Deloitte.

centrum informatiebeveiliging
en privacybescherming



THIRD PARTY RISK MANAGEMENT

INZICHTEN UIT DE PRAKTIJK

26 SEPTEMBER 2024 – HARM KUIPER, REMCO VAN MOSEL



Remco van Mosel

Deloitte – Partner

Remco is een partner die de publieke sector ondersteund om digitaal weerbaar te worden. Hij helpt klanten bij het navigeren door de uitdagingen van een snel digitaliserende wereld en het realiseren van hun digitale ambities door te adviseren over de bijbehorende risico's.



Harm Kuiper

Deloitte – TPRM Expert

Harm is een vooraanstaand expert in het beveiligen van toeleverancierssketens tegen cyberrisico's. Hij is een groot voorstander van het volgen van een risicogebaseerde aanpak en het in staat stellen van contracteigenaren om de juiste beslissingen te nemen.

VOOR VANDAAG

Context

Scoping

Contract-eigenaren ondersteunen

In minder dan 20 minuten



Third Party Risk hebben wij geen last van, toch?



5 juni 21:27

Rijk onderzoekt groot lek in online vergadersysteem bewindslieden

Van onze redacteur

In het kort

- De Duitse krant Die Zeit onthulde woensdag hoe informatie over vergaderingen via videoplatform Webex online vindbaar was.
- Dit systeem wordt door veel overheden in Europa gebruikt omdat het veiliger zou zijn.
- Het lukte de journalist zelfs om in te bellen bij vergaderingen van bewindslieden.
- Demissionair staatssecretaris Van Huffelen is geschrokken en kondigt onderzoek aan.

NL: Webex-kwetsbaarheid



Nieuws

Backdoor in opnamesoftware voor rechtbanken aangetroffen

donderdag 23 mei 2024, 15:38 door **Redactie**, 6 **reacties**

Onderzoekers hebben in opnamesoftware die wordt gebruikt door rechtbanken, gevangenissen, alsmede voor hoorzittingen, colleges en vergaderingen, een backdoor aangetroffen waarmee aanvallers volledige controle over het onderliggende systeem krijgen. Organisaties die met Justice AV Solutions (JAVS) werken wordt opgeroepen om getroffen systemen opnieuw te installeren en inloggegevens te wijzigen.

Justice AV Solutions is een Amerikaans bedrijf dat zich vooral richt op het aanbieden van audiovisuele oplossingen voor partijen in de justitieketen. Het bedrijf claimt wereldwijd meer dan tienduizend installaties. Het gaat onder andere om de **JAVS Suite**, beheersoftware voor digitale opnames. Eén van de onderdelen van de JAVS Suite is de JAVS Viewer, waarmee log- en mediabestanden zijn te bekijken.

In de officiële versie van JAVS Viewer versie 8.3.7 is een backdoor aangetroffen die gelinkt is aan de **GateDoor/Rustdoor-malware**, zo meldt securitybedrijf **Rapid7**. Begin april werd er al **op X gewaarschuwd** voor de aanwezigheid van malware in de JAVS Viewer. De malware is gesigneerd, maar niet met een certificaat van Justice AV Solutions. Rapid7 deed onderzoek naar de malware en informeerde de Amerikaanse overheid.

Na ontdekking van de malware heeft JAVS de eigen wachtwoorden gereset en een audit naar de eigen systemen laten uitvoeren. Hoe de besmette versie van de software op de officiële website terechtkwam laat het softwarebedrijf niet weten. Organisaties die met de software werken moeten getroffen systemen opnieuw installeren, versie 8.3.8 of nieuwer installeren en alle inloggegevens die op het systeem zijn gebruikt veranderen.

NL: Kwetsbaarheid in JAVS Viewer

Toeleveringsketens zijn steeds relevanter

Met behulp van de AVG als sjabloon dekt regelgeving steeds meer de noodzaak om uw derde partijen te beheren.

ePrivacy Regulation
Regulates the protection of personal data and the use of cookies in electronic communications

Cybersecurity Resilience Act
Establish common cyber security standards for products (especially connected objects) and services on our market

Market in Crypto-Assets Regulation
Regulates the services related to digital assets dependent on cryptography and distributed ledger technology

Digital Operational Resilience Act
Regulates the ICT risk requirements for financial and critical ICT service providers

