Handreiking Inkoop ICO

Inkoopeisen Cybersecurity Overheid

April 2026 [versie 2.6 definitief]

Het CIP betracht zorgvuldigheid bij het samenstellen van zijn publicaties. Het kan voorkomen dat er toch sprake is van omissies, onjuistheden en/of gedateerdheid. Het is altijd de verantwoordelijkheid van de lezer zelf dit te beoordelen en desgewenst te corrigeren indien hij zich baseert op of gebruik maakt van een CIP-publicatie. Het CIP ontvangt graag correctieverzoeken en suggesties.



©Centrum Informatiebeveiliging en Privacybescherming. Het CIP heeft voor deze publicatie licentie Creative Commons Naamsvermelding-NietCommercieel-GelijkDelen (CC BY-NC-SA 4.0) verleend. Voor meer informatie zie: https://creativecommons.org/licenses/by-nc-sa/4.0/deed.nl.

ICO-Wizard

Titel	Handreiking ICO-Wizard
Datum	April 2026
Versie	2.6 Definitief
Opdrachtgever	Centrum Informatiebeveiliging en Privacybescherming (CIP)
Regime	Becommentarieerde praktijk
Auteurs	CIP-kernteamleden

Versie en status	Datum	Wijziging	Door
1.0	15/10/2020		CIP-kernteamleden
1.1	7/12/2020	Toevoegen aanpassingen ICO-Wizard, aanvulling Inkoopproces	CIP-kernteamleden
1.2	18/1/2021	Nieuw CIP template	CIP-kernteamleden
1.3	21/1/2021	Feedback verwerkt	CIP-kernteamleden
2.0	25/11/2021	Systematiek van aanvullende selecties, procesautomatisering, Privacy, BIO-O-maatregelen aangepast	CIP-kernteamleden
2.3	15/3/2023	Actualisatie en herstructurering	CIP-kernteamleden
2.4	8/11/2024 1/12/2025	Niet-werkende links vervangen (2024) en waardering eisen in output (2025)	CIP-kernteamleden
2.5	10-2-2026	ABRO in ICO-Wizard en BBN vervallen	CIP-kernteamleden
2.6	29-4-2026	Visuele aanpassingen	CIP-kernteamleden

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	5
1.1	Veilig inkopen begint met toegespitste veiligheidseisen	5
1.2	Dit document	5
2	Het inkoopproces, rollen en betrokkenheid bij de Inkoopeisen	6
2.1	Inkoopprocessen en security-eisen	6
2.2	Rol opdrachtgever-behoeftesteller	7
2.3	Rol inkoper	7
2.4	Rol contract- of leveranciersmanager	8
2.5	Rol leverancier	8
2.6	Rol opdrachtgever-acceptant	8
2.7	Rol (C)ISO	8
3	Toepassing van de ICO-Wizard	9
3.1	Selectiemogelijkheden in de ICO-Wizard	9
3.2	Resultaat	10
3.3	Gebruik van Rapport maken	10
3.4	Gebruik van de Export (xlsx)	11
4	Risicomanagement en gewichtsbepaling inkoopeisen	13
4.1	Risicomanagement	13
4.2	Gewichtsbepaling bij aanbestedingen	13
5	Inkooponderdelen, nadere toelichting	14
5.1	Beveiligingseisen Software	14
5.2	Beveiligingseisen Serverplatform	15
5.3	Beveiligingseisen Communicatievoorzieningen	15
5.4	Beveiligingseisen Huisvesting IV	16
5.5	Beveiligingseisen Toegangsbeveiliging	16
5.6	Beveiligingseisen Clouddiensten	16
5.7	Beveiligingseisen Procesautomatisering	17
5.8	Algemene eisen Ketenpartners	17
6	Supplementen, nadere toelichting	18
6.1	Privacy-supplementen	18

6.2	BIO-Overheidsmaatregelen.	18
6.3	ABRO	18
7	Verificatiemethode(n), nadere toelichting	20

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, in de tweede plaats zijn zij als belangrijke gebruiker van ICT-producten en -diensten verantwoordelijk om een bredere impact in de markt te 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 Veilig inkopen begint met toegespitste veiligheidseisen

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 om 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 uiteraard nader toegespitst kan worden o.b.v. risicoanalyse en specifieke karakteristieken van de inkoop/aanbesteding.

