IT RISK ASSURANCE

WHITEPAPER

Interne beheersing in de techsector

Waar moet u op letten?

Inhoud

Inleiding

De techsector ondergaat voortdurende veranderingen, gedreven door ontwikkelingen zoals kunstmatige intelligentie (AI) en cloud computing. Deze vooruitgang brengt zowel kansen als risico's met zich mee.

Toezichthouders erkennen deze nieuwe risico's en leggen steeds meer nadruk op naleving van wet- en regelgeving, zoals de NIS2 (Network and Information Security)-richtlijn en DORA (Digital Operational Resilience Act). Organisaties voelen de urgentie om zich aan te passen aan deze veranderende omgeving en gaan aan de slag met relevante onderwerpen, zoals informatiebeveiliging en incidentenbeheer.

Hoewel het belang van deze onderwerpen wordt erkend, is het inspelen op compliance-eisen vaak een reactieve maatregel. Het betreft een pleister die het probleem tijdelijk oplost. In deze whitepaper richten we ons op een proactieve benadering: interne beheersing. We beschrijven hoe interne beheersing kan bijdragen aan de groeifase van uw organisatie. Door risico's bij de wortels aan te pakken en in te spelen op wat uw organisatie zelf belangrijk vindt, kunt u de relevante interne en externe omgeving beheersen nog voordat wetgeving dit vereist. Zo kunt u inspelen op de behoeften van uw organisatie en klanten, en zelf bepalen wanneer actie nodig is.

Interne beheersing: een overzicht

Interne beheersing is de ruggengraat van iedere organisatie, waarbij een positieve cultuur, effectieve beheersingsmaatregelen en aantoonbaarheid van groot belang zijn. Voor techbedrijven betekent dit dat ze niet alleen verantwoordelijk zijn voor hun producten en diensten, maar ook voor de beheersingsomgeving ervan.

Interne beheersing is dus een cruciaal aspect van bedrijfsvoering, lees hier meer over de uitdagingen die dit met zich meebrengt.

1. **Interne omgeving**
   De interne omgeving omvat de organisatiecultuur, structuur en beleidskaders. Een positieve cultuur die gericht is op waardecreatie, integriteit en verantwoordelijkheid is essentieel voor effectieve interne beheersing.

2. **Doelstellingen en risico's**
   Interne beheersing draait om het identificeren van gewenste doelstellingen en de risico's die deze doelstellingen bedreigen. Door deze risico's te mitigeren, kunnen organisaties hun doelen effectiever bereiken.

3. **Beheersingsmaatregelen**
   Organisaties stellen beheersingsmaatregelen op om risico's te beheersen. Dit omvat procedures, beleid, processen en technologische oplossingen. Denk aan toegangscontroles, beveiligingsprotocollen en monitoringssystemen.

4. **Communicatie en monitoring**
   Organisaties moeten relevante ontwikkelingen, resultaten en beslissingen communiceren zodat betrokkenen hierop kunnen acteren. Daarnaast is het monitoren van de effectiviteit van beheersingsmaatregelen van groot belang.

Traditioneel waren techbedrijven alleen verantwoordelijk voor de ontwikkeling en implementatie van hun producten en diensten in het IT-landschap van klanten. Met de opkomst van cloud computing zijn verantwoordelijkheden uitgebreid en zijn techbedrijven zelf verantwoordelijk voor de beheersings-omgeving van hun producten, waaronder de beveiliging en beschikbaarheid. Deze verantwoordelijkheid, ook wel keten-verantwoordelijkheid genoemd, stelt nieuwe eisen aan tech-bedrijven op het gebied van aantoonbaarheid.

Interne beheersing wordt in de praktijk geformaliseerd door de implementatie van een risicobeheersingsraamwerk met relevante doelstellingen, risico's en beheersingsmaatregelen. Dit raamwerk wordt vervolgens geïmplementeerd, waarbij de effectiviteit door (externe) auditors wordt beoordeeld om aan te tonen dat aan klantbehoeften en wettelijke vereisten wordt voldaan.

