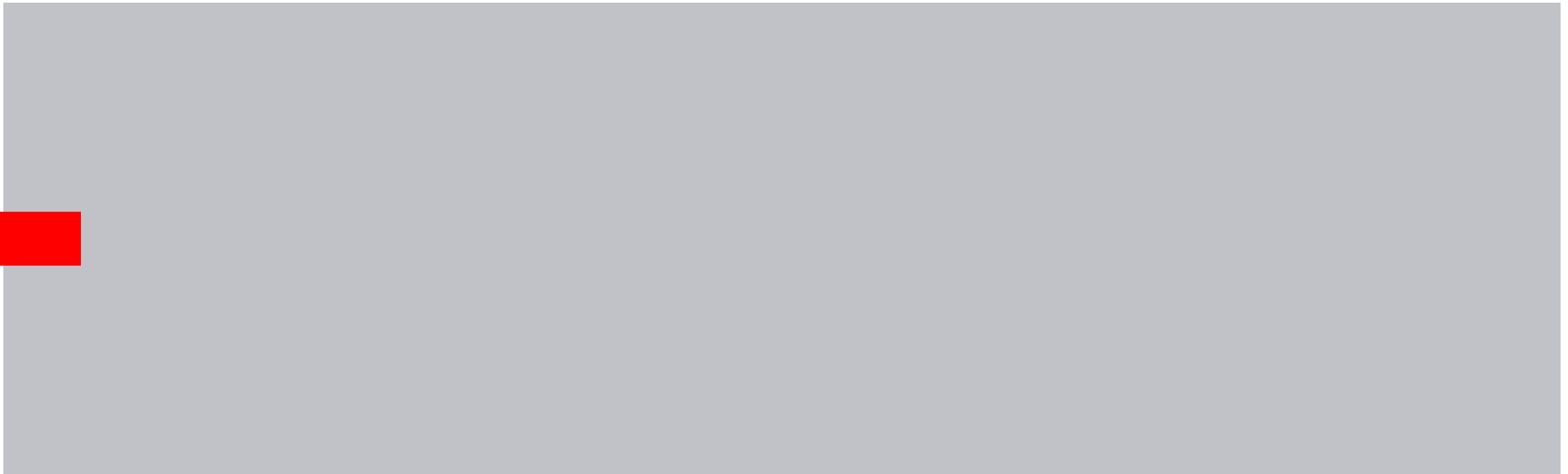




De interne compliancefunctie

Handreiking voor missie, visie en omgevingsscan





Handreiking

algemeen

1. Doel van de Handreiking
2. Verantwoording van de Handreiking
3. Opzet van de Handreiking
4. Gebruik van de Handreiking
5. (Relatie met) overige 'bouwstenen' voor de inrichting van de interne compliancefunctie

1. Doel van de Handreiking

Voor veel in Nederland gevestigde ondernemingen gelden nationale en internationale regels ten aanzien van corporate governance binnen een organisatie. Een voorwaarde voor een robuuste governance is o.a. de inrichting van een interne compliancefunctie,

Deze handreiking is bedoeld als 'bouwsteen' voor de inrichting van de interne compliancefunctie binnen een specifieke organisatie en kan worden gebruikt als strategisch startpunt daarvan. Ook kan de Handreiking na verloop van tijd gebruikt worden om de missie, visie en kernwaarden van de interne compliancefunctie te herijken.

De Handreiking draagt bij aan het doel van de VCO om professionals met een focus op ethiek, integriteit en compliance van handvatten te voorzien voor de inrichting van de interne compliancefunctie. De Handreiking is (enkel) een hulpmiddel daartoe, er kunnen dan ook geen rechten worden ontleend aan dit document.



2. Verantwoording van de Handreiking

Bij het opstellen van deze Handreiking heeft de VCO ook nadrukkelijk gekeken naar de beschikbare “guidance” en “best practices” vanuit verschillende sectorale toezichthouders, en is met gebruikmaking van de ruim beschikbare kennis en ervaring bij de leden van de *Kennistafel Inrichting van de Compliancefunctie* al doende een document ontwikkeld dat in verschillende organisaties kan worden gebruikt als basis waarop verder kan worden gebouwd,

Let op: de compliancefunctie dient altijd te worden ingericht op een wijze die recht doet aan de feitelijke situatie en omgeving waarbinnen de organisatie opereert.



