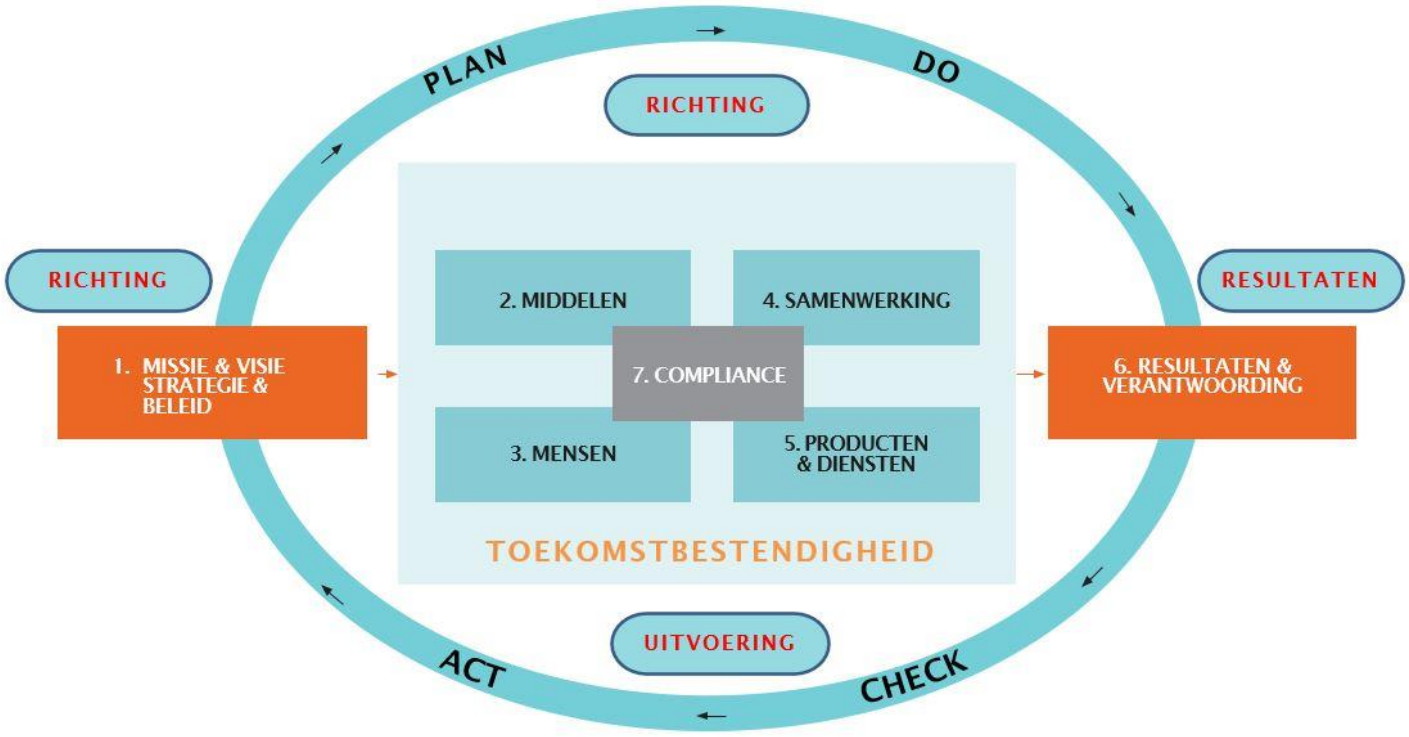
Compliance is niet zo moeilijk

De norm Compliance maakt deel uit van *Kwaliteit in Beeld. Certificeringskader bibliotheekwerk, cultuur en taal.* Om je te ondersteunen bij de voorbereiding op de audit, leggen we in deze whitepaper uit wat de plaats van de norm Compliance is. De verschillende aspecten van deze norm komen aan bod en we lichten de toetsing bij de audit toe.

DE NORM COMPLIANCE

Het certificeringskader bestaat uit zeven normen. Compliance is de zevende norm die aan bod komt in de audit:

Compliance gaat in essentie over het voldoen aan relevante wetten en regels. Ook gaat het over specifieke (branche)codes waaraan organisaties zich hebben verbonden of die (financiële) opdrachtgevers opleggen. Daarnaast gaat het om naleving van eisen van stakeholders en eigen bedrijfsregels. Bij die laatste kun je denken aan regels voor integere bedrijfsvoering.
Voor bibliotheken is er een specifieke eis voor het voldoen aan de invulling van de Wsob.



