NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

NOREA model handboek Kwaliteitsbeheersing

IT-audit organisatie

NOREA RKBN

Vastgesteld door	[IT-audit organisatie]
Goedgekeurd door	[Directieverantwoordelijke]
Handtekening	
Versie	x.x
Status	[status]
Datum	[datum vastgesteld door directie]
Aantal bladzijden	13

Versie	Datum	Status	Naam	Omschrijving
0.1-0.8	05-08-2013	werkversies	F. Kossen RE	Template Handboek KITA opgesteld in opdracht van NOREA
0.9	08-09-2013	Conceptversie	F. Kossen RE	Om commentaar voorgelegd aan CKO
0.99	09-10-2013	Conceptversie	F. Kossen RE	Commentaar CKO (H. de Zwart) verwerkt Om commentaar voorgelegd aan Commissie Beroepsregels en Vaktechnische Commissie
2.0	05-02-2020	Concept	Jan de Heer	Aanpassen aan actualiteit en vaktechnische verbeteringen aangebracht

Colofon

NOREA heeft dit model-handboek opgesteld om haar leden te ondersteunen bij het opstellen van een intern Handboek Kwaliteitsbeheersing. In de praktijk is gebleken dat met name de kleinschalige IT-auditorganisaties (KITA's) hier behoefte aan hebben.

Nadrukkelijk merkt NOREA op dat de IT-auditorganisatie het model-handboek zelf verder dient te concretiseren naar de eigen situatie en de beschreven beheersingsmaatregelen in haar organisatie dient te implementeren.

Voor actuele informatie zie www.norea.nl.

Dit model-handboek kan worden gebruikt voor de opzet van een kwaliteitsbeheersingssysteem binnen een KITA. Om het handboek voor een brede doelgroep bruikbaar te maken, is ervoor gekozen uit te gaan van twee vormen van KITA's:

1. Een zelfstandig opererende IT-auditor, zonder personeel
2. Een organisatie bestaande uit een IT-auditor (RE) en een zeer beperkt aantal personeelsleden, die al dan niet zijn ingeschreven als RE

Ook andere (grotere) IT-auditorganisaties kunnen (delen van) dit model-handboek gebruiken bij het opzetten van een dergelijk systeem. De voor een KITA geldende beperkingen zijn in dat geval niet van toepassing.

Inhoudsopgave

1 Inleiding

1.1 Aanleiding

Op 1 januari 2009 is het Reglement Kwaliteitsbeheersing NOREA (RKBN) in werking getreden en is van toepassing op alle IT-auditors, ongeacht de omvang van de [IT-auditorganisatie] waarbinnen zij professionele diensten verrichten. Dit reglement stelt de grondbeginselen en procedures vast en geeft aanwijzingen met betrekking tot de verantwoordelijkheden van IT-auditors voor het kwaliteitsbeheersingssysteem dat moet worden gehanteerd bij het uitvoeren van professionele diensten.

Het kwaliteitssysteem van de [IT-auditorganisatie] moet zodanig van opzet zijn, dat een redelijke mate van zekerheid wordt geboden dat wordt voldaan aan de (vaktechnische) reglementen, richtlijnen en handreikingen en ook aan de door wet- en regelgeving gestelde eisen.

In relatie tot de invoering van het RKBN heeft het Bestuur in de Algemene Ledenvergadering van juni 2009 toegezegd een concrete handreiking voor de implementatie van een eenvoudig en doelmatig kwaliteitsstelsel ten behoeve van ZZP-ers en kleinschalige organisaties te ontwikkelen.

In 2020 is het handboek aangepast naar aanleiding van regelgeving en feedback van RE's.

1.2 Verklaring van uitgifte

In dit Handboek kwaliteitsbeheersing beschrijft [IT-audit organisatie] de gedragslijnen en procedures van het kwaliteitsbeheersingssysteem.

De directie van [IT-audit organisatie] aanvaardt met de goedkeuring en ondertekening van dit Handboek kwaliteitsbeheersing de eindverantwoordelijkheid voor het kwaliteitsbeheersingssysteem van de [IT-auditorganisatie].

Het kwaliteitsbeheersingssysteem van de [IT-audit organisatie] is gericht op het onderhouden en beheersen van alle processen welke noodzakelijk c.q. vereist zijn om audit- en advies-activiteiten uit te kunnen voeren onder toezicht van de NOREA. Het systeem is gebaseerd op het Reglement Kwaliteitsbeheersing NOREA (RKBN).

Dit Handboek kwaliteitsbeheersing moet als geheel worden gezien met de samenhangende documenten (o.a. richtlijnen en handreikingen van de NOREA). Het beschrijft het kwaliteits-beheersingssysteem en hoe uitvoering wordt gegeven aan de eisen uit de RKBN. Het doel van het Handboek is inzicht te geven in de wijze waarop binnen de [IT-auditorganisatie] het beleid en bedrijfsprocessen zijn geborgd.

Dit Handboek Kwaliteitsbeheersing wordt bekend gemaakt aan de medewerkers van de auditorganisatie en anderen die namens de [IT-auditorganisatie] professionele diensten uitvoeren door bijv. publicatie op het interne netwerk, meesturen met samenwerkings-overeenkomsten.

1.3 Opbouw van het Handboek kwaliteitsbeheersing

Dit Handboek omschrijft de wijze waarop [IT-auditorganisatie] de audit- en adviesactiviteiten uitvoert in relatie tot de RKBN. Het Handboek geeft de managementinterpretatie weer van de vereisten die zijn beschreven in het RKBN en hoe die tot uitvoering dient te komen in de dagelijkse praktijk. Om te waarborgen dat de vereisten uit het Handboek worden opgevolgd kunnen binnen de [IT-auditorganisatie] geconcretiseerde richtlijnen en werkinstructies worden opgesteld.