Door dit beheersingsraamwerk in de praktijk te implementeren en vervolgens te laten auditen, toont het techbedrijf aan dat hij in staat is om te voldoen aan zijn eigen ambities, klantwensen en/of relevante wetgeving.

Kritieke succesfactoren

Om interne beheersing succesvol te implementeren, dient rekening gehouden te worden met de volgende succesfactoren:

1. **Interne betrokkenheid**
   De implementatie van interne beheersing (raamwerken) betreft een uitdagende klus. Om (snel) vooruitgang te boeken kan externe kennis worden ingehuurd, bijvoorbeeld als sparringpartner, om structuur aan te brengen of simpelweg om ervaringen te delen. Uiteindelijk moeten beheersingsmaatregelen echter worden uitgevoerd door de medewerkers van de organisatie. Om ervoor te zorgen dat maatregelen in de praktijk uitvoerbaar zijn en passen bij de bedrijfscultuur is betrokkenheid van interne medewerkers bij de totstandkoming van beheersingsmaatregelen van essentieel belang.

2. **Eigen ambitie als basis**
   Betrokkenheid vanuit de leiding van de organisatie is essentieel. Zij bepalen de ambitie op het gebied van interne beheersing. Het middenmanagement en uitvoerende organisatie vertaalt de ambitie naar concrete actiepunten. Hoewel bij de totstandkoming van interne beheersing rekening moet worden gehouden met klantwensen en complianceverplichtingen, blijft de interne ambitie de leidraad.

3. **Interne beheersing is dynamisch**
   Interne beheersing wordt vaak ten onrechte als statisch beschouwd. In werkelijkheid is het een voortdurend proces dat zich aanpast aan veranderende omstandigheden, zoals interne ambities, klantbehoeften en wetgeving. Het is dan ook belangrijk dat de effectiviteit van interne beheersingsraamwerken worden gemonitord, risicoanalyses worden herzien en risicobeheersingsraamwerken worden geüpdatet waar nodig.

4. **Groei en complexiteit**
   Techbedrijven groeien vaak snel, gestimuleerd door bijvoorbeeld nieuwe technologie, klantgerichtheid en efficiëntie. Deze snelle groei kan uitdagend zijn voor de interne beheersing, omdat risico's veranderen en de complexiteit van de organisatie toeneemt. Wanneer de interne beheersing niet met dezelfde snelheid meegroeit, kan er na verloop van tijd een 'GAP' ontstaan. Indien er een urgent vraagstuk ontstaat dat hoort bij de (nieuwe) omvang van de organisatie, bijvoorbeeld voldoen aan wet- en regelgeving, moet er een enorme inhaalslag gemaakt worden. Om dit te voorkomen is het essentieel dat de organisatie tijdig start met beheersingsactiviteiten die passen bij de fase van de organisatie.

5. **Uniformiteit en kennisdeling**
   Bij grotere organisaties kunnen verschillende afdelingen een andere benadering van interne beheersing hanteren. Dit kan leiden tot gemiste efficiëntievoordelen. Interne afstemming, het gebruik van de juiste tooling en kennisdeling is cruciaal om interne beheersing organisatiebreed te waarborgen.

Interne beheersing is een strategisch instrument om risico's te minimaliseren, klantvertrouwen te behouden en duurzaam succes te waarborgen. Indien u rekening houdt met de hiervoor genoemde punten kan interne beheersing een kritieke succesfactor zijn voor uw onderneming.

Interne beheersing per groeifase

In de afgelopen decennia hebben techbedrijven, al dan niet gesteund door externe investeerders of overnames, indrukwekkende groei weten te realiseren. Tijdens elke groeifase verandert zowel de interne als de externe omgeving, wat nieuwe kansen maar ook risico's met zich meebrengt.