HET BEGRIP COMPLIANCE

Onder compliance wordt verstaan: 'het voldoen aan wet- en regelgeving en interne regels van de organisatie'. Klanten, subsidiënten en andere stakeholders moeten erop kunnen vertrouwen dat een organisatie zich consequent aan wetten, regels en afgesproken codes houdt, oftewel *compliant* is. Dit geldt zowel extern als intern. Ook al wordt de wet- en regelgeving niet overtreden, de organisatie kan wel schade oplopen (imago van onbetrouwbaarheid, niet transparant, etc.). In het geval niet voldaan wordt aan de wet- en regelgeving, dan dient de organisatie zich bewust te zijn van de (afbreuk)risico's die dit met zich meebrengt en wat ze hier wel of niet aan kan doen. Het voldoen aan de wet- en regelgeving (compliance-management) is hiermee nauw verwerven met het beheersen van risico's (risicomanagement).

WAT VALT ONDER COMPLIANCE?

Onder wet- en regelgeving vallen de algemene wetten zoals bijvoorbeeld de belasting- en sociale zekerheids-wetten, de Arbowet, Verdrag inzake de rechten van personen met een handicap (over toegankelijkheid van gebouwen), de Algemene Verordening Persoons-gegevens (AVG) en Wet bestuur en toezicht rechtspersonen (Wbtr). Maar ook de bindende afspraken die de organisatie zelf heeft gemaakt met haar gemeente (financieringsafspraken bijvoorbeeld) of samenwerkingsovereenkomsten (bijv. dBos) vallen onder compliance. Daarnaast kunnen er in bepaalde sectoren ook sectorspecifieke wetten van toepassing zijn. In de bibliotheekwereld is dat bijvoorbeeld de *Wet Stelsel Openbare Bibliotheekvoorzieningen (Wsob)*.

Naast wetten en regels vallen ook verschillende codes onder compliance, als de organisatie zich daaraan direct of indirect gebonden heeft. Denk aan de *Gedragscode voor Vrijwilligers*, *Governance Code Cultuur* en de *Code Cultuursponsoring*.

INDICATOREN M.B.T. DE NORM COMPLIANCE

Aan de hand van vijf indicatoren (in de vorm van stellingen) ontstaat een eerste beeld van de manier waarop de organisatie vorm en inhoud kan geven aan de norm Compliance.

Deze indicatoren beantwoordt de organisatie met "ja" of "nee" en zij kan deze voorzien van ondersteunende documentatie.

Indicatoren geven een *inleidend beeld* over wat je als organisatie doet, hebt en welke keuzes je maakt. De indicatoren bieden *ruimte* om lokale en/of organisatie specifieke zaken toe te lichten.
In samenhang met de overige informatie ondersteunen de indicatoren de auditor uiteindelijk bij het bepalen van de score bij de beoordelings-vragen. Het is dus een misverstand te denken dat "ja" altijd een goed antwoord is en "nee" een verkeerd antwoord. Een "nee" kan immers voortkomen uit een bewuste beleidskeuze.

1.

De organisatie heeft goed inzicht in de voor haar relevante wet- en regelgeving en specifieke (branche)codes waaraan zij moet voldoen.

De auditoren willen allereerst zien dat de organisatie goed zicht heeft op de wet- en regelgeving en specifieke (branche)codes waaraan zij moet en wil voldoen. Achterin vind je een lijst met voorbeelden van wetten, regels en codes die je wat meer op weg helpen bij het bepalen van wat relevant is voor jouw organisatie. Voor de auditoren volstaat het als de organisatie een lijst heeft met een overzicht van wat voor de organisatie relevant is voor compliance. Ook overeenkomsten en beschikkingen vallen onder compliance.

2.

De organisatie heeft aantoonbaar zicht op de risico's die verbonden zijn aan het niet (kunnen) voldoen aan de voor haar relevante wet- en regelgeving en specifieke (branche)codes.