3. Opzet van de Handreiking

De Handreiking bestaat uit verschillende onderdelen:

- Een omschrijving van *kader en doel* van de interne compliancefunctie;
- Een stappenplan voor het vaststellen van de *missie, visie en kernwaarden* voor de interne compliancefunctie; en
- Een voorzet voor het uitvoeren van een *in- en externe omgevingsscan* voor de inrichting van de interne compliancefunctie.



4. Gebruik van de Handreiking 1/2

Stappenplan

Aan de hand van het stappenplan kunnen de missie, visie en kernwaarden van de compliancefunctie worden vastgesteld (stappen 1 en 2). In stap 3 wordt nader ingegaan op compliance managementsystemen die kunnen helpen bij de praktische borging van de interne compliancefunctie en hoe deze kan worden gebruikt voor 'compliance in control' (stap 4). Stap 5 betreft de formulering van de visie op compliance en stap 6 kan helpen bij het uitvoeren van die visie door een 'roadmap' op te stellen.

Omgevingsscan

Met behulp van de in- en externe omgevingsscan worden inzichten gegenereerd die kunnen helpen bij het doorlopen van de verschillende hierboven omschreven stappen.

Aan de hand van de interne omgevingsscan kan inzicht worden verkregen in het potentiële spectrum van activiteiten die van belang zijn voor de compliancefunctie, en welke specifieke omstandigheden mogelijk verhoogd aandacht behoeven. Daarnaast wordt aandacht besteed aan aspecten die te maken hebben met (de verkenning van) gedrag en cultuur binnen de betreffende organisatie, en de praktische borging van de compliancefunctie.

De externe omgevingsscan zoals neergelegd in de Handreiking focust met name op het juridisch kader dat van belang is voor een goede invulling van de interne compliancefunctie, en relevante externe stakeholders.



4. Gebruik van de Handreiking 2/2

Gebruik naar eigen inzicht

In de Handreiking worden voorstellen gegeven voor te nemen stappen en de wijze waarop een omgevingsscan kan worden uitgevoerd. Deze zijn niet limitatief en kunnen naar eigen inzicht worden aangevuld.

Het is van belang om deze stappen en de omgevingsscan zo uit te voeren die goed passen bij de eigen organisatie. Een voorbeeld: stakeholders zoals aandeelhouders en leden zijn in deze Handreiking onderdeel van de externe omgevingsscan. Is er binnen de betreffende organisatie aanleiding om dergelijke stakeholders mee te nemen in de interne omgevingsscan, dan kan dat natuurlijk.



5. (Relatie met) overige bouwstenen voor het inrichten van de interne compliancefunctie 1/2

Compliance Charter

Het compliance charter is in feite een basisdocument of leidraad voor de compliancefunctie, waarin een aantal elementaire beginselen is vastgelegd. Zo dient een charter in ieder geval de volgende elementen te bezitten:

- De missie en doelstellingen van de compliance functie.
- De positionering van de compliance functie in de organisatie en de reikwijdte van de functie.
- De taken, bevoegdheden en verantwoordelijkheden van de compliance functie.

Het compliance charter geeft dus de primaire taken, middelen, verantwoordelijkheden en rapportagelijnen van de compliancefunctie weer. De Handreiking helpt bij het vaststellen deze primaire taken die vervolgens in het charter vastgelegd kunnen worden.



5. (Relatie met) overige bouwstenen voor het inrichten van de interne compliancefunctie 2/2

Beroepscompetentieprofiel

Het VCO beroepscompetentieprofiel draagt bij aan het doel van de VCO om professionals met een focus op ethiek, integriteit en compliance handvatten te geven bij wat van hen beroepsmatig kan worden verwacht en welke competenties daarvoor nodig zijn in diverse fasen van hun loopbaan. Hierbij is rekening gehouden met de kernwaarden, normen en verwachtingen die zijn opgenomen in de VCO Beroepscode.

De kernwaarden expertise, autonomie, zorgvuldigheid en betrokkenheid zijn nader omschreven in zowel het beroepscompetentieprofiel als in de beroepscode. Onder meer deze waarden kunnen van belang zijn voor het vaststellen van de missie, visie en kernwaarden van de interne compliancefunctie,





Handreiking

missie/visie/
omgevingsscan

- A. Kader en doel van compliance
- B. Missie, visie en kernwaarden voor Compliance - stappenplan
- C. Omgevingsscan – intern en extern

A. Kader en doel compliance

- **Kader:** *license to operate**: wet- en regelgeving die essentieel is voor het kunnen uitvoeren van de “core-business” van de organisatie. Dit vormt het juridisch kader voor compliance.
- **Doel:** het bevorderen van integer handelen: integriteit is het fundament van elke organisatie.