Om kansen te benutten en risico's te beheersen, moet interne beheersing meegroeien met de organisatie, afhankelijk van het type en de fase van de organisatie. Het herkennen van welke vorm van interne beheersing past bij het type organisatie, vereist een diepgaand begrip van de bedrijfscultuur, de groeifase en de specifieke uitdagingen waarmee de organisatie te maken heeft.

In deze whitepaper onderscheiden wij de volgende vijf groeifases die een techbedrijf kan doorlopen.

Vijf groeifases van een techleverancier				
Start-up	Rollercoaster	Decentralisatie	Scale-up	Flow
Groei door pionieren.	Focus op formeel leiderschap en (interne en financiële) beheersing.	Focus op het delegeren van verantwoordelijkheden en budgettering.	Focus op groei door een profit center-benadering en het aantrekken van competenties.	Focus op stabiliteit, schaalbaarheid en marktbewerking.

In deze whitepaper beschrijven wij de belangrijkste aandachtspunten op het gebied van interne beheersing per groeifase.

Start-up-fase

De start-up-fase bestaat vooral uit pionieren en het opbouwen van bestaansrecht. Organisaties die zich in deze fase bevinden worden vaak gekenmerkt door vakmanschap, flexibiliteit, creativiteit en een informeel karakter. Interne beheersing bestaat in deze fase voornamelijk uit het benoemen van verantwoordelijkheden en het creëren van risicobewustzijn.

Rollercoaster-fase

Na de start-up-fase komen organisaties in een zogeheten rollercoaster terecht vanwege de snelle en vaak chaotische groei die ze doormaken. Door behoefte aan sturing ontstaat formeel leiderschap en de regulering van kwaliteit, kosten en baten. Interne beheersing is essentieel om bedrijfsrisico's te mitigeren en kansen te benutten.

Als onderdeel van de groei, krijgen organisaties voor het eerst te maken met compliance-eisen vanuit klanten. In de praktijk wordt vaak ad hoc gereageerd op verzoeken, bijvoorbeeld om te voldoen aan ISO 27001, zonder dat er sprake is van gestructureerd risicomanagement. Ook wetgeving zoals GDPR (General Data Protection Regulation), DORA en NIS2 stimuleert techbedrijven om hun klanten inzicht te geven in hoe de IT-omgeving wordt beheerd en hoe belangrijke onderwerpen zoals veiligheid en data-integriteit worden gewaarborgd.

Hoewel het voldoen aan compliance-eisen een commitment vereist van techbedrijven als leverancier, kan dit ook commerciële kansen bieden. Door middel van zogenaamde assuranceonderzoeken, uitgevoerd door onafhankelijke auditors, kunnen techbedrijven hun klanten inzicht en zekerheid bieden over hoe hun klantomgevingen worden beheerd. Bekende voorbeelden van dergelijke assurancerapportages zijn SOC 1 (ISAE 3402), SOC 2 (ISAE 3000) en SOC 3.

Om te komen tot een assurancerapportage dient een organisatie een eigenrisicocontroleraamwerk te ontwerpen. De eerste stap in de totstandkoming van dit raamwerk is het identificeren van relevante bedrijfsdoelstellingen.

Vervolgens worden risicoanalyses uitgevoerd die identificeren welke risico's bedreigen dat doelstellingen worden behaald. Op basis van deze analyses en specifieke klantwensen wordt de structuur van het risicocontroleraamwerk ontworpen. De laatste stap is het implementeren van beheersingsmaatregelen die de geïdentificeerde risico's mitigeren. Deze maatregelen kunnen variëren van het gebruik van automatische monitoringssystemen en technische configuraties die gewenst gedrag afdwingen, tot automatische rapportagefuncties en handmatige controles op de naleving van procedures.

