



ICT TriOpSys x Cember

Continu inzicht en structurele regie op cybersecurity

Cybersecurity is geen momentopname. Toenemende cyberdreigingen, veranderende wet- en regelgeving en de groeiende afhankelijkheid van digitale processen maken duidelijk dat informatiebeveiliging continu aandacht en sturing vereist. Effectieve cybersecurity vraagt daarom om doorlopend inzicht, duidelijke regie en consistente opvolging.

Het beste van mens en technologie

Vanuit ICT TriOpSys werken we met technologie om continu inzicht te hebben in de actuele status van risico's, dreigingen en prioriteiten. Op deze manier kunnen wij u efficiënter en gericht helpen om veiliger te worden. Wij bewegen mee en passen de inzet aan waar nodig zonder rigide scope.

ICT TriOpSys werkt daarom samen met **Cember** als technologiepartner om cybersecurity eenvoudiger, toegankelijker en beter beheersbaar te maken.

Technologie voor compliance en advies

Cybersecurity en compliance vragen om overzicht, structuur en samenhang. Normenkaders zoals ISO27001, NIS2 en sector-specifieke eisen brengen grote hoeveelheden informatie samen: beleid, risicoanalyses, maatregelen, bewijslast en rapportages.

In de praktijk is deze informatie vaak verspreid over documenten, tooling en teams, waardoor het lastig is om continu grip te houden op compliance en voortgang.

Eén werkwijze, ondersteund door technologie

Binnen deze samenwerking bundelen we expertise en technologie:

-  **ICT TriOpSys** richt zich op de advisering m.b.t. governance, risico's, techniek en compliance richting de klant. Onze consultants toetsen en duiden die analyse voordat die bij u op tafel komt.
-  **Cember** ondersteunt de advisering door informatie automatisch te structureren, te analyseren en actueel te houden.
-  **De opdrachtgever** behoudt de regierol en bepaalt prioriteiten.



Alles met één doel: uw organisatie weerbaarder maken

Wij ondersteunen deze activiteiten door informatie centraal, consistent en actueel beschikbaar te maken, waardoor analyses en rapportages efficiënter en beter onderbouwd zijn. De combinatie van onze experts met technologie zorgt voor:

- ✔ Structurele grip op informatiebeveiliging.
- ✔ Altijd een actueel risicoprofiel.
- ✔ Minder afhankelijkheid van handmatige processen.
- ✔ Betere bestuurlijke besluitvorming.
- ✔ Een schaalbare aanpak zonder verlies van kwaliteit.

Versimpelen en toegankelijk maken van security-informatie

- ✔ Compliance-status is continu actueel in plaats van momentopnames.
- ✔ Documenten, risico's, maatregelen en bewijslast worden automatisch geanalyseerd.
- ✔ Relaties tussen risico's, controls en normvereisten worden inzichtelijk gemaakt.
- ✔ Dreigingen en risico's worden specifiek gemaakt en daardoor weten we continu wat we moeten verbeteren en waarom.
- ✔ Bij nieuwe informatie ziet u welke risico's en maatregelen dat raakt, en welke bron de aanleiding was.
- ✔ Maatregelen hebben een eigenaar, een deadline en een status, geprioriteerd op het risico dat ze afdekken.

Hierdoor ontstaat één consistent en gedeeld beeld van de security-positie, en weet je waar je aan moet werken.

