DUIJNBORGH CERTIFICATION®

Duijnborgh Certification B.V.

Audit proces

DUIJNBORGH CERTIFICATION®

Inhoudsopgave

1 Doel

In dit document is het audit proces als onderdeel van het gehele certificeringtraject beschreven.

2 Auditproces

2.1 Overzicht van het beoordelingsproces

Het beoordelingsproces kan worden opgedeeld in de volgende elementen:

1. beoordeling van het systeemontwerp en de definitie;
2. beoordeling van zelfbestuur m.b.t. het systeem (management verplichting);
3. planning van het implementatiebezoek;
4. beoordeling van de systeemimplementatie.

2.1.1 Algemeen

2.1.1.1 Tijdens openingsbijeenkomst

Elke audit op locatie van de klant wordt geopend met een formele bijeenkomst. Er worden een aantal vaste onderwerpen besproken. De diepgang per onderwerp wordt door de audit teamleider bepaald o.b.v. de kennis en bekendheid van het certificatietraject van de klant.

2.1.1.2 Verzamelen van objectief bewijs

Een combinatie van onderstaande methoden zal gebruikt worden om informatie en conformiteit tegen de doelstellingen, reikwijdte en criteria aan te tonen:

a) interviews;

b) observaties van processen en activiteiten;

c) beoordeling van documenten en registraties.

2.1.1.3 Identificeren en vastleggen van auditbevindingen

Audit evidence wordt in het dossier worden opgenomen als deze (mogelijke) MiNC's en MaNC's onderbouwen. Het wordt vernietigd als de tekortkoming is opgelost.

Mogelijkheden tot verbeteren kunnen worden geïdentificeerd en in het auditrapport worden opgenomen. Tekortkomingen worden niet als mogelijkheid tot verbeteren worden geclassificeerd. Het is de auditor niet toegestaan om de oorzaak of de oplossing voor een tekortkoming aan te dragen.

2.1.2 Presenteren bevindingen

2.1.2.1 Voor de afsluit bijeenkomst

Het auditresultaat en de bevindingen (o.a. tekortkomingen) worden middels een afsluit bijeenkomst naar de klant gecommuniceerd. Hiervoor zal het auditteam:

a. de bevindingen tegen de reikwijdte, criteria en auditdoelstellingen vergelijken (conformiteit versus non-conformiteit) en de tekortkomingen classificeren;
b. de auditconclusie bepalen;
c. opvolg acties bepalen;
d. een gepast audit programma bepalen o.b.v. de bevindingen, maar ook in het licht van de frequentie van de surveillance audits en de competenties van het auditteam.

2.1.2.2 Tijdens afsluit bijeenkomst

Tijdens de afsluitbijeenkomst worden de hiervoor genoemde onderwerpen besproken met het management van de klant. Eventuele meningsverschillen of verschillen van inzicht tussen het auditteam en de klant die niet kunnen worden opgelost, worden geregistreerd.

2.2 Initiële certificatie

Het initiële beoordelingproces van het te certificeren managementsysteem bestaat uit twee (2) fasen.

2.2.1 Fase 1 beoordeling

Tijdens Fase 1 worden de volgende elementen beoordeeld c.q. uitgevoerd:

- Er wordt een onderzoek uitgevoerd naar de opzet van het gedocumenteerde systeem om te controleren of het gedocumenteerde managementsysteem voldoet aan de gestelde eisen en vastgestelde audit reikwijdte (scope). Tevens dient inzicht in geldende wet- en regelgeving te worden verkregen;
- Er wordt beoordeeld of voldoende registraties aanwezig zijn voor verificatie van implementatie voor fase2;
- Er wordt een kort gesprek met (top) management gevoerd om inzicht te krijgen in de reden voor certificering, kennis van de eisen uit de norm(en), organisatiebeleid, doelstellingen, interne audits, risico analyses, directiebeoordeling, missie en visie van de organisatie, management verantwoordelijkheden en verbintenis (commitment). Het gesprek kan, indien gewenst, via moderne communicatietechnologieën worden gevoerd, zoals video-conferencing en Social Media;
- Een deskresearch, om inzicht te krijgen in de actuele situatie van de klant, zijn processen, niveaus van de vastgestelde maatregelen en gebruikte bedrijfsmiddelen en het verifiëren of definiëren van de uiteindelijke reikwijdte (scope) van de certificering. Ook is het van belang dat inzicht wordt verkregen in de reden voor certificering, kennis van de eisen uit de norm(en), organisatiebeleid, doelstellingen, interne audits, risico analyses, directiebeoordeling, missie en visie van de organisatie, management verantwoordelijkheden en verbintenis (commitment);
- Controle van de contractgegevens:
    - ‘kern’ processen, organisatiegegevens, opgegeven reikwijdte, uitsluitingen, organisatiecodes, klopt de audit tijdberekening op basis van locatiebezoek;
- Vaststelling of de organisatie klaar is voor de fase 2 beoordeling. Hiertoe moet worden vastgesteld dat de interne audits en een management review zijn gepland en worden uitgevoerd en dat het managementsysteem in voldoende mate is geïmplementeerd;
- Informeer de klant over de benodigde informatie tijdens fase 2 beoordeling.

