combinaties zijn

mogelijk. De i-blokjes achter de omschrijvingen geven aan wanneer je de keus voor het desbetreffende inkooponderdeel zou kunnen maken. In deze handreiking, bij hoofdstuk 3, kun je daar meer informatie over vinden. Ook kun je onderin de linker kolom voor de privacy-aanvullingen kiezen.

Opdrachtnemer of opdrachtgever

De ICO-Wizard is primair bedoeld om eisen aan de producten/diensten van een leverancier/opdrachtnemer te stellen. Bijna altijd zijn er ook informatiebeveiligingseisen voor jezelf van kracht. Naast het selecteren van een eisenpakket voor de opdrachtnemer is hier ook mogelijk gemaakt een pakket te selecteren met eisen waarbij de opdrachtgever zelf een rol heeft. Dit is een 'of/of'-knop: je selecteert hiermee dus of een pakket voor de opdrachtnemer of voor de opdrachtgever.

Proces en/of producteisen

De ICO-Wizard gaat er standaard vanuit dat zowel proces- als producteisen van toepassing zijn. Je kunt afhankelijk van je inkoop impactanalyse ook expliciet kiezen voor één 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 of maatwerk, een serverplatform, etc. Proceseisen zijn met name van belang wanneer het gaat om eisen t.b.v. mantels, waarbij levering van producten/diensten (nog) niet aan de orde zijn. Met deze knop kun je dus een deel van de eisen uitschakelen.

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, waarmee die eisen worden uitgeschakeld.

6.2 Resultaat

Met een klik op de knop 'Resultaat', krijg je op het scherm de beveiligingseisen te zien die op jouw selectie van toepassing zijn. Bovenaan staat het aantal eisen uit de selectie. Wanneer je geen resultaat krijgt, heb je een niet bestaande combinatie van selecties gemaakt.

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.

De eisen worden hier met een korte omschrijving gepresenteerd. De kolommen voorafgaande aan de omschrijving bevatten de referenties naar de brondocumenten, waarin de uitwerkingen van de eisen te vinden zijn. Dit is met name van belang voor de leveranciers en later bij de beoordeling van de levering.

Voor de beoordeling van de levering is een kolom met mogelijke validatievormen weergegeven.

Als het resultaat op het scherm staat, verschijnen ook knoppen voor de Resultaat, Rapport maken en Export (xlsx), waarover meer in de volgende paragrafen.

Wanneer je weer naar boven beweegt, kun je de selectie opnieuw maken en met gebruik van de Resultaat knop wordt het nieuwe resultaat getoond.

6.3 Gebruik van Rapport maken

Na het opvragen van het resultaat, kun je door een klik op de knop 'Rapport opmaken' een Word-document downloaden met de gegevens van de selectie. Dit document is bedoeld om - na aanvulling met gegevens van de eigen organisatie en evt. aanpassingen en verwijderingen van eisen - mee te

sturen als onderdeel van de documentatie die naar de leverancier(s) gaat. (RFP, offerteaanvraag, contract, etc).

In dit document kun je op de eerste 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 derde 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 de uitwerking van de eisen die in het rapport staan. Bij de toets op de uiteindelijke levering dienen ze als achtergrond voor auditors en testers.

Vanaf de vierde 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.
- BIO-O-maatregel van toepassing. Dit signaleert dat een (in de BIO verplichte) overheidsmaatregel onderdeel uitmaakt van de eis.
- 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.
- Mogelijke 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 risicoanalyse of op verzoek van de opdrachtgever/behoeftesteller wil toevoegen.

In sommige situaties zal er behoefte kunnen bestaan eisen te verwijderen. Bijvoorbeeld bij eisen die betrekking hebben op functionaliteit die niet passen in de scope van de in te kopen functionaliteit. In dat geval kunnen de desbetreffende eisen verwijderd worden uit het Word-document. Ook risicoafwegingen kunnen leiden tot bijstellen van de eisen. Zie hierover verder bij gebruik van de Excel-export en bij Risicomanagement.