Meer specifiek:

- Compliance bevordert :
 - naleving en handhaving van wet- en regelgeving en
 - de integriteit van de organisatie, haar bestuur en de medewerkers.
- Daartoe:
 - ondersteunt Compliance bij de identificatie van integriteitsgerelateerde risico's, en
 - draagt Compliance bij aan het beheersen van die risico's, en het voorkomen/beperken van schade uit die risico's.

* Om deze Handreiking zo praktisch mogelijk te houden, is gekozen voor een kader dat zich beperkt tot de juridische ‘license to operate’. Feitelijk is dit kader ruimer omdat ook rekening gehouden dient te worden met bijvoorbeeld de maatschappelijke omgeving waarin de organisatie opereert, interne normen en waarden, etc.



B. Missie, visie en kernwaarden compliance – stappenplan 1/4

Inleiding

Om Compliance een goede basis te geven binnen de organisatie, is het van belang om de missie, visie en kernwaarden ervan vast te stellen. Deze kunnen vervolgens vastgelegd worden bijvoorbeeld in het compliance charter of als apart document. Hierna volgen definities en een stappenplan die hierbij kunnen helpen.

Voor verschillende stappen kan gebruik gemaakt worden van de omgevingsscan die in onderdeel 3 nader uitgelegd wordt.

Definities

- Missie: richt zich op het bestaansdoel en de fundamentele reden van de organisatie en beschrijft diens kernactiviteiten, waarden en het bestaansrecht.
- Visie: richt zich op de gewenste toekomst van de organisatie
- Compliance: verschillende definities zijn beschikbaar. Zie hiernaast de definitie die de VCO hanteert.

Definitie Compliance – VCO

Compliance is het versterken van de integriteit van de organisatie om daarmee bij te dragen aan duurzame waardecreatie door de organisatie.

De Compliancefunctie heeft twee kerntaken:

1. Het toezien op de naleving van interne en externe normen;
2. Het bevorderen van een integriteitsbewuste bedrijfscultuur.

Samengevat gaat compliance over gedrag: *Het goede doen; ook als niemand kijkt. Dat geldt zowel richting klanten en leveranciers als voor medewerkers onderling.*



B. Missie, visie en kernwaarden compliance – stappenplan 2/4

Stap 1:

Stel met behulp van een omgevingsscan (onder meer) het volgende vast:

- a. Organisatie: wat is het voor organisatie, wat zijn haar activiteiten en in welke omgeving/sector is zij actief?
- b. Positie van Compliance en de compliancefunctie binnen de organisatie.
- c. Volwassenheid van Compliance en de compliancefunctie binnen de organisatie.
- d. Wat is de aanleiding om een missie voor en visie op Compliance te schrijven.
- e. Zijn binnen de organisatie reeds kernwaarden vastgesteld?
 - Zo ja, gebruik die kernwaarden ook voor Compliance;
 - Zo nee, stel maximaal vijf krachtige kernwaarden op die gaan helpen, bijvoorbeeld bij het verder uitdragen van Compliance binnen de organisatie.

Stap 2:

Beschrijf Compliance binnen de organisatie aan de hand van de volgende vragen:

i. Ondersteunende vragen:

1. Waar staat de organisatie voor: wat is haar missie? Vaak is er een overkoepelende missie
2. Waar staan we voor?
3. Welke normen en waarden hebben we?
4. Welke overtuigingen motiveren ons?
5. Wat is ons bestaansrecht?



B. Missie, visie en kernwaarden compliance – stappenplan 3/4

Vervolg stap 2:

ii. Visie: Waar gaan we voor? Wat is onze toekomstdroom o.g.v. Compliance?

1. Wat wordt er binnen de organisatie verstaan onder 'Compliance'? Er zijn verschillende definities:
 - a. Enge definitie (alleen voldoen aan wet- en regelgeving)
 - b. Bredere definities zoals die van de VCO.
2. Wat willen we bereiken? Zijn er rapporten/documenten (audit – accountant – toezichthouders) die iets zeggen over compliance c.q. de compliance functie?

iii. Kernwaarden: Stel aan de hand van bovenvermelde vragen (ook) de kernwaarden voor Compliance op. Kijk in dit verband ook naar de kernwaarden zoals vermeld in de VCO Beroepscode en het VCO Beroepscompetentieprofiel.