NB. Het opleggen 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.

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. Dan volgt een toelichting op het gebruik van de ICO-Wizard en de relatie met risicomanagement. De laatste hoofstukken zijn gewijd aan nadere toelichting op de belangrijkste onderdelen van de Wizard.

2 Het inkoopproces, rollen en betrokkenheid bij de Inkoopeisen

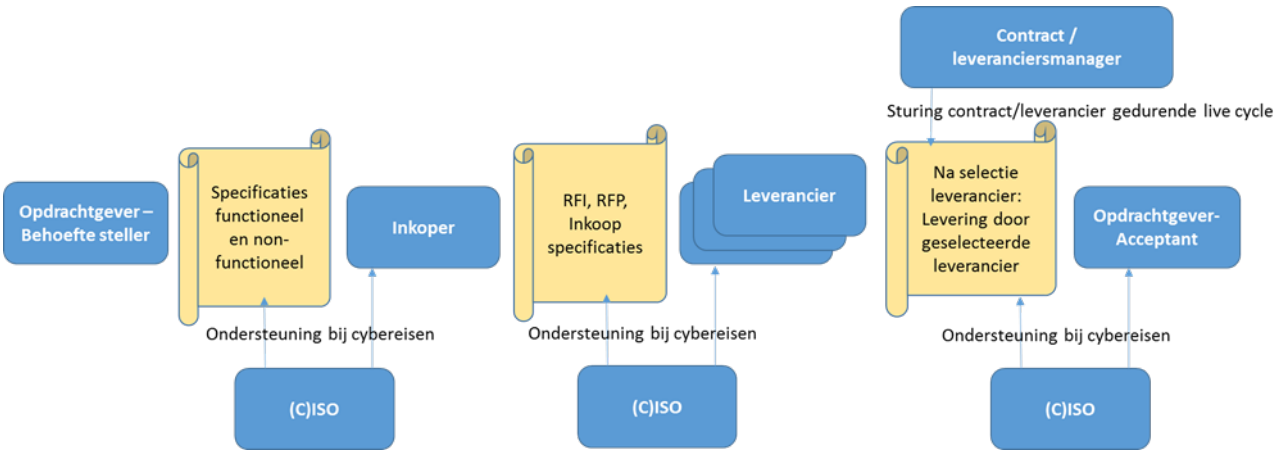
Hieronder volgt een overzicht van de rollen in het inkoopproces en de betrokkenheid bij de eisen. Omdat het stellen van eisen alleen zin heeft wanneer die ook worden nagekomen en getoetst, is gekozen voor een brede processcope, van behoefte tot levering. De duiding van de rollen is zo generiek mogelijk 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:
    a. Europese aanbestedingen van mantels, van specifieke producten, van diensten, van projecten, etc.;
    b. Minicompetities binnen mantels;
    c. Inkopen/offerteaanvragen, bijv. met driepartijen-offertes of direct naar één partij;
    d. Uitbestedingen aan Shares Service Centra;
    e. 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 afbeelding 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: Rollen in de organisatie die zijn betrokken bij het stellen van informatiebeveiligingseisen (Cybereisen) bij aanbestedingen/inkopen.

2.2 Rol opdrachtgever-behoeftesteller

De opdrachtgever-behoeftesteller is degene die verantwoordelijk is voor het informatiesysteem waarop de in te kopen producten en diensten betrekking hebben. In de praktijk kan dat bijvoorbeeld een businessverantwoordelijke, een productmanager of een informatiemanager zijn.

De opdrachtgever is binnen de organisatie 'eigenaar' van de inkopen in zijn domein. Hij is daarmee ook verantwoordelijk voor de risico's op het gebied van de informatieveiligheid van de ingekochte middelen. Om die risico's goed te overzien, dient hij een risicoanalyse uit te (laten) voeren.

De uitkomst van de risicoanalyse is de bril waardoor de informatieveiligheidseisen die met de ICO-Wizard worden verkregen, worden bezien.

