10 steg för att implementera ett hållbart riskhanteringsprogram för tredje part

1. Tydligt definiera och beskriva omfattningen av organisationens risktolerans.

Titta på branschen och de olika jurisdiktioner där ditt företag är verksamt i samband med företagets egen risktoleranströskel. Finns det särskilda risker med att bedriva verksamhet i en viss ekonomisk sektor, ett visst land eller en viss region? Har företaget noggrant identifierat dessa särskilda risker under riskbedömningsprocessen? Vilka mildrande åtgärder eller andra försiktighetsåtgärder har företaget kommit överens om att vidta för att hantera dessa risker?

2. Utarbeta och använd en policy för riskhantering för tredje part (TPRM) som fastställer den procedur som organisationen kan använda för att på rätt sätt granska, anlita och vid behov koppla bort leverantörer.

Organisationen bör anta en specifik policy som fungerar som grund för riskhantering av tredje part i hela organisationen och dess olika verksamhetsenheter. Policyn bör i detalj beskriva **processen som organisationen använder för *att identifiera, granska, välja ut, utvärdera* och *övervaka* potentiella leverantörer.**

Helst bör TPRM-policyn också innehålla *en uppförandekod eller etiska riktlinjer för affärspartners (kod).* På en mycket hög nivå bör koden beskriva organisationens förväntningar på acceptabelt beteende. Alla tredje parter som organisationen ingår avtal med är skyldiga att följa koden. Brott mot koden ska utgöra omedelbar grund för uppsägning av avtalet.

TPRM-policyn bör också tydligt fastställa *roller och ansvarsområden*. Detta inkluderar att identifiera vilka affärsenheter eller individer som ansvarar för genomförandet av särskilda policykomponenter: val av leverantör, inledande screening av avvisade parter, avtalsförhandlingar, revision/inspektion, förnyelse och uppsägning osv.

3. Tilldela en riskklassificering till varje tredje part med hjälp av en lämplig skala

En TPRM-skala bör tydligt dela in risker i tre primära kategorier: *hög risk, medelhög risk och låg risk*. Den bör förlita sig på objektiva kriterier för att hjälpa efterlevnadsfunktionen att på ett överskådligt sätt identifiera de mest kritiska riskerna som organisationen står inför.

Resurser från tredje part som Transparens Internationals Corruptions Perceptions Index (CPI) kan effektivisera denna process med avseende på särskilda problemområden. Sedan beräknas en totalpoäng för varje leverantör och den bör tar hänsyn till den fullständiga översikten över risker som organisationen identifierar som relevanta. Diskretion är avgörande för att säkerställa att endast en liten procentandel av riskerna faktiskt klassificeras som hög risk. Det gör det möjligt för företaget att mer effektivt tilldela resurser för riskreducerande åtgärder.

4. Kartlägg i möjligaste mån hela företagets leveranskedja för att maximera insynen i hela produktens/tjänstens livscykel och visuellt identifiera var de största riskerna finns.

Det här kanske verkar vara en långtråkig uppgift men ett samarbete med kunniga interna intressenter är en oumbärlig del av modern TPRM-praxis för att förstå tredje parts bidrag till företagets produkt- och tjänstelivscykel. Detta gäller framför allt när företaget kan vara föremål för regelverk som EU:s Corporate Sustainability Due Diligence Directive (CSDDD), den tyska lagstiftningen för leverantörskedjor eller Uyghur Forced Labor Prevention Act.

I varje enskilt fall krävs kartläggning av leveranskedjan för att identifiera bristande efterlevnad av föreskrivna standarder för miljön och/eller mänskliga rättigheter. Ur ett företagsriskperspektiv kan kartläggning också hjälpa organisationen att konkret identifiera och ta itu med operativa sårbarheter som kan uppstå till följd av samarbete med en tredje part.

5. Välj ut och implementera ett automatiserat TPRM-system för användning i samband med administrationen av TPRM-programmet.

För alla organisationer kräver hanteringen av tredjepartsrelationer användning av en **automatiserad TPRM-lösning** som konsoliderar TPRM-administrationsfunktioner till en enda plattform. Det räcker inte att bara lita på manuella processer och det gör det svårt att uppfylla nuvarande regulatoriska förväntningar. Det lägger också stor vikt vid organisationens förmåga att utföra due diligence, hantera utbildning, utföra revisioner, utfärda efterlevnadscertifieringar och anpassa företags- och efterlevnadsrisker effektivt.

Detta kräver användning av en automatiserad lösning som NAVEX One informationssystem för styrning, risk och efterlevnad (GRC-IS) som gör det möjligt för efterlevnadsfunktionen att integrera, granska, prioritera och övervaka leverantörsriskinformation i realtid.

6. Granska alla standardavtalsformer som vanligtvis används med organisationens leverantörer för att inkludera viktiga efterlevnadsavtal, utfästelser och garantier.

En viktig del av en effektiv TPRM-lösning är att definiera tydliga avtalsstandarder i samband med eventuella slutgiltiga avtal som ingåtts mellan den primära avtalsorganisationen och tredje part.

Utöver att vara bunden av organisationens uppförandekod bör avtalet i sig kräva att tredje part med rimligt varsel tillåter granskning och inspektion av deras bokföring och register. Avtalet bör också innehålla bestämmelser om hävningsrätt i händelse av att tredje part inte följer koden eller någon materiell bestämmelse i det slutgiltiga avtalet som kräver att särskilda lagar eller förordningar följs.

7. Överväg att erbjuda utbildning till tredje parter inom områden som är av stor betydelse.

Att erbjuda utbildning till tredje part är ett praktiskt sätt att betona att den primära upphandlande organisationen tar sina efterlevnadsskyldigheter på allvar. För detta ändamål kan organisationen erbjuda utbildning till tredje part inom de områden med högst risk som identifierats under tredjepartsscreeningen och introduktionsprocessen. I ett land med lägre CPI-poäng än genomsnittet (vilket tyder på systemisk korruption) skulle till exempel målinriktad utbildning i form av exponering för principer mot mutor och korruption (ABAC) förstärka budskapet att företaget inte har någon tolerans för olagliga försök att påverka tredje part genom att betala mutor eller ge gåvor.

8. Se till att tredje part kan rapportera överträdelser av organisationens kod eller andra etiska och juridiska överträdelser.

Där det är möjligt bör företag överväga att utnyttja sitt befintliga system för incidentrapportering för att tillåta externa parter, inklusive anställda hos affärspartners, att rapportera frågor som innebär brott mot koden eller andra etiska och/eller juridiska överträdelser av företagets anställda, entreprenörer och agenter. Denna rapporteringsförmåga krävs i allt högre grad av regelverk som fokuserar på transparens i leveranskedjan.

9. Försök att i största möjliga mån förhindra fragmentering av information från tredje part.

Den kanske största utmaningen för dagens företag är kombinera och hantera olika informationsbarriärer. Det allra mest effektiva sättet är att lagra all information som rör en viss tredje part på en enda plats som är allmänt tillgänglig för viktiga intressenter i organisationen. Tillgång till en komplett fil som innehåller leverantörsinformation är avgörande för att upprätthålla en tillförlitlig riskprofil.

10. Regelbundet granska och uppdatera TPRM-policyer och -procedurer mot bakgrund av regelverksutveckling och insikter.

Det säger sig självt att organisationen regelbundet bör se över sina egna policyer och rutiner i förhållande till TPRM för att göra förbättringar baserat på olika insikter och på kommande regulatoriska förväntningar. Maximera TPRM-programmets effektivitet genom att se över policyer och procedurer minst en gång om året för att fastställa om några ändringar behövs.