Nederlands Certificatie Instituut

Certificeren zoals het hoort!

Algemene informatie
ISO 27001

ISO 27001 CERTIFICAAT

Algemene informatie ISO 27001 0134
versie 01.1 26-04-2019

Obalaan 8
3233 BL Oostvoorne
info@nci-bv.nl
(+31) 181 – 481949
www.nci-bv.nl
KVK: 24338796
IBAN:NL61 ABNA 0610 4718 72

Inleiding

In deze algemene informatie leggen we u uit wat de ISO 27001 norm inhoudt en wat u moet doen om deze norm te behalen.

De ISO 27001 norm is een kwaliteitsnorm. Uw organisatie dient volgens gestelde richtlijnen te werken om deze certificering te behalen. De norm heeft betrekking op informatiebeveiliging.

Inhoudsopgave

1. ISO 27001 cyclus

In onderstaande tabel vindt u de cyclus van de ISO 27001. Uw ISO 27001 certificaat is drie jaar geldig.

2. Wat kunt u verwachten?

Voordat uw certificatie-audit plaatsvindt, moet u drie maanden volgens de ISO 27001 werken. Dit noemen we de implementatie fase.

2.1 Ontvangst certificaat

Wanneer u de audit in het eerste jaar positief afrondt, ontvangt u het certificaat. Uw ISO 27001 certificaat is drie jaar geldig. Uw certificaat zal aangemeld worden op de website van NCI (www.nci-bv.nl). Na het derde jaar begint de auditcyclus opnieuw, dan met een hercertificatie-audit.

2.2 Inplannen hercertificatie-audit

Uw hercertificatie-audit plannen we drie maanden voor de verloopdatum van uw huidige certificaat in. Dit stelt u in de gelegenheid om eventuele vastgestelde afwijkingen in het managementsysteem op te lossen voor de verloopdatum van uw certificaat. Wanneer u besluit de audit korter te laten plaatsvinden op de vervaldatum dan is dit op eigen risico. De opvolgende twee controle-audits vinden een ongeveer een jaar later plaats.

Voorafgaand aan de audit ontvangt u van ons een e-mail met daarin de audit datum en de benodigde documenten die u dient toe te sturen voorafgaand aan de audit. Bij de ISO 27001 kunt u hierbij denken aan het KvK-uittreksel, interne audit verslagen, directiebeoordeling en de klachtenprocedure.

2.3 Aanwezigheid adviesbureau

De aanwezigheid van een (extern veiligheids-) adviseur is tijdens de audit toegestaan mits de gecertificeerde organisatie zorgdraagt dat de rol van de adviseur beperkt blijft tot toezien.

2.4 Klachten over een gecertificeerde organisatie

Klachten die in relatie staan met de eisen voor de certificatie worden door de gecertificeerde organisatie geregistreerd. De gecertificeerde organisatie zal al het mogelijke te doen om escalatie van het onderwerp van de klacht en herhaling te voorkomen. De gecertificeerde organisatie zal klachten op een zo kort mogelijke termijn adequaat afhandelen. De registratie hiervan zal bij iedere audit door de auditor van NCI worden ingezien.

Wanneer een klacht bij NCI wordt ingediend die betrekking heeft op het managementsysteem van de gecertificeerde organisatie, wordt deze door NCI beoordeeld, indien nodig nader onderzocht en aan de gecertificeerde organisatie medegedeeld. De beoordeling en/of het onderzoek hiervan kunnen leiden tot een bijkomend onderzoek, tot schorsing of tot intrekken van het certificaat.

NCI kan niet aansprakelijk gesteld worden voor schade aan door de gecertificeerde organisatie geleverde producten en/of diensten van welke aard dan ook.

2.5 Monitoring auditor

De Raad voor Accreditatie verlangt van NCI dat er periodiek monitoringen plaatsvinden. Deze monitoringen kunnen zowel uitgevoerd worden door auditoren van NCI als de Raad van Accreditatie. De waarnemers behoren niet tot het auditteam en kunnen de audit niet beïnvloeden. Om monitoringen mogelijk te maken verwacht de Raad voor Accreditatie en NCI medewerking van de gecertificeerde organisatie.