De voor goed opdrachtgeverschap belangrijke stappen zijn dan:

- Het (laten) opvragen uit de ICO-Wizard van een op de aanbesteding toegesneden lijst met eisen.
- Het zorgen voor een risicoanalyse.
- Het (doen) finetunen van de eisenlijst o.b.v. de risicoanalyse en de specifieke karakteristieken van de aanbesteding/inkoop.[1]
- Het verbinden van de al of niet aangepaste eisenlijst uit de ICO-Wizard als informatieveiligheidseisen bij de aanbesteding d.m.v. een formele verwijzing daarnaar in RFI, RPF of contract.

2.3 Rol inkoper

De inkoper is de bewaker van het inkoopproces. Hij heeft toezicht op het zorgvuldig uitvoeren van de stappen in het proces en het beschikbaar komen van alle informatie die van belang is. De inkoper zet de vraag in de markt uit. Dat kan via een aanbesteding, een meer-partijen-offerte of een onderhandse offerte.

De inkoper ziet erop toe dat de (al of niet aangepaste) uitkomsten van de ICO-Wizard meegaan met de RFI, de RFP of het contract. 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 moeten beantwoord 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.[2]

De inkoper ziet erop toe dat in de afspraken over acceptatie van de levering, de realisatie van de beveiligingsmaatregelen door de leverancier zelf is getoetst en aan de opdrachtgever bevestigd. 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.

---

[1] Indien uit de risicoanalyse van de opdrachtgever en/of o.b.v. de projectkarakteristieken blijkt dat bepaalde eisen achterwege kunnen blijven dan wel moeten worden verzwaard, wordt dat verwerkt in output van de ICO-Wizard alvorens die mee te sturen naar de opdrachtnemer(s).

[2] Het achterliggende materiaal is direct bereikbaar met hyperlinks in de ICO-output.

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 (Service Level Agreement) 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.[3]

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 informatieveiligheidsmaatregelen.

2.6 Rol opdrachtgever-acceptant

Het stellen van eisen in inkoopprocessen is pas effectief als ook wordt geverifieerd 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 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 verificatiemethoden 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.

Het is van belang dat de CISO zijn verantwoordelijkheid kan nemen in het inkoopproces. Door het specialistische karakter van het vakgebied zal zijn kennis ook nodig zijn om de juiste afwegingen te maken, zowel bij de risicoanalyse, als bij het opvragen en finetunen van de ICO-eisen, als in de rol van adviseur bij de gesprekken met leveranciers.

[3] [3] Het achterliggende materiaal is direct bereikbaar met hyperlinks in de ICO-output.

3 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 inkoopselecties die onderdelen bevatten uit meerdere inkoopsegmenten, wordt het eisenpakket samengesteld uit de eisen die op al deze segmenten betrekking hebben.

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

3.1 Selectiemogelijkheden in de ICO-Wizard

Inkooponderdelen

De voornaamste selecties zijn de selecties van de inkooponderdelen. Klik de onderdelen aan die van toepassing zijn op de inkoop/aanbesteding die in de markt wordt gezet. Meerdere combinaties zijn mogelijk. De i-blokjes achter de omschrijvingen geven aan wanneer je de keus voor het desbetreffende inkooponderdeel zou kunnen maken.

Zie hoofdstuk 5 voor een nadere toelichting op de inkooponderdelen.

Supplementen

Indien gewenst kunnen meerdere supplementen bij de geselecteerde inkooponderdelen worden mee-gekozen:

- Privacyaanvullingen, indien de uitbesteding ook gevoelige persoonsgegevens omvat;
- BIO-overheidsmaatregelen in het geval je wilt zien of er onderliggende verplichte overheidsmaatregelen voorkomen;
- ABRO-eisen in het geval het bedrijven betreft die voor de overheid een opdracht uitvoeren met risico's voor de nationale veiligheid.

Zie hoofdstuk 6 voor een nadere toelichting op de supplementen.

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 de inkopende organisatie zelf 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 óf 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 de 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. Vink in die situatie het selectieveld aan om de desbetreffende eisen uit te schakelen.

3.2 Resultaat

Met één klik op de knop 'Resultaat', worden op het scherm de beveiligingseisen getoond die bij de opgegeven 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, pas de selectie dan aan en druk opnieuw op resultaat. De aangepaste selectie wordt getoond.

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. (Zie hoofdstuk 7 voor een nadere toelichting).

