Tips voor gebruik van de ICO-Wizard

Waarom de ICO-Wizard?

De ICO-Wizard is bedoeld om de opdrachtgever, inkoper en Informatiebeveiliging en Privacy (IB&P) professional te ondersteunen bij het bepalen van de eisen die gesteld moeten worden aan in te kopen producten en/of diensten. De tool kan daarbij zowel de eisen opleveren die gesteld moeten worden aan de leverancier en/of de door hem te leveren producten en/of diensten als ook de eisen die in het kader van de inkoop en het gebruik van nieuwe producten/diensten aan de eigen inkopende organisatie gesteld moeten worden.

De eisen uit de ICO-Wizard zijn gericht op informatiebeveiliging[1], gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO), en ook op privacybescherming (op basis van het concept Privacy-By-Design) en voorzien van een advies voor verificatie van aan een leverancier gestelde eisen.

De BIO beoogt de beveiliging van informatie(systemen) bij alle bestuurslagen en bestuursorganen van de overheid te bevorderen. Overheidsorganisaties kunnen er dan op vertrouwen dat onderling uitgewisselde gegevens, in lijn met wet- en regelgeving, passend beveiligd zijn.

Informatiebeveiliging en privacybescherming borgen in het inkoopproces

Geadviseerd wordt de ICO-Wizard te implementeren in het inkoopproces. De inkoop- of contractmanagers kunnen dan op eenvoudige wijze de informatiebeveiligingseisen verwerken in de door hen te produceren documenten voor en naar aanleiding van een inkoop/aanbesteding. De ICO-Wizard ondersteunt dit m.b.v. een rapport met eisen dat de tool kan opleveren en dat aan het Programma van Eisen (PvE) voor de inkoop/aanbesteding kan worden toegevoegd.

Integratie van gebruik van de ICO-Wizard in het inkoop-/aanbestedingsproces levert daarnaast tijdwinst op en voorkomt dat het inkoop- of beheercontract onvolledig of onjuist wordt afgesloten qua informatiebeveiligingseisen. Indien 'aan de voorkant' de juiste beveiligingseisen aan de opdrachtnemer/leverancier worden gesteld voorkomt dit op een later moment herstelwerk, wat hoge kosten en een lange doorlooptijd met zich mee kan brengen.

In dit document staan handige tips voor het, met behulp van de ICO-Wizard, incorporeren van IB&P-eisen in het inkoop-/aanbestedingsproces.

Risico gebaseerd

De BIO stimuleert risico gebaseerd werken. De ICO-Wizard is gebaseerd op de BIO en is dus ook risico gebaseerd. We raden aan om voorafgaand aan een ICT-inkoop/aanbesteding een inkoop-risicoanalyse uit te voeren. Het resultaat daarvan kan helpen bij het prioriteren van de te stellen informatiebeveiligingseisen.

[1] Let op dat het feit dat de tool zich richt op eisen m.b.t. informatiebeveiliging niet betekent dat de tool dan alleen bij de inkoop/aanbesteding van **ICT**-producten/diensten van toepassing is: steeds meer producten zijn 'smart' en kennen internetkoppelingen zodat ook bij niet ICT-producten sprake is van eisen m.b.t. informatiebeveiliging en privacybescherming.

Help de opdrachtnemer

Als overheidspartij wil je dat je opdrachtnemer/leverancier het gevraagde product conform de maatregelen uit de BIO ontwikkelt en beheert (indien van toepassing).

Wanneer de opdrachtgever alleen eist dat aan de BIO voldaan moet worden, zal het antwoord van de opdrachtnemer/leverancier vaak zijn dat ze dat doen. Deze eis is echter veel te algemeen en niet passend. De BIO is immers bedoeld voor overheidsorganisaties zelf en betreft met name de informatiebeveiliging van hun eigen bedrijfsvoering, niet die voor opdrachtnemer/leverancier. De opdrachtgever dient exact te specificeren aan welke informatiebeveiligingseisen (passend bij de in te kopen producten/diensten) moet worden voldaan. Bovendien moet het voor de opdrachtgever en opdrachtnemer helder zijn hoe geverifieerd kan worden dat daadwerkelijk aan de gevraagde informatiebeveiligingseisen wordt voldaan.

Gebruik van de (resultaten van de) ICO-Wizard

Door het gebruik van de ICO-Wizard kan eenvoudig en nauwkeurig gespecificeerd worden aan welke eisen uit de BIO en andere kaders en richtlijnen voldaan dient te worden. Per eis geeft de ICO-Wizard een advies hoe aangetoond en geverifieerd kan worden dat daadwerkelijk aan deze eis wordt/is voldaan. Voor het maken van een (Word-) rapport of (Excel-) lijst met de bruto risico's[2] volstaat opgave van:

- type in te kopen product(en)/dienst(en) oftewel inkooponderde(e)l(en);
- of de eisen voor opdrachtgever en/of opdrachtnemer zijn;
- of het product- en/of proceseisen betreft;
- of privacy-maatregelen wel/niet meegenomen moeten worden;
- of overheidsmaatregelen wel/niet meegenomen moeten worden;
- of ABRO-eisen wel/niet meegenomen moeten worden*.