Na de Fase 1 beoordeling worden de volgende aspecten gedocumenteerd in het dossier:

- Effectieve audit tijdbesteding op basis van audit tijdsberekening methode en inzicht tijdens Fase 1;
- Tijdelijke planning van Fase 2 audit (< 3 maanden) met daarin verwerkt de hoog risico aspecten van de organisatie (o.a. uitbesteden activiteiten);
- Een definitieve reikwijdte bepaling waartegen de implementatieaudit (Fase 2) wordt uitgevoerd;
- Een onderbouwing van de steekproef in het geval van ‘meerdere vestigingen’.

Dit is afhankelijk van de grote van de organisatie, locatie(s), risico’s en ervaringen binnen het activiteitengebied. De lead-auditor is er voor verantwoordelijk dat alle in de ISO 17021 genoemde doelstellingen worden bereikt.

De uitkomst van een fase 1 beoordeling wordt niet in termen van MiNC en MaNC gerapporteerd. Wel wordt een indicatie gegeven wat de tekortkoming in fase 2 voor gevolgen heeft. Het voordeel van deze aanpak is, dat tekortkomingen niet direct op de tekortkomingenlijst terechtkomen. Het rapport achter de initiële certificatie en de driejaarlijkse beoordeling zijn daarmee beter toonbaar aan de belangengroepen van de klant. Het fase 1 rapport hoeft niet noodzakelijkerwijze te voldoen aan alle eisen van een auditrapport.

2.2.1.1 ISMS specifiek

Tijdens een Fase 1 ISMS audit dienen de volgende aspecten mimimaal te worden getoetst:

- Een duidelijk overzicht van de processen van het ISMS om te kunnen voldoen aan de eisen van de norm;

- Zijn de documenten uit ISO/IEC 27001 §4.3.1. inzichtelijk (+ Annex relevante documenten);
- De gekozen risicobeoordeling, maatregelen en Verklaring van Toepasselijkheid;
- Beheersing van uitbesteedde activiteiten.

2.2.2 Tijd tussen Fase 1 en Fase 2 beoordeling

Bij voorkeur vindt de Fase 2 beoordeling tussen de 6 weken en 3 maanden na de Fase 1 beoordeling plaats. Korter dan 6 weken kan leiden tot het risico dat eventuele bevindingen niet correct en volledig zijn doorgevoerd en langer dan 3 maanden heeft het risico dat het managementsysteem wijzigt t.o.v. de initiële beoordeling. Uiteindelijk bepaalt de klant de omvang van de tussenliggende periode.

Indien Fase 2 tussen 3 en 6 maanden na de Fase 1 beoordeling wordt uitgevoerd, zal er een extra verificatie worden uitgevoerd om te controleren dat eventuele wijzigingen aan het managementsysteem en/of de organisatie invloed hebben op de Fase 2 planning en contract samenstelling. Na 6 maanden dient er een nieuwe Fase 1 te worden uitgevoerd.

Vanuit de technische review wordt uiteindelijk bepaald of de fase 2 beoordeling volgens de planning zal worden uitgevoerd. De tijdelijke planning zal definitief worden. Indien de fase 2 beoordeling niet volgens de tijdelijk afgesproken planning zal plaatsvinden, wordt de toekomstig planning met de klant overlegd.

Een fase 2 beoordeling kan alleen worden uitgevoerd als de klant een interne audit heeft uitgevoerd over het volledige managementsysteem, inclusief de Annex A maatregelen. Bovendien moet het management een directiebeoordeling hebben uitgevoerd. Hierdoor kan de fase 2 beoordeling in theorie geen bijzonderheden voor het management opleveren.

2.2.3 Fase 2 beoordeling

Tijdens de Fase 2 wordt beoordeeld of het managementsysteem voldoet aan de certificatie-eisen binnen de reikwijdte (scope). Hierbij dienen uitsluitend de criteria te worden toegepast die volgen uit de gehanteerde norm ISO27001 inclusief Annex A of andere normatieve documenten. Dit houdt nadrukkelijk in dat geen andere documentatie, en/of best practices (zoals de ISO27002) mogen worden toegepast. De beoordeling vindt plaats op de locatie(s) van de klant.

