Cingulum
CRANIUM

Opdrachtencentrale
Centrale des marchés

Third Party Risk Management

Cybersecurity monitoring & leveranciersbeheer

Raamovereenkomst OC/2024/210/DVDB - Perceel 1

www.cingulum.eu

Inhoud

Je leveranciersrisico's, continu in beeld 2
Wat is TPRM en wat mag je verwachten?

Hoe werkt deze dienst? 3
Eén aanpak, twee platformen.

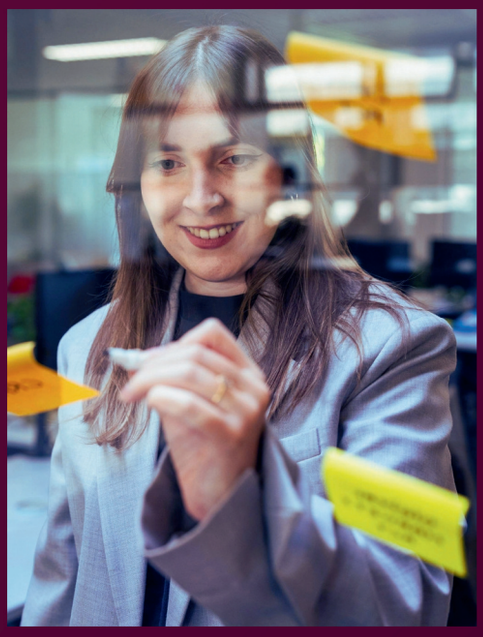
Van score naar actie 4
Hoe snel zie je resultaten?

Wat kost het? 5
Een uitgebreid pakket, aangepast aan jouw bedrijfscontext en -grootte.

Van aanvraag tot actieve monitoring 7
Hoe loopt het traject?

Over Cingulum 8
Leer ons wat beter kennen.

Je leveranciersrisico's, continu in beeld



Je organisatie werkt met tientallen, soms honderden leveranciers. Veel van hen hebben toegang tot je systemen, je data of je processen. Weet je hoe goed zij hun security op orde hebben? En merk je het op tijd als dat verandert?

Valt je organisatie onder NIS2? Dan moet je kunnen aantonen dat je de risico's in je toeleveringsketen kent en opvolgt. Dat vraagt een vaste werkwijze, die je jaar na jaar kunt herhalen.

Cingulum helpt je daarbij met een geïntegreerde TPRM-dienst.

We combineren twee platformen met de kennis van onze cybersecurityexperts. Zo beoordeel je leveranciers op een gestructureerde manier, volg je hen continu op en grijp je gericht in waar het nodig is.

Wat is TPRM?

Third Party Risk Management (TPRM) is het opvolgen van de risico's die ontstaan doordat je samenwerkt met externe partijen, zoals leveranciers, dienstverleners en partners.

Wat mag je verwachten?

- Gestructureerde leveranciersbeoordelingen. Vragenlijsten via ons eigen TPRM-platform, met bewijsstukken, goedkeuringsflows en vaste momenten voor herbeoordeling.
- Continue monitoring van buitenaf. RiskRecon volgt je leveranciers dagelijks op en geeft een actuele risicoscore.
- Rapportage en overleg. Op regelmatige basis, afgestemd op het pakket dat je kiest.
- Gerichte opvolging waar nodig. Actieplannen, interviews en audits door gecertificeerde Cingulum-auditoren.

Hoe werkt deze dienst?

Eén aanpak, twee platformen

Een vragenlijst toont hoe een leverancier zijn eigen security beschrijft. Een externe scan toont wat er van buitenaf zichtbaar is. Samen geven ze een volledig beeld. Daarom combineren we twee platformen die samen je leveranciersrisico's in kaart brengen:

- Cingulum TPRM-platform voor governance, vragenlijsten en leveranciersdossiers.
- RiskRecon®, technologie van Mastercard, voor continue externe monitoring en meldingen bij nieuwe risico's.

