



Informatiebeveiliging geborgd in contracten

Introductie

CIP heeft in samenwerking met meerdere publieke en private partijen gewerkt aan een generieke werkwijze voor Informatiebeveiliging (IB) binnen inkooptrajecten. Deze factsheet bevat een korte uitleg van de huidige situatie, de bedachte oplossing en de toegevoegde waarde.

Huidige situatie

De overheid heeft de ambitie om vooruitstrevend en efficiënt ICT in te zetten om burgers en het bedrijfsleven zo optimaal mogelijk te ondersteunen. Spil in deze strategie is publiek-private interactie bij het leveren van adequate oplossingen. IB is onlosmakelijk verbonden met het leveren van deze ondersteunende (digitale) diensten. Binnen overheidsorganisaties zijn kaders zoals de BIO opgesteld om IB op een juist niveau te borgen.

Bij het inzetten van diensten van marktpartijen voor deze dienstverlening wordt regelmatig het volledige eisenpakket waaraan de overheid moet voldoen opgelegd aan de leveranciers. Dit leidt tot een vermindering van creativiteit, het geforceerd voldoen aan te veel eisen en het verschillend interpreteren en beschrijven van dezelfde achterliggende eis in de contractteksten.

Oplossing

Een werkgroep uit het CIP-netwerk heeft een generieke werkwijze ontwikkeld op basis van een model van Rijkswaterstaat, waarmee IB wordt gebracht als beheersdoel. Het model bestaat uit een koppeling tussen de eisen, de beheersdoelen en de contractteksten. Daarnaast geeft het heldere criteria die het voor de opdrachtnemer gemakkelijker maakt aan deze eisen te voldoen. Een heldere beschrijving zorgt voor een makkelijkere haalbaarheidstoets.

De beheersdoelen bieden de markt meer mogelijkheden om creativiteit in te zetten voor het behalen ervan.

Eisen

- BIO / ISO-27002
- Aanvullende eisen

Beheersdoelen

- Proceseisen
- Systemeisen
- ARBIT/ARVODI

Contractteksten

- Aangevuld met diverse richtlijnen

Aanvullend op dit model is een vragenlijst met bijbehorend tool ontwikkeld waarmee in een aantal simpele vragen kan worden bepaald aan welke beheersdoelen moet worden voldaan binnen een aanbesteding. Dit is per organisatie aan te passen en zal ervoor zorgen dat overheidsinstanties meer uniforme uitvragen doen voor dezelfde producten.

Het model zal bovendien worden aangepast op basis van opmerkingen en ervaringen uit de gebruikspraktijk, waarmee een proces van continue verbetering en actualisatie ontstaat.

Toegevoegde waarde

Het model brengt een vijftal voordelen met zich mee die zorgen voor een makkelijker en soepeler proces bij zowel de Aanbestedende Dienst (AD) als de opdrachtnemer. Deze voordelen komen het beste tot hun recht als het niet alleen wordt opgelegd (Angelsaksisch model) door de Aanbestedende dienst, maar juist wanneer de dialoog (Rijnlands model) wordt gevoerd met leveranciers om zo samen te werken aan verbetering. De vijf voordelen zijn:



Voorspelbaar & goed opdrachtgeverschap

AD: Deze werkwijze zorgt dat een AD een betere afweging kan maken voor de bepaling van de proces- en systeemeisen. Dit kan worden gebruikt als input voor de strategiebepaling tussen inkoop, IM en de interne opdrachtgever. Het leidt tot heldere eisen aan opdrachtnemers/ markt.

Markt: Met het gebruik van een duidelijke en transparante methodiek door de opdrachtgever ontstaat voor de opdrachtnemer meer duidelijkheid.

Herleidbaarheid eisen/ transparantie

AD: Het is makkelijker om contractteksten en beheersdoelen aan te passen wanneer er iets in een bovenliggend eisenkader wordt aangepast.

Markt: Door de beschreven systematiek is het voor alle gevraagde proces- en systeemeisen duidelijk wat de achterliggende gedachte is en waarop deze eisen zijn gebaseerd. Dit werkt extra krachtig als de AD de ingevulde tool ook als toelichting meestuurt.

Sturen op IB beheersdoelen i.p.v. 'afvinken' framework

AD: In plaats van het afvinken van een lijstje met de eisen van de BIO stuurt de AD met deze systematiek op de beheersdoelen van dit framework.

Markt: De eisen worden makkelijker te beheren, omdat de leverancier niet de volledige set aan normeringen krijgt, maar alleen de normeringen die van toepassing zijn op de onderhanden aanbesteding.

Herhaalbaarheid

AD: Bij een nieuwe uitvraag kan de AD bij gelijke eisen eerder opgestelde teksten opnieuw gebruiken om zo efficiënter te kunnen werken. De teksten zijn dan reeds getoetst en zijn nog steeds herleidbaar naar de onderliggende beheersdoelen.

Markt: Er hoeft niet bij elke aanbesteding opnieuw gekeken te worden naar decontractteksten en waaraan zij refereren: ze zijn immers al bekend en uniform. Er kan gemakkelijker beoordeeld worden of de aangeboden producten aan alle eisen voldoen.

Uniformering werkwijze tussen gelijksoortige organisaties

AD: Het is gemakkelijker om voor andere aanbestedende diensten opdrachten uit te voeren enerzijds, en het is makkelijker om knowhow te krijgen van collega's die hetzelfde product eerder hebben ingekocht.

Markt: Opdrachtnemers kunnen makkelijker beoordelen wat gevraagd wordt en wat de rationale is bij bepaalde eisen en contractteksten. Hoe meer opdrachtgevers deze werkwijze toepassen, hoe gemakkelijker het is voor opdrachtnemers om voor dezelfde producten in te schrijven, bij verschillende aanbestedende diensten, aangezien de eisen veelal uniform zullen zijn.

Contact

Heb je vragen of opmerkingen over deze generieke werkwijze ten aanzien van Security Proof Inkopen, laat dan een bericht achter op de contactpagina van onze site:

cip-overheid.nl/contact