DIGITAL

WHITEPAPER

Third Party Risk Management

Kans- en risico-optimalisatie in uw keten

nieuwe perspectieven

BDO

Organisaties zijn steeds vaker onderdeel van een ecosysteem waarin ze met andere partijen samenwerken. Hoewel dit veel voordelen biedt, creëert het ook risico's. Als u onvoldoende zicht hebt op de keten waarvan uw organisatie onderdeel uitmaakt, kan dit leiden tot continuïteitsrisico's, reputatieschade of performance issues. Na het lezen van deze whitepaper weet u hoe u deze risico's kunt herkennen én aanpakken.

Samenwerking met derde partijen is altijd al een belangrijke voorwaarde geweest om succesvol te ondernemen. Toch ziet Noël Jansen, Senior Manager Internal Audit, Risk & Compliance bij BDO, dat organisaties steeds meer gebruikmaken van de diensten van derde partijen. Dit komt doordat zij zich meer focussen op het creëren van toegevoegde waarde voor hun klanten. Activiteiten die daar niet direct aan bijdragen, laten ze uitvoeren door andere partijen. Vaak is het ook kostenefficiënter om een gespecialiseerde partij in te huren, in plaats van een eigen afdeling in te richten. Neem dataopslag als voorbeeld. Dat gebeurt op grote schaal “in de cloud” in plaats van middels fysieke servers die worden beheerd binnen de eigen organisatie. Samenwerken met derde partijen heeft dus veel voordelen. Tegelijkertijd kent het belangrijke risico's. ‘Om hier goed mee om te gaan is het belangrijk dat een onderneming flexibel genoeg is om zich snel aan te passen wanneer omstandigheden bij bijvoorbeeld toeleveranciers daarom vragen’, legt Jansen uit. ‘Dat vereist in de eerste plaats zicht op wat er zich in de keten afspeelt en daarnaast een duidelijk plan om met onzekerheden in die keten om te gaan.’

Wanneer is Third Party Risk Management relevant?

Als u samenwerkt met derde partijen, bent u in feite al bezig met Third Party Risk Management. U wilt ook nu al zakendoen met betrouwbare partijen en tegen een eerlijke prijs. Wij zien echter ook steeds meer regelgeving ontstaan dat actief risicomanagement in de keten vereist. Organisaties zijn er expliciet voor verantwoordelijk dat aan hun verbonden ketenpartijen zich aan bepaalde minimumstandaarden houden voor bijvoorbeeld (sociale) veiligheid. Jansen geeft een aantal voorbeelden: ‘ESG-regelgeving bevat tal van verplichtingen voor organisaties om eisen te stellen aan en toezicht te houden op verbonden partijen. De aankomende Corporate Sustainability Due Diligence (CSDD)-verordening zal daar nog een schepje bovenop doen. Op grond van de CSDD zijn bepaalde (grote) ondernemingen verplicht om de negatieve effecten op het gebied van mensenrechten en milieu in hun keten van activiteiten te identificeren en aan te pakken.’

Een ander voorbeeld is de Europese Digital Operational Resilience Act (DORA). DORA heeft tot doel om risico’s op het gebied van cybercrime in de gehele EU steviger te verkleinen. Digitale operationele weerbaarheid speelt hierbij een sleutelrol. In de DORA is dan ook opgenomen dat Third Party Risk Management integraal onderdeel moet zijn van het ICT-beleid van financiële instellingen. ‘Daarnaast zijn er nog tal van andere voorbeelden van (aankomende) wet- en regelgeving waar organisaties zich aan moeten houden. Het gaat niet enkel om voldoen aan wet- en regelgeving. De samenleving eist steeds nadrukkelijker een eigen moreel kompas van organisaties. Omdat de maatschappij een hogere standaard verlangt, kunnen ook organisaties die juridisch gezien voldoen aan wet- en regelgeving een behoorlijke deuk in hun reputatie oplopen.’

Jeroen van Schajik, Partner IT Risk Assurance bij BDO, voegt daaraan toe dat organisaties in bepaalde sectoren ook te maken gaan krijgen met eisen of wetgeving van toezichthouders. ‘Zo heeft De Nederlandsche Bank gedetailleerde eisen gesteld aan banken en verzekeraars aan uitbesteding en beheersing door de instelling zelf.’

Welke risico's loopt mijn organisatie?

Van Schajik en Jansen benadrukken dat veel organisaties met Third Party Risk Management te maken zullen krijgen als er iets mis is gegaan. In het bijzonder als dit uw organisatie raakt in primaire processen loopt u een continuïteitsrisico. ‘Wanneer de bedrijfsvoering sterk afhankelijk is van bijvoorbeeld een IT-leverancier, kunt u de operatie niet meer voortzetten als deze leverancier uitvalt’, aldus Van Schajik. Er kan ook sprake zijn van achterblijvende performance. Als de levertijden van partijen uit de keten te hoog oplopen, krijgt u een probleem bij het produceren van producten. Dan is er nog het risico op reputatieschade. Wanneer uw leveranciers fouten maken of moreel verwerpelijk handelen, straalt dit af op uw organisatie. Zo kan uw eigen reputatie geschaad worden. ‘Wij zien dat dit risico in de praktijk nog vaak wordt onderschat’, zegt Jansen.