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

3.3 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. Dit kan zijn een RFP (Request for Proposal), offerteaanvraag, contract, PvE (Pakket van Eisen) etc.

In het Word-document kun je op de eerste pagina het 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 selectiecriteria en het aantal eisen dat is gegenereerd. 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:

1. Het referentiedocument behorende bij het geselecteerde inkooponderdeel. (De hyperlink geeft direct toegang tot de vindplaats van het document).
2. De referentiecode van de norm binnen dit referentiedocument. (Waar mogelijk met hyperlink naar een pagina waarop de norm verder is uitgewerkt of kan worden opgezocht).
3. BIO-O-maatregel van toepassing. Dit signaleert dat een (in de BIO verplichte) overheidsmaatregel onderdeel uitmaakt van de eis.
4. Relevante standaard PToLU-lijst Forum Standaardisatie: wanneer op de betreffende beveiligingslijst een standaard uit de lijst van toepassing is, wordt deze hier getoond.

5. 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.
6. Mogelijke verificatiemethoden: betreft een advisering op welke wijze je kunt toetsen bij de leverancier of aan de eis is voldaan.
7. 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.
8. Waardering van de eis:
   MUST – deze eis wordt gewaardeerd als **vereiste**,
   NEED – deze eis wordt gewaardeerd als **moeten willen**,
   NICE – deze eis wordt gewaardeerd als **raadzaam.**

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.

3.4 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.

Waardering eisen:

Bij de getoonde eisen uit de ICO-Wizard is een waardering (MUST, NEED, NICE) toegevoegd in de output (Word én Excel). De waardering van eisen om te stellen aan de opdrachtnemer/opdrachtgever uitgelegd:

MUST – deze eis wordt gewaardeerd als **vereiste**,
NEED – deze eis wordt gewaardeerd als **moeten willen**,
NICE – deze eis wordt gewaardeerd als **raadzaam.**

Dit wil niet zeggen dat alleen de eisen met een waardering **MUST** gesteld moeten worden aan de opdrachtnemer of aan jezelf als opdrachtgever. De waardering geeft richting in belangrijkheid. Het stellen van eisen blijft afhankelijk van de eigen risico-afweging/risico-analyse binnen de organisatie voor het in te kopen product of dienst.

Als inkoper/inkoopteam blijf je verantwoordelijk voor de eisen die gesteld worden. De uitkomsten uit de ICO-Wizard zijn ter ondersteuning (zie ook elders in de handreiking).

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.

4 Risicomanagement en gewichtsbepaling inkoopeisen

4.1 Risicomanagement

De hoeksteen van informatiebeveiliging is risicomanagement. Op basis van een risicoanalyse kunnen maatregelen proportioneel aan de risico's worden gerelateerd: minder(zware) maatregelen bij lage risico's, zwaardere bij hoge risico's. Voor de overheid is risicomanagement verankerd in de BIO. Uitgangspunt bij het hanteren van de BIO is dat de maatregelen moeten (en mogen) worden gebaseerd op bewuste risicoafwegingen van de proceseigenaar.

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 moeten worden verzwaard. 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 in wat we samen inkopen in plaats van steeds wisselende uitvragen en dito leveringen.

4.2 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.

5 Inkooponderdelen, nadere toelichting

Het primaire selectiecriterium in de ICO-Wizard is de selectie van inkooponderdelen. Een inkooponderdeel is op te vatten als een samenhangend deel van het ICT-landschap. Bijv. Cloud en Toegangsbeveiliging, Standaardpakket. Voor elk inkooponderdeel bevat ICO een samenhangende set van informatieveiligheidseisen. Deze inrichting maakt het mogelijk om een set van eisen samen te stellen die in behoorlijke mate past bij de scope van een specifieke aanbesteding. Meerdere inkooponderdelen kunnen tegelijkertijd worden gekozen.

Dit hoofdstuk beschrijft van elk inkooponderdeel kort de inhoud en de context binnen de ICO-Wizard. Daarnaast worden de onderliggende documenten genoemd waarop het inkooponderdeel is gebaseerd, met directe hyperlinks naar de vindplaatsen.