Stap 3: Compliance managementsysteem

- i. Beschrijf wat je verstaat onder een compliance managementsysteem*
- ii. Maak een keuze voor de te gebruiken methodiek inclusief onderbouwing keuze.*
Voorbeelden van methodieken zijn 'Plan-Do-Check-Act (Demming)', COSO en ISO 37301. Zie ook jaarverslagen van grote organisaties voor voorbeelden.



2. Missie, visie en kernwaarden compliance – stappenplan 4/4

Stap 4:

Compliance in control

- i. Hoe past het gekozen compliance managementsysteem (CMS) binnen het geheel van overige control framework, zoals bijvoorbeeld het riskmanagement framework?*
- ii. Hoe past het CMS in de planning- en control cyclus?*
- iii. Hoe wordt de effectiviteit geborgd? (Bijvoorbeeld door selfassessment, internal audit, externe audit)*

Stap 5:

Formuleer de visie op compliance/integriteit/ethiek. Hiertoe kan je de algemene visie van de organisatie gebruiken en die meer specifiek maken naar de compliance doelstellingen.

Stap 6:

Hoe nu verder: roadmap

Vragen die je jezelf kunt stellen, betreffen de volgende:

- a. Hoe ga je e.e.a. implementeren?
- b. Wat is het tijdspad?
- c. Wie zijn betrokken en wie is verantwoordelijk?



C. Omgevingsscan - algemeen

Algemeen

Met een omgevingsscan wordt in kaart gebracht zowel de interne als de externe omgeving waarbinnen de organisatie opereert. Een dergelijke scan is van waarde om te kunnen bepalen wat de positie is van de Compliance functie binnen de organisatie, waar aandachtspunten voor Compliance liggen, en welke – hoog over – risico's kunnen worden geïdentificeerd. Zie ook de **stappen 1 en 2** voor het vaststellen van de missie, visie en kernwaarden voor de compliance functie.

In dit onderdeel worden suggesties gegeven voor de uitvoeren van een dergelijke scan, met een onderscheid in onderwerpen die van belang zijn voor de scan.

C. Omgevingsscan – intern 1/4

Basale vragen

De interne omgevingsscan begint met een aantal basale vragen:

- Hoe groot is de organisatie?
- Hoe complex zijn haar producten en diensten?
- In welke (gereguleerde) omgeving is de organisatie actief?
- Welke doelgroepen worden bediend? Zijn producten/diensten bijvoorbeeld gericht op consumenten?

Afhankelijk van de antwoorden op deze vragen, kun je vaststellen hoe het potentiële spectrum van activiteiten eruit ziet voor de compliancefunctie. Is het groot en complex of juist relatief klein en overzichtelijk? De mate van complexiteit van de organisatie zal zijn weerslag hebben op de complexiteit van de compliancefunctie.

Specifieke omstandigheden (acties i.v.m. toezicht, incidenten?)

Ga verder na welke specifieke omstandigheden mogelijk verhoogd aandacht behoeven, bijvoorbeeld vanwege lopende dossiers vanuit het toezicht of vanwege (recente, grote) integriteitgerelateerde incidenten.

3. Omgevingsscan – intern 2/4

Gedrag en cultuur

Verken de cultuur van de organisatie, bijvoorbeeld aan de hand van engagement scan resultaten of andere instrumenten zoals soft controls/behavioral control model. Wat zegt dit over het risicobewustzijn?

Ga verder na welke normen en waarden de organisatie nastreeft. Is er een gedragscode en wat staat in de gedragscode opgenomen mbt integriteit en ethiek?

Praktisch

Welke afspraken zijn gemaakt waardoor je als compliance (extra) taken op je neemt (of krijgt...) Welke afspraken zijn er niet gemaakt waar je in de praktijk tegenaan loopt, hetzij nu hetzij in de toekomst? Denk aan:

- Tooling, bijvoorbeeld learning systemen, KYC-systemen.
- Risk appetite van de organisatie: is dit bekend en eventueel uitgewerkt? Worden hier specifieke compliance risico's in benoemd?
- Structuur van de organisatie: volwassenheid van de organisatie, samenstelling bestuur, aanwezigheid raad van commissarissen, eigendomsstructuur en zeggenschap, risk functie, audit functie.