Door proactief een eigen raamwerk en rapportage op te stellen, voorkomt de organisatie dat zij ad hoc moet inspelen op klantverzoeken en wordt een continu risicomanagementproces gewaarborgd. Het is belangrijk dat organisaties tijdens dit proces trouw blijven aan hun eigen identiteit. Wij adviseren organisaties om hun eigen 'kroonjuwelen' te definiëren, goed te luisteren naar de wensen van hun klanten en vooral hun intrinsieke motivatie te concretiseren. Beheersingsmaatregelen moeten niet worden gezien als een 'verplicht nummer', maar als een zelfgekozen activiteit die waarde toevoegt aan de organisatie. Cruciaal is dat de beheersingsmaatregelen de risico's afdekken van bestaande processen en cultuur van de organisatie.

De activiteiten die behoren bij de rollercoaster-fase, zijn ook relevant voor (bijvoorbeeld) scale-ups die een nieuw product of nieuwe dienstverlening introduceren waarbij nieuwe bedrijfsprocessen en/of structuren worden geïmplementeerd.

Decentralisatie-fase

Het risico bestaat dat, naarmate organisaties doorgroeien, formalisatie kan leiden tot een toename van hiërarchische lijnen en trage besluitvorming. Om dit te voorkomen, decentraliseren organisaties waarbij flexibiliteit en snelle besluitvorming wordt gewaarborgd.

In deze fase wordt een start gemaakt met product-markt-combinaties, waarbij managers duidelijke taken en verantwoordelijkheden krijgen om de product-marktcombinatie naar successen te leiden. Naarmate het aantal medewerkers, de complexiteit van de organisatie en de noodzaak om schaalbaar te worden toenemen, ontstaat de noodzaak tot standaardisatie en documentatie van bedrijfsprocessen.

Deze wens tot standaardisatie wordt versterkt indien teams actief zijn in verschillende landen.

Om te borgen dat teams conform organisatierichtlijnen werken, worden richtlijnen geformaliseerd naar beleidsdocumenten welke centraal worden gecoördineerd. Denk hierbij aan beleidslijnen, procedures en werkinstructies. Om het management tijdig te informeren worden formele rapportagelijnen ingericht.

Hoewel deze fase voornamelijk intern gericht is, kan de hernieuwde organisatiestructuur leiden tot nieuwe risico's en/of kansen. Het is in deze fase belangrijk om risicoanalyses te updaten en risicocontroleraamwerken aan te vullen waar nodig.

Scale-up-fase

In de scale-up-fase worden profit centers ingericht om de steeds groter wordende product-marktcombinaties te beheren. Deze profit centers zijn verantwoordelijk voor zowel de kosten als de opbrengsten die ze genereren. Omdat elk profit center actief is in een andere markt, ontstaan er marktspecifieke klantwensen en compliancedruk. Dit brengt ook het risico op reputatieschade met zich mee als een van de profit centers niet de gewenste kwaliteit levert.

Door specialisatie in een specifieke markt kan de scale-up grotere klanten bedienen en belangrijker worden voor bestaande klanten, wat leidt tot nieuwe eisen aan kwaliteit en zekerheid op het gebied van risicomanagement. Waar in eerdere fases deze eisen voornamelijk voortkwamen uit algemene compliancevragen (denk aan ISO 27001), ontstaat in de scale-up-fase de wens tot verantwoording richting externe en/of interne toezichthouders. Dit kan zich uiten in specifieke vragen over informatiebeveiliging, maar bijvoorbeeld ook de wijze van beschikbaarheidsmanagement, continuïteitsbeheer, data-integriteit of privacy.

Hierna zijn drie belangrijke ontwikkelingen beschreven, waar organisaties in de scale-up-fase mee te maken krijgen. Wij adviseren organisaties om te overwegen om deze ontwikkelingen te onderzoeken en te bepalen in hoeverre zij moeten worden vertaald naar wijzigingen in de wijze van interne beheersing:

1. **Dynamiek in vereisten en risico's**
   De organisatie moet een grondig begrip hebben van zowel interne als externe vereisten en de bijbehorende risico's. Eerder is al benoemd dat externe vereisten toenemen naarmate de organisatie belangrijker wordt voor klanten. Nieuwe interne vereisten ontstaan door de complexere interne omgeving welke nodig is om aan verhoogde klantwensen te voldoen, zoals het gebruik van nieuwe technologieën of de implementatie van een Security Operations Center (SOC).

