

Compliance Charter

[Naam organisatie]

[Dit is een template voor een Compliance Charter dat als handvat gebruikt kan worden voor het ontwikkelen van het Compliance Charter van de eigen organisatie. De invulling is afhankelijk van de eigen organisatie.]

Gepubliceerd door

[Compliance of vergelijkbaar]

Goedgekeurd door

[Raad van Bestuur of vergelijkbaar]

Datum in werking

Versie

Inhoudsopgave

1	Inleiding	3
2	Doelstelling van de compliancefunctie	3
3	Compliancerisico management	4
4	Rollen, taken en verantwoordelijkheden ten aanzien van compliance	5
4.1	Raad van Bestuur <i>[of equivalent]</i>	5
4.2	Eerste lijn	5
4.3	Tweede lijn	5
4.4	Derde lijn	6
5	De compliancefunctie en samenwerking met andere functies	6

Versiebeheer

Versie	Datum	Goedgekeurd door	Wijzigingen
1.0	19-07-2024	Raad van Bestuur	Noem de voornaamste wijzigingen ten opzichte van de vorige versie

1 Inleiding

[Beschrijf kort wat de activiteiten zijn van de organisatie en in welke omgeving en sector de organisatie actief is. Beschrijf vervolgens kort wat de missie, visie en kernwaarden zijn van de organisatie en hoe de compliancefunctie daaraan op onafhankelijke wijze kan bijdragen¹. Zie voor meer informatie het document over het vast- en opstellen van de visie en missie van compliance gepubliceerd door de VCO]. Om de langetermijn doelstellingen te behalen, zijn het voeren van een integere en beheerste bedrijfsvoering en het volgen van de op ons van toepassing zijnde wet- en regelgeving een belangrijke voorwaarde.

De *[Raad van Bestuur of vergelijkbaar]* is eindverantwoordelijk voor een integere en beheerste bedrijfsvoering en de naleving van wet- en regelgeving en is daarom verantwoordelijk voor de goedkeuring en naleving van dit Compliance Charter (hierna: 'Charter'). *[Indien van toepassing: de Raad van bestuur legt hierover verantwoording af aan de Raad van Commissarissen of vergelijkbaar]*

Als onderdeel van het interne controle raamwerk heeft *[naam organisatie]* een permanente en onafhankelijke compliancefunctie ingericht. De compliancefunctie identificeert, beoordeelt, monitort en rapporteert over de verschillende compliancerisico's. Het Charter beschrijft de reikwijdte, doelstellingen, positie, rollen, bevoegdheden en verantwoordelijkheden van de compliancefunctie.

De eigenaar van het Charter is de afdeling Compliance van *[naam organisatie]*. Het Charter wordt iedere *[getal, bijvoorbeeld twee]* jaar geëvalueerd of eerder als gevolg van wijzigingen in wet- en regelgeving en/of interne of externe ontwikkelingen die verband houden met *[naam organisatie]*.

Dit Charter is van toepassing op *[naam organisatie en haar geconsolideerde groepsmaatschappijen en deelnemingen. Op basis van lokale wet- en regelgeving is het mogelijk dat deelnemingen een eigen Charter opstellen zolang deze lokale Charter in lijn is met dit Charter.]* en al haar medewerkers².

2 Doelstelling van de compliancefunctie

Het doel van de compliancefunctie is om op onafhankelijke wijze de relevante medewerkers van *[naam organisatie]* tijdig te adviseren bij het waarborgen van de integere bedrijfsvoering en compliance met wet- en regelgeving, gedragsregels en maatschappelijke normen ten behoeve van het behalen van de langetermijn doelstellingen. De compliancefunctie houdt hierbij rekening met alle mogelijke belanghebbenden van *[naam organisatie]*, waaronder medewerkers, klanten, investeerders, aandeelhouders en de toezichthouder(s). Ten behoeve van deze doelstelling, voert de compliancefunctie de volgende werkzaamheden uit:

- het opstellen en uitvoeren van het complianceprogramma waarin de risicogebaseerde operationele activiteiten van de compliancefunctie voor de komende periode worden toegelicht;
- het (mede-)signaleren van nieuwe of gewijzigde wet- en regelgeving, gedragsregels of maatschappelijke normen in samenwerking met de juridische afdeling;
- het opstellen en onderhouden van beleidsdocumenten ten behoeve van de bevordering van de naleving van wet- en regelgeving, gedragsregels en maatschappelijke normen;
- het opstellen en onderhouden van een risicogebaseerd monitoring programma waarin compliance- en integriteitsrisico's op een effectieve manier geïdentificeerd, onderzocht en gerapporteerd worden;
- het vergroten van het risicobewustzijn door middel van een doorlopend training programma voor medewerkers;
- het op peil houden van de kennis en ervaring van de compliancefunctie;

¹ Zie ook het document over de missie, visie en omgevingsscan van de organisatie op de VCO website

² Inclusief statutair bestuurders, ingehuurd krachten en stagiaires.