Om verschillende redenen (bijv. gebrek aan tijd, middelen of mensen) kan het zijn dat je (nog) niet voldoet aan de compliance-eisen die aan de organisatie worden gesteld. Soms kan het voorkomen dat het bevoegd gezag bij de inwerkingtreding van een wet, tijd en ruimte biedt om op een later moment wel te voldoen aan wet- en regelgeving. Als hiervan sprake is, willen de auditoren aantoonbaar bewijs dat je weet wat de gevolgen ervan zijn als je (nog) niet (kunt) voldoen aan de compliance-eisen. Het is dan ook aan te bevelen om dit aan te geven in de eerder genoemde lijst met een overzicht van relevante wet- en regelgeving en specifieke (branche)codes.

3.

De organisatie heeft (ook voor het IDO en educatieve dienstverlening / leesbevordering) een gedocumenteerde aanpak ten behoeve van de informatiebeveiliging (incl. persoonsgegevens). Ook in geval van calamiteiten.

Gezien het grote belang van informatiebeveiliging en de bescherming van privacygevoelige informatie wordt gevraagd om een gedocumenteerde aanpak op dit gebied. Jouw klanten en medewerkers moeten er immers op vertrouwen dat hun informatie in veilige handen is.

In je aanpak is beschreven hoe de organisatie op basis van risicobepaling tot concrete beheersmaatregelen voor informatiebeveiliging komt. Als er calamiteiten optreden (zoals bijv. een hack of een datalek), moet ook beschreven zijn hoe de organisatie en haar medewerkers hiermee omgaan (continuïteitsplan), ook naar de Autoriteit persoonsgegevens. Aanvullend is beschreven wat de organisatie doet om het bewustzijn van medewerkers en vrijwilligers te bevorderen en wat geregeld is in het geval dat informatiebeveiliging is uitbesteed aan derden. Jouw organisatie is en blijft daarmee (eind)verantwoordelijk. Let op: het outsourcen naar externe partijen ontslaat de organisatie niet van haar wettelijke verantwoordelijkheid op dit gebied.

4.

De organisatie laat zien (ook voor het IDO en educatieve dienstverlening/leesbevordering) op welke wijze zij omgaat met geheimhoudingsverklaringen en VOG's voor medewerkers en vrijwilligers.

De auditoren willen zien wat beleid en praktijk is op het gebied van geheimhoudingsverklaringen en VOG's. Auditoren zijn benieuwd naar de gemaakte keuzes, voor wie de geheimhoudingsverklaringen en VOG's van toepassing zijn en naar de toepassing van procedures. Auditoren kunnen steekproefsgewijs vragen naar geheimhoudingsverklaringen en VOG's.

ALLEEN VOOR LEDEN VOB

5.

De organisatie geeft invulling aan de vijf functies (conform artikel 5) en de zes activiteiten (conform artikel 8) uit de Wsob, alsmede – in het geval van POI's – aan de specifieke functies die vanuit de Wsob gesteld worden.

Tijdens de auditdag stellen de auditoren vast in hoeverre bij bibliotheekorganisaties en POI's de voor hen van toepassing zijnde functies in het dagelijkse bedrijfsbeleid aantoonbaar zijn. Voor bibliotheek-organisaties gaat het om:

- ter beschikking stellen van kennis en informatie;
- bieden van mogelijkheden tot ontwikkeling en educatie;
- bevorderen van lezen en het laten kennismaken met literatuur;
- organiseren van ontmoeting en debat;
- laten kennis maken met kunst en cultuur.

De auditoren leiden uit beleid en praktijk van de organisatie af in hoeverre deze functies feitelijk vervuld worden.

DE AUDIT

Tijdens de auditdag(en) toetsen de auditoren aan de hand van de zelfevaluatie, de geüploade documenten, de interviews en hun eigen observaties, of papier en realiteit met elkaar overeenkomen. De bevindingen en conclusies van de audit moeten antwoord geven op deze vraag: certificering ja, voorwaardelijk of nee. De verbeterpunten geven de richting aan voor verdere ontwikkeling.