2. **Ketenverantwoordelijkheid**
   Nieuwe wetgeving, zoals DORA en NIS2, verwacht dat techbedrijven, vooral die van financiële of kritieke instellingen, in zekere mate voldoen aan de eisen van de wetgeving waaraan haar klanten zelf moet voldoen. Dit wordt ook wel ketenverantwoordelijkheid genoemd. Dit betekent dat techbedrijven inzicht dienen te hebben in de compliancevereisten in zowel de eigen IT-markt als van de markten waarin haar klanten actief zijn. Met de opkomst van bijvoorbeeld de AI Act en Digital Services Act, zal de ketenverantwoordelijkheid in de toekomst toenemen.

3. **Overlap en efficiëntie**
   Elk profit center moet voldoen aan diverse compliancevereisten. Door een gedetailleerde mapping van deze vereisten en risico's te maken, kan de organisatie vaststellen waar overlap bestaat. Dit is vooral relevant op het gebied van informatiebeveiliging, waar klanten eisen dat IT-leveranciers voldoen aan meerdere raamwerken zoals ISO 27001, SOC 2 en de DNB Good Practice Informatiebeveiliging. Deze raamwerken hebben veel vergelijkbare eisen. Door gebruik te maken van slimme oplossingen, zoals geïntegreerde vulnerability scanning, kunnen organisaties efficiënt aan alle drie de raamwerken voldoen. Het integreren van deze raamwerken in een SOC 2+ raamwerk maakt het mogelijk om de onderlinge samenhang eenvoudig aan klanten te tonen. Dit vermindert de auditdruk aanzienlijk in vergelijking met het afzonderlijk voldoen aan elk raamwerk.

Flow-fase

In deze fase hebben techbedrijven een succesvolle inkomstenstroom gegenereerd, heeft het als merk een sterke marktpositie, is het in staat om op grotere schaal te opereren zonder dat dit ten koste gaat van kwaliteit of efficiency en is de governance van de organisatie goed gedefinieerd. Deze diversiteit brengt uitdagingen met zich mee, zoals de behoefte aan branchekennis, uiteenlopende assuranceverzoeken van klanten en het voldoen aan branchespecifieke complianceeisen. Tegelijkertijd groeit de behoefte aan effectief sturen, wat hogere eisen stelt aan bijvoorbeeld datamanagement.

De flow-fase is dan ook een cruciale periode waarin organisaties zich moeten focussen op multicompliance, integratie (van verschillende werkwijzen) en schaalvoordelen (door o.a. efficiency). We onderscheiden vier aspecten die organisaties helpen om succesvol te zijn in de flow-fase.

1. **Standaardisatie en kwaliteitsborging**
   Om de toename van compliancevereisten en complexiteit beheersbaar en betaalbaar te houden, is aandacht voor standaardisatie en kwaliteitsborging essentieel. Centrale compliancefuncties zorgen voor overzicht en stellen het hogere management in staat grip te krijgen op kwaliteit en compliance.

