Tips om de ICO-Wizard te gebruiken

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 juiste informatiebeveiligingseisen gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO), voor zowel de eigen organisatie als de Leverancier.

De eisen uit de ICO-Wizard zijn specifiek gericht op informatiebeveiliging en voorzien van een advies voor verificatie per eis wanneer deze eis aan de leverancier is gesteld. Vanaf oktober 2021 zijn de Privacy-By-Design-eisen gericht op privacy binnen informatiebeveiliging toegevoegd.

De ICO-Wizard levert desgewenst een rapport op dat aan het Programma van Eisen (PvE), voor de ICT-inkoop/aanbesteding, kan worden toegevoegd. Wij adviseren de ICO-Wizard te implementeren in het inkoopproces. De inkoop- of contractmanagers kunnen dan op eenvoudige wijze de informatiebeveiligingseisen verwerken in de door hun te produceren documenten voor en naar aanleiding van een ICT-inkoop/aanbesteding.

Informatiebeveiliging borgen in het inkoopproces

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

In deze notitie staan handige tips hoe de informatiebeveiligingseisen, met het gebruik van de ICO-Wizard, in het inkoop-/aanbestedingsproces geïncorporeerd kunnen worden.

Help de Opdrachtnemer

Als overheidspartij wil je dat je Opdrachtnemer/Leverancier het gevraagde product conform de maatregelen uit de BIO ontwikkelt en, indien van toepassing, beheert.

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. Immers de BIO is bedoeld voor overheidsorganisaties zelf, met name de informatiebeveiliging van hun eigen bedrijfsvoering, en niet voor Opdrachtnemer/Leverancier. De Opdrachtgever dient exact te specificeren aan welke informatiebeveiligingseisen (passend bij de gewenste ICT-inkoop) moet worden voldaan. Bovendien moet het voor de opdrachtgever en opdrachtnemer helder zijn hoe geverifieerd kan worden dat aan de gevraagde informatiebeveiligingseisen wordt voldaan.

Gebruik de ICO-Wizard

Door het gebruik van de ICO-Wizard kan nauwkeurig en eenvoudig gespecificeerd worden aan welke exacte eisen uit de BIO voldaan dient te worden. Per eis geeft de ICO-Wizard een advies hoe aangetoond en geverifieerd kan worden dat aan deze eis wordt/is voldaan.

Voor het maken van een rapport of Excel lijst met de bruto risico's hoeft alleen een keuze gemaakt te worden in:

- Inkooponderdeel, dit kunnen er meerdere zijn;
- Opdrachtgever/Opdrachtnemer;
- Proces en/of producteisen;
- Privacy-maatregelen mee selecteren.

Deze bruto lijst kan bewerkt worden tot een netto lijst die aan het PvE wordt toegevoegd.

Door de bruto lijst naast het resultaat van een risicoanalyse te leggen, kan het inkoop team van betrokken functionarissen (Opdrachtgever, IB&P professional en Inkoper) de lijst terugbrengen tot een netto lijst. Hierbij kunnen zij gebruik maken van het MOSCOW principe.

In de Excel-export wordt aangegeven welke dreiging (risico) door het voldoen aan de bewuste eis gemitigeerd kan worden.

Wie bepaalt de eisen

In het contact met de Opdrachtnemer/Leverancier zal de Inkoper het voortouw nemen.

Echter deze Inkoper kan waarschijnlijk onvoldoende in detail 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 kan goed inschatten welke risico's hij ziet 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 binnen het bestaande ICT-landschap inschatten wat de technische risico's zijn, welke maatregelen reeds getroffen zijn en welke aanvullende maatregelen getroffen dienen te worden bij de inkoop van ICT-middelen.

Daarom is het invullen van de ICO-Wizard een samenspel tussen de functies Opdrachtgever, IB&P professional en de Inkoper. Ieder heeft binnen deze driehoek zijn eigen rol en verantwoordelijkheid. De Inkoper voert regie op het Inkoopproces.

Wanneer de ICO-Wizard is ingevuld, kunnen deze drie partijen samen overeenstemming bereiken over het resultaat en o.b.v. de specifieke situatie en risicoprofiel hierin nog aanpassingen doen. Gezamenlijk bepalen zij het palet van te stellen eisen. Sommige eisen zouden daarbij kunnen komen te vervallen en andere kunnen extra gewicht mee krijgen bij weging van de eisen.

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-risico-analyse uit te voeren. Het resultaat van deze sessie kan helpen bij het prioriteren van de te stellen informatiebeveiligingseisen.

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 (potentiele) Opdrachtnemer/Leverancier dientl het PvE (RFC, RFP, enz.) te worden toegelicht. De beveiligingseisen kunnen worden toegelicht door de IB&P professional van de Opdrachtgever, indien de Inkoper onvoldoende beschikt over de juiste technische kennis, aan de potentiele Opdrachtnemer/Leverancier.

Contract

Zowel in het leveringscontract als in het eventuele onderhoudscontract kan de Inkoper de informatiebeveiligingseisen uit het 'PvE' vastleggen. Op deze wijze zal geen verschil ontstaan tussen dat wat aan de "voorkant" is gevraagd/geëist en dat wat in het vervolg van het inkoop-/aanbestedingsproces wordt vastgelegd.

PDCA

Wanneer na verloop van tijd om welke reden dan ook, het contract met de Opdrachtnemer wordt herzien of geëvalueerd, vul dan samen met de eerder genoemde driehoek (Inkoper, IB&P-professional en Opdrachtgever) en aangevuld met de Contractmanager de ICO-Wizard nog eens in. Na verloop van tijd kunnen de risico's veranderen en dit kan leiden tot een aanvullende lijst met beveiligingseisen, waarover met de Leverancier dan weer nieuwe afspraken moeten worden gemaakt.

Eenvoudig vergroten van de kennis van de ICO-Wizard

Indien de organisatie en vooral de Inkoop-, IB&P- en Opdrachtgeversfunctie op een snelle manier willen worden meegenomen in het eenvoudige gebruik van de ICO-Wizard dan kan CIP een presentatie verzorgen. Deze presentatie duurt afhankelijk van de respons minimaal 20 minuten en maximaal zo lang als er vragen zijn. Indien IB&P professionals de ICO-Wizard al enkele keren hebben gebruikt zijn deze medewerkers goed in staat om, binnen de eigen organisatie, deze presentatie te verzorgen.

Resultaat gebruik ICO-Wizard

Door het gebruik van de ICO-Wizard komt op een eenvoudige wijze de volledige lijst van mogelijke eisen aan de Opdrachtnemer/Leverancier beschikbaar. Deze lijst is 'vraag' specifiek te maken. Het resultaat is een rapport dat door de aanbestedende organisatie voorzien kan worden van bedrijfslogo e.d. en kan worden toegevoegd aan het 'PvE' als specifiek hoofdstuk of als bijlage.

Inkoop-/aanbestedingsproces

Wij adviseren om het gebruik van de ICO-Wizard op te nemen in het inkoop-/aanbestedingsproces. Dit levert tijdwinst op en voorkomt dat het inkoop- of beheercontract van ICT hard- en/of software 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, die hoge kosten en lange doorlooptijd kunnen vragen.