Factsheet
Inkoopeisen Cybersecurity Overheid (ICO)

Inleiding

Digitale veiligheid is een essentiële randvoorwaarde voor vertrouwen in onze digitale economie en samenleving. De overheid heeft ervoor gekozen een samenhangend niveau van veiligheid na te streven door in alle geledingen de op ISO27002 gebaseerde 'Baseline Informatiebeveiliging Overheid' (de BIO) te hanteren. Ook in haar inkoopbeleid wil de overheid een lijn trekken met als doel de (vele) hardware- en softwareproducten en -diensten die zij op de markt verwerft, veilig te doen zijn. De overheid ziet het als haar taak een goed voorbeeld te geven, haar rol als goed opdrachtgever te versterken en daarmee ook een algemene beweging in de markt te stimuleren naar het ontwikkelen en aanbieden van veilige ICT-producten en diensten.

Het programma ICO levert instrumentarium om deze doelstellingen te helpen verwezenlijken: sets van inkoopeisen, een basisprocesbeschrijving en een 'wizard' waarmee voor specifieke aanbestedingen/inkopen relevante eisen kunnen worden geselecteerd.

Waarom specifieke cybersecuritycriteria voor leveranciers?

De BIO is gericht op overheidsorganisaties. Voor eisen die overheidsorganisaties aan veilige producten van leveranciers stellen, is de BIO te breed omdat het allerlei facetten bevat die alleen op de processen van de eigen organisatie betrekking hebben. Daarnaast is de BIO te weinig specifiek voor het stellen van scherpe eisen aan de veiligheid op het niveau van ingekochte producten en diensten van leveranciers. De noodzaak om die scherpere eisen te stellen heeft geleid tot verdiepende, naar thema's georiënteerde uitwerkingen, die steunen op de BIO-normen en die blinde vlekken aanvullen met behulp van normen uit andere marktstandaards.

De ICO-Wizard

Met de ICO-Wizard kunnen eisenpakketten worden geselecteerd die aansluiten op verschillende typen aan te besteden/in te kopen producten/diensten.

De eisen in de wizard zijn gebaseerd op de BIO (ISO27002). De BIO vormt de basis voor nadere uitwerkingen naar samenhangende thema's. De ICO-Wizard maakt gebruik van deze thema-uitwerkingen en aanvullende normenkaders en standaarden, vertaald naar inkooponderdelen, waardoor de noodzakelijke scherpte in de eisen voor aanbestedingen en inkopen wordt bereikt.

In onderstaande afbeelding is de inhoud en werking van de ICO-Wizard gevisualiseerd.

© Centrum Informatiebeveiliging en Privacybescherming, Factsheet ICO v1.7



De gebruiker geeft primair aan welke inkooponderdelen van toepassing zijn en kan desgewenst enkele extra selecties meegeven, zoals de keuze tussen product- en/of proceseisen en het wel of niet meenemen van aanvullende privacy-eisen, expliciet tonen van verplichte BIO-Overheidsmaatregelen en/of toepassen van de ABRO-eisen.

Op basis van deze opgave selecteert de ICO-Wizard vanuit de BIO, de BIO thema-uitwerkingen en andere normenkaders en standaarden het relevante (basis) eisenpakket.

De aanvullende privacy-eisen zijn onder meer gebaseerd op de zeven Privacy-by-Design-principes, de privacy baseline en de ISO27701 en zijn nuttig als privacy een rol speelt in de aanbesteding.

De BIO-Overheidsmaatregelen zijn verplicht voor overheidsorganisaties. Ze zijn weliswaar verwerkt in het standaard eisenpakket maar het kan soms nuttig zijn ze expliciet te tonen.

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). 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).

Risicoanalyse in de ICO-Wizard

De informatiebeveiliging (IB) maatregelen die een organisatie treft buiten de in de BIO voorgeschreven maatregelen, zijn afhankelijk van de te mitigeren risico's. Het werken met de BIO veronderstelt dan ook het maken van risicoafwegingen/risicoanalyses. De eisen die aan leveranciers worden gesteld, moeten worden beschouwd in het licht van deze risicoafwegingen.

De ICO-Wizard is erop gericht de opdrachtgever en het inkoopteam te ondersteunen bij het stellen van de juiste informatiebeveiligingseisen. Het door de wizard voorgestelde eisenpakket kan echter worden aangepast o.b.v. de risicoafwegingen. De wizard helpt hierbij door per geselecteerde eis de risico's te tonen die (mede) door de desbetreffende eis gemitigeerd kunnen worden.

Feitelijk is dit een opt-out aanpak: de eisen gelden, tenzij je ze o.b.v. risicoafweging wijzigt of laat vallen. Het voordeel van het tonen van de gemitigeerde risico's is dat de actoren in het inkoopproces - ook als ze vooraf geen risicoanalyse hebben uitgevoerd - toch worden geconfronteerd met de potentiële risico's die uitnodigen tot een bewuste keuze.

De gehanteerde risico's steunen onder andere op de tabel standaarddreigingen van de open source tool voor risicoanalyse RAVIB en zijn aangevuld met specifieke risico's uit gehanteerde brondocumenten.

Selectie en exportmogelijkheden ICO-Wizard

Het eisenpakket dat de ICO-Wizard als output presenteert, bevat per eis een korte beschrijving, een verwijzing naar de uitgebreide beschrijving in het bijbehorende brondocument en suggesties voor de verificatiemethode (de wijze van toetsing of aan de eis is voldaan).

Al dan niet in combinatie met door de opdrachtgever vanuit risicoafweging meegegeven wijzigingen kunnen deze eisen als uitgangspunt gelden voor de aanbesteding, contracten, acceptatie en levering van het product/de dienst.

Waardering eisen in de output

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.

Export in Word

De opgeleverde set van eisen door de ICO-Wizard kan opgeleverd worden in de vorm van een Word-document dat (evt. met eigen aanvullingen/wijzigingen) met de aanbestedingsdocumenten meegestuurd kan worden naar de inschrijvers/leveranciers.

Export in Excel

De door de ICO-Wizard opgestelde set van eisen bevat, naast de standaard set van gegevens in de Word-export, aanvullende informatie. Met name de samenhang tussen de beveiligingseisen en de risico's die ze helpen mitigeren is hierin terug te vinden. Daarnaast bevat de Excel werkkolommen voor het vastleggen van de uitvraag van de eisen en (RFC) criteria voor de beoordeling van inschrijvingen op de aanbesteding.