KEURMERK

ZEKER-ONLINE

Zeker-OnLine is een onafhankelijk en transparant keurmerk voor online administratieve diensten (ook wel administratieve cloudoplossingen genoemd).

Auditprotocol

(deze vervangt versie 2.0 zoals opgenomen in het Document 2.0)

Versienummer 3.1
Ingangsdatum: per direct 1 januari 2016
Werkversie: 3.14
Datum eerste versie 3.0: 1 oktober 2015

6. Audit protocol

6.1 Inleiding

Een belangrijke pijler onder het keurmerk is de assurance verkregen door middel van een onafhankelijke audit. Om in aanmerking te kunnen komen voor het Keurmerk Zeker-OnLine dienen de aanbieders van online diensten – de Deelnemers van de Stichting Zeker-OnLine – de geformuleerde beheersdoelstellingen die een betrouwbare en continue verwerking van transacties waarborgen aantoonbaar te behalen.
Deze beheersdoelstellingen en beheersmaatregelen ook wel kwaliteitseisen zijn vastgelegd in sectie 5 "Normenkader Zeker-OnLine".

6.2 Audit cycle

Ter verkrijging en behouden van het Keurmerk Zeker-OnLine worden audits uitgevoerd in een driejarige cyclus. Ter verkrijging van het Keurmerk is een initiële audit op het voldoen aan deze kwaliteitseisen vereist. Dit betreft zowel een onderzoek naar de opzet en het bestaan alsmede naar de werking over een minimale periode van 6 maanden, van de door de aanbieder getroffen en ingevoerde maatregelen om aan de controledoelstellingen van Zeker-OnLine te behalen. Deze audit vindt plaats binnen 1 jaar na toekenning van het deelnemerschap. Het bestuur kan op verzoek een verlenging van deze periode toekennen.
Na het verkrijgen van het Keurmerk Zeker-Online gebaseerd op de initiële audit op basis van het uitgebreide normenkader worden in de daaropvolgende twee jaren minder uitgebreide audits op basis van een verkort normenkader uitgevoerd waarna een nieuwe periode van drie jaar start. Iedere drie-jaarsperiode start met een uitgebreide audit op basis van een uitgebreid normenkader en wordt vervolgd met twee jaren met minder uitgebreide audits op basis van een verkort normenkader.

6.3 Aanstellen onafhankelijke auditorganisatie/auditor

De Deelnemer moet zelfstandig de keuze voor een onafhankelijke auditorganisatie maken, waarbij als randvoorwaarden gelden:

- dat de auditorganisatie over voldoende expertise beschikt om de audit uit te kunnen voeren;
- dat de aan de auditorganisatie verbonden verantwoordelijke auditor minimaal is ingeschreven in het register van één van de volgende beroepsorganisaties:
  - de Nederlandse Beroepsorganisatie van Accountants (NBA) als RA en/of
  - de Nederlandse Organisatie van Register EDP-Auditors (NOREA);
- dat het uitvoerende auditteam over relevante ervaring en expertise beschikt op de onderscheiden gebieden van het normenkader;
- dat de auditor kennis heeft genomen van de door de Stichting voorgeschreven rapportagetemplate en verklaart in zijn opdrachtbevestiging deze template te gebruiken voor de rapportage.

De Deelnemer stelt het bestuur van de Stichting vooraf in kennis van de voorgenomen keuze voor een auditorganisatie en auditor. Het bestuur van de Stichting stelt een 'format' vast voor een zodanige inkennisstelling. Dit verplicht te volgen format is te downloaden van de website onder het hoofdstuk documenten " Formulier aanstellen onafhankelijk auditorganisatie/auditor.

Het bestuur van de Stichting stelt vast of een auditor voldoet aan de genoemde voorwaarden en geeft een bindend en gefundeerd advies ten aanzien van de keuze van de auditorganisatie en auditor. Het bestuur van de Stichting accrediteert daarmee de auditorganisatie voor het uitvoeren van audits bij de Deelnemer. Indien de auditorganisatie of auditor door het bestuur van de Stichting niet wordt geaccrediteerd, stelt de Deelnemer een andere auditorganisatie of auditor voor. Een advies vanuit de Stichting voor een bepaalde auditorganisatie of auditor behoort tot de mogelijkheden.

Het aangaan van een overeenkomst tot opdracht met de auditorganisatie/auditor rust bij de Deelnemer. De Deelnemer contracteert de auditorganisatie/auditor zelfstandig en zal de kosten voor deze audit rechtstreeks voldoen aan de auditorganisatie/auditor. De kosten van een audit kunnen worden beperkt, indien de Deelnemer een document aanlevert met daarin per norm aangegeven welke maatregelen zijn getroffen. Het bestuur heeft hiervoor een format beschikbaar dat opvraagbaar is bij het secretariaat van de Stichting.
De Stichting ontvangt van de Deelnemer de door partijen getekende opdrachtbrief om vast te stellen dat de scoping overeenkomstig de gevraagde assurance is.

