Auteurs: Suyi Guo is Information Security Officier en TPSRM capability owner. Suyi is te bereiken via suyi@protect9.nl.
Sven Enthoven is Information Security Officer. Sven is te bereiken via sven.enthoven@mountaininfosec.com.

Tips en tricks voor het MKB om te starten met Third Party Risc Management (TRPM)

In sectoren die een sterk compliance gedreven aanpak vereisen, hebben bedrijven de laatste jaren hun TPRM-raamwerk opgezet en deze steeds verder uitgebreid. Door middel van onze ervaringen met deze raamwerken willen wij het MKB helpen door een aantal praktische voorbeelden en handvatten aan te reiken. Middels deze tips en tricks kan het MKB, denken wij, een goede start maken met de eigen TPRM-activiteiten.

Organisaties kiezen er steeds vaker voor om bepaalde diensten uit te besteden. Een begrijpelijke keuze, want organisaties doen graag die zaken waar ze goed in zijn en voor het MKB ligt deze stap wellicht nog meer voor de hand. Maar daarbij wordt ook een stukje controle uit handen gegeven. Het uitbesteden van (kern)activiteiten brengt namelijk ook risico's met zich mee. Aanvullende wet- en regelgeving, zoals Digital Operational Resilience Act (DORA) en Network and Information Security (NIS2) eisen dat de focus steeds meer gelegd moet worden op de controle van de (keten van) derde partijen.

Buiten de strengere wet- en regelgeving zijn er tegenwoordig ook legio voorbeelden te vinden waarbij een aanval op een leverancier zorgt voor beveiligingsincidenten bij afnemers. Denk daarbij bijvoorbeeld aan Solarwinds (1), waardoor Microsoft gehackt werd of aan de recentelijke hack bij AddComm waardoor een kwaadwillende potentieel toegang zou hebben gehad tot gevoelige gegevens van ABN AMRO en Waterbedrijf Groningen (2). Dit geeft aan dat het onmogelijk is om alle risico's op voorhand inzichtelijk te hebben en te voorkomen dat een leverancier gehackt wordt. Een TPRM-raamwerk en de daarbij behorende processen bieden inzicht in de potentiële risico's die een organisatie loopt met een leverancier. Een dergelijk inzicht helpt de organisatie om gedegen keuzes te maken in het aantrekken en behouden van de juiste leveranciers.
Het MKB heeft vanwege de beperkte omvang minder kennisgebieden binnen de organisatie. Bij grote organisaties zijn verschillende teams betrokken bij het opzetten en beheren van verschillende raamwerken, zoals bij een TPRM-raamwerk. Bij het MKB ligt dat ongetwijfeld anders, een medewerker van een MKB-bedrijf kan verschillende expertisegebieden hebben, waarbij de medewerkers bij een grote organisatie duidelijkere kaders hebben.

Figuur 1: TPRM Framework.

TPRM-raamwerk

Verschillende organisaties hebben een TPRM-raamwerk gepubliceerd waarin een continue cyclus van stappen wordt doorlopen. Deze raamwerken houden rekening met het vooronderzoek, de levenscyclus van het contract en de afronding. Price Waterhouse Cooper (PWC) heeft een raamwerk opgesteld dat in de afbeedling is weergegeven (3).

Stappen voor een kleinschalige aanpak

In het raamwerk zijn diverse ondersteunende processen en bedrijfsactiviteiten beschreven. Sommige processen en bedrijfsactiviteiten zijn niet exclusief opgetuigd om TPRM te realiseren. TPRM maakt hier enkel handig gebruik van. Binnen het MKB kan

TPRM is een continu proces, waarbij het assessment periodiek herhaald moet worden

het zijn dat deze onderwerpen niet volledig zijn uitgewerkt maar wel onderdeel zijn van het bedrijf.

Om de vertaalslag van het raamwerk naar een kleinschalige, risicogebaseerde aanpak van TPRM te beschrijven, staan hieronder globaal de processtappen voor het aangaan van een nieuw contract. Na een initieel assessment moeten bestaande contracten via continue monitoring worden bijgehouden. Een voorbeeld hiervan zal in het Tiering-onderdeel worden beschreven. Afhankelijk van de eisen van uw organisatie kunnen onderstaande stappen afwijken.