De effectiviteit van het kwaliteitsbeheersingssysteem wordt geborgd door de jaarlijks in te vullen self assessment en het 4 jaarlijks kwaliteitsonderzoek (onder regie van het CKO).

1.4 Reikwijdte van het Handboek kwaliteitsbeheersing

De reikwijdte van dit Handboek kwaliteitsbeheersing betreft alle professionele diensten zoals audits, adviezen, detachering, consultancy uitgevoerd door [IT-audit organisatie].

1.5 Beheer van het Handboek kwaliteitsbeheersing

Het beheer van dit Handboek en bijbehorende documenten ligt bij [ROL/FUNCTIE]. Voor de inhoud van het Handboek draagt [ROL/FUNCTIE] de eindverantwoordelijkheid. Om deze verantwoordelijkheid gestalten te geven, wordt het Handboek goedgekeurd door [ROL/FUNCTIE].

Het Handboek kan om diverse redenen gewijzigd worden. De [ROL/FUNCTIE] controleert periodiek (minimaal 1 keer per jaar) met behulp van onder andere het self assessment van NOREA of de inhoud van dit Handboek in overeenstemming is met de richtlijnen van de NOREA en het praktisch functioneren van de [IT-auditorganisatie]. Als dit niet het geval is, worden aanpassingen gemaakt. Ook kunnen er opmerkingen gemaakt worden door anderen partijen die in overweging worden genomen door de organisatie. Ook grote wijzigingen in processen, procedures, bedrijfsvoering, technologieën en/of wet- en regelgeving kunnen leiden tot wijziging van het Handboek.

1.6 Organisatiestructuur [IT-audit organisatie]

De organisatiestructuur is dusdanig opgezet dat risico's op het gebied van integriteit, objectiviteit, deskundigheid en zorgvuldigheid, geheimhouding en professioneel gedrag (de grondbeginselen van de Gedrag- en Beroepsregels RE) worden geminimaliseerd. Het

kleinschalige karakter van [IT-auditorganisatie] leidt er toe dat binnen de organisatie voor de realisatie van de eisen die zijn geformuleerd in het RKBN, andere oplossingen zijn gezocht. De belangrijkste knelpunten zijn de opdrachtgerichte kwaliteitsbeoordeling en het monitoren van het kwaliteitsbeheersingssysteem. Deze leemten worden ondervangen door de inzet van [samenwerkingsorganisatie], een vaktechnisch deskundige organisatie op het gebied van IT-auditing, waarmee (schriftelijke) afspraken zijn gemaakt voor samenwerking op het gebied van het kwaliteitsbeheersingssysteem.

Geef hier een beschrijving van de organisatie:

Rechtsvorm: voorbeeld eenmanszaak , VOF, BV,NV, CV, etc.

Aantal personeelsleden

Vestigingsplaats(en) Let op: bij meerdere vestigingsplaatsen is het van belang of de vestigingen gebruik maken van hetzelfde kwaliteitsstelsel

Directie / eigenaarschap (groot aandeelhouder)

Evt. beschrijving van de samenwerkingsorganisatie

Aard van de uitgevoerde werkzaamheden

Kamer van Koophandel gegevens

[Plaats voor organogram]

2 Principes

2.1 Toepassing ethische normen

Het kwaliteitsbeheersingssysteem is gebaseerd op vijf grondbeginselen uit de Gedragscode Register IT-auditors.

[IT-audit organisatie] onderkent de noodzaak van deze grondbeginselen binnen haar audit- en adviesdiensten. Het beleid dat door management wordt uitgedragen is erop gericht om risico's op dit gebied te minimaliseren en waar dat niet mogelijk is passende maatregelen te treffen om hierop te sturen en te meten.

In de volgende paragrafen wordt aangegeven hoe [IT-auditorganisatie] borgt dat de bij het uitvoeren van de professionele diensten de grondbeginselen uit de Gedragscode in acht worden genomen en in overeenstemming daarmee wordt gehandeld.

2.1.1 Integriteit

De functie van IT-auditor wordt binnen [IT-auditorganisatie] bekleed door mensen met een onbesproken gedrag. Integriteit en vertrouwelijkheid spelen een zeer grote rol bij het uitvoeren van professionele diensten door de IT-auditor. Om de kwaliteit en integriteit van de IT-auditor te waarborgen, hanteert [IT-auditorganisatie] een streng toelatingsbeleid. IT-auditors van [IT-auditorganisatie] moeten zich houden aan de Gedragscode van de NOREA en de verder voor hen geldende regelgeving, waaronder het RKBN en de regels voor Permanente Educatie. De Gedragscode en het kwaliteitsonderzoek van de NOREA (door het College Kwaliteits-onderzoek – CKO) zijn erop gericht de goede beroepsuitoefening te bevorderen en de belangen van de cliënt te waarborgen.

2.1.2 Objectiviteit

De doelstelling van de maatregelen gericht op het grondbeginsel 'objectiviteit' zijn gericht op het creëren, in wezen en in schijn, van een zo groot mogelijke onafhankelijkheid ten opzichte van de cliënt en andere belanghebbende stakeholders (bijvoorbeeld: nagegaan wordt of geen familiaire en/of financiële relaties bestaan, het niet verstrekken van aanbrengpremies). De maatregelen zijn gericht op onder andere:

a. De gevaren die kleven aan het niet of onvoldoende omgaan met zelfkritiek voor de eigen werkzaamheden, is een attentiepunt dat is opgenomen in de afspraken met [samenwerkingsorganisatie].

b. Het nagaan bij het aanvaarden van een opdracht of de relatie met de cliënt niet leidt een belangenverstrengeling met andere cliënten wier belangen worden behartigd.

c. Het nagaan of de relatie met de cliënt niet kan leiden tot intimidatie waardoor de objectiviteit verloren gaat (bijvoorbeeld: dreigen met opzeggen opdracht, verlagen honorarium).