De verschillende outputvormen van de ICO-Wizard bevatten bondige informatie van de geselecteerde eisen, waaronder naam en korte omschrijving van de eis en referenties naar de onderliggende documenten. In deze brondocumenten zijn de eisen nader uitgewerkt. Bij een flink deel van de eisen is de uitgebreide beschrijving ook ondergebracht in de NORA-online. Is deze gevallen bevat de ICO-output ook een directe link naar de detailinformatie van de specifieke eis.

Door selecties te maken die passen bij de karakteristiek van de in te kopen producten en diensten wordt een set van standaardeisen verkregen. Deze 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.

5.1 Beveiligingseisen Software

Software is een breed aandachtsgebied dat vele aspecten kent. In de ICO-Wizard zijn voor dit onderwerp dan ook meerdere inkooponderdelen opgenomen. We onderscheiden de volgende:

1. Applicatieontwikkeling algemeen. Dit onderdeel bevat eisen aan de informatieveiligheid van het ontwikkelproces. Ze liggen op het terrein van de organisatie, de processen en de borging van informatieveiligheid van het softwareontwikkelproces. Het zijn vooral proceseisen en geen specifieke producteisen. Kies dit onderdeel als het wenselijk is specifieke eisen te stellen aan de processen van de leverancier, bijvoorbeeld in het geval van aanbesteding van een mantel voor ontwikkelorganisaties.
2. Maatwerk of maatwerkpakket. Dit onderdeel bevat eisen die gesteld worden aan het op te leveren product van maatwerk-ontwikkeling of bij selectie van een maatwerkpakket. Onder dit laatste verstaan we applicaties voor specifieke onderwerpen die als pakket leverbaar zijn (bijv. een pakket voor sociale diensten). De eisen van dit inkooponderdeel zijn gebaseerd op Secure Software Development (SSD). Ze lenen zich om toe te passen bij ontwikkel- en onderhoudstrajecten, bij zowel interne ontwikkelafdelingen als externe leveranciers.
   De eisen zijn concreet en meestal goed te testen.
3. Mobiele Applicaties. Dit onderdeel bevat eisen die gesteld worden aan mobiele applicaties (apps). Het betreft concrete eisen die meestal goed getest kunnen worden. Mobiele applicaties zijn applicaties die geïnstalleerd kunnen worden en draaien binnen het besturingssysteem van mobiele apparaten, of als onderdeel van een webpagina meekomen en draaien binnen mobiele browsers. In het normenkader zijn de beveiligingseisen voor 3 soorten apps opgenomen (Webapps: applicaties die alleen in een webbrowser draaien, Native apps: applicaties die draaien binnen het besturingssysteem op het mobiele apparaat en Hybride apps: combinaties van een webapp en native app).

4. Softwarepakketten. Dit onderdeel bevat generieke IB&P-eisen die gehanteerd kunnen worden bij het verwerven van standaardpakketten. Dit zijn softwarepakketten die op de markt beschikbaar zijn en beschikken over standaardfunctionaliteit die door diverse organisaties gebruikt kan worden. Voorbeelden zijn pakketten voor Enterprise Resource Planning (ERP) en zogenaamde office-suites ten behoeve van kantoorautomatisering (KA).
5. DiGiD Applicaties. Dit onderdeel bevat de eisen die verplicht zijn gesteld voor dienstverlening waarbij authenticatie plaatsvindt m.b.v. DigiD. In het algemeen zal je dit onderdeel kiezen in combinatie met inkooponderdelen die te maken hebben met de ontwikkeling van maatwerkapplicaties, pakketten of mobiele apps. Kies dit onderdeel dus als DigiD gebruikt wordt voor de authenticatie van de gebruikers van die applicaties.
6. Middleware. Dit onderdeel bevat eisen voor middleware software. Dit is software die de communicatie en de verbinding regelt tussen verschillende soorten IT-systemen. Bijvoorbeeld de verbinding tussen systeemapplicaties, softwarepakketten, besturingssystemen en bepaalde hardware.

