

ARTIKELN | 14 AUGUSTUS 2023

DE COMPLIANCESCAN: MEER GRIP OP RISICO'S

Auteurs: Mr. Carl De Wannemaeker, EMoC – Drs. Cosmo Schuurmans RA CIA

Beeld: Adobe Stock

Leestijd: 5 min



Hoe zet je de ISO-compliancienorm in om de organisatie te versterken en meer inzicht en grip op de belangrijkste compliancerisico's te geven? Om de norm meer praktisch in te kunnen zetten is deze vertaald naar een compliancescan die het huidige prestatieniveau inzichtelijk maakt, afgezet tegen de norm en het ambitieniveau. Dit is de basis voor een individueel en gericht verbeterplan. Human capital is daarbij een wezenlijke factor.

Waarom lukte het organisaties niet om compliance in te voeren, ondanks mooie raamwerken en steeds weer nieuwe top-compliance officers? Modelneurose gaat soms aan de essentie voorbij, er wordt te weinig rekening gehouden met het waarom voor alle betrokkenen, wat zijn hun doelstellingen? Een duurzame aanpak van compliancerisicobeheersing zorgt dat compliance niet in de weg zit.

Compliancemanagement ondersteunt juist organisaties hun compliancedoelstellingen sneller en veiliger te bereiken, met behoud van reputatie en waarde. Voor internal audit is dit interessante informatie om te gebruiken tijdens het uitvoeren van audits waarin compliancerisico's worden getoetst, of een audit naar het functioneren van compliance binnen een organisatie.

Regeltjes en richtlijnen alleen zorgen niet voor compliant gedrag, daar zijn ook soft controls voor nodig

Gedegen aanpak

Systematisch compliancemanagement werkt met hard en soft controls naar inzicht en grip op de juridische operationele risico's. Dit vraagt om een gedegen aanpak met integrale (samen!)werking. De ISO 37301 compliancennorm heeft dit in een systeem uitgewerkt, ook met inbreng van Nederlandse expertise. De norm vormt een doorbraak dankzij de combinatie van veel risk/compliance-ervaring en gerelateerde benchmarks, zoals toegelicht in mijn scriptie voor executive master of compliance aan de Vrije Universiteit Amsterdam. Mijn praktijkvertaling van deze norm in een compliancescan levert de mogelijkheid om de eigen complianceprestaties (zie hierna) te benchmarken versus de ambitie en/of versus de sector. Op deze wijze biedt de norm een katalysator voor groei in compliance.

Effectiviteit

Hard-controlmaatregelen zijn effectief indien deze worden ondersteund door een cultuur van integriteit. Regeltjes en richtlijnen alleen zorgen niet voor compliant gedrag, daar zijn ook soft controls voor nodig, deze stimuleren een cultuur van integriteit als bedding voor de hard controls. De ISO-compliancennorm benut een aantal aspecten die hieraan bijdragen, zoals leiderschapsdimensies, communicatie en training. De norm werkt ook met preventieve soft controls zoals helderheid, voorbeeldgedrag en betrokkenheid. Detectiesoft-controls zoals transparantie worden ook ingezet. En de responsieve soft control handhaving kan de compliancecultuur maken of breken.

Hoe en wat: ISO-compliancennorm

De ISO-norm 37301 is uitgewerkt in een compliancemanagementsysteem (CMS). Het is samengesteld vanuit een stevige basis met contextanalyse, verbinding met concrete organisatiedoelstellingen, organisatieprincipes voor goed bestuur en een authentieke risk/compliance/integriteitsleiderschapscultuur. Deze vormen de gezonde fundering voor de andere compliancecomponenten in de plan-do-check-actcyclus (PDCA). Het geheel is vervat in een zeventigtal elementen voor compliancemanagement. Zie het kader voor een samenvatting van de norm.

Samenvatting ISO-norm 37301

Context van de organisatie

- De omgevingsanalyse is opgesteld en volledig: context, issues, belanghebbenden, eisen, wensen en verwachtingen
- Identificatie van complianceverplichtingen: er is een goed en actueel overzicht van de wet- en regelgeving
- De compliancerisico's zijn beoordeeld met scores

Leiderschap

- Er is compliancebeleid, met de nadruk op commitment en voorbeeldgedrag
- Duidelijkheid in rollen, verantwoordelijkheden en bevoegdheden met betrekking tot compliance voor bestuur, top- en lijnmanagement en medewerkers. Er is een onafhankelijke compliance officer

Planning

- Vaststellen van compliancedoelstellingen, de focus is bepaald, beperkt en duidelijk afgesproken
- Plannen van maatregelen om compliancerisico's te beheersen. Er ligt een concreet compliancetakenactieplan met

AUDIT

MAGAZINE

tijds kader en vaststelling van eenieders betrokkenheid

Support

- Bewustzijn, competentie en training in compliance
- Gedrag en cultuur
- Communicatie en documentatie

Operatie

- Implementatie maatregelen voor compliance (technisch, procedureel, sturing op gedrag)

Prestatie evaluatie

- Monitoren van compliancenaleving met toepassing van indicatoren
- Analyse van informatie en rapportages van resultaten (intern en extern)

Verbetercyclus

- Corrigerende maatregelen en verbeteracties
- Actie op niet-naleving van eisen en escalatie waar nodig naar hogere managementniveaus

In figuur 1 is een voorbeeld gegeven van het overkoepelend resultaat van een compliancescan, waarbij de scan zelf ook op subniveaus inzoomt. De compliancescan levert scores op die zijn getoetst aan de gemiddelden in de sector en, belangrijker nog, getoetst zijn aan de complianceambitie van de organisatie, om te komen tot een gericht stappenplan voor groei van de beheersing.