De analyse van voorgaande punten wordt vastgelegd in het dossier.

Tijdens het bespreken van de conceptopdracht besteedt [IT-auditorganisatie] aandacht aan de afbakening van de opdracht, de deskundigheid en de aard van de uitkomsten van de werkzaamheden zodat een te vergaand vertrouwen van de cliënt wordt voorkomen. De vastlegging van de bespreking wordt opgenomen in het dossier.

2.1.3 Deskundigheid en zorgvuldigheid

Voor een geloofwaardige, effectieve en juiste beoordeling / uitvoering van opdrachten zijn de juiste competenties van de IT-auditor(s) binnen [IT-auditorganisatie] van groot belang. De IT-auditor(s) binnen [IT-audit organisatie] volgen zowel gestructureerde als ongestructureerde educatie. Minimaal wordt voldaan aan de eisen gesteld in de NOREA Richtlijn Permanente educatie. De directie van [IT-auditorganisatie] ziet hier op toe. Voordat met een opdracht wordt begonnen, wordt vastgesteld of de in te zetten IT-auditor beschikt over voldoende kennis om de opdracht met de vereiste deskundigheid uit te voeren. Indien dit niet het geval is worden maatregelen getroffen (bijvoorbeeld door het inhuren van externe deskundigheid), dan wel wordt de opdracht geweigerd.

Zorgvuldigheid omvat de verantwoordelijkheid van de IT-auditor op te treden in overeenstemming met de eisen die gelden voor de uitvoering van een opdracht, te weten, toewijding, voldoende diepgang en tijdigheid.

2.1.4 Geheimhouding

Tijdens audit- en adviesdiensten kan toegang tot vertrouwelijke informatie van de cliënt noodzakelijk zijn. Binnen [IT-audit organisatie] zijn interne afspraken hierover vastgelegd, gecommuniceerd naar medewerkers (bijvoorbeeld: personeelshandboek, arbeidscontract) en contractueel vastgelegd met cliënten en samenwerkende derde partijen. Deze afspraken geven onder meer aan dat zonder toestemming geen informatie aan derden wordt verstrekt.

2.1.5 Professioneel gedrag

Bij de uitvoering van professionele diensten houdt [IT-auditorganisatie] zich aan de relevante wet- en regelgeving en onthoudt zich van handelen dat het auditberoep in diskrediet brengt. Dit betekent dat:

- [IT-auditorganisatie] het auditberoep niet in diskrediet brengt bij het aanprijzen van zichzelf of haar werk;

- [IT-auditorganisatie] voorkomt dat overdreven verwachtingen ter zake van de diensten die zij kan verlenen, de kwaliteiten die zij bezit en de ervaring waarover zij beschikt, worden gewekt;

- [IT-auditorganisatie] geen afkeurende verwijzingen maakt naar het werk van een derde of hier niet onderbouwde vergelijkingen naar doet.

[IT-auditorganisatie] borgt het professioneel gedrag binnen de organisatie door (bijvoorbeeld: periodiek aandacht te besteden aan dit onderwerp, cursussen te volgen, etc.).

2.2 Verantwoordelijkheid

Het is de verantwoordelijkheid van [IT-audit organisatie] om op basis van voldoende objectief bewijs een uitspraak te kunnen doen over het (IT) onderzoeksobject en de mate waarin dit voldoet aan de gestelde eisen vanuit de te toetsen norm(en). Omdat een beoordeling is o.a. gebaseerd op deelwaarnemingen en steekproeven is er geen garantie dat het onderzoeksobject bij voortduring voor 100% aan de eisen voldoet. Om een bepaalde mate van zekerheid te borgen zijn beoordeling- en rapportage eisen per type beoordeling vastgelegd, op basis van de richtlijnen en handreikingen van de NOREA.

2.3 Afhandeling van klachten

Klachten welke bekend zijn gemaakt richting [IT-audit organisatie] zijn een kans om de dienstverlening te verbeteren, de cliënttevredenheid te verhogen en het vertrouwen in de diensten te borgen. Open communicatie over klachten en opvolging is gewenst met in achtneming van contractuele, organisatorische en/of wettelijke verplichtingen.

De kleinschaligheid van de organisatie brengt met zich mee dat een op de kleinschalige situatie toegespitste procedure is ingericht. Dit kan bestaan uit het wijzen van de cliënt in de algemene leveringsvoorwaarden op de mogelijkheid om:

1. Klachten te bespreken met [samenwerkingsorganisatie]

2. Gebruik te maken van de raad van beroepsethiek van de NOREA en desnoods het tuchtrecht.

3 Generieke eisen

3.1 Wettelijke en contractuele zaken

[IT-audit organisatie] is een opzichzelfstaande juridische entiteit welke is ingeschreven bij de Kamer van Koophandel. Er zal een contract met geldende voorwaarden worden afgesloten met cliënten voor wie audit- of adviesdiensten worden uitgevoerd. Voordat een contractuele overeenkomst wordt opgemaakt, zal de opdracht door [IT-audit organisatie] worden geëvalueerd op haalbaarheid en integriteits- / objectiviteits- / deskundigheids- en zorgvuldigheidsrisico's en wordt alle benodigde informatie geïnventariseerd. De uitkomsten van de analyse van deze grondbeginselen worden vastgelegd en opgenomen in het opdrachtdossier. Uit deze vastlegging blijkt welke mitigerende maatregelen zijn getroffen om de gesignaleerde risico's tot een aanvaardbaar niveau te beperken.