6.4 Gebruik van de Export (xlsx)

Na het opvragen van het resultaat, kun je door een klik op de knop 'Export .xlsx' een Excel-document downloaden met de gegevens van de selectie. Naast de hiervoor opgesomde gegevens in de Word-Export bevat het Excel-sheet aanvullende informatie. Met name de relatie van de beveiligingseisen met dreigingen die ze mitigeren zijn hierin terug te vinden. Daarnaast zijn werkkolommen opgenomen voor het vastleggen van de uitvraag van de eisen en (RFC) criteria bij de beoordeling van inschrijvingen op de aanbesteding.

Deze Excel helpt de opdrachtgever op twee belangrijke terreinen:

1. Verbinding van de geselecteerde inkoopeisen met zijn risicoanalyse c.q. risicoafweging;
2. Bepaling van het gewicht dat men in de aanbesteding aan de eisen wil toekennen.

Deze elementen worden nader geschreven in het volgende hoofdstuk.

7 Risicomanagement en gewichtsbepaling inkoopeisen

7.1 Risicomanagement

Uitgangspunt bij het hanteren van de BIO is dat de maatregelen gebaseerd moeten (en mogen) worden op bewuste risicoafwegingen van de proceseigenaar. Op deze wijze kunnen maatregelen proportioneel aan de risico worden gerelateerd: minder(zware) maatregelen bij lage risico's, zwaardere bij hoge risico's.

Waar het vertaling betreft naar inkoopeisen, zoals die met de ICO-Wizard worden geselecteerd, bestaat principieel ook de mogelijkheid de maatregelen aan te passen aan de risico's. In de Word-export kunnen eisen worden verwijderd en worden aangepast. De beschikbare toelichtingsruimte kan gebruikt worden voor aanvullende teksten, opmerkingen, etc.

In de Excel-export staat per eis genoteerd welke dreigingen worden gemitigeerd. Met deze relatie kan een duidelijke verbinding worden gemaakt met de eigen risicoanalyse. In het geval geen risicoanalyse wordt gemaakt, onderbouwt het verband met de dreigingen het belang van de eisen.

NB. Hoewel in de ICO-Wizard en de gegenereerde producten de mogelijkheid bestaat om eisen te verwijderen en te verzwakken, raden we aan om naar de markt/leveranciers zoveel mogelijk de ICO-selectie als basis aan te houden en de flexibiliteit van de ICO-Wizard alleen te gebruiken als eisen verzwaard moeten worden. Het voorkomt dat een onduidelijk beeld naar de markt ontstaat en dat er geen robuust basisniveau van veiligheid in de leveringen ontstaat. Ofwel: liever een robuust basisniveau (BBN2) in wat we samen inkopen in plaats van steeds wisselende uitvragen en dito leveringen.

7.2 Gewichtsbepaling bij aanbestedingen

In de Excel-export zijn enkele werkkolommen opgenomen, waarmee de toepasselijkheid en het gewicht van de eisen voor de aanbesteding c.q. inkoop kan worden aangegeven. (Overigens kan de gebruiker de Excel zelf ook nog uitbreiden met kolommen die hij nuttig acht).

De opdrachtgever kan hiermee voor het vervolgtraject van inschrijvingen, leveranciersgesprekken en selectieproces aangeven welke weging de eisen moeten hebben.

In het licht van zijn risicoafweging kunnen bepaalde eisen bijvoorbeeld als blokkerend worden aangemerkt, is een beveiligingseis inwisselbaar door een andere oplossing, of wordt bijvoorbeeld met de leverancier een oplossingstijd afgesproken.

Ook kunnen op basis van het overzicht eisen worden geïdentificeerd die te maken hebben met functionaliteit die niet in de scope van de aanbesteding zit. In dat geval kunnen ze als niet relevant worden uitgesloten van de aanbesteding en ook uit de Word-export worden verwijderd.

Na het uitbrengen van de RFP/offerteaanvraag volgen gesprekken met de leverancier(s). De door de opdrachtgever aangevulde Excel kan hierbij dan als leidraad dienen om het gesprek over de eisen te voeren en reële afspraken te maken over de realisatie en nakoming.