6.4 Inkadering opdracht

6.4.1 Opdracht aan auditor

Aan de auditor wordt de opdracht, conform artikel 8 van Standaard 3402[1], gegeven tot:

a. het verkrijgen van een redelijke mate van zekerheid over de vraag of, in alle van materieel belang zijnde opzichten, op basis van geschikte criteria:
    1. een beschrijving van de serviceorganisatie van haar systeem, het systeem getrouw weergeeft zoals dit gedurende de gespecificeerde verslagperiode is opgezet en geïmplementeerd;
    2. de interne beheersingsmaatregelen die verband houden met de controledoelstellingen zoals deze in het normenkader van Zeker-OnLine staan vermeld in de beschrijving van de serviceorganisatie van haar systeem gedurende de gespecificeerde verslagperiode op afdoende wijze zijn opgezet;
    3. de interne beheersingsmaatregelen, effectief werkten om een redelijke mate van zekerheid te verschaffen dat de controledoelstellingen zoals deze in het normenkader van Zeker-OnLine staan vermeld en die in de beschrijving van het systeem van de serviceorganisatie zijn opgenomen, gedurende de gespecificeerde verslagperiode van minimaal 6 maanden zijn bereikt.
b. het rapporteren over de aangelegenheden die hierboven bij (a) staan vermeld in overeenstemming met de bevindingen van de auditor van de serviceorganisatie.

Door het bestuur van de Stichting is voor de rapportage een verplicht te volgen template rapport Zeker-OnLine vastgesteld. Dit template is gebaseerd op de rapporteringseisen uit Standaard 3402 (NBA) en de equivalent Richtlijn 3402 (NOREA). Het is van belang dat in de opdrachtbevestiging die door de Deelnemer aan de auditor wordt gegeven het hanteren van de door de Stichting verplicht gestelde rapportage template wordt vastgelegd.

De opdracht dient te worden uitgevoerd conform een van onderstaande standaarden:

[1] Handleiding Regelgeving Accountancy (HRA) editie 2015, Nadere voorschriften controle- en overige standaarden Standaard (NV COS), Standaard 3402 artikel 8.

1. Standaard 3402 van de NBA; of
2. Richtlijn 3402 van de NOREA; of
3. ISAE 3402 van IFAC.

De ontwikkelingen rondom SOC 2 worden nauwlettend gevolgd door het bestuur van de Stichting en zodra deze standaard een Nederlandse juridische basis heeft, wordt de toepassing verder bepaald.

In de opdracht aan de auditor moet tevens worden opgenomen dat de Deelnemer de auditor ontheft van zijn geheimhoudingsplicht (vertrouwelijkheid) richting het bestuur van de Stichting, voor zover dat nodig is voor een goede oordeelsvorming door het bestuur van de Stichting, in bijvoorbeeld een toelichtend gesprek. Van dossierreview is uitdrukkelijk geen sprake.

In de opdrachtbevestiging moet dus minimaal de scoping, rapportage, gebruik template en ontheffing van de vertrouwelijkheid van informatie richting Zeker-OnLine ten behoeve van oordeelsvorming zijn opgenomen.

6.4.2 Werkzaamheden auditor

De werkzaamheden bestaan uit het vaststellen of de aanbieder van online administratieve dienstverlening zodanige maatregelen heeft genomen dat de in sectie 5 omschreven beheersdoelstellingen worden behaald en dat verder aan de minimale kwaliteitseisen wordt voldaan.

De auditor stelt van de beheersmaatregelen naast opzet en bestaan de werking vast gedurende minimaal 6 maanden. Het normenkader is “principle based” opgezet waarbij beheersmaatregelen een belangrijke uitwerking zijn van het minimaal vereiste niveau waarmee de risico’s aangaande de beheersdoelstellingen worden gemitigeerd. Tot afwijken van de genoemde beheersmaatregelen kan een auditor besluiten in geval van compenserende maatregelen. Indien een uitzondering wordt vastgesteld en deze wordt vervangen door een compenserende maatregel (en) wordt dit verwerkt in de rapportage met beschrijving van de aard van deze compenserende maatregel. Het is aan de auditor om te beoordelen of deze compenserende maatregelen in redelijke mate de risico’s afdekken voor de genoemde beheersdoelstelling. Als het Bestuur van de Stichting een maatregel niet als volledige vervanging ziet voor de in het normenkader genoemde beheersmaatregel worden de principes van “due process” toegepast (review met bevindingen, hoor- en wederhoor, standpuntbepaling). Als de auditor zich niet kan vinden in het standpunt van het Bestuur wordt contact opgenomen met de opdrachtgever. Zowel de deelnemer als het bestuur van de Stichting kunnen ook besluiten om deze maatregel aan de deelnemersraad of de voorzitter van deelnemersraad voor te leggen. Dit proces kan het uitreiken van het certificaat vertragen en daarom adviseert het bestuur om significante wijzigen tijdig te communiceren; bijvoorbeeld al na een “nulmeting”. De Deelnemer kan ook zelfstandig een voorstel tot aanpassing van beheersmaatregel inbrengen in de normcommissie, zodat deze maatregel eventueel wordt meegenomen in een herzien normenkader.