Van alle uit te voeren opdrachten wordt bepaald of een Opdrachtgerichte Kwaliteitsbeoordeling (OKB) noodzakelijk is. De beoordeling van de OKB vindt gezien de kleinschaligheid plaats door de IT-auditorganisatie waarmee wordt samengewerkt.

3.2 Aansprakelijkheden en financiën

Binnen [IT-audit organisatie] wordt een risicoanalyse methodiek gebruikt om financiële- en aansprakelijkheidsrisico's vanuit de audit- en adviesactiviteiten te identificeren, graderen en te reduceren tot een aanvaardbaar risico. De uitkomsten van deze risicoanalyse worden jaarlijks ge-update (zie bijlage 2 voor een voorbeeld).

4 Organisatorische eisen

De organisatiestructuur van [IT-auditorganisatie] is dusdanig opgezet dat integriteits- / objectiviteits- / deskundigheids- en zorgvuldigheidsrisico's worden geminimaliseerd en dat aan de grondbeginselen inzake geheimhouding en professioneel gedrag wordt voldaan. Taken, verantwoordelijkheden en bevoegdheden zijn beschreven binnen de geldende procedures, rolprofielen en/of arbeidscontracten. Een medewerker kan meerdere rolprofielen vertegenwoordigen.

5 Middelen eisen

5.1 Competentie en beschikbaarheid van management en personeel

Om geloofwaardige professionele diensten te kunnen uitvoeren bepaalt [IT-audit organisatie] voor opdrachtaanvaarding welke competenties benodigd zijn en of deze capaciteit beschikbaar is. Naast de benodigde basiscompetenties en beschikbaarheid wordt vastgesteld of ook specifieke technische competenties vereist zijn. Indien de benodigde (technische) kennis niet intern beschikbaar is, zal materiedeskundig personeel worden ingehuurd. De uitkomst van deze analyse wordt in het opdrachtdossier opgenomen .

5.2 Personeel betrokken bij professionele diensten

Bij de selectie van personeel stelt [IT-auditorganisatie] vast dat bij betrokkene gevoel aanwezig is voor eisen die samenhangen met het kwaliteitsbeheersingssysteem. Het personeel van [IT-auditorganisatie] wordt in staat gesteld om het kwaliteitsbeheersingssysteem toe te passen en om aan de PE-verplichting te voldoen. De begeleiding van het personeel wordt afgestemd op de kennis en ervaring in relatie tot de te verrichten werkzaamheden. [IT-auditorganisatie] beschikt over overzichten/matrices waar competenties zijn beschreven. Op basis van uitgevoerde opdrachten worden vaardigheden geëvalueerd. Indien vanuit de evaluaties training behoeften wordt geïdentificeerd wordt hierop geanticipeerd. Middels de activiteitenplanning wordt geborgd dat de juiste personen de werkzaamheden bij de cliënt uitvoeren. De uitkomst van deze evaluatie wordt in het opdrachtdossier opgenomen.

5.3 Gebruik van externe auditors en materiedeskundigen

Indien binnen een opdrachtteam gebruik wordt gemaakt van extern personeel, dient dit zich te committeren aan de gedragsregels van [IT-auditorganisatie]. Er wordt een contract opgesteld tussen [IT-audit organisatie] en de externe dienstverlener waarin alle eisen zijn vastgelegde m.b.t. de dienstverlening.

Indien het externe personeel wordt ingezet voor een specifieke opdracht, maakt dit contract onderdeel uit van het dossier.

5.4 Personeelsdossiers

[IT-audit organisatie] houdt van het eigen personeel dossiers bij met aantoonbare registraties van competenties, kwalificaties, uitgevoerde diensten en werkervaring.

5.5 Uitbesteding

De condities van een in relatie tot een opdracht uitbestede dienst, zijn procedureel vastgelegd en bekend gemaakt aan de externe dienstverlener. De onderlinge afspraken zijn juridisch vastgelegd en betreffen de integriteits- / objectiviteits- / deskundigheids- en zorgvuldigheidsrisico's en ook de grondbeginselen inzake geheimhouding en professioneel gedrag. [IT-audit organisatie] erkent dat zij als eindverantwoordelijke partij richting de cliënt zal op de treden.

De afspraken maken onderdeel uit van het opdrachtdossier.

6 Informatie eisen

6.1 Publiekelijk toegankelijke informatie

De website van [IT-audit organisatie] wordt als belangrijkste communicatiemiddel richting de cliënt gebruikt. Op de website is beschreven hoe [IT-audit organisatie] haar audit- en adviesdiensten uitvoert en welke algemene leveringsvoorwaarden gelden. Tot die voorwaarden behoort een verwijzing naar de voor IT-auditor geldende wet- en regelgeving die op de dienstverlening van toepassing is.

6.2 Rapportage

Van haar auditwerkzaamheden stelt [IT-audit organisatie] een rapport op. Het rapport voldoet aan de door de NOREA vastgestelde richtlijnen voor het betreffende onderzoek.

Voor de overige opdrachten geldt, dat de rapportage over de uitkomsten van de professionele diensten, rekening houdend met de aard van de dienst, in lijn moet liggen met de overige richtlijnen.