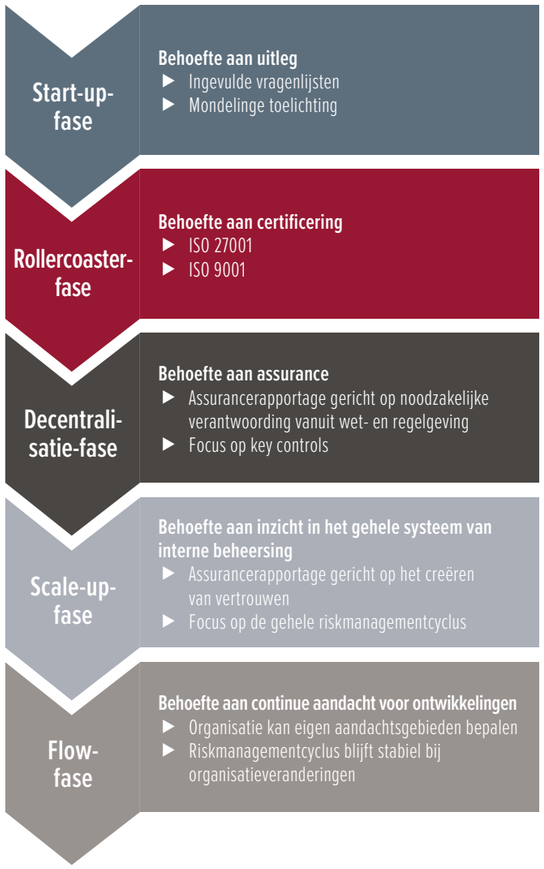
2. **Kennisdeling en draagvlak**
   Overlegstructuren en centrale organen worden opgezet om kennisdeling te stimuleren en gelijke behoeften en compliance te waarborgen. Beslissingen van centrale organen moeten echter draagvlak hebben bij de onderliggende teams om weerstand te voorkomen. Het is dan ook van essentieel belang om de business actief te betrekken bij beslissingen.

3. **Kennisbehoud**
   In een groeiende organisatie ontstaan groeipijnen op het gebied van personeelsmanagement, waaronder personeelsverloop en het feit dat niet alle medewerkers elkaar kennen. Om bij uitdiensttreding kennis te behouden en om nieuwe medewerkers te ondersteunen, is het van belang dat procedures en controleactiviteiten worden gedocumenteerd en dat medewerkers optimaal worden ondersteund bij het uitvoeren van de controleactiviteiten. Vaak maken organisaties hiervoor gebruik van GRC (Governance, Risk and Compliance)-tooling om controleactiviteiten te signaleren, documenteren en te beheren.

4. **Integrale beheersing**
   Organisaties die actief zijn in verschillende markten moeten voldoen aan diverse compliance-eisen. Hierdoor zullen vanuit verschillende afdelingen initiatieven ontstaan om de interne beheersing te verbeteren en/of aantoonbaar te maken. Interne afstemming is noodzakelijk om te voorkomen dat verschillende teams 'het wiel opnieuw uitvinden'. Door het gebruik van GRC-tooling ontstaat op hogermanagementniveau overzicht welke controleactiviteiten op welke afdeling worden uitgevoerd. Integratie van raamwerken, bijvoorbeeld via het eerder genoemde SOC 2+, maakt dat auditors efficiënter kunnen toetsen.

Veranderende klantwensen

Tijdens elke groeifase verandert de interne en externe omgeving, wat leidt tot veranderende klantwensen op het gebied van compliance. In figuur 1 hebben wij per fase een overzicht opgesteld van de meest voorkomende klantwensen.



Figuur 1: *Een overzicht van veel voorkomende klantwensen op het gebied van compliance*

Tot slot

Interne beheersing is geen luxe, maar een noodzaak voor elk techbedrijf. Het stelt u in staat om risico's te minimaliseren, compliance en werkprocessen te verbeteren, continuïteit te waarborgen en vertrouwen op te bouwen bij uw stakeholders. Wacht niet tot externe factoren u dwingen tot actie. Begin vandaag nog met het verkennen van interne beheersing en ontdek hoe het uw organisatie kan versterken.

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

Meer informatie

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

KRISTIAN MEPSCHEN
Senior Manager IT Risk Assurance
E kristian.mepschen@bdo.nl
T 06 - 42 18 38 82

JEROEN VAN SCHAJIK
Partner IT Risk Assurance
E jeroen.van.schajik@bdo.nl
T 06 - 14 23 07 97

www.bdo.nl

10/2024 – BA2445

Een andere kijk op waarde