In secundaire processen, denk aan de administratieve keten, kunnen ook zaken fout gaan. ‘Software voor salarisadministraties hoort bij veel organisaties niet tot het primaire proces, maar het is wel heel erg vervelend als deze uitvalt en salarissen niet worden uitbetaald’, legt Van Schajik uit. Ook het risico op een datalek bij een van uw leveranciers valt in die categorie. Van Schajik: ‘Weet u bijvoorbeeld wat de gevolgen van zo'n datalek voor uw gevoelige klant- en personeelsgegevens en daarmee de reputatie van uw eigen organisatie zijn?’

Aan de slag met Third Party Risk Management

Wanneer u samenwerkt met derde partijen, krijgt u dus te maken met bepaalde risico's. Wilt u werk maken van Third Party Risk Management, en bent u benieuwd waar u het beste kunt beginnen? Onderstaand een aantal belangrijke bouwstenen.

Een gedegen risicoanalyse

Effectief Third Party Risk Management begint met een grondige risicoanalyse van de eigen organisatie. U onderzoekt wat de belangrijkste risico's voor uw organisatie zijn. Vervolgens kijkt u naar de derde partijen in uw waardeketen en welke partijen een grote invloed hebben op het eventueel voordoen van de geïdentificeerde risico's. Zo kunnen relevante partijen worden gescreend, of kunnen er (self-) assessments worden uitgevoerd.

Bij BDO bekijken we welke mogelijke oorzaken bij externe partijen kunnen leiden tot risico's voor uw organisatie. Ook kunnen eventuele assurancerapporten worden opgevraagd om zekerheid te krijgen over de beheersing van processen bij de derde partij. Vervolgens moet worden bepaald welke maatregelen getroffen kunnen worden om de geïdentificeerde risico's te mitigeren. Dit kan uw organisatie via contracten met partijen regelen, maar ook door het verzekeren van risico's of in sommige gevallen door afscheid te nemen van een partij of alternatieve partijen te contracteren.

Third party monitoring en adequaat reageren op risico's

Periodiek dient u te (her)beoordelen of de beheersing adequaat is en blijft en of het risicoprofiel verandert. Regelmatige beoordelingen, bijvoorbeeld jaarlijks of tweejaarlijks, zijn nodig om wijzigingen te identificeren. In de monitoring kunt u worden geholpen door dashboards of (periodieke) rapportages. Ook adequaat reageren op de geconstateerde risico's is cruciaal. Hierbij speelt communicatie en leiderschap richting de partijen in uw keten een belangrijke rol. Zorg ervoor dat u kunt anticiperen op situaties die zich in de toekomst zouden kunnen voordoen. Het hebben van een exitstrategie als er onverhoopt plotseling afscheid zou moeten worden genomen van een kritische leverancier, bijvoorbeeld.

Tooling voor Third Party Risk Management

BDO kan organisaties ondersteunen bij elk van deze processen. Third Party Risk Management-applicaties kunnen een belangrijke rol spelen bij het ondersteunen van het proces. Het kan bijvoorbeeld helpen bij het creëren van overzicht in uw ecosystemen of keten. Daarnaast kan het praktische functionaliteiten bieden zoals het automatisch versturen van selfassessments op vooraf bepaalde momenten of ondersteunen bij monitoring, zoals het controleren van het handelsregister en het scannen van "slechtnieuwsberichten". Daarnaast helpt tooling bij het vastleggen en presenteren van gegevens, waardoor het proces efficiënter wordt.

Effectief Third Party Risk Management vereist een combinatie van strategie, tools en samenwerking met betrouwbare partners. Door de juiste maatregelen te nemen, kan uw organisatie de risico's beheersen en uw regie op de samenwerking optimaliseren.

Third Party Risk Management voor dienstenleveranciers

Zijn uw klanten voor hun bedrijfsvoering afhankelijk van de beschikbaarheid en kwaliteit van de diensten die u als leverancier levert? Dan is het belangrijk om het perspectief van uw klanten te kennen. Dankzij Third Party Risk Management voor dienstenleveranciers weet u aan welke wet- en regelgeving uw klanten moeten voldoen en welke risico's uw klanten lopen als de dienstverlening niet gaat zoals beoogd.

'Klanten stellen steeds hogere eisen aan de kwaliteit, beschikbaarheid en veiligheid van geleverde diensten. Dit resulteert vaak in een overvloed aan vragenlijsten en verzoeken om rapportages', legt Van Schajik uit. 'Klanten vragen dan bijvoorbeeld om ISO-certificering, ISAE- of SOC-assurancerapporten. Als er voor elke klant een andere vragenlijst of auditverzoek komt, verstoort dat het werkproces aanzienlijk.'

