BDO ADVISORY | RISK ADVISORY | THIRD PARTY ASSURANCE

CYBERSECURITY COMPLIANCE

DREIGINGEN ROND CYBERSECURITY NEMEN IN AANTAL EN COMPLEXITEIT TOE, DOET JOUW ORGANISATIE ER ALLES AAN OM ZICHZELF TE BESCHERMEN EN OM JE PARTNERS EN KLANTEN GERUST TE STELLEN OP HET GEBIED VAN CYBERSECURITY?

CYBERSECURITYRISICO'S STAAN BOVENAAN DE BEDRIJFSAGENDA IN 2022

Cybersecurityrisico's nemen over de hele wereld toe. Ze worden steeds complexer en treffen organisaties van elke omvang en industrie. Problemen met cybersecurity kunnen leiden tot financiële verliezen, verstoring van de bedrijfsvoering, juridische gevolgen en reputatieschade. Toch melden veel organisaties over de hele wereld dat ze nog steeds niet voorbereid zijn op dit kritieke gebied van risico's.

Twintig procent van de wereldwijd ondervraagde C-suite executives in onze **Global Risk Landscape van 2021** noemde cybercriminaliteit het risicogebied waarop ze het minst zijn voorbereid. De cijfers zijn nog zorgwekkender voor middelgrote ondernemingen: bijna de helft van de leidinggevenden in het middensegment is van mening dat cybersecurity en dataprivacyrisico's hun grootste uitdaging vormen op het gebied van IT resilience, en 34% zegt dat cyberaanvallen of inbreuken op de privacy hun grootste digitale bedreigingen zijn, volgens BDO's 2021 **Middle Market Digital Transformation Survey**.

HOE VOORBEREID IS JOUW ORGANISATIE – EN JE LEVERANCIERS – OP CYBERPROBLEMEN?

Cybersecurityrisico's zijn een cruciaal aandachtspunt voor C-suite executives en bestuursleden wereldwijd. Het is belangrijk om te onthouden dat dit risico niet alleen moet worden beheerd voor de eigen IT-infrastructuur van een bedrijf, maar ook wanneer IT-infrastructuur en -diensten worden uitbesteed - wat tegenwoordig steeds vaker gebeurt.

Het uitbesteden van (een deel van) IT - of welk kritiek bedrijfsonderdeel dan ook - brengt een extra laag risico's met zich mee. Zelfs wanneer IT of andere diensten worden uitbesteed, zijn het nog steeds de bedrijfsgegevens van jouw organisatie en jouw reputatie die op het spel staan als je leverancier te maken krijgt met een datalek of er niet in slaagt de verwachte service te leveren. Als je zelf een dienstverlenende organisatie of leverancier bent, is het van essentieel belang dat je transparantie kan bieden over de bestaande (cyber)controles, zodat je klanten gerustgesteld zijn.

> JE KAN DE PROCESSEN EN INFRASTRUCTUUR VANJE ORGANISATIE UITBESTEDEN. MAAR DE RISICO'S NIET.

HET AANTONEN VAN CYBERSECURITY COMPLIANCE

Er zijn verschillende manieren waarop je organisatie meer vertrouwen en transparantie op het gebied van cybersecurity in je supply chain kan creëren (meestal als dienstverlener of leverancier) of verkrijgen (als klant). Twee van de meest toegepaste en gevestigde normen zijn

- **ISO/IEC 27001:2013:** Beheer van informatiebeveiliging en de verwante norm ISO/IEC 27002:2022, onlangs herzien; en
- **SOC 2:** Verslag over controles bij een dienstverlenende organisatie met betrekking tot beveiliging, beschikbaarheid, verwerkingsintegriteit, vertrouwelijkheid of privacy.

Hoewel er duidelijke verschillen zijn in aanpak tussen beide normen, bereiken ze vergelijkbare doelstellingen en kunnen ze hand in hand gaan bij de ondersteuning van je Cybersecurity Compliance-traject.

BDO

FACT SHEET

SOC 2

1. Attestatieverslag van erkende accountantskantoren
2. Onderwerpen: 5 potentiële Trust Service Criteria en bijhorende illustratieve Points of Focus
3. Focus op dienstverlenende organisaties en de verleende dienst zelf
4. Belangrijkste resultaten: een uitgebreid auditverslag
5. Flexibel kader dat je toelaat je te concentreren op de relevante criteria voor vertrouwensdiensten en de geïdentificeerde controles die specifiek zijn voor jouw organisatie
6. Jaarlijkse vernieuwing van het attest

ISO27001

1. Certificering door een geaccrediteerde certificeringsinstantie
2. Onderwerpen: 7 clausules over het definiëren en onderhouden van uw ISMS (Information Security Management System) en Annex A met verwijzing naar controledoelstellingen en controles
3. Elke organisatie kan het toepassen en zich richten op het geheel of een deel (delen) van de organisatie
4. Belangrijkste resultaten: gedetailleerd ISMS en certificaat
5. Streng kader dat in detail beschrijft hoe een ISMS moet worden ontworpen en uitgevoerd. Alle controlegebieden van bijlage A moeten aan bod komen, tenzij anders vermeld in uw VvT (Verklaring van Toepasselijkheid)
6. Jaarlijkse toezichtsaudit en driejaarlijkse hercertificeringsaudit

HOE BDO KAN HELPEN

BDO gelooft sterk in de complementaire aard van beide kaders, waardoor dienstverleners of om het even welke organisatie in hun eigen tempo vooruitgang kan boeken in hun Information Security Compliance.

SOC 2 ATTESTATIE

Te beginnen met de SOC 2 Trust Services Criteria, stelt het kader je in staat om controles te definiëren en te implementeren (ook bekend als de Systeembeschrijving) die relevant zijn voor de context van je organisatie. Door de Systeembeschrijving door BDO te laten beoordelen, kan je aantonen dat je voldoet aan de belangrijkste Information Security principes en kan je in een relatief korte tijd inspelen op de beveiligingsbehoeften van interne en externe belanghebbenden.

ISO 27001 IMPLEMENTATIE

Het ontwerpen en implementeren van een ISO 27001 ISMS vergt meer tijd en middelen. Door het gebruiken van een sterke basislijn van controles uit het SOC 2-attest, kunnen wij jouw organisatie ondersteunen bij het voortbouwen op die ervaring en het formaliseren van jouw manier van werken in een reeks beleidslijnen en procedures van jouw Information Security waarin het voortdurende onderhoud van je Information Security programma in detail wordt beschreven.

SOC 2+ ISO27001 ATTESTATIE

Eens de hoekstenen van ISO 27001 geïmplementeerd zijn, kan je bestaande SOC 2-rapport worden uitgebreid tot een SOC 2+. Hierdoor kan je rapporteren over de staat van je ISO 27001-programma zonder formeel gecertificeerd te zijn door een certificatie-instelling.

ISO27001 CERTIFICATIE

Als laatste stap in je compliance proces kunnen wij je helpen bij het verkrijgen van de ISO 27001-certificering via een van onze partners als officiële certificeringsinstantie.

Neem vandaag nog contact met ons op voor een aanpak op maat over hoe je jouw organisatie op het gebied van cybersecurity kan verbeteren.

CHRISTOPHE DAEMS
Senior Manager

E-mail: christophe.daems@bdo.be
Tel.: +32 474 90 78 51

FRANCIS OOSTVOGELS
Senior Manager

E-mail: francis.oostvogels@bdo.be
Tel.: +32 474 92 08 00

NICK HUYSMANS
Advisor

E-mail: nick.huysmans@bdo.be
Tel.: +32 486 31 90 45

▶ Follow us

▶ www.bdo.be