De auditoren vragen naar voorbeelden of nemen steekproeven waaruit blijkt dat de organisatie voldoet aan de eisen. Afhankelijk van de organisatie leggen zij verschillende accenten bij de dienstverlening, de actualiteit van ambities en knelpunten. Voldoet jouw organisatie (nog) niet, dan moet je dit kunnen onderbouwen. Ook vernemen de auditoren graag jouw plan van aanpak om wel aan de norm te voldoen. De auditoren zullen toetsen of je je bewust bent van de gevolgen dan wel risico's van het niet voldoen.

Bij de norm Compliance zoeken de auditoren naar een vastgelegde en uitgewerkte aanpak van compliance en voeren zij steekproeven uit. De auditoren willen vast kunnen stellen dat compliance deel uitmaakt van het kwaliteitsmanagementsysteem en van de cultuur. De auditoren toetsen of je je bewust bent van compliance binnen jouw organisatie, of het onderdeel is van jouw beleid én of je proactief de vraag stelt: 'hoe willen wij in de organisatie en naar de buitenwereld toe omgaan met wetten, regels en andere afspraken en hoe dragen wij dat uit?' Compliance gaat daarmee ook over de waarden die je als organisatie hanteert.

DE BEOORDELINGSVRAGEN VOOR DE NORM COMPLIANCE

De auditoren toetsen de normen 1 tot en met 7 (zie afbeelding op pagina 1) met vier beoordelingsvragen. De auditoren scoren deze beoordelingsvragen aan de hand van de bevindingen tijdens de auditdag(en) met Niet, Beperkt, Grotendeels of Volledig.

Hieronder vind je een toelichting op de beoordelings-vragen (in de vorm van stellingen) voor de norm Compliance.

VRAAG 1

De organisatie heeft compliance als zelfstandig beleidsvraagstuk belegd en vertaald naar een organisatiebrede aanpak.

Compliance als zelfstandig beleidsvraagstuk betekent dat er volwaardig beleid is dat periodiek op de agenda van het management en bestuur/RvT staat. Er is beleid over compliance als je aantoonbaar kunt maken hoe je jouw beleid over compliance hebt geconcretiseerd in een gerichte, samenhangende aanpak en/of werkprocessen. Je hebt het als zelfstandig beleidsvraagstuk geïdentificeerd, je hebt goed in beeld waaraan je moet voldoen en kan dat met voorbeelden aantonen. De auditoren toetsen of je (de leiding) je verantwoordelijk voelt voor compliance en hoe de bevoegdheden en verantwoordelijkheden geregeld zijn.

De vertaling van compliance naar een organisatiebrede aanpak houdt in dat compliance op alle onderdelen en op alle niveaus (van directie en management tot

medewerkers en vrijwilligers) binnen de organisatie is uitgewerkt. Compliance heeft dus betrekking op alle onderdelen van de organisatie en is niet beperkt tot bijv. directie en Raad van Toezicht c.q. bestuur.
Let erop dat het ontvangen van nieuwsbrieven van de brancheorganisatie en tips van de accountant onvoldoende zijn als bewijs voor compliance als zelfstandig beleidsvraagstuk.

Documenten ter onderbouwing zijn bijvoorbeeld:

- beleid over compliance, incl. PDCA-aanpak;
- taken, bevoegdheden en verantwoordelijkheden op het gebied van compliance;
- bewustwordingscampagnes.

VRAAG 2

De organisatie toont aan dat zij voldoet aan relevante wet- en regelgeving, overeenkomsten en codes, ook bij uitbesteding aan derden.

Je kunt aantonen welke maatregelen je genomen hebt om te voldoen aan wetten, regels, codes en beschermingsafspraken en in het bijzonder dat je deze maatregelen zorgvuldig en consistent toepast.

Documenten ter onderbouwing zijn bijvoorbeeld:

- bewerkersovereenkomsten;
- privacy protocollen;
- geheimhoudingsverklaringen;
- (beleidsdocumentatie t.a.v.) VOG's
- implementatiedocumenten over bijvoorbeeld toegankelijkheidsregels en Wbtr;
- (specifieke delen uit) accountantsrapporten.

VRAAG 3

De organisatie is in control met betrekking tot de voor haar geldende wet- en regelgeving, overeenkomsten en codes.