Hoe diep volg je elke leverancier op?

Niet elke leverancier vraagt dezelfde aandacht. Een leverancier die je kernprocessen ondersteunt of toegang heeft tot gevoelige data, deel je in als **kritische leverancier**. Een leverancier met weinig impact op je organisatie wordt **niet-kritische leverancier**.
Het type bepaalt hoe grondig RiskRecon de leverancier scant en hoe vaak je de beoordeling herhaalt. Welke vragenlijst een leverancier krijgt, hangt af van zijn score. Meer daarover lees je op de volgende pagina.

RiskRecon Discovery of Advisory?

RiskRecon werkt met twee niveaus:

Met **Discovery** krijg je een samenvattende score voor de relevante securitydomeinen. Dat volstaat voor leveranciers die **minder kritisch** zijn voor je organisatie.

Advisory gaat een stap verder en geeft een gedetailleerd beeld van onder meer softwareupdates, applicatiebeveiliging, versleuteling van websites, netwerkfiltering, gekende datalekken, reputatie van systemen, e-mailbeveiliging, DNS-beveiliging en hosting.

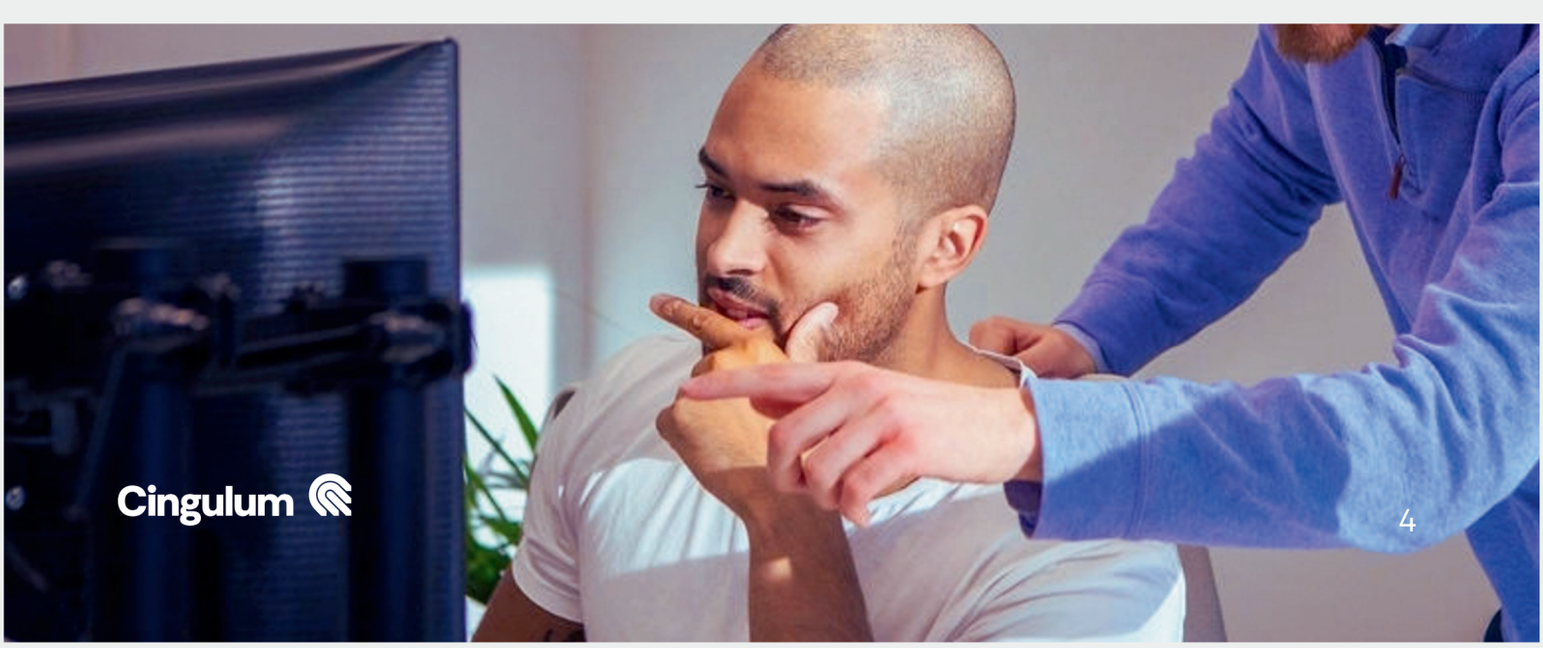
Van score naar actie

Hoe snel zie je resultaten?