Artificial Intelligence Act
Regulates the development, deployment and use of Artificial Intelligence systems

Radio Equipment Directive
To increase for certain categories of radio equipment the level of cybersecurity and privacy

Digital Markets Act
To ensure that "gatekeepers" in digital markets behave in a fair way online



NIS-2 Directive
Regulates the cybersecurity requirements for essential services in the EU, revising NIS-1

Data Governance Act
Regulates data sharing between sectors and improves data availability in the EU

Robots Act
Regulates products of the mechanical engineering industries within the EU

Digital Services Act
Regulates the provision of digital services to create a safer and trusted online environment

Chips Act
Aims to build a state-of-the-art European semi-conductors ecosystem

Identity Regulation
Regulates electronic identification and trust services for electronic transactions in the internal market

Data Act
Regulates business-to-government and business-to business data sharing to improve data access and use

Third Party risk dekt verschillende risicodomeinen

Uw organisatie zal in de toekomst meerdere risicodomeinen moeten oppakken, dus denk groot.

Gegevensbescherming

Een derde partij voldoet niet aan de organisatorische en/of wettelijke/regelgevende normen voor de verwerking en bescherming van de persoonlijke en/of gevoelige gegevens van uw organisatie.

Informatie en cyberbeveiliging

Een derde partij gebruikt of bewaart de gegevens van de organisatie op een manier die niet adequaat is beschermd tegen onbedoelde of kwaadwillige wijziging, vernietiging en ongeoorloofde toegang of openbaarmaking.

Bedrijfscontinuïteit

Het niet leveren van goederen of diensten als gevolg van het onvermogen om een verstorende gebeurtenis in hun toeleveringsketen adequaat te beheren, wat resulteert in nadelige gevolgen voor de organisatie.

ESG

Het niet naleven van ESG-normen door een derde partij kan aanzienlijke risico's voor uw organisatie met zich meebrengen. Milieurisico's zijn onder meer niet-naleving van milieuvoorschriften en niet-duurzame praktijken.

Financiële gezondheid

Een derde partij is financieel niet langer levensvatbaar en daarom niet in staat om een stabiele dienst of product te leveren, wat resulteert in operationele risico's.

Gezondheid en Veiligheid

Een derde partij voldoet niet aan de normen van de organisatie voor gezondheid en veiligheid op de werkplek en levert goederen of diensten op een manier die schade toebrengt aan werknemers of klanten.

Geopolitiek

Een derde partij bevindt zich in een geografie die is blootgesteld aan politieke of economische instabiliteit, waardoor de klantorganisatie kan worden blootgesteld aan risico's in de toeleveringsketen.

Arbeidsrechten

Een derde partij gebruikt onethische arbeidspraktijken om goederen of diensten te leveren, zoals kinderarbeid, dwangarbeid, discriminatie, oneerlijke beloning, wat resulteert in reputatie-, regelgevende, juridische en/of operationele risico's.

Anti-omkoping en corruptie

Een derde partij beschikt niet over adequate controles om het corruptierisico te weerstaan en kan zich bezighouden met onwettige zakelijke praktijken of crimineel gedrag, zoals het witwassen van geld, omkoping of fraude.

Concentratie

Een derde partij wordt uitsluitend gecontracteerd om kritieke/risicovolle functies uit te voeren, waardoor uw organisatie wordt blootgesteld aan een te grote afhankelijkheid van één organisatie voor dienstverlening.