1. De organisatie heeft de noodzaak om een dienst af te nemen en stelt een shortlist van leveranciers op.
2. De leverancier wordt beoordeeld op afhankelijkheid, een veelvoorkomende methode is het gebruiken van een Tiering-model. Dit model wordt later in dit artikel behandeld.
3. Op basis van het Tiering-model wordt de diepgang van het assessment/due diligence opgesteld. Denk hierbij aan de informatiebehoefte om een assessment uit te voeren, de benodigde controls, etc.
4. Het initiële assessment wordt uitgevoerd. In het kader van een voortraject/aanbesteding kan er op basis van het assessment een advies gegeven worden welke leverancier een (on-)acceptabel risiconiveau heeft.
5. De risico's worden met de contracteigenaar en het managementteam besproken.
6. Afhankelijk van de risicoclassificatie van de bevindingen is opvolging en tijdsplanning van toepassing.
7. Afhankelijk van de Tiering zijn er periodiek overleggen nodig om de laatste status van eventuele risico's en afstemming te bespreken.
8. Afhankelijk van de Tiering zijn herbeoordelingen noodzakelijk.

In de voorgaande beschreven stappen is uitgegaan van een nieuwe leverancier. Bij het opzetten van het TPRM-raamwerk dienen deze stappen ook voor bestaande leveranciers uitgevoerd te worden. TPRM is dus een continu proces, waarbij het assessment periodiek herhaald moet worden. Door deze herhaling worden de nieuwste controls en laatste standaarden van het TPRM-raamwerk meegenomen in de beoordeling. Afhankelijk van de bevindingen en of dit voor het tekenen van het contract opgelost dient te worden, kan dit allemaal impact hebben op de planning. En dit kan uiteraard weer per organisatie verschillen.

Voorbeeld van Tiering-model

Het aantal leveranciers die onderdeel zijn van de (kern)activiteiten van een organisatie groeit. Hiermee groeien de risico's en afhankelijkheden die externe leveranciers meebrengen ook. Niet alleen in het kader van wet- en regelgeving, maar ook voor wat betreft bedrijfscontinuïteit is het belangrijk om de risico's inzichtelijk te maken en hier grip op te krijgen. Verschillende organisaties en bedrijven die diensten aanbieden om leveranciers te monitoren maken gebruik van een Tiering-model. Voor meer informatie zie Bluevoyant (4) en UpGuard (5). Gelaagdheid in het Tiering-model kan zo ver gaan als een organisatie zelf wil, dit heeft echter wel impact op de complexiteit van het model. Complexiteit is, zeker in het begin, niet wenselijk en daarom is het aan te raden om klein te beginnen. De verschillende risiconiveaus hebben verschillende vervolgacties en requirements aan zich gekoppeld. Deze vervolgacties zijn verschillend per organisatie. Een eenvoudige opzet van verschillende Tiering-classificaties met drie verschillende risiconiveaus kan er als volgt uitzien:

Tier	Criteria	Activiteiten
1	• Impact op de (kern)activiteiten • Toegang tot gevoelige (bedrijfs)informatie • Complexe wisseling van leveranciers • Omvang van contract • Financiële (en imago)schade is significant • Impact op de bedrijfscontinuïteit is groot	• Jaarlijkse uitvoering van de Due Diligence • Uitgebreide scope van controls van toepassing, afhankelijk van de overeenkomst en opzet van de dienstverlenging • Elke drie of zes maanden overleg met leverancier over (security)incidenten
2	• Belang voor de bedrijfsvoering, maar minder directe impact op de kernactiviteiten • Wisselen van leverancier is mogelijk met enige inspanning • Gelimiteerde toegang tot (bedrijfs)informatie	• Elk ander jaar uitvoering van Due Diligence • Middelmatige scope van controls van toepassing, afhankelijk van de overeenkomst en opzet van de dienstverlenging • Elke drie of zes maanden overleg met leverancier over (security)incidenten
3	• Beperkte toegang tot (bedrijfs)informatie • Eenvoudige vervanging van leverancier	• Eenmalige uitvoering van Due Diligence voor het tekenen van het contract • Beperkte scope van controls van toepassing, afhankelijk van de overeenkomst en opzet van de dienstverlenging

Tabel 1: Voorbeeld Tiering Tabel (afgeleid van (6)).

Door leveranciers in te schalen op een specifiek niveau wordt de organisatie in staat gesteld om op een risicogebaseerde aanpak de leveranciers te beoordelen. Vanzelfsprekend is het zo dat leveranciers met een tier-1 status aan meer controls zullen moeten gaan voldoen, strenger en vaker worden beoordeeld op de controls in vergelijking met een tier-2 of tier-3 leverancier. Een Tiering-model heeft daarnaast als aanvullend voordeel dat wanneer de eisen veranderen voor de leveranciers (denk aan veranderde wetgeving DORA, NIS2), dit eenvoudig te koppelen en toe te passen is op de betreffende leverancier. De samenwerking met een leverancier is ook aan wijzigingen onderhevig. Het advies is ook om periodiek een herbeoordeling van de toegewezen Tiering uit te voeren. Triggers hiervoor kunnen onder andere zijn: wijziging in het contract of periodiek op basis van het TPRM-raamwerk. De periode hangt af van de reeds toegewezen tier. Door de periodieke herbeoordeling van de toegewezen tier, voorkomt een bedrijf dat het leveranciers op een te laag of hoog niveau beoordeeld.