3. Omgevingsscan – intern 3/4

Three Lines Model

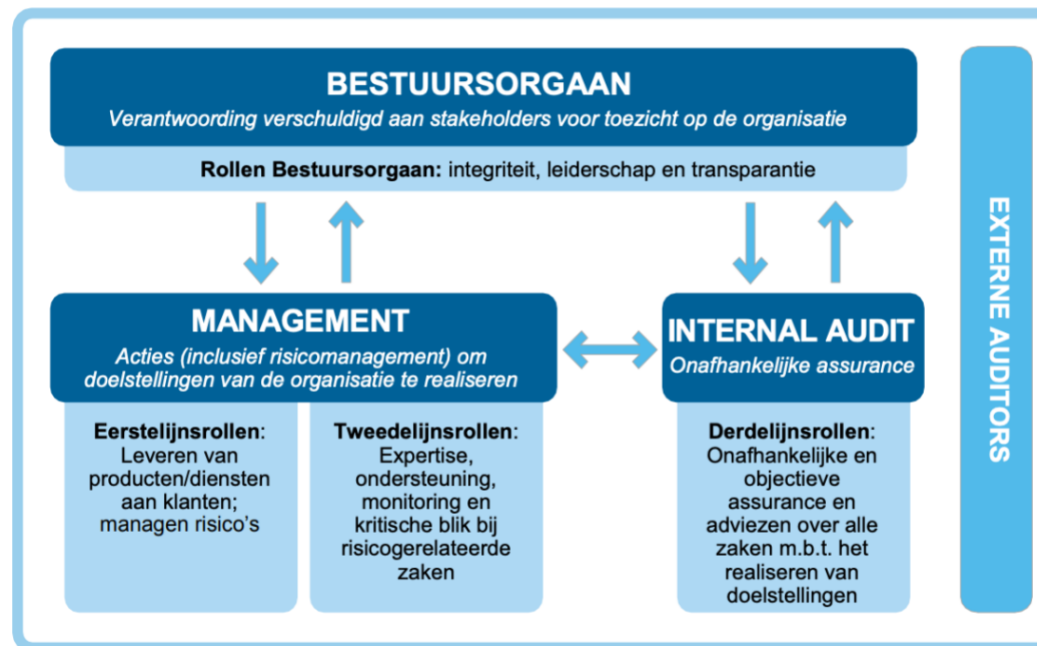
Breng jouw interne omgeving in kaart om te bepalen hoe Compliance in de betreffende organisatie kan:

- ondersteunen bij de identificatie van integriteitsrisico's, en
- adviseren in het beheersen en voorkomen/beperken van schade uit die risico's.

Relevante aandachtspunten:

- Integriteitsrisicomodel,
- Vaststelling bestaande (en eventueel gewenste) governance,
- opstellen RASCI, procesflows,
- Afbakening 1^e/2^e lijn, afbakening tussen Compliance en Risk, Compliance en Legal (en andere 1^e lijnsfuncties zoals HRM, Finance, ICT, etc.)
- Impact van/samenwerking met 3^e lijn.

Het Three Lines Model van het IIA



LEGENDA: ↑ Verantwoording, rapporteren ↓ Delegeren, richting, middelen, toezicht ↔ Afstemming, communicatie, coördinatie, samenwerking

Bron: [publicatie iia - three-lines-model-updated-nl](#) p.4

3. Omgevingsscan – intern 4/4

Aandachtspunten Three Lines voor het MKB

Het Three Lines model werkt vaak niet voor het MKB vanwege – onder meer – de volgende redenen:

- **Te complex:** Het model is te gedetailleerd en te formeel voor de flexibele en snelle besluitvorming die kenmerkend is voor het MKB.
- **Beperkte middelen:** MKB's hebben vaak niet genoeg financiële en personele capaciteit om afzonderlijke, gespecialiseerde functies voor elke verdedigingslijn op te zetten.
- **Roloverlap:** In het MKB kunnen dezelfde personen verantwoordelijk zijn voor meerdere functies die het model probeert te scheiden, wat leidt tot potentiële belangenconflicten en efficiëntieverlies.
- **Informele processen:** De informele en minder gestructureerde bedrijfsprocessen in het MKB passen niet goed bij het formele en gestructureerde aard van het model.
- **Gebrek aan expertise:** Er is vaak een gebrek aan interne expertise om een effectieve tweede en derde verdedigingslijn te implementeren, en externe expertise inhuren kan te kostbaar zijn.
- **Cultuurverschillen:** Het ondernemersklimaat en de bedrijfscultuur in het MKB zijn minder gericht op strikte naleving van formele structuren, wat het moeilijk maakt om het model toe te passen.

Kijk dan ook wat wel werkt binnen jouw MKB-organisatie, leg uit en leg vast.