Gedrag

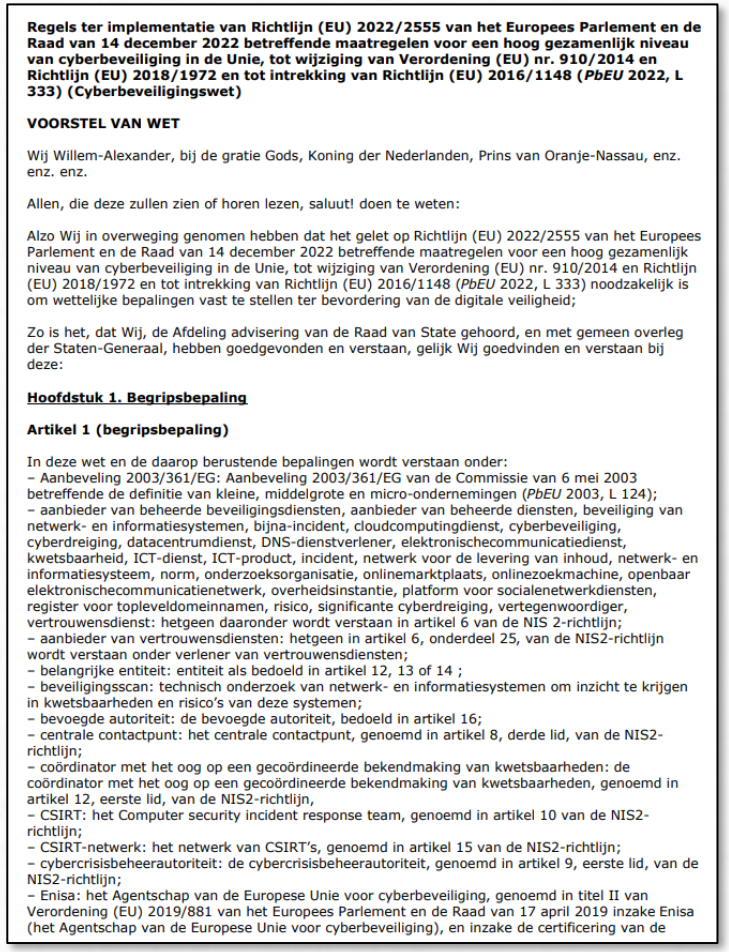
Een derde partij levert namens de organisatie goederen of diensten die leiden tot schade aan de klant of een nadelig effect hebben op de marktstabiliteit of daadwerkelijke concurrentie.

Wat zegt NIS2 over het beveiligen van toeleveringsketens?

In Nederland wordt de NIS2-richtlijn geïmplementeerd in de vorm van de **CYBERBEVEILIGINGSWET (onder toezicht van RDI)**. Met de invoering van de Cyberbeveiligingswet vervangt deze de huidige Wet beveiliging netwerk- en informatiesystemen (Wbni).

TL:DR

- **Wat: Organisaties moeten ervoor zorgen dat er adequate beveiligingsmaatregelen zijn getroffen bij hun leveranciers en serviceproviders om de integriteit en veiligheid van hun netwerken en informatiesystemen te waarborgen.**
- Wie: IT-afdeling, inkoopafdeling, risicobeheer, juridisch, compliance en bedrijfsonderdelen. Onder verantwoordelijkheid van het bestuur.
- Wanneer: Binnenkort™.
- Waarom: Om het risico op verstoringen en beveiligingsincidenten in kritieke services te minimaliseren en de algehele cyberweerbaarheid te vergroten.
- Hoe: Implementeer strenge beveiligingsvereisten in contracten, voer regelmatig audits en monitoring van leveranciers uit en werk samen met leveranciers om beveiligingsproblemen proactief aan te pakken.



Regels ter implementatie van Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (*PbEU* 2022, L 333) (Cyberbeveiligingswet)

VOORSTEL VAN WET

Wij Willem-Alexander, bij de gratie Gods, Koning der Nederlanden, Prins van Oranje-Nassau, enz. enz. enz.

Allen, die deze zullen zien of horen lezen, saluut! doen te weten:

Alzo Wij in overweging genomen hebben dat het gelet op Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (*PbEU* 2022, L 333) noodzakelijk is om wettelijke bepalingen vast te stellen ter bevordering van de digitale veiligheid;

Zo is het, dat Wij, de Afdeling advisering van de Raad van State gehoord, en met gemeen overleg der Staten-Generaal, hebben goedgevonden en verstaan, gelijk Wij goedvinden en verstaan bij deze:

Hoofdstuk 1. Begripsbepaling

Artikel 1 (begripsbepaling)