De Stichting heeft gekozen voor toepassing van Standaard 3402 omdat deze standaard de juiste set van werkzaamheden voorschrijft. De administratieve software zal hoofdzakelijk gebruikt worden voor financiële processen. Een Standaard 3402 rapportage zorgt er ook voor dat accountants in het kader van een jaarrekeningcontrole gebruik kunnen maken van de werkzaamheden die bij de service organisatie zijn verricht in het kader van het verkrijgen van het keurmerk Zeker-OnLine. De werkzaamheden kunnen daarmee meerdere doelen dienen.

6.4.3 Gebruik maken van toeleveranciers

Het keurmerk wordt verleend op de dienst in de volle breedte. Een softwareleverancier kan gebruik maken van toeleveranciers voor bijvoorbeeld housing services en hostingservices. De beheersingsmaatregelen die betrekking hebben op de toeleveranciers moeten meegenomen worden in de audit van de Deelnemer. Indien de beheersmaatregelen van de toeleverancier worden meegenomen met behulp van een onderliggende assurancerapportage dient in het Standaard 3402 type 2 rapport van de auditor aangegeven te worden wat daarvan de weging is geweest. Indien gebruik gemaakt wordt van het Standaard 3402 type 2 rapport van de toeleverancier dan mag deze rapportage op het moment van afgegeven van het Standaard 3402 type 2 van de Deelnemer niet ouder zijn dan 2 maanden. Het is voor de auditor aan te bevelen in deze situatie vroegtijdig met de Deelnemer te overleggen over de periode van de audit en de audit van de toeleverancier/hoster.

Voorbeeld inzake geldigheidsduur onderliggende rapportage:

Audit van de Deelnemer

Periode van onderzoek: 1 april 2015 tot en met 30 september 2015

Afgifte rapportage: tot uiterlijk 15 januari 2016

Rapportage toeleverancier:

Periode van onderzoek: 1 oktober 2014 tot en met 30 september 2015

Afgifte rapportage: 15 november 2015

De afgiftedatum van de rapportage van de toeleverancier is bepalend voor de twee maanden periode; in dit voorbeeld kan de rapportage van de Deelnemer tot uiterlijk 15 januari 2016 worden afgeven: namelijk 15 november 2015 plus 2 maanden.

De basis van de twee maanden ligt gelegen in de geldigheidsduur van een rapportage van de onderliggende periode deze verliest zekerheid al gelang deze rapportage verouderd.

Nota Bene:

De IT- auditor van de softwareleverancier moet de overall conclusie trekken of de dienst door de Deelnemer overeenkomstig het normenkader van Zeker-OnLine wordt aangeboden. Dit moet duidelijk in de opdrachtomschrijving en rapportage van de IT-auditor naar voren komen.

6.4.4 Rapportering auditor

De auditor brengt verslag uit over zijn werkzaamheden in de vorm van de door de Stichting verplicht gestelde format zoals is opgenomen onder punt 6.4.1. Dit format is verstrekt bij de accreditatie van de auditor en is verplicht om in aanmerking te komen voor het keurmerk Zeker-OnLine.

6.5 Jaarlijkse Update

Zeker-OnLine kent de full scope audit bij aanvraag van het keurmerk en voor de volgende jaren ter verlenging. Onder voorwaarden kan bij verlenging gebruik worden gemaakt van een beperktere variant, de Jaarlijkse Update op basis van een verkort normenkader, hierna: "jaarlijkse Update". De Jaarlijkse Update is onder voorwaarden van toepassing. Deze optie staat niet open voor Keurmerkhouders die wezenlijke wijzingen in de interne beheersing hebben aangebracht, welke wijzigingen niet met behulp van deze beperkte audit zijn te beoordelen. De beslissing of een wijziging in de interne beheersing als wezenlijk kwalificeert en daarmee een uitgebreide audit noodzakelijk maakt, is voorbehouden aan de auditor. Overleg met de Deelnemer hieromtrent is evident; overleg met het bestuur van de Stichting is mogelijk. Overigens bestaat er een actieve

informatieplicht bij significante wijzigingen in de administratieve organisatie en/of bedrijfsvoering, zowel naar de IT-auditor als naar het bestuur van Zeker-OnLine. Wijzigingen zijn significant als niet meer zonder meer kan worden vastgesteld dat de dienst voldoet aan het normenkader van Zeker-OnLine. Voorbeelden kunnen zijn wijzigingen in de eigendomsstructuur en wijziging van belangrijke toeleveranciers.