ISO-ref.	ISO-compliance topic	Score 0-3
1	Scope	
2	Normatieve referenties	
3	Termen en definities	
4	Context van de organisatie/verplichtingen	1,4
5	Leiderschap	1,8
6	Planning	2,0
7	Support	1,1
8	Operationele compliance	1,0
9	Evaluatie complianceprestaties	0,8
10	Verbetercyclus	1,0
	Totale score	1,3

0 = voldoet niet 
1 = startend 
2 = goed 
3 = excellent 

Figuur 1. Voorbeeld van resultaat compliancescan

Normneurose?

De ISO-norm is de eerste mondiale aanbeveling door een neutraal, gerenommeerd instituut voor het inrichten en verbeteren van een compliancemanagementsysteem. De ISO-werkgroep integreert strategische, tactische en operationele middelen om te komen tot een compliancemanagementsysteem (CMS).

Sterke punten van de compliancennorm:

- transparante en integrale compliancebeheersing met contextanalyse;
- strategische en operationele verankering (PDCA) in de organisatie;
- integrale compliancebeheersing door focus op gedrag en cultuur;
- compliancebeheersing als lerende organisatie: verbetermanagement.

De norm had verder kunnen gaan in het specificeren van soft-controlelementen uit de nieuwste wetenschappelijke inzichten, maar dat zal wellicht in de toekomst aan de norm toegevoegd worden. In het uitbouwen van gedegen compliancemanagement moeten we ons niet blindstaren op een model. Iedere norm is slechts een leidraad voor verbetering. Deze norm vormt een waardevolle samenvatting van de recente ervaring en veel nieuwe wetenschappelijke inzichten.

Het is belangrijk om compliancerisicobeheersing breed te verankeren met een effectieve inzet van human capital

Kritische succesfactoren voor de praktijk

Hoe ga je dan verder in de praktische invulling? Wat zijn de valkuilen?

Compliancebeleid

Een weldoordacht compliancebeleid levert betrokkenheid op van alle spelers, met een gedragen focus op specifieke wetgeving. In het beleid bepaal je op welke belangrijke juridische risico's je gaat sturen en bouw je verder op de risicobereidheid per thema. Bijvoorbeeld heel streng en strak sturen op veiligheidsrisico's en meer ruimte opzoeken in – creatiever – portfoliomanagement?

Stappenplan

Hoe zet je het beleid om in een realistisch stappenplan? Voor iedere fase in de plan-do-check-actcyclus moet je duidelijk bepalen wat, waarmee en door wie er wordt geleverd om de fase af te sluiten en de cyclus – op termijn – continu te laten werken.

Inbedding

Het is belangrijk om compliancerisicobeheersing breed te verankeren met een effectieve inzet van human capital. De inbedding in de afdelingen control, risk en compliance, audit, juridische zaken en de uitwerking naar de operationele afdelingen zijn doorslaggevend voor het succes. Geen silovorming, maar samenwerking in een uniforme risk/control/auditaanpak. Dit geeft eenduidigheid in de uitwerking en duurzame resultaten in de eerste lijn.

In twee weken tijd ontstaat inzicht in het huidige compliancemanagementniveau, met een gericht verbeterplan vanuit het vastgestelde ambitieniveau

Prioriteren

Bepaal op basis van de top-juridische risico's hoe je gaat meten en bijsturen. De rapportage op macro- en microvlak grijpen op elkaar in zonder rapportageoverkill. In de markt is uitstekende compliancesoftware beschikbaar, waarbij extra focus kan worden gelegd op de invalshoeken die je zelf kiest: per afdeling, maar ook bijvoorbeeld thematisch zoals privacy door de hele organisatie.

Compliancescan

AUDIT

MAGAZINE

De hiervoor genoemde succesfactoren komen sneller aan het licht door het uitvoeren van een compliancescan. In twee weken tijd ontstaat inzicht in het huidige compliancemanagementniveau, met een gericht verbeterplan vanuit het vastgestelde ambitieniveau. De reacties van de reeds geleverde scans in de corporatiesector tonen een belangrijke bijvangst: 'meer betrokkenheid en meer energie' om compliancemanagement te verbeteren en te verankeren.

Samenwerking met internal audit

Internal audit heeft ook een rol in compliancemanagement. Internal audit kan in haar werkzaamheden compliancerisico's meenemen. Daarnaast biedt de ISO-norm een belangrijk raamwerk om te toetsen op welke manier een organisatie omgaat met compliance en de juiste keuzen daarin maakt.

Gezond fundament

Deze praktische dimensies geven aan dat compliancemanagement enkel zal werken door te bouwen op human capital, in een integrale aanpak. De compliancescanaanpak levert met deze invulling een gezond fundament voor duurzaam inzicht en grip op de beheersing van juridische risico's. Het resulteert in de optimale inzet van de ISO-compliancienorm met human capital naar een cultuur van compliance en integriteit.

Over

Mr. Carl De Wannemaeker EMoC (VU) maakt de ISO-compliancerichtlijn bruikbaar: 'Compliancescan, een compliancegroeykatalysator'.

Drs. Cosmo Schuurmans RA CIA is partner bij EBBEN Partners bv, een onderzoeks- en adviesbureau op het gebied van integriteit, risicomanagement en compliance.

Tags: compliance, ISO

Bron url: <https://auditmagazine.nl/artikelen/de-compliancescan-meer-grip-op-risicos/>