Indien delen van het managementsysteem tijdens Fase 1 voldeden aan de certificeringeisen en als effectief zijn getoetst, kunnen deze delen tijdens Fase 2 buiten beschouwing worden gehouden mits:

1. Er een duidelijke verwijzing is naar conformiteit tijdens Fase 1;
2. Conformiteit tegen de eisen nog steeds aantoonbaar is;
3. Zich geen grote wijzigingen hebben voorgedaan die van invloed zijn op dat deel van het managementsysteem.

De Fase 2 beoordeling wordt uitgevoerd volgens de vastgestelde auditplanning (Fase 1). Indien hiervan wordt afgeweken dient dit gemotiveerd te worden en de planning dient te worden aangepast.

Na een Fase 2 beoordeling dienen de volgende aspecten opgeleverd te worden:

- Een auditrapportage;
- Overeenstemming over de gevonden bevindingen en methode van aanpak;
- Vervolgbezoek (tussentijds, hercertificering of speciaal opvolgingsbezoek).

De grote tekortkomingen (MaNC) moeten binnen een periode van 6 maanden na de laatste dag van fase 2 zijn geïmplementeerd en opgelost, anders moet opnieuw een fase 2 worden uitgevoerd voordat de organisatie voor certificatie mag worden voorgedragen.

2.2.3.1 ISMS specifiek

Tijdens een Fase 2 ISMS audit worden de volgende aspecten getoetst:

- Het leiderschap van het management, de betrokkenheid bij het informatiebeveiligingsbeleid en de informatiebeveiligingsdoelstellingen;
- Uitvoer en reproduceerbaarheid van de risicobeoordeling;
- Gedocumenteerde eisen uit ISO/IEC 27001 §4.3.1;

- De beheersdoelstellingen en beheerscontrolemaatregelen op basis van de risicobeoordeling en risicobeheersplan;
- Effectiviteitbepaling ISMS en effectiviteitmetingen beheerscontrolemaatregelen in lijn met de ISMS doelstellingen;
- Interne ISMS audits en Directiebeoordeling;
- Directie verantwoordelijkheid voor het ISMS beleid;
- Samenhang tussen beheerscontrolemaatregelen – Toepasselijkheidverklaring – risicobeoordeling – ISMS beleid / doelstellingen;
- Implementatie beheerscontrolemaatregelen (ISO/IEC 27001, Annex A) (effectiviteitmetingen en behalen doelstellingen);
- Aantoonbaarheid van directiebeslissingen en koppeling met ISMS beleid en doelstellingen;
- De geschiktheid van het managementsysteem en zijn prestaties opdat wordt voldaan aan de statutaire en contractuele eisen en van toepassing zijnde wet- en regelgeving.

2.3 Evaluatiebeoordeling

Tijdens een opvolgbezoek wordt het volgende beoordeeld:

- De effectiviteit van het ISMS in relatie tot het bereiken van de doelstellingen van het informatiebeveiligingsbeleid;
- Het functioneren van procedures voor de periodieke beoordeling en review van de naleving met relevante informatiebeveiligingswet- en regelgeving;
- Wijziging van de bepaalde maatregelen en wijziging van de verklaring van toepasselijkheid;
- Implementatie en effectiviteit van maatregelen volgens het auditprogramma;
- Het managementsysteem nog voldoet aan de eisen en verwachtingen van de certificatie belanghebbenden;
- Het managementsysteem in staat is om continu te verbeteren;
- Zich organisatorische of managementsysteem wijzigingen hebben voorgedaan en deze correct in het managementsysteem zijn doorgevoerd of contractuele aanpassingen nodig zijn (o.a. reikwijdte bepaling);
- Het managementsysteem nog voldoet aan de certificatie-eisen.

De frequentie van de opvolgbezoeken is jaarlijks (12 maanden). De eerste surveillance beoordeling na de initiële audit moet binnen 12 maanden na de afsluitbijeenkomst van de initiële audit worden uitgevoerd. Er mag frequenter dan jaarlijks worden geaudit. De frequentie heeft geen invloed op het aantal bepaalde auditdagen voor een geheel certificeringtraject (3 jaar).

Evaluatiebezoeken worden in beginsel op locatie uitgevoerd. Delen van de audit kunnen, indien gewenst, via moderne communicatietechnologieën worden gevoerd, zoals video-conferencing en Social Media.