In deze wet en de daarop berustende bepalingen wordt verstaan onder:
– Aanbeveling 2003/361/EG: Aanbeveling 2003/361/EG van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen (*PbEU* 2003, L 124);
– aanbieder van beheerde beveiligingsdiensten, aanbieder van beheerde diensten, beveiliging van netwerk- en informatiesystemen, bijna-incident, cloudcomputingdienst, cyberbeveiliging, cyberdreiging, datacentrumdienst, DNS-dienstverlener, elektronischecommunicatiedienst, kwetsbaarheid, ICT-dienst, ICT-product, incident, netwerk voor de levering van inhoud, netwerk- en informatiesysteem, norm, onderzoeksorganisatie, onlinemarktplaats, onlinezoekmachine, openbaar elektronischecommunicatienetwerk, overheidsinstantie, platform voor socialenetwerkdiensten, register voor topleveldomeinnamen, risico, significante cyberdreiging, vertegenwoordiger, vertrouwensdienst: hetgeen daaronder wordt verstaan in artikel 6 van de NIS 2-richtlijn;
– aanbieder van vertrouwensdiensten: hetgeen in artikel 6, onderdeel 25, van de NIS2-richtlijn wordt verstaan onder verlener van vertrouwensdiensten;
– belangrijke entiteit: entiteit als bedoeld in artikel 12, 13 of 14 ;
– beveiligingsscan: technisch onderzoek van netwerk- en informatiesystemen om inzicht te krijgen in kwetsbaarheden en risico's van deze systemen;
– bevoegde autoriteit: de bevoegde autoriteit, bedoeld in artikel 16;
– centrale contactpunt: het centrale contactpunt, genoemd in artikel 8, derde lid, van de NIS2-richtlijn;
– coördinator met het oog op een gecoördineerde bekendmaking van kwetsbaarheden: de coördinator met het oog op een gecoördineerde bekendmaking van kwetsbaarheden, genoemd in artikel 12, eerste lid, van de NIS2-richtlijn,
– CSIRT: het Computer security incident response team, genoemd in artikel 10 van de NIS2-richtlijn;
– CSIRT-netwerk: het netwerk van CSIRT's, genoemd in artikel 15 van de NIS2-richtlijn;
– cybercrisisbeheerautoriteit: de cybercrisisbeheerautoriteit, genoemd in artikel 9, eerste lid, van de NIS2-richtlijn;
– Enisa: het Agentschap van de Europese Unie voor cyberbeveiliging, genoemd in titel II van Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de