RiskRecon geeft elke leverancier **een score van A tot F.** Die score toont hoe sterk de security van een leverancier is, bekeken van buitenaf. A is de beste score, F de zwakste. Op basis van die score bepalen we welke opvolging nodig is. Zo gaan je tijd en energie naar de leveranciers waar het risico het grootst is.

Score	Actie
A-B	Een korte intakevragenlijst. Een geldig certificaat kan de beoordeling eenvoudiger maken.
C-D	Een online actieplan met deadlines om de risico's weg te werken.
E-F	Een actieplan, aangevuld met een gedetailleerde vragenlijst of een interview. Zo schatten we het risico juist in.

Staat een leverancier al in het scanportfolio van RiskRecon? Dan zijn de resultaten meteen beschikbaar. Zo niet, dan is de eerste scan klaar binnen één tot drie werkdagen.



Wat kost het?

De prijs bestaat uit drie delen. Eerst is er een **basis per pakket:** de licenties voor het platform en een eenmalige activatie met training. Daarnaast betaal je per leverancier, afhankelijk van het type dat je toekent. Tot slot zijn er de diensten die je effectief gebruikt, zoals rapportage, interviews en onboarding. Alle prijzen zijn exclusief btw.

Component	Kleine onderneming <50 FTE	Middelgrote onderneming 50-250 FTE	Grote onderneming >250 FTE
Activatie platform (eenmalige training)	€ 430	€ 430	€ 860
Rapportage & afstemming	Max. per kwartaal (4 dagen)	Max. per 2 maanden (6 dagen)	Max. maandelijks (12 dagen)
Licenties platform	€ 577,50	€ 866,25	€ 1.155
RiskRecon Kritisch (per leverancier)	€ 462	€ 462	€ 462
RiskRecon Niet-Kritisch (per leverancier)	€ 52	€ 52	€ 52

Diensten op basis van gebruik

Dienst	Kleine onderneming <50 FTE	Middelgrote onderneming 50-250 FTE	Grote onderneming >250 FTE
Rapportage & afstemming	Max. € 3.465	Max. € 5.197,50	Max. € 10.395
Interview	€ 346,50 per interview	€ 346,50 per interview	€ 346,50 per interview
Onboarding	€ 173 per leverancier	€ 173 per leverancier	€ 173 per leverancier

Goed om te weten voor je budget

Voor rapportage en overleg geldt een maximum aantal dagen per jaar. Volg je minder leveranciers op, dan ligt de werkelijke kost vaak lager dan dat maximum. Elke nieuwe leverancier wordt in het eerste jaar bevraagd. Daarna volgt de herbeoordeling volgens het type dat je aan die leverancier hebt toegekend. Updates van beide platformen zitten in de prijs, net als online technische support.

Extra diensten en uitbreidingen

Extra diensten zet je alleen in als je ze nodig hebt of er zelf voor kiest.

Audits

Een audit gebeurt alleen als jij daartoe beslist en als het contract met de leverancier een audit toelaat.

<50 FTE	50-250 FTE	>250 FTE
€1.100	€2.200	Prijs op aanvraag

Aanvullende securitydiensten

Naast TPRM kan Cingulum je ook ondersteunen met bredere cybersecurityexpertise. Je vindt alle mogelijkheden in onze brochure met aanvullende diensten. De prijs hangt af van de dienst en de concrete opdracht.