- communicatie over de integere en beheerste bedrijfsvoering op basis van het complianceprogramma en risicogebaseerd monitoring programma en compliance met de interne en externe toezichthouders, inclusief eventuele rapportage;
- het onderzoeken of laten onderzoeken van (vermoedelijke) overtredingen van wet- en regelgeving, gedragsregels of maatschappelijke normen en advisering over eventuele sancties als gevolg van deze overtredingen aan de Raad van Bestuur.

3 Compliancerisico management

De compliancefunctie is verantwoordelijk voor het identificeren, onderzoeken, monitoren en rapporteren van compliancerisico's. Een compliancerisico is als volgt gedefinieerd:

Het risico dat *[naam organisatie]* (mogelijk) niet langer voldoet of kan voldoen aan de geldende (inter)nationale wet- en regelgeving, gedragsregels en maatschappelijke/sectorale normen met financiële verliezen, reputatieschade of juridische sancties tot gevolg.

Voor het monitoren van de compliancerisico's gebruikt *[naam organisatie]* het volgende risicomanagement systeem *[uitleg risicomanagement systeem en de verschillende stappen, bijvoorbeeld COSO Enterprise Risk Management Framework, NEN-ISO 37301:2021 Plan-Do-Check-Act cyclus, Systematische Integriteitsrisico Analyse zoals beschreven door DNB en AFM, of vergelijkbaar]*.

De compliancefunctie identificeert en categoriseert de compliancerisico's in verband met de activiteiten en locaties van *[naam organisatie]*. Daarbij worden de volgende categorieën compliancerisico's onderscheiden *[bepaal welke risico's van toepassing zijn op de organisatie en onder het toezicht van de compliancefunctie vallen]*³:

- witwassen;
- financieren van terrorisme;
- omzeilen van sanctiewetgeving;
- corruptie;
- belangenverstrengeling;
- interne en externe fraude;
- belastingontduiking of -ontwijking;
- marktmanipulatie en voorwetenschap;
- cyberdreigingen en -criminaliteit;
- maatschappelijk onbetamelijk gedrag;
- gedrag van (individuele) medewerkers;
- privacy;
- omgang met vertrouwelijke informatie;
- mededinging;
- beschermen van klanten en investeerders;
- duurzaamheid;
- uitbesteding en aanbesteding.

Andere risicocategorieën die hier niet genoemd worden, behoren tot het aandachtsgebied van andere functies binnen *[naam organisatie]*, zoals *[risk management, fiscale zaken, HR, enzovoort]*. In het geval dat deze andere risicocategorieën leiden tot een mogelijk risico voor de integere of beheerste bedrijfsvoering of overtreding van de van toepassing zijnde wet- en regelgeving, moeten deze incidenten gerapporteerd worden aan de compliancefunctie.

³ De genoemde risicocategorieën zijn afgeleid van de risico's die worden behandeld in de systematische integriteitsrisico-analyse (SIRA) zoals beschreven door De Nederlandsche Bank (DNB) en aangevuld met andere risico's die relevant zijn voor de compliance functie. Het uitvoeren van de SIRA is verplicht voor financiële instellingen en accountants, maar ook relevant voor andere organisaties.

4 Rollen, taken en verantwoordelijkheden ten aanzien van compliance

De rollen, taken en verantwoordelijkheden zijn binnen *[naam organisatie]* ingericht volgens het three lines model⁴ *[het kan zijn dat de organisatie een alternatief governance model hanteert of dat de eerste en de tweede lijn gemengd zijn in het three lines model]*. Het uitgangspunt van dit model is dat de eerste lijn de producten en diensten aan klanten levert en daarom de operationele verantwoordelijkheid draagt voor het beheer van risico's. De tweede lijn, waaronder de compliancefunctie, bestaat uit specialisten die toezicht houden op de eerste lijn en adviseren bij risicogerelateerde zaken. De derde lijn wordt gevormd door Internal Audit die door middel van het uitvoeren van audits de werking en effectiviteit van het risicomanagement- en interne controle systeem onafhankelijk beoordeelt. Dit leidt ten aanzien van de compliancefunctie tot de volgende rolverdeling.

4.1 Raad van Bestuur *[of equivalent]*

De Raad van Bestuur is eindverantwoordelijk voor het inrichten van een transparante en efficiënte organisatiestructuur, waarin een integere bedrijfscultuur wordt gestimuleerd en bevorderd. De Raad van Bestuur stelt de risicobereidheid van de organisatie vast en houdt toezicht op de implementatie van het interne controle raamwerk om binnen de risicobereidheid te zijn en blijven. De Raad van Bestuur legt hierover verantwoording af aan de belanghebbenden van *[naam organisatie, bijvoorbeeld aan de aandeelhouders en de Raad van Commissarissen]*.