6.3 Vertrouwelijkheid

Vertrouwelijkheid tussen [IT-audit organisatie] en de cliënt is contractueel vastgelegd. De richtlijnen met betrekking tot vertrouwelijkheid zijn vastgelegd (bijvoorbeeld in arbeidscontracten, personeelshandboek). Eén van de maatregelen in dit kader is het tekenen van een geheimhoudingsverklaring door bij [IT-auditorganisatie] en/of een opdracht betrokken medewerkers. De procedures met betrekking tot gedragsregels worden gecommuniceerd richting interne en externe medewerkers. Het openbaar maken van vertrouwelijke gegevens zal alleen in overleg met de cliënt plaatsvinden.

6.4 Informatie-uitwisseling tussen IT-auditorganisatie en cliënt

De cliënt zal geïnformeerd worden betreffende alle activiteiten (en wijzigingen daarin) binnen de audit- of adviesdiensten. Relevante afspraken zullen juridisch worden vastgelegd in een opdrachtbevestiging/contract.

7 IT-audit- en adviesopdrachten

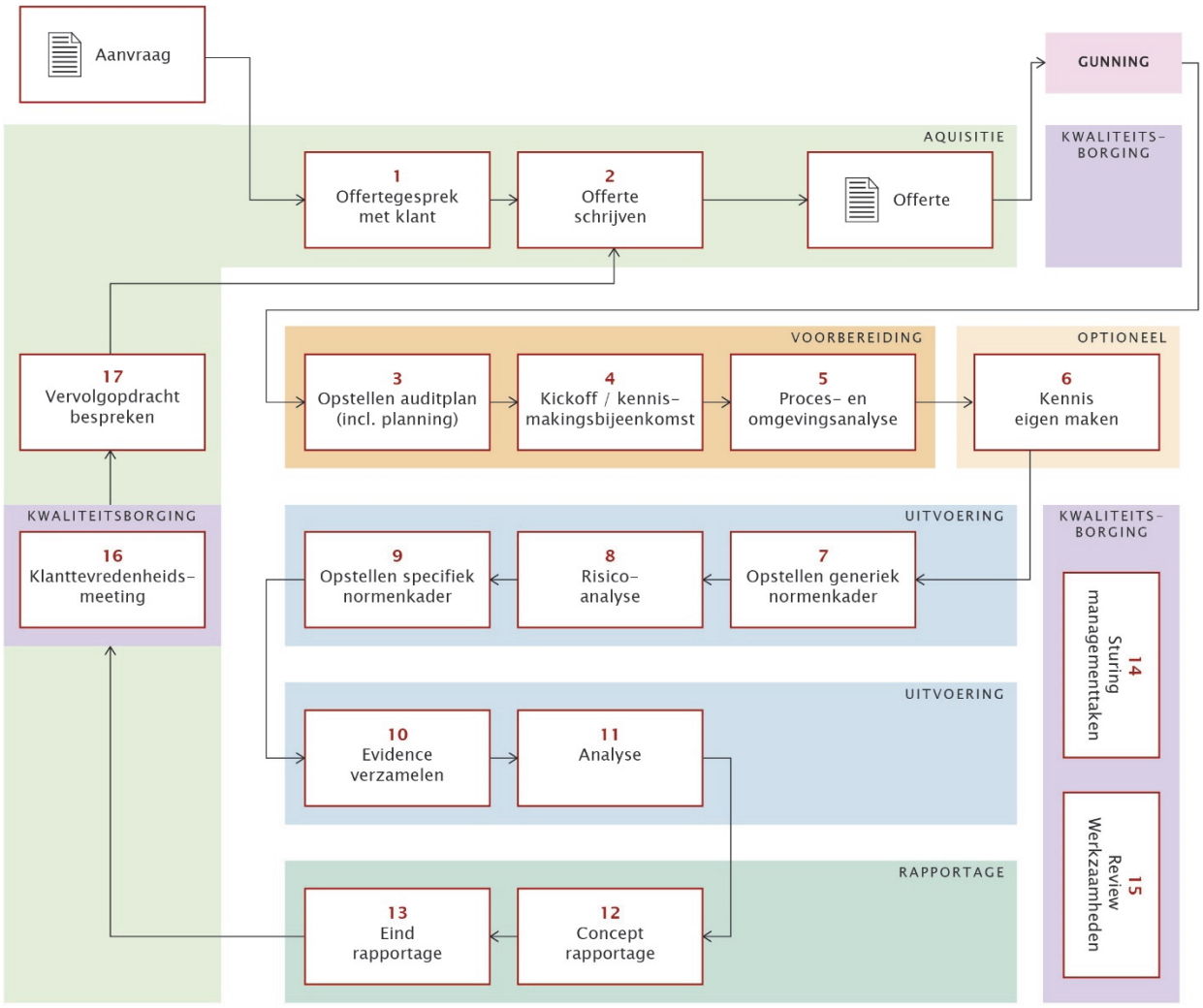
Het primaire werkproces binnen [IT-audit organisatie] is het uitvoeren van IT-audits en aan IT-audit gerelateerde opdrachten (adviesdiensten) op verzoek van de cliënt. Samengevat vallen deze diensten onder de noemer 'professionele diensten'. Het uitvoeren van IT-audits en adviesdiensten dient te geschieden op basis van vooraf, met de cliënt, opgestelde planningen en afspraken en met inachtneming van wet - en regelgeving, w.o. de richtlijnen van de NOREA.

In dit hoofdstuk is beschreven hoe de achtereenvolgende fasen in een IT-audit- of adviestraject ingevuld worden. De uitvoering is steeds gericht op het adequaat, professioneel en efficiënt kunnen beantwoorden van de onderzoeksvragen van de cliënt (opdrachtgever).