Als dienstenleverancier kunt u zelf een audit laten doen en op basis daarvan een voor alle klanten bruikbaar assurancerapport op (laten) stellen. Wanneer een (nieuwe) klant u vraagt om vragenlijsten in te vullen of een auditor wenst te sturen, levert u een dergelijk rapport. Dat scheelt veel tijd en kweekt vertrouwen.

Het juiste assurancerapport

Bij het opstellen van een dergelijk rapport, bepaalt u eerst wie de beoogde lezer van het rapport is. Is het een externe accountant of iemand van de security-afdeling? 'Het is van groot belang om inzicht te hebben in de lezers van deze rapportages', stelt Van Schajik. 'Elke lezer heeft zijn eigen specifieke behoeften en doelstelling.'

Er zijn verschillende typen rapportages gebruikelijk om te rapporteren over geleverde diensten, zoals SOC 1 of ISAE 3402 en SOC 2. SOC 1- of ISAE 3402-rapporten richten zich voornamelijk op doelstellingen die belangrijk zijn voor controlerende accountants van klanten, zoals de salarisverwerking. SOC 2-rapporten gaan meer in op informatiebeveiliging en cybersecurity en zijn daarom zeer relevant voor IT-leveranciers of IT-serviceorganisaties.

Third Party Risk Management: the next step

De bouwstenen uit deze whitepaper kunnen u helpen om een robuust Third Party Risk Management op te zetten. Houd er echter rekening mee dat dit thema nooit afgerond is. Third Party Risk Management is een continu proces waarbij de risico-beheersing van uw eigen organisatie en die van uw partners regelmatig onder de loep wordt genomen.

Hoe zorgvuldig en goed geïmplementeerd uw Third Party Risk Management ook is, elke organisatie krijgt te maken met onvoorziene omstandigheden. Denk bijvoorbeeld aan een cyberaanval, of aan een samenwerkende partij die niet kan leveren door een plotseling oplaaiend conflict, zoals de invasie van Oekraïne.

In de wereld van vandaag moeten organisaties proactief zijn en zich voortdurend kunnen aanpassen aan veranderende omstandigheden. Houd leveranciers scherp en blijf als leverancier zelf in gesprek met klanten over risico's én maatregelen in de keten. Zo kan de impact op de bedrijfsvoering bij incidenten aanzienlijk beperkt worden.

Investeer in Third Party Risk Management

Het effectief beheren van de risico's die voortkomen uit de samenwerking met derde partijen, is essentieel om de continuïteit, reputatie en veiligheid van een organisatie te waarborgen. Door actief Third Party Risk Management toe te passen, kunt u de risico's beperken. BDO kan uw organisatie ondersteunen met advies en operationele ondersteuning op het gebied van Third Party Risk Management. Daarnaast verrichten wij onderzoeken die resulteren in SOC 1/ISAE 3402- en SOC 2-rapportages voor serviceorganisaties.

Benieuwd naar de mogelijkheden? Vraag dan een vrijblijvend gesprek aan.

Meer informatie

Neem voor meer informatie vrijblijvend contact op met één van onze adviseurs.

Noël Jansen
Senior Manager Internal Audit, Risk & Compliance
E noel.jansen@bdo.nl
T 06 - 24 73 10 39

Jeroen van Schajik
Partner IT Risk Assurance
E jeroen.van.schajik@bdo.nl
T 06 - 14 23 07 97

bdo.nl

Deze publicatie is zorgvuldig voorbereid en tot stand gekomen, maar is in algemene bewoordingen gesteld en bevat alleen informatie van algemene aard. Deze publicatie bevat geen advies voor concrete situaties, zodat uitdrukkelijk wordt afgeraden om zonder advies van een deskundige op basis van de informatie in deze publicatie te handelen, na te laten of besluiten te nemen. Voor het verkrijgen van een advies dat is toegesneden op uw concrete situatie, kunt u zich wenden tot BDO Advisory B.V. of een van haar adviseurs. BDO Advisory B.V., de met haar gelieerde partijen en haar adviseurs aanvaarden geen aansprakelijkheid voor schade die het gevolg is van handelen, nalaten of het nemen van besluiten op basis van de informatie in deze publicatie.

BDO is een op naam van Stichting BDO te Amsterdam geregistreerd merk.

In deze publicatie wordt **BDO** gebruikt ter aanduiding van de organisatie die onder de merknaam 'BDO' actief is op het gebied van de professionele dienstverlening (accountancy, belastingadvies en advisory).

BDO Advisory B.V. is lid van BDO International Ltd, een rechtspersoon naar Engels recht met beperkte aansprakelijkheid, en maakt deel uit van het wereldwijde netwerk van juridisch zelfstandige organisaties die onder de naam 'BDO' optreden.

BDO is de merknaam die wordt gebruikt ter aanduiding van het BDO-netwerk en van elk van de BDO Member Firms.

07/2023 – AD2329