Het toepassen van het Tiering-model dient zowel voor bestaande, als potentiële leveranciers in het aanbestedingstraject worden toegepast, zodat er ook vooraf requirements gedeeld kunnen worden. De bepaling van de geschikte risicoclassificatie (tier) zal een samenspraak van de verschillende betrokkenen zijn, zoals beschreven in de volgende alinea.

Rollen en verantwoordelijkheden

Om de rollen en de bijbehorende verantwoordelijkheden effectief te kunnen beleggen binnen een organisatie,

dienen ze vastgelegd te worden in een beleidsstuk dat ondersteund wordt door het managementteam. Hieronder proberen we inzicht te verschaffen in de activiteiten die een expertrol zou kunnen bieden in een uitbestedingstraject. We benadrukken dat TPRM leunt op bestaande change-processen. De korte beschrijving van de rollen is een versimpelde versie en kan per organisatie verschillen. Eén persoon kan meerdere rollen vervullen. Er moet wel maar één eigenaar toegekend worden zodat het duidelijk is wie de accountability draagt.

Contracteigenaar (servicemanager)

De persoon die bevoegd is om namens het bedrijf te tekenen en uiteindelijk ook verantwoordelijk is voor het verlengen dan wel het beëindigen van het contract met de leverancier. De eigenaar monitort de dienstverlening op de daadwerkelijk geleverde kwaliteiten, vergelijkt deze met de afspraken in het contract en wint adviezen in van experts om een goed beeld te vormen van de dienstverlening. De contracteigenaar zou dit kunnen delegeren naar een servicemanager.

Subject Matter Experts (SME)

De vereiste expertise kan per organisatie en contract verschillen. Bij veel MKB-organisaties zijn bepaalde expertises belegd bij één persoon. TPRM zou in principe geïntegreerd moeten worden in bestaande (risk en change) processen. Hierbij doen we een suggestie naar de mogelijke experts die een organisatie kan hebben om een contracteigenaar te adviseren:

- Security: beoordeelt en adviseert over informatiebeveiligingsonderwerpen
- Legal/compliance: beoordeelt en adviseert of het contract voldoet aan interne eisen en de wet- en regelgeving
- Inkoop: begeleidt het proces van selectie tot aan het beëindigen van het contract. TPRM valt vaak binnen de afdeling Inkoop omdat de levenscyclus van het contract leidend is
- Architectuur: beoordeelt of de (IT-)uitbesteding past binnen de architecturale principes en ontwerp

Het is belangrijk om te benadrukken dat de verantwoordelijkheid van diverse aspecten gedeeld wordt tussen leverancier en afnemer (shared responsibility model), echter is de afnemer altijd verantwoordelijk. De accountability kan niet uitbesteed worden. Voor het beoordelen van de dienstverlening is het belangrijk om dit in gedachte te houden. Voorgaande lijst is niet uitputtend, en is puur bedoeld als voorbeeld. De lijst zou verder aangevuld kunnen worden met Privacy en Financiële expertise. Het management bepaalt vervolgens of de uitbesteding een (verhoogd/(on)-acceptabel) risico met zich meebrengt en bepaalt vervolgens of het contract getekend mag worden.

Due diligence

De volgende fase uit het TPRM-framework is due diligence en onder het kopje Rollen en verantwoordelijkheden blijkt dat de beoordeling van een uitbesteding een multidisciplinaire aangelegenheid is en dat de beoordeling per organisatie kan verschillen. Het wordt aangeraden om hiervoor bestaande 'vragenlijsten' te gebruiken. Het verbond van verzekeraars heeft een gestandaardiseerde vragenlijst (7) (gebaseerd op de ISO 27002 en) beschikbaar gesteld. Organisaties zouden deze vragenlijst op basis van hun tier-lijst kunnen inrichten, door bijvoorbeeld te kijken naar welke maatregelen altijd beschikbaar moeten zijn en welke beschikbaar moeten zijn bij een hogere tier-uitbesteding. Hierbij een simpel voorbeeld wat voor een SaaS-uitbesteding van toepassing zou kunnen zijn (zie tabel 2).