2.3.1 Planning

Een auditplanning voor een opvolgbezoek wordt bij voorkeur tijdens het bezoek vastgesteld en opgenomen in de rapportage. De planning bevat minimaal toetsing van de volgende aspecten om de effectiviteit van het managementsysteem aan te tonen (zie ook 4.4.1):

- Interne audits en managementreview;
- Een review van acties die zijn uitgevoerd ter oplossing van tekortkomingen die tijdens eerder uitgevoerde audits zijn geconstateerd;
- Behandeling van klachten;
- Effectiviteit van het managementsysteem ten aanzien van het bereiken van de doelstellingen en verwachte resultaten van het managementsysteem;
- Voortgang in de geplande activiteiten gericht op continu verbeteren;
- Doorlopende operationele beheersing;
- Review van wijzigingen;

- Gebruik van logo's en andere referenties naar de certificatie.

2.4 Driejaarlijkse evaluatiebeoordeling

Een certificatieperiode is geldig voor 3 jaar. Binnen 3 jaar na de initiële certificatiebeslissing dient het gehele managementsysteem, onder de reikwijdte van het certificaat, te worden beoordeeld op conformiteit.

De hercertificatie moet tijdig worden gepland en uitgevoerd, opdat het certificaat vernieuwd kan worden voordat het verloopt. Ook eventueel geconstateerde grote tekortkomingen (MaNC) moeten de correctieve en corrigerende acties zijn geïmplementeerd en geverifieerd voordat het certificaat verloopt. Als dit niet mogelijk blijkt, zal het certificaat niet worden verlengd, totdat verificatie heeft plaatsgevonden. Als dat binnen 6 maanden na het verlopen van het certificaat nog niet is gebeurd, moet op zijn minst een fase 2 worden uitgevoerd. In alle gevallen blijft de verloopdatum van het nieuwe certificaat gehandhaafd op die van de voorgaande + 3 jaar. De effectieve datum wordt gelijk gesteld aan de datum van de certificatiebeslissing. De klant wordt op de hoogte gesteld van de gevolgen van een niet valide certificaat.

Tijdens de driejaarlijkse evaluatie worden de volgende aspecten beoordeeld:

- Zijn alle (kritische) processen onder de reikwijdte van de certificatie c.q. beoordeling conform de normeisen, het organisatiebeleid, de relevante wet- en regelgeving en de contractuele verplichtingen;
- Functioneert het managementsysteem effectief, ook na veranderingen.

Voor het beoordelen van het functioneren worden de volgende acties uitgevoerd:

1. Er wordt een summiere documentbeoordeling uitgevoerd om te toetsen of het gedocumenteerde systeem nog in lijn is met de activiteiten onder de reikwijdte van het managementsysteem;
2. Op basis van een review van de rapportages van de eerdere surveillanceaudits en de prestaties van het managementsysteem gedurende de meest recente certificatiecyclus wordt gekeken naar de gevonden tekortkomingen en overige trends om inzicht te krijgen in het functioneren van het managementsysteem;
3. Een gesprek met het (top)management met de volgende onderwerpen:
    a. Review: De sterke en zwakte punten van het managementsysteem (zie 2) en de ervaringen betreffende het systeem en de audits;
    b. Preview: Welke toekomstige ontwikkelingen verwacht de klant op het gebied van organisatie, marktontwikkeling, managementsysteem, wet- en regelgeving en beleidsvoering;
    c. Planning: Bespreek hoe Duijnborgh Certification de organisatie kan bijstaan in het (toekomstige) beleid;
4. Controle of alle contractgegevens nog actueel zijn en eventueel het contract aanpassen. Bij de controle dient een nieuw 'Certificatie aanvraagformulier' te worden ingevuld;
5. Er wordt een certificatieplanning opgesteld voor de driejaarlijkse beoordeling. Indien op basis van de beoordeling significante wijzigingen zijn opgetreden binnen de organisatie, het managementsysteem of belangrijke processen (activiteiten, wet- en regelgeving) dan kan een aanvullende fase 1 beoordeling worden overwogen. De audittijd neemt in dat geval toe (1/3 van de mandagen voor de initiële audit).