** Let op: 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). 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. Het resultaat van de ICO-Wizard kan ondersteunend worden gebruikt bij de controle door het NBIV.

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

[2] Een bruto risico is de inschatting van een risico zonder daarbij eventueel aanwezige beheersmaatregelen in ogenschouw te nemen. Een netto (rest) risico is het risico waarbij de huidige aanwezige beheersmaatregelen wel in beschouwing worden genomen.

In de export van de ICO-Wizard wordt per eis aangegeven welke dreigingen (risico's) worden gemitigeerd indien aan de eis is voldaan.

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/risicoanalyse 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.

Door de bruto lijst naast het resultaat van een risicoanalyse te leggen, kan het inkoopteam van betrokken functionarissen (inkoper, opdrachtgever, IB&P-professional en eventuele andere relevante rollen) de lijst terugbrengen tot een netto lijst. Hierbij kunnen zij gebruik maken van het MOSCOW-principe, zie ook de volgende paragraaf 'Wie bepaalt de eisen'.

Zowel het rapport als de lijst die de ICO-Wizard kan produceren kunnen dus vraag-specifiek gemaakt worden, aangepast worden naar aanleiding van de interne risicoanalyse en desgewenst voorzien worden van aanvullende of aangepaste teksten en het eigen organisatielogo. De documenten kunnen dan worden toegevoegd aan het 'PvE' als specifiek hoofdstuk of als bijlage.

Wie bepaalt de eisen

In het contact met de opdrachtnemer/leverancier zal de inkoper het voortouw nemen en de regie voeren op het inkoopproces. Hij/zij kan waarschijnlijk onvoldoende gedetailleerd specificeren welke informatiebeveiligingseisen van toepassing zijn of zouden moeten zijn en welke risico's de organisatie loopt wanneer niet aan deze eisen wordt voldaan.

De opdrachtgever is degene die wel goed kan inschatten welke business risico's aan de orde zijn en wat de importantie van deze risico's is (kans en impact).

De IB&P-professional heeft meer kennis van het bestaande ICT-landschap dan de inkoper en opdrachtgever en kan daardoor beter inschatten wat de technische risico's zijn (binnen dit ICT-landschap), welke maatregelen reeds getroffen zijn en welke aanvullende maatregelen aan de orde zijn bij de in te kopen producten en/of diensten.

Daarom is het bepalen van de input voor en output van de ICO-Wizard een samenspel tussen de opdrachtgever, IB&P-professional en inkoper. Ieder heeft binnen deze driehoek zijn eigen invalshoek, rol en verantwoordelijkheid.

Wanneer de ICO-Wizard wordt toegepast kunnen deze partijen gezamenlijk de resultaten beoordelen en o.b.v. de specifieke situatie en risicoprofiel hierin nog aanpassingen doen om tot een definitief pakket van (netto) eisen te komen. Zo kunnen op basis van de risico-afwegingen eisen vervallen of qua gewicht/importantie bijgesteld worden.

Overleg met de opdrachtnemer

In het totale PvE bij een inkoop/aanbesteding is het deel informatiebeveiliging slechts een klein, maar zeer belangrijk, onderdeel/hoofdstuk. Wanneer 'aan de voorkant' geen rekening wordt gehouden met de informatiebeveiligingseisen kan dit bij of na in productie name en bij beheer leiden tot hoge kosten en een lange doorlooptijd om alsnog de juiste informatiebeveiligingseisen in te bouwen.

In overleg met de (potentiële) opdrachtnemer/leverancier dient het onderdeel IB&P-eisen in het PvE (of RFC/RFP) te worden toegelicht. Indien de inkoper onvoldoende beschikt over de juiste technische kennis kan de IB&P-professional deze toelichting verzorgen.

Contract

Zowel in het leveringscontract als in het eventuele onderhoudscontract kan de inkoper of contractmanager de IB&P-eisen uit het PvE vastleggen. Op deze wijze zal geen verschil ontstaan tussen hetgeen 'aan de voorkant' is gevraagd/geëist en wat in het vervolg van het inkoop-/aanbestedingsproces wordt vastgelegd.

Wanneer na verloop van tijd om welke reden dan ook, het contract met de opdrachtnemer wordt herzien of geëvalueerd, vul dan, samen met de eerdergenoemde driehoek (inkoper, opdrachtgever en IB&P-professional) en de contractmanager, de ICO-Wizard nog eens in. Na verloop van tijd kunnen risico's veranderen en dit kan leiden tot een herziene lijst met IB&P-eisen, waarover met de leverancier dan weer nieuwe afspraken gemaakt moeten worden.