De Jaarlijkse Update is gebaseerd op de volgende veronderstellingen:

1. Het beheerskader bestaat voor een groot deel uit beheersmaatregelen waarvan, als ze zijn geïmplementeerd, de verwachting bestaat dat deze beheersmaatregelen de beheersdoelstelling blijvend afdekken voor een periode van 3 jaar. De Deelnemer wordt gevraagd deze beheersmaatregelen, die te maken hebben met inrichting van de beheersorganisatie, te bevestigen in jaar 2 en 3. Middels de beschrijving van de interne serviceorganisatie. .
2. Als gevolg van bovenstaand komen de beheersmaatregelen uit de juridische en applicatie laag in principe niet in aanmerking voor de audit in jaar 2 en 3.
3. Actuele ontwikkelingen of specifieke aanwijzingen van het bestuur van de Stichting worden verwerkt in de beschrijving van de interne serviceorganisatie of toegevoegd aan de jaarlijkse update uitgevoerd door IT-auditor afhankelijk van de aard van de maatregel.
4. Beheersmaatregelen waarvan alleen opzet en bestaan is vastgesteld vanwege het niet beschikbaar zijn van test-items gedurende de auditperiode worden expliciet meegenomen in de Jaarlijkse Update van jaar 2 en 3.

De rapportage in jaar 2 en 3 vindt plaats op basis van Standaard 3000 of Standaard 3402 en bevat

1. een beschrijving van de serviceorganisatie van haar systeem die het systeem getrouw weergeeft zoals dit gedurende de gespecificeerde verslagperiode is opgezet en geïmplementeerd;
2. de interne beheersingsmaatregelen, die verband houden met de controledoelstellingen zoals deze in het normenkader van Zeker-OnLine en die staan vermeld in de beschrijving van de serviceorganisatie van haar systeem gedurende de gespecificeerde verslagperiode en of deze op afdoende wijze zijn opgezet;

Aan de IT-Auditor wordt gevraagd om conform Standaard 3402 of 3000 te rapporteren over de opzet, bestaan en werking en werking van de beheersmaatregelen over een periode van 6 maanden. De geselecteerde maatregelen voor de Jaarlijkse Update zijn opgenomen in de template Jaarlijkse Update. Deze template wordt verstrekt aan de keurmerkhouders.

6.6 Uitbreiding audit en intrekken Keurmerk

Zoals in punt 6.2 is aangegeven, behelst de audit cycle een periode van 3 jaar, bestaande uit een uitgebreide audit gevolgd door twee Jaarlijkse Updates. Indien het Bestuur van de Stichting op gegronde redenen tussentijds tot het oordeel komt dat een aanvullende audit vereist is om te kunnen bepalen of het Keurmerk in stand kan blijven bij een Dienst, dan zal de Deelnemer een nieuwe audit laten uitvoeren en alle kosten daarvoor dragen. Hetzelfde geldt indien de Dienst wijzigingen heeft ondergaan welke naar het oordeel van het Bestuur van de Stichting de kwaliteitseisen en het normenkader raken.

Indien in jaar 2 en 3 blijkt dat de zekerheid van het Keurmerk Zeker-Online onder druk komt te staan is het Bestuur van de Stichting gerechtigd een tussentijdse volledige audit te vereisen.

De Deelnemer heeft, ook op grond van de deelnemersvoorwaarden, een actieve informatieplicht naar de Stichting over wijzigingen in de organisatie, de processen en het kwaliteitssysteem die van invloed zijn op de dienst.

De snelheid in de ontwikkelingen op het gebied van online dienstverlening kunnen aanleiding zijn om aanvullende maatregelen of herformuleringen op te nemen in de handreiking.

De uitkomst van de Jaarlijkse Update dan wel een full scope audit bepaalt of de Deelnemer het Keurmerk op de dienst mag blijven voeren. Indien aanwijzingen van het Bestuur van de Stichting niet, dan wel niet adequaat of tijdig worden opgevolgd, kan dit het intrekken van het keurmerk ten gevolge hebben.