3. (Schriftelijk) bijkomend onderzoek

Wanneer de auditor tijdens de audit één of meerdere afwijkingen vaststelt, zal er een (schriftelijk) bijkomend onderzoek (SBO of BO) starten. Dit is afhankelijk van het soort afwijking dat de auditor uitschrijft. Afwijkingen bij de ISO 27001 norm zijn 'major' of 'minor'.

- Een major afwijking is een tekortkoming die direct negatief effect op de kwaliteit van het eindproduct heeft, dan wel het niet voldoen aan een strikte eis van de norm.
- Een minor afwijking is een tekortkoming die op termijn een negatief effect kan hebben op de kwaliteit van het eindproduct, dan wel onvoldoende implementatie van een eis volgens de norm.

De auditor kan ook een opmerking uitschrijven. Een opmerking is een onderwerp waarvoor het auditteam van het bedrijf aandacht vraagt, ter verbetering van het systeem, zonder dat dit onderwerp een negatief effect heeft op de kwaliteit van het eindproduct.

3.1 Ontvangst tekortkomingenformulier

Indien er tekortkomingen zijn geconstateerd, ontvangt u tijdens de audit formulieren met hierop de geconstateerde tekortkomingen.

3.2 Tekortkomingen oplossen

In het tekortkomingrenformulier beschrijft u de oorzaak, omvang en oplossingsrichting van de tekortkoming(en). Volgens de norm dient u de tekortkomingen uiterlijk drie maanden na de audit aantoonbaar gecorrigeerd te hebben, anders wordt er een 2e (S)BO uitgeschreven.

3.3 Beoordeling

SBO: De auditor zal de door u aangeleverde bewijsvoering beoordelen en bij een positieve beoordeling tenslotte de tekortkoming opheffen.
BO: De auditor komt de implementatie van de corrigerende maatregelen ter plaatse verifiëren en bij een positieve beoordeling tenslotte de tekortkoming opheffen.

3.4 Rapport

De auditor zal het tekortkomingenformulier als rapport opstellen en ter beoordeling neerleggen bij één van onze reviewers. Zodra het rapport door zowel de auditor als de reviewer als positief is beoordeeld, ontvangt u van ons per e-mail het rapport en daarmee de definitieve beslissing.

4. Certificaat

4.1 Verstrekking van het certificaat

Na goedkeuring van het rapport zullen wij bij een (her)certificering uw certificaat opstellen. U ontvangt een scan van het certificaat per e-mail. Het originele certificaat, dat drie jaar geldig is, sturen wij per post naar u toe. Bij een 1e of 2e controle audit ontvangt u geen nieuw certificaat, maar mag u met uw certificaat trots naar buiten blijven treden als gecertificeerd bedrijf.

4.2 Schorsen van het certificaat

Bij het niet tijdig kunnen oplossen van de tekortkoming of het niet tijdige kunnen uitvoeren van de controle-audit is NCI verplicht het certificaat te schorsen. Ingeval van schorsing is het certificaat tijdelijk ongeldig. NCI informeert schriftelijk de voorwaarden waaraan voldaan moet worden om de schorsing op te heffen en geeft aan dat er niet meer naar buiten getreden mag worden als gecertificeerd bedrijf. Daarnaast maakt NCI op haar website bekend dat het certificaat geschorst is.

4.3 Intrekken van het certificaat

Er zijn een aantal situaties waarin NCI het recht heeft het certificaat in te trekken, namelijk:

- er wordt niet voldaan aan de geldende eisen op het moment van de audit en er geen vertrouwen is dat adequaat corrigerende maatregelen worden genomen
- corrigerende maatregelen worden niet aantoonbaar ingevoerd
- een negatieve eindbeslissing door de directie van NCI
- er niet wordt voldaan aan de tussentijds aangepaste eisen.
- de verplichtingen voortkomend uit de certificatie overeenkomst niet worden nagekomen
- het onjuist blijven voeren van het certificaat en/of beeldmerk.
- bij het niet nakomen van financiële verplichtingen aan NCI.
- als de organisatie voor meer dan 6 maanden stopt met het leveren van de producten, processen en/of diensten die zijn opgenomen in de scope (het werkterrein) van het certificaat
- bij klachten als omschreven in hoofdstuk 2.4.

Intrekken van het certificaat wordt door NCI schriftelijk meegedeeld en gaat 30 dagen na de dag van verzenden van het bericht in, tenzij anders vermeld.