Een organisatie is over compliance in control als zij enerzijds aantoonbaar zicht heeft op wijzigingen in wet- en regelgeving en welke bronnen zij daarbij gebruikt (bijv. door een registratie van relevante wet- en regelgeving). Anderzijds is de organisatie in control als zij met haar aanpak effectief kan inspelen op veranderingen en afwijkingen. Dit geldt ook voor het doorvoeren van herstelmaatregelen (bijv. in het geval van een datalek). Het beleggen van taken, verantwoordelijkheden en bevoegdheden over compliance onder personeelsleden en de leiding van de organisatie (directie en bestuur/RvT) maakt deel uit van zo'n aanpak.

Documenten ter onderbouwing zijn bijvoorbeeld:

- een overzicht met wet- en regelgeving en specifieke (branche)codes die van toepassing zijn;
- beheersmaatregelen, zoals een handelingsplannen n.a.v. een datalek.

VRAAG 4

De organisatie evalueert periodiek de aanpak met betrekking tot compliance en volgt zij deze zo nodig op met concrete verbetermaatregelen.

De organisatie kan aantonen dat zij niet alleen het beleid over compliance, maar ook situaties met afwijkingen en herstelmaatregelen periodiek evalueert.

Wanneer je wel in beeld hebt waaraan jouw organisatie moet voldoen, maar er nog niet feitelijk aan voldoet, moet je dit ook kunnen verklaren. Bovendien willen de auditoren horen wat je plan van aanpak is om er wel aan te voldoen. De auditoren zullen toetsen of je je bewust bent en op de hoogte bent van de (aanvaardbare en niet aanvaardbare) risico's als je er niet aan voldoet.

Documenten ter onderbouwing zijn bijvoorbeeld:
- evaluaties
- verbetermaatregelen
- plannen van aanpak

OVERZICHT WET- EN REGELGEVING EN SPECIFIEKE (BRANCHE)CODES

Hieronder vind je een overzicht van de belangrijkste wet- en regelgeving en specifieke (branche)codes. Deze opsomming is een handreiking, geen uitputtende lijst. Niet alles uit deze lijst is altijd of geheel van toepassing, dat kan per organisatie verschillen. Laat dit goed nagaan door je interne of externe jurist.

- subsidiebeschikking(en), incl. de onderliggende voorwaarden tot verlening van subsidie tussen gemeente/provincie en auditee;
- Wet bestuur en toezicht rechtspersonen (Wbtr);
- cao's Openbare Bibliotheken en Kunsteducatie (algemeen verbindend verklaard);
- Arbeidsomstandighedenwet (denk met name aan RI&E);
- Wet stelsel openbare bibliotheekvoorzieningen (Wsob) incl. de Regeling Gegevenslevering openbare bibliotheekvoorzieningen (alleen van toepassing voor bibliotheken en POI's);
- Wet werk en zekerheid (Arbeidsrecht/boek 7 titel 10 BW);
- Algemene Verordening Gegevensbescherming (AVG) en Uitvoeringswet AVG (van af 25 mei 2018)
- VN-verdrag inzake de rechten van personen met een handicap (gaat over eisen over toegankelijkheid), van toepassing sinds 2016;
- governance Code Cultuur;
- fair practice code cultuur 2.0;
- bij Financiële wet- en regelgeving: check op controle/verklaring door een externe accountant van de jaarrekening en de opstelling van een managementletter;
- fiscale regelgeving: is binnen of buiten de organisatie belegd dat de aangescherpte Vpb-regels en – indien van toepassing – de aangescherpte regels over het behoud van de ANBI-status – gevolgd worden?;
- bij aangaan van arbeidsrelatie: Verklaring omtrent gedrag (VOG);
- bij aangaan van vrijwilligersrelatie: afsluiten van vrijwilligersovereenkomst, incl. bepalingen over af te sluiten verzekeringen.

OVERIGE RELEVANTE REGELS, WETTEN EN CODES

- Wet werk en zekerheid
- Ziektewet
- Wet verbetering Poortwachter
- Diverse codes m.b.t. vrijwilligers, diversiteit (Code Diversiteit & Inclusie), duurzaamheid etc.
- Wet op de Ondernemingsraden
- Telecommunicatiewet (Tw) (i.v.m. cookiewet en spamverbod)
- Code voor Informatiebeveiliging (ISO 27001 en ISO 27002)
- Wet Open Overheid (WOO)