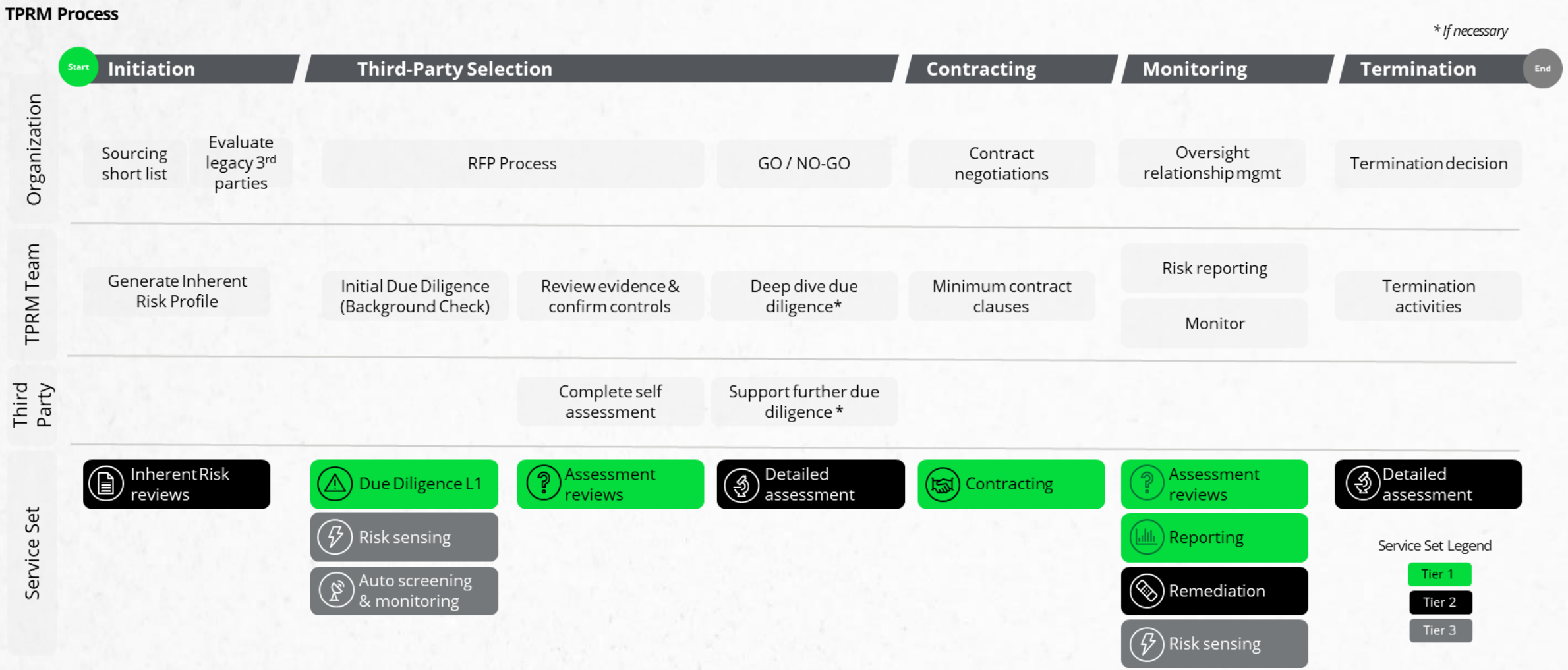
In de praktijk

Scope bepalen



Het TPRM-proces

De scoping van leveranciers is vaak een struikelblok wat tot discussies leidt



Uitwerken van een Inherent Risk Questionnaire

Om het bruto risico te bepalen zien we in de praktijk dat een korte vragenlijst wordt ingevuld door de contract-eigenaren binnen de organisatie.

Gemiddeld aantal vragen in de IRQs:
Ongeveer 38 vragen per IRQ.

Aantal risicodomeinen afgedekt:
Meest voorkomende risicodomeinen (9):

1. Anti-Bribery & Corruption
2. Business Continuity
3. Conduct Risk
4. Data Privacy
5. Export Controls
6. Financial Risk
7. Information Security
8. IT Risk
9. Labour Rights en HSE

	Top 5 Inzichten
1	**Conditionele Logica** Gebruik voorwaardelijke (knock-out) vragen om het proces te stroomlijnen.
2	**Uitgebreide Dekking** Dek alle relevante risicodomeinen af.
3	**Eenvoudige vragen** Zorg voor vragen die kunnen worden ingevuld zonder externe input
4	**Scoresysteem** Implementeer een scoresysteem om risiconiveaus te kwantificeren.
5	**Documentatie en Bewijs** Vraag om ondersteunende documentatie voor kritische antwoorden.