4.4 Nietig verklaren van het certificaat

Een certificaat wordt nietig verklaard als een opdrachtgever gedurende de certificatieperiode de certificatieovereenkomst schriftelijk opzegt dan wel schriftelijk aangeeft geen prijs meer te stellen op het certificaat.

5. Bijzonder onderzoek

NCI kan om verschillende redenen de gecertificeerde organisatie tussentijds geheel of gedeeltelijk auditen. NCI informeert vooraf over de reden en eventuele kosten voor het uitvoeren van het bijzonder onderzoek.
Een bijzonder onderzoek kan worden overwogen wanneer:

- er een ernstig incident en/of overtreding van de regelgeving is gemeld
- om klachten te bestuderen
- naar aanleiding van veranderingen
- bij wijze van follow-up bij opgeschorte klanten

Een bijzonder onderzoek hoeft niet altijd op locatie van de gecertificeerde organisatie te worden uitgevoerd. Dit kan in sommige gevallen ook door het opvragen van relevante informatie om tot een oordeel te komen. Van het bijzonder onderzoek wordt een rapportage gemaakt met daarin de uitkomsten. De uitkomsten van dit onderzoek kunnen van invloed zijn op de status van het certificaat.

Tot slot

Er zijn meerdere sectoren waarin wij u kunnen certificeren. U kunt op de website van de Raad voor Accreditatie (www.rva.nl) zien of u door ons gecertificeerd kunt worden. Mocht u hier vragen over hebben dan kunt u contact met ons opnemen.

Zodra u gecertificeerd bent, heeft u het recht om de bijbehorende logo's te voeren. We verwijzen u hiervoor graag naar de meegestuurde ‘Procedure voor toepassen van logo's’.

Niet tevreden?

Wanneer u niet tevreden bent over onze dienstverlening of één van onze medewerkers, dan kunt u uiteraard ook contact met ons opnemen. Wij helpen u hier graag mee. Elke klacht of beroep wordt vertrouwelijk behandeld met betrekking tot degene die de klacht indient en het onderwerp van de klacht. Voor meer uitleg over onze klachtenprocedure verwijzen wij u naar de Procedure Klachten en Beroep NCI op onze website.

Wij hopen u hiermee voldoende geïnformeerd te hebben. Mocht u nog vragen hebben dan kunt u altijd contact met ons opnemen:

E-mail: info@nci-bv.nl
Telefoon: 0181-481949

BIJLAGE
Definities en afkortingen

Bijlage: Definities en afkortingen

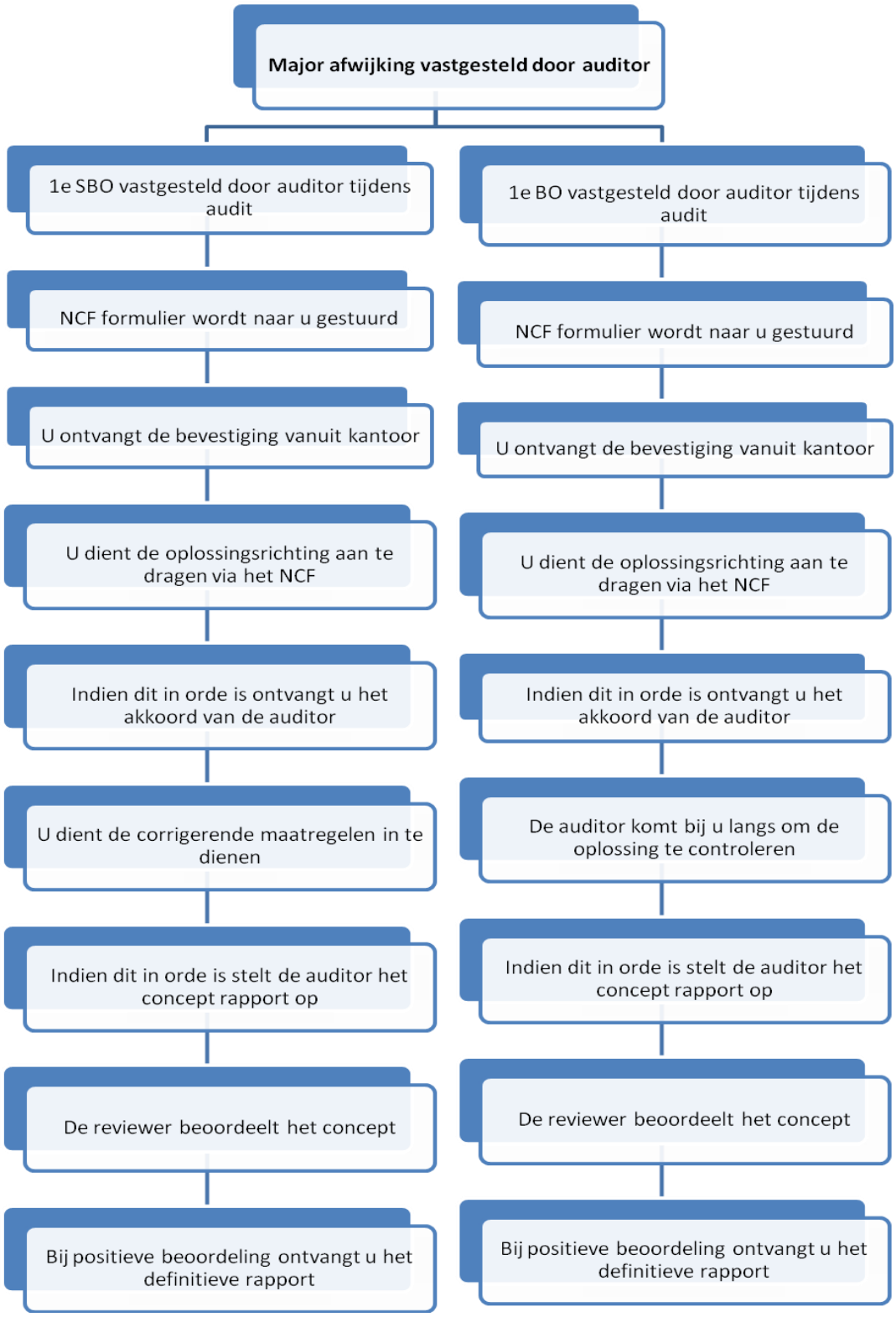
Organisatie	
RvA	Raad voor Accreditatie
NCI	Nederlands Certificatie Instituut B.V.
BO	Bijkomend Onderzoek
SBO	Schriftelijk Bijkomend Onderzoek
Certificatiepersoneel	Alle personeel dat werkzaamheden verricht binnen de organisatie van NCI
Audit	Het geheel van activiteiten vanaf planning t/m rapportage van de beoordeling van een managementsysteem tegen een vooraf overeengekomen norm.
Organisatie	Bedrijf of instelling dat/die een aanvraag doet of heeft gedaan voor certificatie, dan wel een contract hiervoor is aangegaan met NCI.
Reviewer	is verantwoordelijk voor het vaststellen of het managementsysteem van een organisatie certificatiewaardig is en is verantwoordelijk voor alle beslissingen binnen het auditproces om de informatie te verkrijgen op grond waarvan een uitspraak gedaan kan worden over de certificatiewaardigheid van het systeem.
ISO 27001-auditor	De persoon die namens NCI de beoordeling van de organisatie uitvoert
Lead-auditor	De persoon die de verantwoordelijkheid heeft voor een auditteam (meerdere auditors bij één audit)
Auditprogramma	Overzicht van te bezoeken vestigingen met te interviewen functies en per functie de onderwerpen uit de ISO 27001 norm die aan de orde worden gesteld.
Auditplan	Een beschrijving van de activiteiten en voorzieningen voor een audit. (tijdschema voor het uitvoeren van een audit, waarin opgenomen de te bezoeken vestigingen met te interviewen functies en , aangegeven per functie welke onderwerpen van de betrokken norm worden behandeld.)
Certificatietermijn	Termijn dat een certificaat geldig is. Dit is aangegeven op het certificaat.
NACE-Code	Europese codering van bedrijfstakken. Revisie 2.
Major	Een major afwijking is een tekortkoming die direct negatief effect op de kwaliteit van het eindproduct heeft, dan wel het niet voldoen aan een strikte eis van de norm.

BIJLAGE

Stroomschema

(schriftelijk) bijkomend onderzoek

Bijlage Stroomschema (schriftelijk) bijkomend onderzoek



BIJLAGE

Overzicht consequenties negatieve beoordeling 1e (S)BO

Bijlage: Overzicht consequenties negatieve beoordeling 1e (S)BO