Leveranciers kunnen zelf ook assurance rapporten beschikbaar stellen die door erkende onafhankelijke partijen opgesteld zijn. De gebruikelijke rapporten zijn SOC 2 type 2 en de ISAE 3000 type 2. Deze rapporten zouden de vragenlijst kunnen vervangen. Zo'n assurance rapport biedt inzicht in de geïmplementeerde controls en of deze controls effectief zijn. Het is zeker raadzaam om vóór het tekenen van het contract deze rapportage op te vragen en zeker ook na het tekenen van het contract te blijven opvragen en te reviewen.

Contractonderhandeling

De bevindingen uit de due diligence fase dienen behandeld te worden in het bestaande riskproces. In de praktijk betekent dat accepteren of mitigeren. Elke organisatie heeft een ander risicoprofiel met een bijbehorende risk appetite. Wat voor de ene organisatie acceptabel is om de bevindingen voor het tekenen van het contract op te lossen, is het acceptabel voor een ander om dit op te nemen als een punt te monitoren tijdens de relatie. De security-SME zal tijdens de analyse een inschatting maken van het securityrisico en dit bespreken met de contracteigenaar. Risico's die vallen onder de risk appetite van de organisatie kunnen, in geval van risicoacceptatie, geaccepteerd worden binnen de kaders van de contract-

Referentie	Control	Vereiste minimale tier
11	Heeft uw organisatie een Secure Development Life Cycle geïmplementeerd en is deze ingericht in lijn met een markt standaard (b.v. Microsoft Security Development Lifecycle (SDL), OpenSAMM, BSIMM, SSE CMM, SafeCode of de NIST SSDF? (ISO: 8.25 Secure development life cycle) Penetration Testing is onderdeel van deze cyclus. In (assurance, audit) rapporten moet worden aangetoond dat minstens één keer per jaar een pentest is uitgevoerd en dat de bevindingen uit de test zijn opgelost op basis van de ernst van de bevindingen. (ISO: 8.29 Security testing in development and acceptance)	Tier 1
17	Maakt u gebruik van gescheiden omgevingen voor ontwikkeling, test, acceptatie en productie? Zijn deze voor iedere klant gescheiden (fysiek of logisch)? (ISO: 8.31 Separation of development, test and production environments)	Tier 3 Tier 2 Tier 1

Tabel 2: Voorbeeld van controls in Tiering-model.

eigenaar. Risico's met een onacceptabele rating dienen gemitigeerd te worden: dit kan zowel door compenserende maatregelen te treffen of er moet daarover door de leverancier worden onderhandeld. Hierbij een aantal suggesties om mee te nemen in het contract:

- De periodiek te ontvangen (assurance)rapportages
  - o SOC 2 type 2 / ISAE 3000 type 2
  - o Pentest rapporten
  - o (Her-)certificering van ISO 27001
- De leverancier werkt mee aan de periodieke (her-)beoordeling van hun securitylandschap
- Periodieke overleggen en/of rapportages waarbij de organisatie inzicht krijgt in bepaalde zaken zoals security, performance en incidenten.
- Geïnformeerd worden bij een hack of wanneer er data gelekt is.

Ook kan een organisatie nadenken over het beëindigen van het contract en punten hiervoor opnemen in het contract, een zogenaamde exit plan (8). Punten die in het contract meegenomen kunnen worden zijn:

- Het formaat van hoe de data beschikbaar gesteld wordt en vernietigd wordt na het beëindiging van het contract.
- Ondersteuning vanuit de leverancier om de data te migreren.
- Kennis en expertise die tijdens de migratie beschikbaar dient te komen van de leverancier. Ook hier kan natuurlijk per Tier de eisen verschillen, en niet elke leverancier kan voldoen aan de gestelde eisen en wensen.

Ongoing monitoring

In de voorgaande fases zijn de requirements in kaart gebracht, is de uitbesteding aan diverse SME's beoordeeld en is het contract getekend.. In deze fase willen we met name de tier-1 dienstverleningen en de daarbij behorende leveranciers gaan monitoren. Eerder is al aangegeven dat leveranciers periodiek beoordeeld moeten worden. Hier kunnen we kijken naar het verleden door het lezen van (assurance)rapporten, maar ook door gesprekken te voeren met de leveranciers over toekomstige wijzigingen. De volgende securityonderwerpen kunnen terugkomen:

- Bevindingen uit (assurance)rapporten
- Securityverbeteringen in het SaaSproduct en de organisatie
- Openstaande security-bevindingen

- (Aankomende) significante wijzigingen binnen de organisatie. Daarnaast zijn er diverse diensten beschikbaar die organisaties monitoren op kwetsbaarheden maar ook op het nieuws (9). Sommige bieden aanvullende diensten aan waardoor je als organisatie meer inzicht krijgt in je leveranciers en het risicoprofiel.

