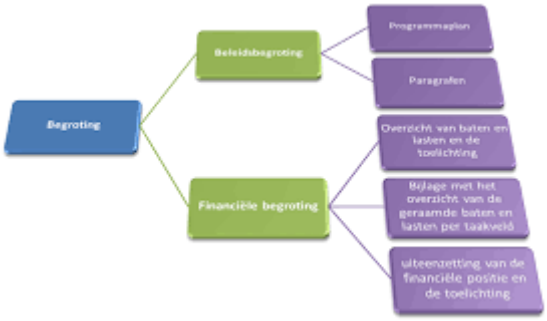
Van rechtmatigheidsverantwoording naar een ICS

Vanaf 2021 zijn lokale overheden verplicht binnen de rechtmatigheidsverantwoording ook aan te geven dat zij de financiële baten goed en rechtmatig hebben aangewend.

Deze rechtmatigheidsverantwoording kan gebruikt worden in de In Control Statement (ICS) over de kwaliteit van de bedrijfsvoering. De ICS geeft hiermee inzicht in de mate waarin de bedrijfsprocessen op orde zijn.



De solution geeft de organisatie handvatten en beheersingsmaatregelen, waarmee zij blijvend kunnen voldoen aan de wettelijke bepalingen om de integriteit, voortdurende beschikbaarheid en beveiliging van de geautomatiseerde gegevensverwerking te waarborgen zoals o.a. aangegeven in de Baseline Informatiebeveiliging Overheid (BIO).

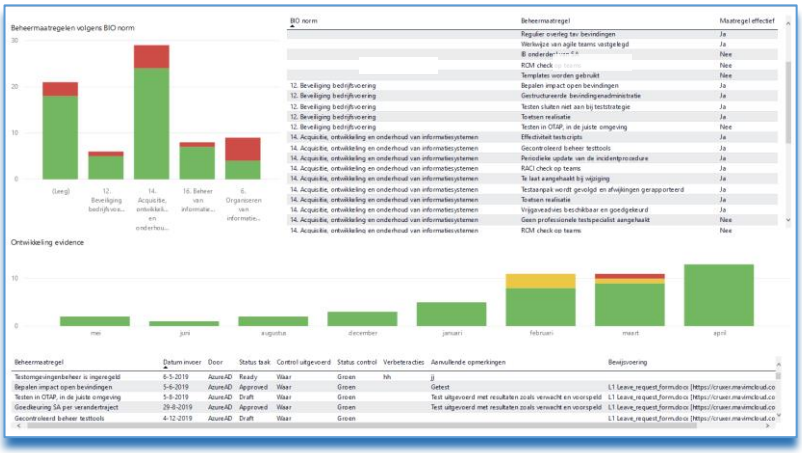
Omdat de solution de relaties legt met de bedrijfs- en werkprocessen en de inrichting hiervan binnen de organisatie is hiermee de onderbouwing van de In Control Statement mogelijk.

De solution is gebouwd in het Management Control Framework en biedt de volgende functionaliteit:

- Inzicht in de normen en de controls die vanuit de BIO zijn gesteld om aan de baseline informatiebeveiliging te voldoen
- Een volledigheidsmatrix waaruit blijkt of in welke mate de baseline wordt afgedekt en waar nog maatregelen nodig zijn danwel gewenst
- Een dossier waarin de complete evidence, gerelateerd aan de vereisten i.v.m. informatiebeveiliging beschikbaar wordt gesteld. Zowel de actuele status als de ontwikkeling over de afgelopen periode wordt inzichtelijk gemaakt, waarbij aangetoond kan worden op welke manier een organisatie zich ontwikkeld als het gaat om informatiebeveiliging
- De relatie tussen de BIO normen en de eigen risk-managementcycle van de organisatie zoals de beheermaatregelen, key-controls, key-risks etc, en de onderliggende processen, verantwoordelijkheden binnen deze processen
- Rapportage over de opzet van de processen, gerelateerd aan de specifieke vereisten i.v.m. informatiebeveiliging. Beschikbaar via een portaal, in combinatie met power-bi rapportages
- Controleplanning voor de eigen beheermaatregelen, gericht op het uitvragen van de noodzakelijke evidence voor informatiebeveiliging
- Workflows waarin per beheermaatregel de evidence wordt gevraagd aan de verantwoordelijke eigenaar of gedelegeerd eigenaar
- Vanuit het BIO normenkader is de relatie gelegd met externe frameworks zoals Norea Volwassenheidsmodel Informatiebeveiliging 2019 en ISO27002. Als organisatie kun je gebruik maken van de best-practices voor het definiëren van je eigen beheermaatregelen.

Dashboards

Vanuit de solution worden een aantal dashboards aangeboden. Met deze dashboards kan de werking van de beheermaatregelen aangetoond worden, zowel qua actuele status als de ontwikkeling van deze beheermaatregelen in de tijd.



Dossier BIO

Inzichtelijk is in welke mate de vereisten vanuit de BIO worden afgedekt door beheermaatregelen. Naast de actuele status is ook de ontwikkeling van de onderliggende evidence in de tijd gezien inzichtelijk.

Risico Control Dashboard

Inzichtelijk is in hoeverre de interne beheer maatregelen zijn aangeleverd. Onderscheid hierbinnen naar risico's, KPI's en de impact. Tevens zijn er selectiemogelijkheden op afdeling/team en verantwoordelijke.

Overige solutions

De solution maakt onderdeel uit van een set aan solutions zoals:

- Baseline informatiebeveiliging Overheid (BIO)
- ISO27001 / 27002 – Informatiebeveiliging & risicoanalyse
- RODIN (Referentiekader opbouw digitaal informatiebeheer 2107)

Naast deze verplichte practices worden ook frameworks aangeboden die de organisatie helpen om verder te verbeteren en snel te starten. Daarbij kan gedacht worden aan de volgende frameworks:

- Norea Volwassenheidsmodel Informatiebeveiliging 2019
- GDPR – Algemene verordening gegevensbescherming (AVG)

Contact

CRUXER

Eric van Mierlo
eric@cruxer.nl
+31 (0)6 - 23229553

René van der Reijden
rene@cruxer.nl
+31 (0)6 - 29259616