3. Omgevingsscan extern

‘License to operate’

Wet- en regelgeving die essentieel is voor het kunnen uitvoeren van de ‘*core business*’ van de organisatie, vormt de ‘*license to operate*’/het juridisch kader voor Compliance. Dit kader verschilt per organisatie. Breng daarom in kaart welke wet- en regelgeving van belang is voor de organisatie, het type onderneming, de producten en diensten.

Voorbeelden hiervan worden in het volgende onderdeel van deze Handreiking besproken. De voorbeelden betreffen de vaststelling van het juridisch kader voor een financiële instelling (bank), een juridisch dienstverlener, een MKB-bedrijf en een internationale groothandels- of industriële onderneming (grootbedrijf).

Stakeholderanalyse

Maak ook een stakeholderanalyse als onderdeel van de externe omgevingsscan. Denk hierbij aan:

- Klanten
- Maatschappij / publieke opinie
- Activistische groepen
- Aandeelhouders / leden
- ESG benchmarks
- Rating agencies
- Analisten

Voor Compliance is relevant te begrijpen welke eisen en verwachtingen deze stakeholders stellen/hebben t.a.v. de integriteit van de onderneming en ethische vraagstukken.





Handreiking

Voorbeelden juridisch
kader

1. Financiële instelling (bank)
2. Juridisch dienstverlener
3. MKB-bedrijf
4. Internationale groothandels- of
industriële onderneming (grootbedrijf)

Voorbeelden vaststelling juridisch kader 1/2

Voor het kunnen vaststellen van het juridisch kader/‘license to operate’ van de organisatie, is hierna een aantal voorbeelden gegeven van dergelijke kaders voor specifieke sectoren/branches.

Voor het opstellen van deze kaders is rekening gehouden met verschillende doelen (niet-limitatief) waaraan Compliance kan bijdragen.

1. Financiële sector:

- Strikte en complexe compliance vereisten (mede vanuit toezichthouders).
- Moeten voldoen aan diverse Nederlandse en Europese wet- en regelgeving voor financiële instellingen.
- *Doel: (bevorderen van) financiële stabiliteit, betalingsverkeer, preventie van financieel-economische criminaliteit (fraude, witwassen, financieren van terrorisme), klantenbescherming (zorgplicht, privacy), goede werking van financiële markten.*

2. Juridische dienstverlening:

- Compliance gericht op professionele ethiek en vertrouwelijkheid van dienstverlening en (cliënt)informatie (o.a. het beroepsgeheim).
- Verschillende beroepsregimes van toepassing op juridische dienstverleners,
- Verschillende regimes van toepassing op cliëntenonderzoek (Wwft en niet-Wwft zaken, persoonlijke verantwoordelijkheid naleving wet- en regelgeving voor notarissen en advocaten)
- *Doel: (bevorderen van) ethische beroepspraktijk, preventie van financieel-economische criminaliteit, naleving van (overige) specifieke beroepsregels.*



Voorbeelden vaststelling juridisch kader 2/2

3. MKB (Midden- en Kleinbedrijf):

- Minder complexe compliance vereisten in vergelijking met banken en zakelijke dienstverleners.
- Moeten algemene arbeidswetgeving en gezondheids- en veiligheidsregels volgen.
- Eventuele specifieke industrie-regelgeving en milieuregels kunnen van toepassing zijn.
- *Doel: (bevorderen van) operationele compliance, risicobeheersing, voorkomen van boetes en reputatieschade.*

4. Internationale groothandels- of industriële onderneming (grootbedrijf)

- In beginsel als het midden- en kleinbedrijf, maar met een grotere mate van complexiteit.
- Veel (nieuwe) regels die in bepaalde gevallen van toepassing (kunnen) zijn, zoals rond witwassen, corruptie, export, mededinging en duurzaamheid.
- Verschillende, soms met elkaar strijdige, regels uit verschillende landen.
- *Doel: (bevorderen van) operationele compliance, risicobeheersing, voorkomen van boetes en reputatieschade.*