In alle audit- en adviestrajecten worden de volgende processtappen onderkend:

1. Cliëntacceptatie
2. Opdrachtaanvaarding en -bevestiging
3. Uitvoering van de opdracht
4. Kwaliteitsbewaking uitvoering
5. Opdrachtgerichte kwaliteitsbeoordeling
6. Dossiervorming en documentatie
7. Rapportage en (verplichte formulering inzake) oordelen

Een voorbeeld van een schematische uitwerking van het proces van professionele diensten die door [IT-audit organisatie] worden uitgevoerd is hierna weergegeven:



7.1 Klantacceptatie

Voordat een organisatie door [IT-audit organisatie] als cliënt wordt geaccepteerd, vindt een afweging van de hiermee verbonden risico's plaats. Deze afweging wordt gemaakt aan de hand van een checklist (zie bijlage 1, voorbeeld cliënt-acceptatieformulier). De afweging wordt door de directie gemaakt dan wel bekrachtigd. Bij de afweging is onder andere het volgende van belang:

- Publiekrechtelijke status of een private onderneming
- Branche(s) waarin de (aspirant)cliënt actief is
- Voor zover te achterhalen / bekend : reputatie van de (toekomstige) cliënt
- Afhankelijk van de omvang van de mogelijke opdracht: de financiële soliditeit van de (toekomstige) cliënt

Voor het vergaren van deze informatie wordt gebruik gemaakt van internet en de sociale media. De uitkomsten van dit proces worden vastgelegd in het cliëntdossier (veelal aanwezig bij langdurige relaties of meerdere opdrachten) of het opdrachtdossier (bij éénmalige opdrachten).

7.2 Opdrachtaanvaarding en -bevestiging

Teneinde misverstanden met betrekking tot de opdracht te vermijden, hebben zowel de opdrachtgever als de IT-auditor er belang bij dat de IT-auditor de opdracht schriftelijk bevestigt. [IT-audit organisatie] geeft hier invulling aan door in elke offerte/voorstel voor het uitvoeren van professionele diensten het doel en de reikwijdte van de opdracht, de omvang van de verantwoordelijkheid van de IT-auditor ten opzichte van de opdrachtgever en de wijze van rapportering te beschrijven. In deze opdrachtbeschrijving (of in de daaraan gehechte algemene leveringsvoorwaarden[1]) wordt verwezen naar de wet- en regelgeving die de IT-auditor bij zijn werkzaamheden in acht moet nemen. Door ondertekening van het voorstel gaat de opdrachtgever akkoord met hetgeen erin is beschreven. De getekende offerte wordt beschouwd als opdrachtbevestiging.

Indien (achteraf) informatie wordt verkregen die zou hebben geleid tot het weigeren van een opdracht, wordt bepaald welke vaktechnische en juridische verantwoordelijkheden gelden en welke in- en externe organen of regelgevende instanties hiervan in kennis moeten worden gesteld. In dergelijke situaties wordt tevens nagegaan of de opdracht kan worden teruggegeven en de relatie met de cliënt kan worden verbroken.

De resultaten van het voorgaande analyses worden vastgelegd in het opdrachtdossier.

7.3 Uitvoering van de opdracht

Alle professionele diensten worden door [IT-audit organisatie] uitgevoerd met inachtneming van de geldende NOREA Richtlijnen.

7.4 Kwaliteitsbewaking uitvoering

Binnen [IT-audit organisatie] gelden het self-assessment en de OKB als instrumenten om de kwaliteitsbewaking te borgen.

Indien de aard van het onderzoek (bijvoorbeeld: integriteit cliënt, branche, complexiteit structuur cliënt, onvoldoende ervaring met de typologie van de cliënt) daartoe aanleiding geeft,

[1] Indien de opdracht wordt aanvaard onder verwijzing naar algemene voorwaarden, dienen deze voorwaarden verwijzingen te bevatten naar de wet- en regelgeving waaraan de IT-auditor gehouden is. Indien deze verwijzingen niet in de AV zijn opgenomen, dient de verwijzing naar de wet- en regelgeving te worden opgenomen in de brief waarmee de opdracht wordt aanvaard.

wordt een voldoende gekwalificeerde externe deskundige ingezet. De inzet vindt op een zodanige wijze plaats dat de verantwoordelijkheid voor de door de externe deskundige uitgevoerde werkzaamheden, kan worden gedragen. De opdracht voor de externe deskundige wordt mondeling besproken zodat geen misverstanden ontstaan omtrent de scope van de werkzaamheden in relatie tot de opdracht. De afspraken worden schriftelijk vastgelegd en door beide partijen ondertekend. De bevindingen van de externe deskundige worden besproken en tevens wordt het dossier van deze deskundige gereviewd. De belangrijkste delen van het dossier van de externe deskundige worden toegevoegd aan het eigen dossier. Deze activiteiten blijken uit vastleggingen in het dossier.

Opdrachtgerichte kwaliteitsbeoordeling

Voor sommige opdrachten dient een Opdrachtgerichte Kwaliteitsbeoordeling door een RE te worden uitgevoerd. Om te bepalen of een OKB moet worden uitgevoerd, wordt de Handreiking Opdrachtgerichte kwaliteitsbeoordeling (OKB) gebruikt. Voor aanvang van elke opdracht wordt bepaald of een OKB nodig is.

De geldende criteria (zie Handreiking OKB) zijn (deze dienen expliciet te worden uitgewerkt):

- De aard van de opdracht, alsmede de mate waarin het openbaar belang daarbij betrokken is;
- Het signaleren van ongebruikelijke omstandigheden of risico's ten aanzien van een opdracht of groep opdrachten;
- De omstandigheid dat wet- of regelgeving een opdrachtgerichte kwaliteitsbeoordeling voorschrijft.