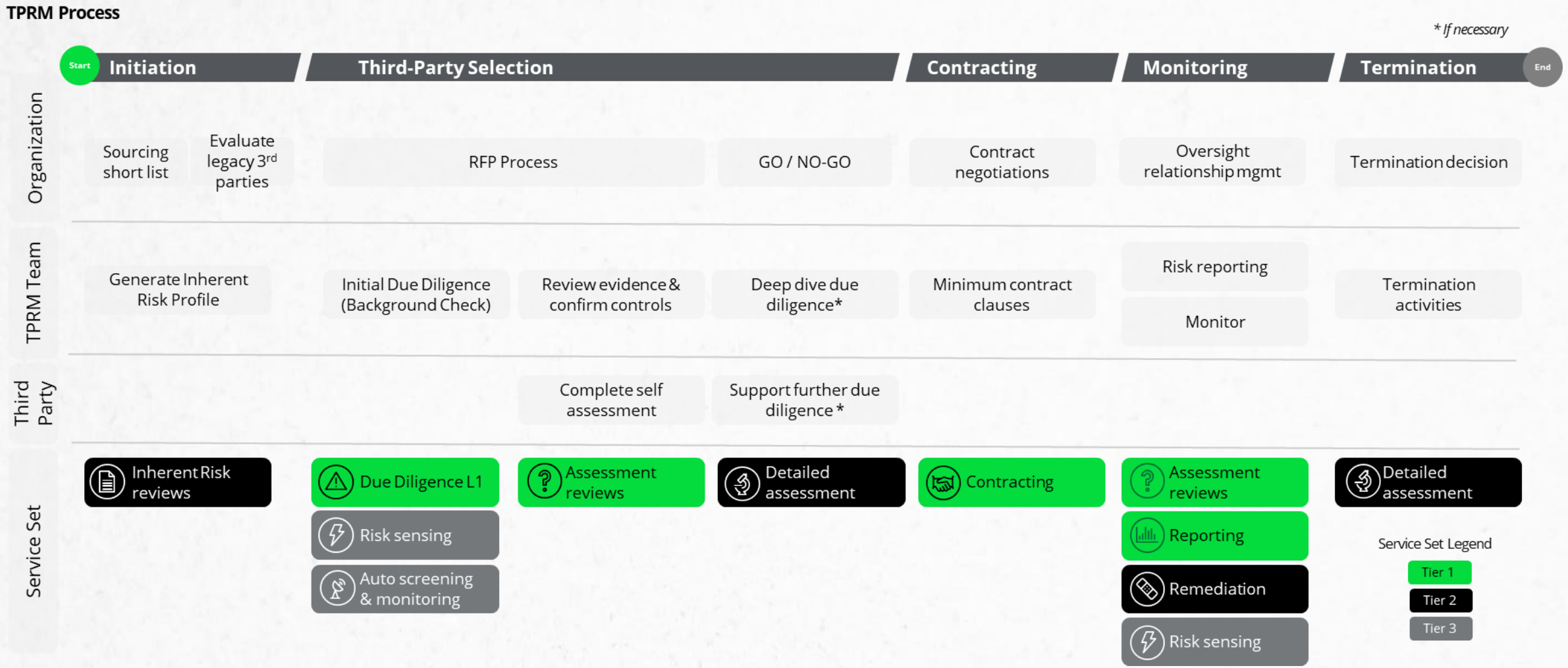
In de praktijk

Contract-eigenaren helpen



Het TPRM-proces met touchpoints

De contract-eigenaar is het meest geholpen met een bruikbaar risico rapport wat met hem/haar wordt gedeeld.



Uitwerken van sterk rapport

Maak een samenvatting welk te lezen is in 1 oog opslag.

1. ASSESSMENT SUMMARY

SUPPLIER	ASSESSOR	RISK SENSOR	OVERALL RATING
The Company	H Kuiper	A	GOOD
DUNS NUMBER	**ASSESSMENT INITIATED**	**ASSESSMENT SCORE**	**MONITORING STATUS**
03487843B	26-09-2024	89%	KEEP MONITORING

Uitwerken van sterk rapport

Vergroot de effectiviteit van de samenvatting door de volgende 3 elementen op te nemen:

1

Assessment Overview: The company has obtained a Good rating with an 'A' ExternalRiskSensor rating and an assessment score of 89%. They have provided their ISO27001 certification along with a Statement of Applicability, SOC 2 report, and detailed comments on their information security management processes and controls, indicating a solid commitment to information security practices. The assessment identified no immediate risk for the supplier.

Areas of Concern:

- System Development: Lack of evidence that DDoS testing is performed at the frequency determined by the client.
- Business Application Management: Incomplete implementation of security controls in business applications and lack of development methodologies for End User Developed Applications (EUDA).
- Supply Chain Management: Clarification required on security assurance checks within the supply chain that affect the client.
- Threat and Incident Management: Lack of detailed evidence on threat management and security incident processes.

2

Recommended Action for Contract Owner: Keep monitoring: Given the 'Good' rating and the absence of immediate risk, it is recommended to continue monitoring the supplier's adherence to security practices and their response to the remediation actions suggested.

3

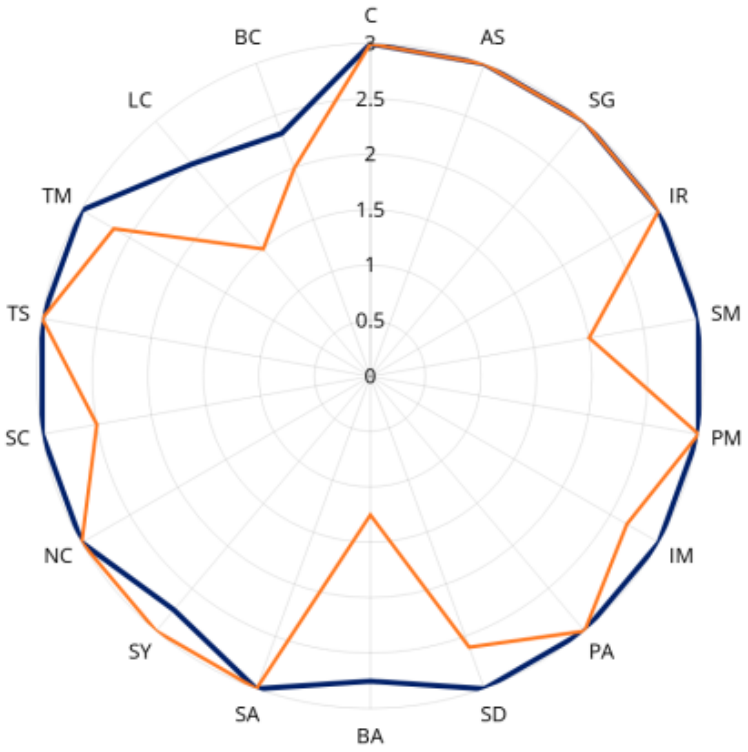
Recommended Remediation Actions for the supplier:

- Threat and Incident Management: Present evidence of a comprehensive threat management process and an incident management framework specific to client services.
- Local Environment Management: Confirm the appointment of local security coordinators and the protection of critical facilities.
- Business Continuity: Ensure business continuity plans are established and tested in collaboration with the client.

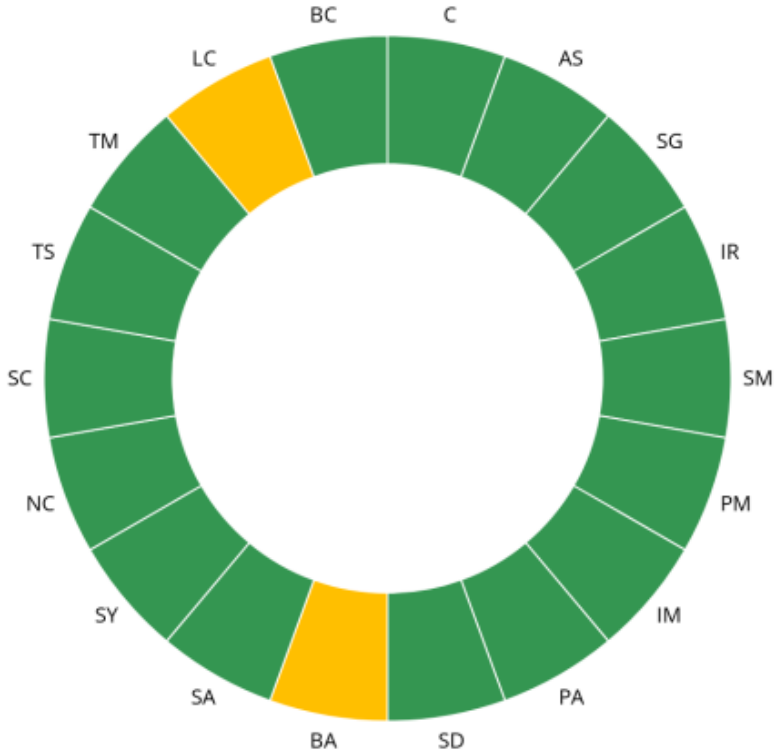
Uitwerken van sterk rapport

Gebruik een visual voor besprekingen tussen de contract-eigenaar, de risk manager, en mogelijk de leverancier.

The below chart indicates instances where there is a discrepancy between the supplier's self-assessed score and the assessor's concluded score.



The below chart highlights domains with a low score, based on the legend below. Domains with a RED score will have remediation actions described in the next section. Remediation actions will give guidance on how to achieve a YELLOW or GREEN score.



DOMAIN LEGEND

C	Certification
AS	Security Assurance
SG	Security Governance
IR	Information Risk Assessment
SM	Security Management
PM	People Management
IM	Information Management
PA	Physical Asset Management
SD	System Development
BA	Business Application Management
SA	System Access
SY	System Management
NC	Networks and Communications
SC	Supply Chain Management
TS	Technical Security Management
TM	Threat and Incident Management
LC	Local Environment Management
BC	Business Continuity

Vragen?



Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte provides industry-leading audit and assurance, tax and legal, consulting, financial advisory, and risk advisory services to nearly 90% of the Fortune Global 500® and thousands of private companies. Our professionals deliver measurable and lasting results that help reinforce public trust in capital markets, enable clients to transform and thrive, and lead the way toward a stronger economy, a more equitable society and a sustainable world. Building on its 175-plus year history, Deloitte spans more than 150 countries and territories. Learn how Deloitte’s more than 345,000 people worldwide make an impact that matters at www.deloitte.com.

This communication contains general information only, and none of DTTL, its global network of member firms or their related entities is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte organization shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

© 2024. For information, contact Deloitte Netherlands.