Van aanvraag tot actieve monitoring

Je kan klein starten en de scope later uitbreiden. Zo beheer je leveranciersrisico's op een manier die je kan aantonen, herhalen en laten meegroeien.

Kies je pakket

Klein, middelgroot of groot, afhankelijk van hoe groot je onerneming is (zie p.5).

Bepaal welke leveranciers je opvolgt

Deel ze in als kritische of niet-kritische leveranciers, volgens risico en gewenste diepgang.

Activeer en onboard

Cingulum zet de platformen op, maakt de leverancierprofielen aan en start de scans en de eerste bevraging.

Volg op en stuur bij

Op basis van scores en vragenlijsten zetten we waar nodig interview, extra support of audits in.

Contractueel kader

Deze brochure vat het aanbod samen binnen perceel 1, Analysetools Cybersecurity, van raamovereenkomst OC/2024/210/DVDB.
Deze raamovereenkomst is opgezet voor afnemers van Opdrachtencentrale vzw.
Bij bestelling gelden de contractuele bepalingen en prijsafspraken van de raamovereenkomst.

Cingulum

Opdrachtencentrale
Centrale des marchés

Over Cingulum

Cingulum is een Belgisch cybersecuritybedrijf dat kmo's, overheden en kritieke sectoren ondersteunt bij het opbouwen van een weerbare digitale organisatie.
We combineren technische diepgang met beleidsmatige helderheid, zodat je niet alleen ontdekt wat nodig is, maar ook hoe je het concreet kan waarmaken.

Waarom kies je voor Cingulum?

Pragmatische aanpak

We passen onze werkwijze aan aan jouw context en sector, en werken met een gestandaardiseerde methode waar mogelijk. Zo werken we snel en efficiënt.,

Pakketten op maat

Onze pakketten zijn flexibel en volledig af te stemmen op jouw noden en bedrijfscontext. Stel eenvoudig zelf je ideale pakket samen uit ons aanbod.

Pragmatische partner

Cingulum behoort tot de CRANIUM Group. Op die manier kunnen we op pragmatische manier werken als one-stop-shop voor digital compliance & governance.

Focus op cybersecurity governance

Cingulum is gespecialiseerd in cybersecurity governance en het opzetten van een ISMS. Deze expertise en ervaring nemen we rechtstreeks mee in je organisatie.

Onze missie

Wij willen elke organisatie, klein of groot, helpen om beter bestand te zijn tegen digitale dreigingen. Niet door angst aan te wakkeren, maar door helderheid, structuur en vertrouwen te bieden. Zo maken we cybersecurity werkbaar én doeltreffend.

Cingulum

Klaar om je leveranciers in beeld te brengen?

Als afnemer van Opdrachtencentrale vzw kun je rechtstreeks bestellen via de raamovereenkomst, zonder eigen aanbestedingsprocedure. Twijfel je nog over het juiste pakket of over hoe je je leveranciers best indeelt? Plan dan een vrijblijvend gesprek met een van onze experts. Samen brengen we je leveranciers in kaart en kiezen we de opvolging die past bij jouw organisatie.



willem.magerman@cingulum.eu
+32 (0) 471 93 63 65

lisa.botteldoorn@cingulum.eu
+32 (0) 472 84 29 34

Cingulum

Geïnspireerd? Vragen over de raamovereenkomst met de Opdrachtencentrale vzw? Contacteer Willem of Lisa en ontdek wat we voor jou kunnen betekenen.

lisa.botteldoorn@cingulum.eu
+32 (0)472 84 29 34
willem.magerman@cingulum.eu
+32 (0) 471 93 63 65

Algemeen telefoonnummer:
02 310 39 63

© Cingulum, 2026
Alle rechten voorbehouden.
Niets uit deze uitgave mag verveelvoudigd en/of openbaar gemaakt worden door middel van druk, fotokopie, microfilm of op welke andere wijze ook, zonder voorafgaande toestemming van Cingulum.

www.cingulum.eu | info@cingulum.eu