



Factsheet

IT-compliance in de cloud



Aanleiding

Bedrijven houden zich aan – *oftewel zijn compliant met* – hun eigen beleid, relevante wet- en regelgeving en contractuele afspraken. Met name de wettelijke en contractuele verplichtingen die een bedrijf opgelegd krijgt groeien, en daarmee de kosten voor het afleggen van verantwoording aan verschillende toezichthouders.

De wettelijke verplichtingen hangen af van de bedrijfsactiviteiten. Voor alle bedrijven gelden fiscale, commerciële, statistische en privacy compliance-verplichtingen. Betreffen de bedrijfsactiviteiten bepaalde sectoren of internationale handel dan kunnen compliance-verplichtingen toenemen. De wetgever en toezichthouders geven aan wat de verplichtingen zijn. Ook contractuele afspraken kunnen compliance-verplichtingen met zich meebrengen. Zo is een verwerker van gegevens contractueel verplicht zich aan de verwerkingsverantwoordelijke te verantwoorden voor het beschermen van persoonsgegevens.

De verplichtingen nemen niet toe als het bedrijf (ten dele) overstapt naar IT-clouddiensten. De manier van werken verandert echter wel. De gebruikelijke cloudleveranciers zoals Microsoft, Google en Amazon onderkennen de groeiende inspanningen van bedrijven om verantwoordelijkheid te nemen – *oftewel accountable te zijn* – voor het organiseren van compliance met beleidsmatige, wettelijke en contractuele verplichtingen. De cloudleveranciers faciliteren hun klanten door effectieve beheers- en beveiligingsmaatregelen, IT-riskmanagement en compliance management ‘by design’ op te nemen in hun IT-clouddiensten. Hiermee is het mogelijk dat een bedrijf effectieve en kostenefficiënte IT-clouddiensten implementeert en beheert.

Zie de factsheet [‘IT-risk management in de cloud’](#).

Zoals gezegd is het beheren van IT-clouddiensten anders dan beheer van IT on premise. De andere werkwijze van cloud-beheer wordt versterkt door de wens van de bedrijfsleiding het organiseren van compliance integraal aan te pakken. Met een integrale aanpak bedoelen we het eenmalig implementeren en beheren van een compliance-proces, waarmee meerdere toezichthouders tevreden worden gesteld. Het organiseren van een integrale aanpak begint met het ontdebellen van normenkaders die door toezichthouders worden gebruikt. Daarnaast vraagt het om planning en uitvoering: de basis vormt de IT-compliance in de cloud.

Compliance-management

Het organiseren van compliance maakt gebruik van de systematische verzameling van het bewijs van effectieve werking van getroffen beheers- en beveiligingsmaatregelen. Het inzichtelijk maken van de verplichtingen van het bedrijf én de getroffen maatregelen van administratieve organisatie en interne controle vormen de basis van waaruit compliance management werkt.

Onderdeel van compliance management is IT-compliance management in de cloud. Veel bedrijven gebruiken MS 365 tenant voor het ondersteunen van de interne bedrijfsprocessen en Azure tenants voor het effectief organiseren van bedrijfsactiviteiten met behulp van bedrijfsprocessen. Vanuit de MS 365 en de bedrijfssystemen op Azure stelt het bedrijf de verantwoordingen voor compliance met beleidsmatige, wettelijke en contractuele verplichtingen samen. Het compliance-management is gericht op het vaststellen dat de beheers- en

beveiligingsmaatregelen adequaat en “by design” in de processen zijn opgenomen én dat de maatregelen “by default” ook effectief zijn geweest. Deze procesmatige én gegevensgerichte compliance-aanpak brengt – *in principe* – betrouwbare (volledige, juiste en tijdige) verantwoordingen voort. Uiteraard is een kritische beoordeling van het direct verantwoordelijke management en de compliance officer noodzakelijk.

De compliance officer

Bij het uitbesteden van het beheer aan IT-bureaus van IT-clouddiensten zoals MS 365 tenant en of Azure tenants is het tevens uitbesteden van compliance management aan dit soort bureaus controletechnisch ongepast. Bovendien beschikt het IT-bureau veelal niet over de kennis en ervaring om de rol van compliance officer effectief uit te voeren.

De scope en reikwijdte van de rol van de compliance officer is ruim omdat de compliance-processen betrekking hebben op beleidsmatige, wettelijke en contractuele verplichtingen. De basis voor het organiseren van compliance zijn de bedrijfsprocessen waarin beheersmaatregelen “by design” zijn opgenomen. Van de IT-compliance in de cloud maken alle processen gebruik.

Specifieke compliance-processen zijn bijvoorbeeld het vaststellen dat de bedrijfsgeheimen effectief beschermd zijn of dat de persoonsgegevens adequaat verwerkt worden. De compliance-officer zou tevens de rol van FG kunnen vervullen.

In de MS 365 tenant en Azure tenants beoordeelt de compliance officer de uitkomsten in Purview Compliance Manager en maakt de vertaalslag naar begrijpelijke handelingen voor medewerkers die passen binnen het kennis- en verandermanagement van de bedrijfsorganisatie. De compliance officer zorgt voor overzichtelijke rapportages aan het management en toezichthouders.

Toegevoegde waarde en businesscase

Compliance maakt gebruik van de uitkomsten van de werkzaamheden van riskmanagement. Het aanstellen van een compliance-officer die gebruik maakt van de compliance/ FG rol in MS 365 tenant en Azure tenants kan krachtig acteren. Het komt voor dat de bedrijfsleiding riskmanagement en compliance-management samen wenst te organiseren.

Het integraal organiseren van de verantwoordingen voor de bedrijfsleiding, toezichthouders en partners tegen acceptabele kosten biedt veel toegevoegde waarde. Niet alleen het organiseren van één compliance-aanpak voor veelvuldig gebruik is effectief en kostenefficiënt. De bedrijfsprocessen waarmee bedrijfsactiviteiten georganiseerd worden, worden tevens gestroomlijnd. Wij voeren graag met u een oriënterend gesprek over een aanpak, implementatie en beheer voor uw bedrijf.

Vertrouwensdiensten

Wij voeren in opdracht van MYOBI gesprekken met gebruikers van [het MYOBI Vertrouwensnetwerk](#) over de [Accountability Seal](#) als verantwoording voor het organiseren van compliance met de TTP Gedragscode AVG. De in deze factsheet beschreven compliance-aanpak kunnen wij voor uw organisatie specifiek maken.



Afspraak maken en contact

Wilt u meer weten? Neem dan contact op met ons via onderstaande gegevens. Of bezoek onze website: www.duthler.nl

Kantoor:

Frankenslag 137

2582 HH Den Haag

+31 (0) 70 392 22 09

info@duthler.nl

Direct contract:

drs André J. Biesheuvel RE RA RFG

a.j.biesheuvel@duthler.nl

Caroline Willemse RE AA RFG

c.willemse@duthler.nl