Voorbeeld vaststelling (juridisch) kader - financiële sector/banken

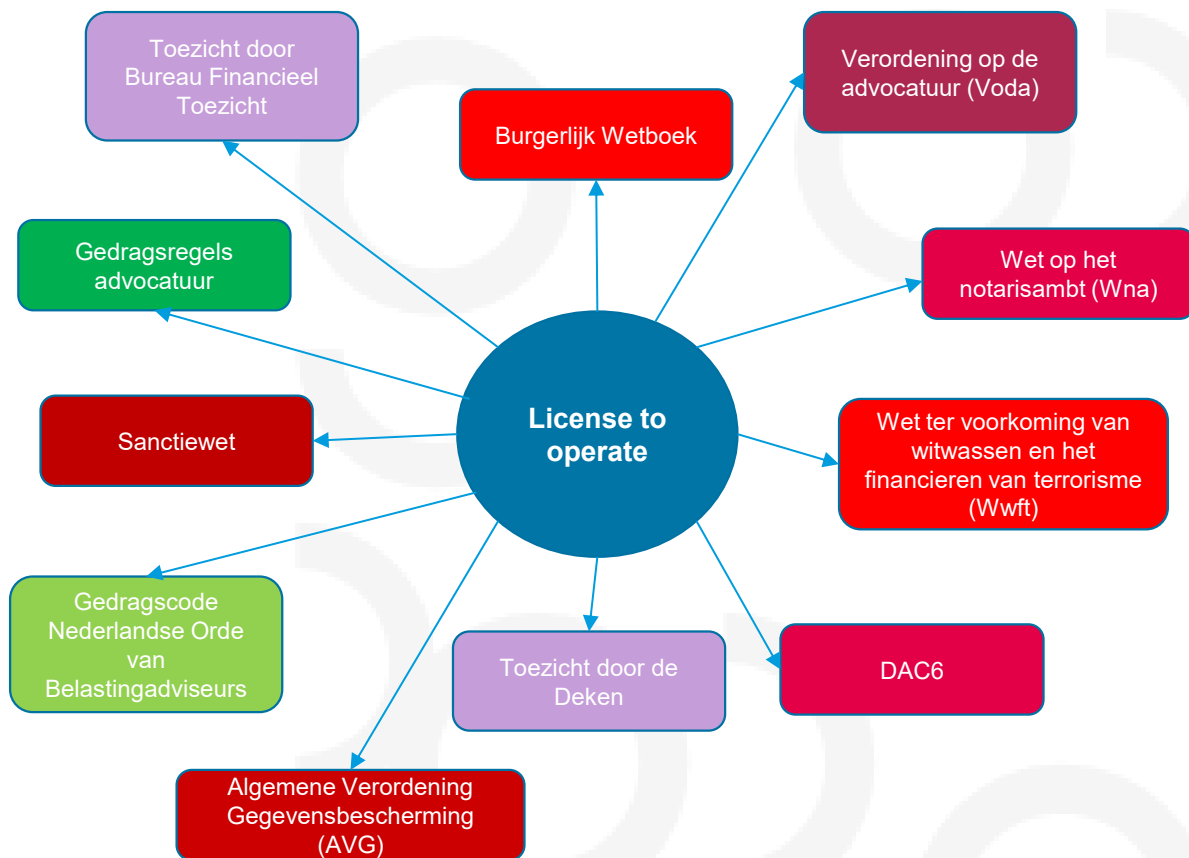


Wetgeving o.a.:

- Burgerlijk Wetboek
- Wet financieel toezicht
- Besluit Gedragstoezicht financiële ondernemingen
- Besluit prudentiële regels Wft
- Algemene verordening gegevensbescherming
- Wet ter voorkoming van witwassen en het financieren van terrorisme
- Sanctiewet
- Europese wet- en regelgeving zoals:
 - Digital Operational Resilience Act
 - Artificial Intelligence Act
 - European Market Infrastructure Regulation
 - Market Abuse Regulation
 - Markets in Financial Institutions Regulation
 - Capital Requirements Regulation
 - Investment Firm Regulation
- Diverse gedrags- en beleidsregels van toezichthouders (o.a. AFM, DNB, ECB, AP, ACM)



Voorbeeld vaststelling (juridisch) kader – juridisch dienstverlener



Wetgeving o.a.:

- Burgerlijk Wetboek (o.a. boek 2)
- Advocatenwet
- Wet op het notarisambt
- Algemene verordening gegevensbescherming (AVG)
- Sanctiewet
- Wet ter voorkoming van witwassen en het financieren van terrorisme (en daarmee samenhangend de Handelsregisterwet en het Implementatiebesluit registratie UBO's trusts en FGRs)
- DAC wet- en regelgeving
- Diverse gedrags- en beleidsregels van toezichthouders (BFT en Deken) en beroepsorganisaties (NovA, KNB, NOB)