2.4.1 Evaluatieplanning

Een evaluatiebeoordeling programma bevat de volgende aandachtspunten:

- De evaluatie en onderhoud van het managementsysteem (directiebeoordelingen, interne audits, corrigerende en preventieve maatregelen, klachten);
- De effectiviteit van het managementsysteem om de doelstellingen vanuit het beleid te halen;
- De effectiviteit van het managementsysteem voor identificatie, evaluatie en opvolging van relevante wet- en regelgeving en andere eisen van belanghebbenden;
- Het juiste gebruik van logo's en certificatie;
- Communicatie en registraties betreffende belanghebbenden;
- Wijzigen betreffende documentatie, managementsysteem en/of organisatieactiviteiten;

- Geselecteerde elementen vanuit de norm(en) (binnen de 3-jaarlijkse evaluatiecyclus dienen alle norm elementen minimaal eenmaal te zijn beoordeeld);
- Opvolging van voormalige auditbevindingen;
- (optioneel) gemelde klachten betreffende de organisatie bij Duijnborgh Certification.

2.5 Speciale bezoeken

2.5.1 Uitbreiding van de reikwijdte en belangrijke wijzigingen

In het geval dat zich grote wijzigingen voordoen of dat de klant verzoekt om uitbreiding van de reikwijdte, moet op basis van een review worden vastgesteld of een tussentijdse audit moet plaatsvinden om te bepalen of de uitbreiding mag worden goedgekeurd respectievelijk de wijzigingen de effectiviteit van het managementsysteem zodanig beïnvloeden dat de doelstellingen niet meer worden gerealiseerd. Een dergelijke audit mag samenvallen met een surveillanceaudit. De audittijd van een aanvullende audit bij uitbreiding van de reikwijdte en belangrijke wijzigingen mag worden gecompenseerd met de audittijd voor surveillance audits. Mocht die al zijn opgesoupeerd, dan kan een vervroegde hercertificatie worden overwogen.

Een gevolg van de wijziging en de uitbreiding van de reikwijdte kan zijn dat de mandagen moeten worden aangepast. Dat heeft wel gevolgen voor de audittijd van de tussentijdse audit en nog komende surveillance en hercertificatieaudits.

Bij zeer complexe en omvangrijke uitbreidingen van de reikwijdte en wijzigingen kan een fase 1 worden overwogen. De audittijd die daarmee gemoeid is (1/3 van de mandagen voor een initiële audit) wordt niet gecompenseerd met de audittijd voor surveillance audits.

2.5.2 Overname certificaat

In het voorkomende geval dat een certificaat wordt overgenomen van een collega certificerende instelling, zal de audit worden uitgevoerd volgens de procedure ‘Overname van certificaat’.

2.5.3 Speciale opvolgbezoeken

Speciale opvolgbezoeken worden uitgevoerd als extra tijd naast de audittijd berekening op basis van een 3-jarige certificatiecyclus, indien tijdens een audit een grote tekortkoming op het managementsysteem is geconstateerd. Een speciaal opvolgingsbezoek is gelijk aan een normaal opvolgbezoek met de volgende uitzonderingen:

- Evalueer de aspecten m.b.t. de gevonden grote afwijking en verifieer dat de klant de juiste corrigerende maatregelen heeft getroffen op basis van een risicoanalyse en de effectiviteit van de maatregelen heeft getoetst. Dit alles dient aantoonbaar te zijn. De klant is verantwoordelijk om de effectiviteit te bepalen, niet de auditor.
- Informeer de klant over de mogelijke gevolgen van een speciaal opvolgingsbezoek indien de grote tekortkoming onvoldoende is opgepakt. Namelijk opschorting of inname van het certificaat;
- Rapportage betreffende speciale opvolgbezoeken worden altijd via een technische review gecontroleerd. Voor wat betreft rapportage kan worden volstaan met de invulling van de bevindingen in het meest recente rapport. Er hoeft dus geen apart rapport te worden opgemaakt.

Voor sommige audits kan gebruik worden gemaakt van locatiebezoeken die zeer kort voor de uitvoering worden aangekondigd zelfs wat datum betreft niet worden aangekondigd. Het gaat dan om audits die ten doel hebben klachten te onderzoeken, wijzigingen te wegen of de situatie van een certificaatschorsing te onderzoeken. Voordat hiervan gebruik wordt gemaakt moet de klant op de hoogte zijn gesteld van de voorwaarden waaronder dergelijke audits worden uitgevoerd. Omdat de klant weinig tot geen tijd heeft om bezwaar te maken tegen leden van het auditteam, moet extra zorg worden besteed aan het toewijzen van auditors.

2.6 Wijzigingen

Indien zich wijzigingen voordoen die van invloed zijn op de contractsamenstelling, de reikwijdte van het managementsysteem (scope) of de organisatorische samenstelling dient de auditor hiervan melding te maken in het rapport en de consequenties in te schatten. Wijzigingen worden met de klant besproken.