De Raad van Bestuur is ook verantwoordelijk voor het aanstellen, beoordelen en ontslaan van de medewerkers van de compliancefunctie *[indien van toepassing, na goedkeuring van de Raad van Commissarissen]* en geeft jaarlijks goedkeuring over het budget van de compliancefunctie met betrekking tot de nodige middelen (technologie, training, communicatie, expertise) en medewerkers.

4.2 Eerste lijn

De operationele afdelingen en hun management zijn verantwoordelijk voor de levering van de producten en diensten aan klanten en het bijbehorende beheer van de desbetreffende risico's binnen de gestelde risicobereidheid. Het management van de operationele afdelingen is de eigenaar van de desbetreffende risico's en heeft daarbij een voorbeeldfunctie. Het management heeft in die functie een actieve, sturende en faciliterende rol bij het stimuleren van de integere en beheerste bedrijfsvoering. Randvoorwaardelijk is een open en veilige omgeving waarin medewerkers elkaar aan kunnen spreken op gedrag en dilemma's kunnen en durven bespreken.

De medewerkers van de eerste lijn zijn zelf verantwoordelijk voor het naleven van de beleidsdocumenten en het melden van eventuele incidenten bij de compliancefunctie.

4.3 Tweede lijn

De tweede lijn overziet het volledige interne controle raamwerk en voorziet de eerste lijn van expertise, ondersteuning, monitoring en een kritische blik met betrekking tot risicomanagement. De tweede lijn bestaat uit de compliancefunctie, risicomanagementfunctie *[vul aan voor de eigen organisatie, bijvoorbeeld juridische zaken, fiscale zaken, financiën, enzovoorts]*. De tweede lijn rapporteert over de effectiviteit en volledigheid van de opzet, het bestaan en de werking van het interne controle raamwerk met betrekking tot risicomanagement, inclusief het waarborgen van de integere en beheerste bedrijfsvoering en compliance met wet- en regelgeving, gedragsregels en maatschappelijke normen ten behoeve van het behalen van de langetermijn doelstellingen.

⁴ Het three lines model is een governance model van de Institute of Internal Auditors (IIA)

De compliancefunctie is onderdeel van de tweede lijn en opereert onafhankelijk. Zij adviseert het management van de eerste lijn over de inrichting van het interne controle raamwerk op het gebied van compliancerisico's in de dagelijkse praktijk. De compliancefunctie volgt daarbij de methodiek van het compliancerisicomangement systeem zoals beschreven in hoofdstuk 3. Voor het effectief uitvoeren van de compliancefunctie is het van belang dat de Compliancefunctie vrije toegang heeft tot alle medewerkers, documentatie en informatie van de organisatie ten behoeve van de uitvoering van de functie. De compliancefunctie kan zowel worden uitgevoerd door een Compliancefunctie binnen *[naam organisatie]* of worden uitbesteed aan een derde partij.

Om de onafhankelijkheid te waarborgen, rapporteert de compliancefunctie haar bevindingen over (ontwikkeling van) de compliancerisico's direct en periodiek aan de Raad van Bestuur. *[indien van toepassing, de compliancefunctie escaleert zo nodig aan de Raad van Commissarissen]*. De compliancefunctie *[indien relevant: adviseert de Raad van Bestuur ook over het beloningsbeleid van de organisatie en]* neemt deel aan strategische beslissingen die invloed hebben op de compliancerisico's of het interne controle raamwerk.

4.4 Derde lijn

De derde lijn bestaat uit de interne auditfunctie. De interne auditfunctie voert risicogebaseerde audits uit waarin de governance en structuur, processen en interne controle raamwerken worden beoordeeld in zowel de eerste als tweede lijn. De interne auditfunctie voert haar taken onafhankelijk uit van de eerste en tweede lijn en adviseert de Raad van Bestuur over de haalbaarheid van de gestelde doelen binnen de risicobereidheid. De interne auditfunctie kan zowel worden uitgevoerd door een interne auditfunctie binnen *[naam organisatie]* of worden uitbesteed aan een derde partij.

5 De compliancefunctie en samenwerking met andere functies

Om de doelstellingen van de organisatie te behalen, moeten alle drie de lijnen efficiënt met elkaar samenwerken en de werkzaamheden van alle lijnen op elkaar zijn afgestemd.

[Indien van toepassing: De compliancefunctie heeft een directe lijn met de Functionaris voor Gegevensbescherming (FG). De FG heeft dezelfde taken en verantwoordelijkheden als de compliancefunctie, maar enkel in relatie tot het compliancerisico privacy, waar het verwerken van persoonsgegevens onderdeel van is. De FG heeft voor het identificeren, onderzoeken, monitoren en adviseren omtrent het privacyrisico een specifiek privacy programma dat is afgestemd met de compliancefunctie. Onderdeel van dit programma zijn het uitvoeren van Data Protection Impact Assessments (DPIA) en het afhandelen van interne meldingen van datalekken, inclusief eventuele rapportage aan de Autoriteit Persoonsgegevens.]