Voorbeeld vaststelling (juridisch) kader – MKB-bedrijf



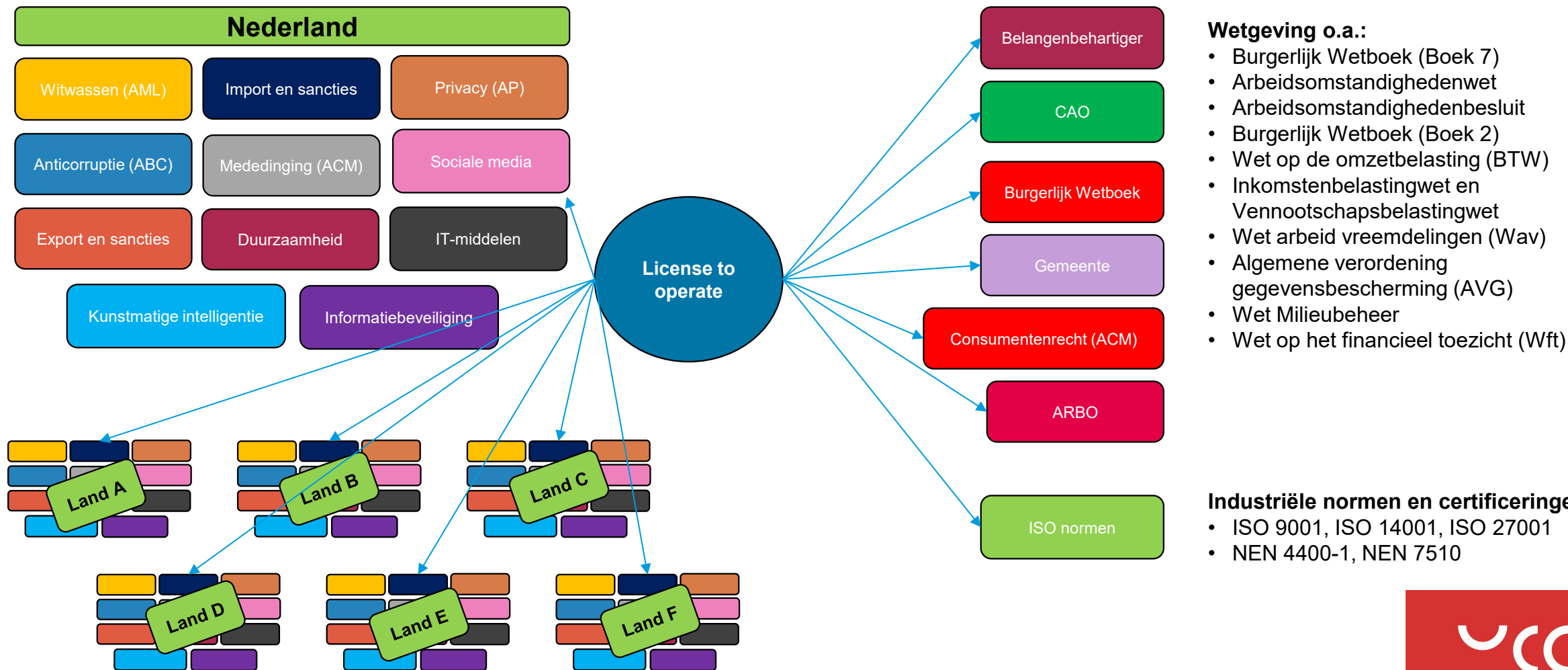
Industriële normen en certificeringen
ISO 9001
ISO 14001
ISO 27001
NEN 4400-1
NEN 7510

Wetgeving o.a.:

- Burgerlijk Wetboek (Boek 7)
- Arbeidsomstandighedenwet
- Arbeidsomstandighedenbesluit
- Burgerlijk Wetboek (Boek 2)
- Wet op de omzetbelasting (BTW)
- Inkomstenbelastingwet en Vennootschapsbelastingwet
- Wet arbeid vreemdelingen (Wav)
- Algemene verordening gegevensbescherming (AVG)
- Wet Milieubeheer
- Wet op het financieel toezicht (Wft)



Voorbeeld vaststelling (juridisch) kader – grootbedrijf



Ondernemingen dienen aan verschillende regels voor (veel) dezelfde onderwerpen in verschillende landen te voldoen: complexiteit





Voor vragen, opmerkingen of nadere toelichting over de Handreiking kan altijd contact worden opgenomen met de VCO middels navolgende contactgegevens:

<contactgegevens kennistafel>

Handreiking

Contact