Afronding

Met de toenemende mate van afhankelijkheden ten opzichte van leveranciers is het belangrijk om tijdig te beginnen met de stappen binnen het TPRM-proces. TPRM begint al voor het tekenen van het contract en is een doorlopend proces (Plan Do Check Act). Door TPRM toe te passen voordat het contract is getekend, kunnen leveranciers die onacceptabele risico's vormen worden uitgesloten. Ook afscheid nemen van een leverancier is een belangrijk onderdeel binnen het proces. Hiermee wordt het hele lifecyclemanagement op leveranciers uitgevoerd. Als een leverancier vertrekt, is het goed om te weten welke informatie is opgeslagen en hoe het bedrijf ervoor zorgt dat de informatie op juiste en volledige manier wordt verwijderd.

Het in kaart brengen van leveranciers en het toekennen van een tier, kan een grootschalig en complex proces worden. Het advies is om klein te beginnen en gaandeweg uit te breiden. Afhankelijk van het aantal leveranciers kan de benodigde werkomvang berekend worden. Zeker in het begin, bij het opzetten van het raamwerk en het opdoen van de eerste ervaringen zal tijd gemoeid zijn.

Door middel van het toepassen van een risicogebaseerde aanpak wordt de organisatie in staat gesteld om zich te focussen op de leveranciers met de grootste impact. Door middel van het toepassen van het Tiering-model en het gebruiken van bestaande vragenlijsten is een organisatie in staat om snel inzicht te krijgen in de huidige risico's. Bovenstaande handvatten is een begin en de lijst is zeker niet volledig, maar naar ons inziens een goed begin om snel inzicht te kunnen krijgen en vervolgens uit te voeren.

De output van het TPRM-proces dient opgenomen te worden binnen reeds bestaande risicovastlegging en opvolgingsprocessen. MKB-bedrijven moeten de risico's in een managementteamoverleg bespreken en de benodigde vervolgstappen bepalen.

TPRM moet gedragen worden door verschillende expertisegebieden in de organisatie. Door met zijn allen een steentje bij te dragen zal de MKB-organisatie de risico's voor de belangrijkste leveranciers inzichtelijk kunnen maken en hierop kunnen acteren. Dit artikel richt zich voornamelijk op de punten vóór het tekenen van het contract, echter is het continue monitoren van de leveranciers net zo belangrijk, de Nederlandse Bank (DNB) heeft de Good Practice voor informatiebeveiliging 2023 beschikbaar gesteld (10). Onder het kopje Outsourcing staan hier aanvullende handvatten (waar dit artikel verder niet op ingaat) voor het inrichten van third party risk management. Ook hier geldt het advies om een risk-based aanpak te hanteren, waarbij men kijkt naar effectiviteit en haalbaarheid van de maatregelen.

In dit artikel is een beeld geschetst van een TPRM-opzet binnen een MKB-bedrijf, afgeleid van de grotere organisaties. Het is het fundament voor een uitgebreider en volwassener TPRM-proces. Gezien de toenemende mate van afhankelijkheid ten opzichte van leveranciers en de risicogedreven aanpak hiervoor is het van belang om de risico's binnen de gehele keten in kaart te hebben. Zonder het inzichtelijk hebben van de risico's op de bedrijfsactiviteiten is het haast onmogelijk om tijdig bij te sturen en de blootstelling aan risico's tot een acceptabel niveau te beperken.

Referenties

(1) https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know
(2) https://www.dutchitchannel.nl/news/458170/eneco-abn-amro-en-anderen-getroffen-door-cyberaanval-op-addcomm
(3) https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/tprm-protecting-operations-brand-reputation.html
(4) https://www.bluevoyant.com/knowledge-center/third-party-risk-management-tprm-a-complete-guide
(5) https://www.upguard.com/blog/vendor-Tiering-best-practices
(6) https://adoptech.co.uk/wp-content/uploads/2020/05/Third-Party-Tiering-Template-1.pdf
(7) https://www.verzekeraars.nl/publicaties/actueel/verbond-stelt-vragenlijst-leverancierselectie-informatiebeveiliging-op
(8) https://www.legalz.nl/blog/exit-plan
(9) https://www.gartner.com/reviews/market/it-vendor-risk-management-solutions
(10) good-practice-ib-2023.pdf (dnb.nl)