Zo kan een OKB bijvoorbeeld worden uitgevoerd bij (niet limitatief):

- Assuranceopdrachten
- Opdrachten met een grotere fee dan […]
- Opdrachten voor beursgenoteerde ondernemingen
- Opdrachten voor financiële instellingen
- Opdrachten waarbij een externe deskundige wordt ingeschakeld
- Opdrachten buiten de landsgrenzen
- Rapporten voor brede verspreidingskring

Bij de OKB wordt gekeken naar o.a. (ontleend uit de Handreiking OKB):

- de deskundigheid van het opdrachtteam
- de onafhankelijkheid van het opdrachtteam ten opzichte van de opdrachtgever
- de afbakening van verantwoordelijkheden van de [IT-auditorganisatie] ten opzichte van de opdrachtgever in de opdrachtbevestiging
- de inhoud van de opdrachtbevestiging
- het werkprogramma
- de (concept)rapportage
- signalering van risico's
- werkzaamheden van opdrachtteam en eindverantwoordelijke

Om te voorkomen dat de opdrachtgerichte kwaliteitsbeoordeling tot belangrijke bevindingen leidt die niet (meer) kunnen worden opgelost, wordt het onderzoek tijdig op daartoe geschikte momenten tijdens de uitvoering van de opdracht uitgevoerd.

Gezien het kleinschalige karakter van [IT-auditorganisatie] zijn met de samenwerkings-organisatie de volgende afspraken over het uitvoeren van de OKB gemaakt:

- de OKB wordt uitgevoerd op basis van de meest recente versie van de 'Handreiking Opdrachtgerichte kwaliteitsbeoordeling (OKB)' van NOREA;
- de samenwerkingsorganisatie bewaakt dat haar objectiviteit niet negatief wordt beïnvloed als gevolg van consultaties en/of een review over de uitvoering van de opdracht;
- de samenwerkingsorganisatie rapporteert haar bevindingen schriftelijk op een zodanig tijdstip dat de door [IT-audit-organisatie] met de cliënt overeengekomen rapportagedatum kan worden gerealiseerd;
- de samenwerkingsorganisatie verstrekt een kopie van haar dossier over de OKB aan [IT-audit-organisatie].

Bij een verschil van inzicht over de inhoud van de rapportage, wordt de afweging om het rapport toch uit te brengen expliciet vastgelegd in het dossier. De bevindingen van de samenwerkings-organisatie worden in het dossier opgenomen.

7.5 Dossiervorming en documentatie

Tenzij anders vermeld vindt dossiervorming digitaal plaats. Alle aangemaakte (werk)documenten, offertes, audit-evidence en (concept-)rapportages worden opgeslagen in [informatiesysteem].

Het belangrijkste uitgangspunt voor het opstellen en bewaren van documentatie is dat dit zodanig plaatsvindt dat een ervaren IT-auditor die voorheen niet betrokken was bij de opdracht in staat is om inzicht te verkrijgen in de aard, de tijdsfasering en de omvang van de werkzaamheden die zijn uitgevoerd om te voldoen aan:

- de Richtlijnen en de vereisten voortkomend uit de van toepassing zijnde wet- en regelgeving;
- de uitkomsten van de werkzaamheden en de verkregen informatie voor de onderbouwing van de uitkomst van de professionele dienst waarbij sprake is van een(eind)rapport;
- de belangrijke onderwerpen die tijdens de uitvoering van de opdracht aan het licht zijn gekomen;
- de daaruit getrokken conclusies en belangrijke vakkundige oordeelsvormingen bij het trekken van die conclusies.

Het dossier bevat daarvoor de relatie tussen:

- de opdracht,
- de gehanteerde normering,
- het controleplan
- de uitvoering van het onderzoek
- de bevindingen
- de conclusies
- het oordeel / advies / de bevindingen, et cetera.

Voor de documentatie van opdrachten waarbij sprake is van een (eind)rapport, geldt de Richtlijn Documentatie 230 van de NOREA. [IT-audit organisatie] volgt de aanwijzingen in deze richtlijn

voor alle professionele diensten, ook bij opdrachten waarbij geen sprake is van een (eind)rapport.

Toegang tot het dossier moet worden beperkt tot de daarvoor door de [IT-auditorganisatie] aangewezen - bevoegde personen.

Het proces 'dossiervormingen documentatie' start op het moment dat een offerte wordt opgesteld.

Het opdrachtdossier heeft bijvoorbeeld de volgende submappen:

Naar behoefte kan het dossier nog andere submappen bevatten, bijvoorbeeld 'Data-analyse'.

Dossiers worden minimaal 7 jaar bewaard zodat deze voor de evaluatie van de werking van de kwaliteitsbewakingsprocedures uitvoeren beschikbaar zijn. In gevallen dat wet- of regelgeving hier bijzondere richtlijnen voor geven, worden de termijnen van de betreffende wet- of regelgeving aangehouden.

7.6 Rapportage en (verplichte formulering inzake) oordelen

Een belangrijk 'product' van de diensten van [IT-audit organisatie] is het (eind)rapport. Het rapport bevat een oordeel (assurance), bevindingen, conclusies en/of aanbevelingen, adviezen en toont aan dat de IT-auditor heeft voldaan aan de vereisten om tot een oordeel, de bevindingen en/of conclusies dan wel adviezen te komen.

Voor rapportage inzake de verschillende diensten (Assurance, IT-audit, advies, et cetera) zijn (worden) door de NOREA verschillende templates ontwikkeld. In beginsel gebruikt [IT-auditorganisatie] de templates van de NOREA.