De brondocumenten van de verschillende software-inkooponderdelen met gedetailleerde informatie over de eisen volgen hieronder:

1. BIO-Thema-uitwerking Applicatieontwikkeling
2. Secure Software Development (SSD) Eisen aan (Web-)applicaties
3. Secure Software Development (SSD) Eisen aan mobiele applicaties
4. Softwarepakketten
5. Beveiligingsrichtlijnen WEB-applicaties
6. Middleware

5.2 Beveiligingseisen Serverplatform

Het onderdeel 'Serverplatform' bevat generieke informatieveiligheidseisen aan serverplatforms en het beheer daarvan. Het begrip serverplatform omvat componenten als server-hardware, virtualisatietechnologie en besturingssystemen. Kies dit onderdeel als het gaat om aanschaf van dit type technologie of uitbesteding van hosting of platformbeheer.

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

5.3 Beveiligingseisen Communicatievoorzieningen

Het onderdeel 'Communicatievoorzieningen' bevat informatieveiligheidseisen aan verschillende typen communicatievoorzieningen. Dit kunnen zijn:

1. Openbare diensten zoals instant messaging, chatten en sociale media;

2. Elektronische berichten, ook de inhoud van deze berichten;

3. Informatietransport via communicatiefaciliteiten zoals email, telefoon, video (ook de inhoud);

4. Netwerkdiensten, i.c. het leveren van aansluitingen zoals firewalls, gateways, detectiesystemen en technieken voor te beveiligen netwerkdiensten, zoals authenticatie, netwerkinfrastructuur. Het betreft zowel de fysieke als logische verbindingen.

Kies dit onderdeel als je een of meer van dit type diensten aanbesteedt/inkoopt.

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

5.4 Beveiligingseisen Huisvesting IV

Het onderdeel 'Huisvesting IV' bevat eisen aan de fysieke bescherming van rekencentra, terreinen en gebouwen, alsmede de middelen en apparatuur t.b.v. verwerking, transport en opslag van data. Kies dit onderdeel bij uitbesteding van housing en hosting.

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

5.5 Beveiligingseisen Toegangsbeveiliging

Het onderdeel 'Toegangsbeveiliging' bevat informatieveiligheidseisen aan het geheel van beheersingsprocessen en faciliteiten die noodzakelijk zijn voor het verschaffen van toegang tot digitale middelen van de organisatie. Deze omvatten informatiesystemen, besturingssystemen, netwerken, mobiele devices en telewerken. Meestal zal je dit onderdeel willen kiezen in combinatie met andere inkooponderdelen, waaraan nadrukkelijk eisen moeten worden toegevoegd op het gebied van toegang.

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

5.6 Beveiligingseisen Clouddiensten

Het onderdeel 'Clouddiensten' bevat generieke informatieveiligheidseisen voor de verschillende vormen van clouddiensten (zoals IAAS, PAAS en SAAS[4], zowel in de vorm van Public- als Private Cloud[5]). De eisen doen geen uitspraak over de vraag in welke situaties de inzet van Cloud in geoorloofd. Dit is volledig afhankelijk van organisatie- of sectorbeleid.

Kiest dit onderdeel als je enige vorm van dienstverlening in de Cloud gaat afnemen. Afhankelijk van de in de Cloud af te nemen functies, kunnen extra eisen worden toegevoegd door andere van toepassing zijnde inkooponderdelen mee te selecteren.

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

---

[4] SAAS (Software as a Service): de applicatie staat volledig onder controle van de dienstverlener.

PAAS (Platform as a Service): alleen de platformen en de infrastructuur worden beheerd door de dienstverlener; niet de applicaties.

IAAS (Infrastructure as a Service): alleen de infrastructuur wordt beheerd door de dienstverlener; niet de applicaties en de platformen.

[5] [5] Private Cloud (met een dedicated infrastructuur): De IT-voorzieningen zijn ingericht voor één klant.

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).

Public Cloud: De IT-voorzieningen zijn toegankelijk via het Internet. De voorzieningen worden meestal gedeeld met andere klanten.

5.7 Beveiligingseisen Procesautomatisering

Het inkooponderdeel Procesautomatisering omvat proces- en systeemeisen die moeten worden gesteld 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.

5.8 Algemene eisen Ketenpartners

Naast de inkoop-specifieke selectiemogelijkheden kan het voorkomen dat buiten de specifieke eisen het 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 algemene eisen die opgelegd kunnen worden indien hiervan sprake is.
NB. De keuze voor Algemeen Ketenpartners komt niet in de plaats van de specifieke inkooponderdelen. Selecteer aanvullend op dit onderdeel dus ook de inkooponderdelen die betrekking hebben op de verschillende diensten die afgenomen worden.

6 Supplementen, nadere toelichting

Naast de basisselectie op de inkooponderdelen in hoofdstuk 3, biedt ICO-Wizard ook de mogelijkheid aanvullingen uit andere normenkaders te selecteren. Als je aanvullingen mee-selecteert, worden uitsluitend de aanvullingen op de gekozen inkooponderdelen getoond.

De volgende aanvullingen kunnen worden opgevraagd:

- Privacy-aanvullingen;
- BIO-overheidsmaatregelen;
- ABRO-maatregelen. (ABRO staat voor Algemene Beveiligingseisen voor Rijksoverheidopdrachten).

De verschillende aanvullingen zijn divers van karakter. Ze worden in de volgende paragrafen toegelicht.

6.1 Privacy-supplementen

Naar aanleiding van de motie Kröger in februari 2021 is ICO-Wizard 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.

Kies voor deze aanvulling als er in de uitbesteding sprake is van te beschermen persoonsgegevens.

De privacy-aanvullingen zijn gebundeld in één document. Gedetailleerde informatie over deze eisen is opgenomen in het document Privacy-supplementen BIO-Thema-uitwerkingen.

6.2 BIO-Overheidsmaatregelen.

De basisselectie van ICO is gebaseerd op de BIO-thema-uitwerkingen. In deze thema-uitwerkingen zijn de BIO-eisen thematisch bij elkaar gebracht en ook aangevuld met eisen uit anders kaders, zoals NIST, SoGP, BSI etc. Daarmee sluiten ze goed aan op veelvuldig in de praktijk voorkomende verantwoordelijkheden in organisaties en ook op in de markt uit te zetten aanbestedingen.

Het kan het nuttig zijn te zien welke BIO-maatregelen onderliggend zijn aan de eisen van het ICO-basispakket. Vandaar dat mogelijk is gemaakt deze maatregelen ook te tonen.

Deze maatregelen kunnen worden opgevraagd in twee delen: de maatregelen op BBN1-niveau en op BBN2-niveau.

6.3 ABRO

Vanaf 1 januari 2026 gelden er nieuwe beveiligingseisen voor bedrijven die voor de overheid een opdracht uitvoeren met risico’s voor de nationale veiligheid. Dat zijn de Algemene Beveiligingseisen voor Rijksoverheidsopdrachten (ABRO). De ABRO bestaat uit een samenhangende set aan beveiligingseisen. Afhankelijk van de aard van de bijzondere opdracht zijn verschillende hoofdstukken of onderdelen van ABRO 2026 van toepassing. Dat geldt dan onverkort voor alle eisen in die hoofdstukken of onderdelen. Inkopende organisaties die de ABRO moeten toepassen kunnen daar niet van afwijken.

Het Nationaal Bureau Industrieveiligheid (NBIV) controleert of een bedrijf aan de ABRO voldoet.

De ABRO wordt stapsgewijs ingevoerd binnen de overheid. Voor het overzicht van de inkopende met hun invoeringsdata zie Invoeringsdatum en geplande invoering ABRO door inkopende organisaties in tranche 1 | Publicatie | Rijksoverheid.nl

De ABRO onderkent 4 niveaus van te beveiligen belangen (TBB-niveaus):

- TBB1 - Zeer geheim;
- TBB2 – Geheim;
- TBB3 – Confidentieel;
- TBB4 - Departementaal vertrouwelijk.

Veel van de ABRO-eisen komen voor op meerdere van deze niveaus. De eisenpakketten op de 4 TBB-niveaus zijn daarmee overlappend. In de ICO-Wizard kunnen ze op de verschillende niveaus worden gekozen en tevens in combinatie.

Navigeer hier voor meer informatie over de Beveiligingseisen bij overheidsopdrachten met risico's voor nationale veiligheid (ABRO).

7 Verificatiemethode(n), nadere toelichting

Het stellen van eisen in inkoopprocessen is pas effectief als ook wordt geverifieerd 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.

Tabel 1 Verificatiemethode en toelichting