8 Monitoren en verbeteren kwaliteitsbeheersingssysteem

De kleinschaligheid van de organisatie brengt mee dat aandacht moet worden besteed om op een objectieve wijze aan de eisen ten aanzien van het monitoren van het kwaliteits-beheersingssysteem te kunnen voldoen. Met de volgende maatregelen wordt hier aan voldaan:

a. Het jaarlijks invullen van het self assessment van NOREA en het zo nodig aanpassen van het kwaliteitsbeheersingssysteem op basis van de uitkomsten van het assessment.

b. De door [samenwerkingsorganisatie] uitgevoerde OKB voor opdrachten die aan de criteria voldoen en het zo nodig aanpassen van het kwaliteitsbeheersingssysteem op basis van de uitkomsten van de OKB.

Bijlage 1 voorbeeld cliënt-acceptatieformulier

SAMENVATTING VAN HET CLIËNT ACCEPTATIEPROCES

Cliënt gegevens	
Organisatienaam	
Branche	
Cliënt risicoprofiel (indien gebruikt)	

[Korte toelichting waarom de (toekomstige cliënt kan worden geaccepteerd / de relatie met de bestaande cliënt kan worden gecontinueerd]

Conclusie

(gebaseerd op de in de vragenlijst vermelde bevindingen)

I	Betekent de (toekomstige) cliënt een verhoogd risico voor de reputatie van de IT-auditorganisatie? *Indien 'Ja', specificeer het antwoord*	Ja/Nee
II	Zijn ten aanzien van de (toekomstige) cliënt gegevens bekend met betrekking tot financiële problemen of zaken die de algehele continuïteit van de onderneming betreffen, waardoor het risico bestaat dat deze niet in staat is de afgesproken fee te betalen? *Indien 'Ja', specificeer het antwoord*	Ja/Nee

Risico classificatie en mitigatie

Gebaseerd op de evaluatie is het risicoprofiel van de (toekomstige) cliënt:	Hoog / Medium / Laag risico
Indien het risico is geclassificeerd als 'Hoog' of 'Medium', kan het risico worden gemitigeerd? *Indien 'Ja', specificeer de gewenste activiteiten om het risico / de risico's te mitigeren*	Ja/Nee

Beslissing client acceptatie

Functie	Naam	Datum	Approved
[Beslisser]			Ja/Nee/ onder voorwaarden

Voorwaarden waaronder de (toekomstige) cliënt kan worden geaccepteerd / de relatie met de bestaande cliënt kan worden gecontinueerd:

VRAGENLIJST CLIENT ACCEPTATIE

Opmerking: Deze vragenlijst kan zowel worden gebruikt voor acceptatie van een nieuwe cliënt als de voortzetting van een bestaande cliënt-relatie.

Hoofdstuk 1 – Geassocieerde risico's – Identiteit en Integriteit

1.0	Zijn er -op basis van de achtergrondcheck en de bestaande kennis van de (toekomstige) cliënt, bedenkingen of twijfels met betrekking tot de integriteit van: • De (toekomstige) cliënt • Het management • De audit committee (indien van toepassing) • De eigenaren, aandeelhouders, het bestuur en/of het besturend orgaan? *[Indien 'Ja' vul dan in de onderstaande textbox de aard van de bedenkingen of twijfels in]*	Ja/Nee
1.0.1	Zijn er sinds de laatste cliënt evaluatie wijzigingen opgetreden in strategisch management of eigenaarschap? [*alleen van toepassing bij voortzetting bestaande cliënt-relatie*]	Ja/Nee
1.1.1	Bevestig dat adequate identiteitscontroles hebben plaatsgevonden, vereist door wet- en regelgeving (inclusief toepasselijke anti wit-was wetgeving)	Ja/Nee
1.1.2	Bevestig dat toepasselijke achtergrondchecks zijn uitgevoerd en gedocumenteerd.	Ja/Nee
1.1.3	Bevestig dat er geen (familiaire) banden bestaan met individuen in de organisatie van de (toekomstige) cliënt die een toezichthoudende taak hebben.	Ja/Nee
1.2.1	Zijn één of meer van de volgende issues geïdentificeerd in relatie tot 1.0? • Aanzienlijke wetsovertreding, of • Onderzoeken (bestaand of in het verleden) door geschillen met autoriteiten, of • Verdenking van wit-wassen, fraude, oneigenlijk gebruik van fondsen, of • Bedenkelijke bedrijfsethiek?	Ja/Nee

Eventuele toelichting (Hoofdstuk 1)

Hoofdstuk 2 – Geassocieerde risico's – gelieerd aan de business van de cliënt

2.0	Is er sprake van een verhoogd risico door de aard van de business of de manier van zaken doen door de (toekomstige) cliënt? (denk aan financiële risico's, negatieve publiciteit, etc.) *[Indien 'Ja' vul dan in de onderstaande textbox de aard van de verhoogde risico's in]*	Ja/Nee
2.1.1	Beschrijf in Bijlage 1 in het kort de business (processen) van de (toekomstige) cliënt.	
2.1.2	Selecteer uit onderstaande lijst de van belang zijnde risico-indicatoren bij de (toekomstige) cliënt: • betrokkenheid in het bedrijfsleven / industrie die wordt gezien als potentieel onethisch (bv. internet gaming, andere als lokaal geïdentificeerde) of hoger risico. • management is niet bekwaam in de specifieke branche. • historie van mislukte ondernemingen. • historie van geschillen met adviseurs en andere partijen. • recente, significante wijzigingen in de aard van de business. • recente, significante wijzigingen en/of niet verklaarbare wijziging in strategisch management. • Gebrek aan capaciteit voor het operationele en financiële beheer. • Gebrek aan corporate governance[2] • Ontbreken van een duidelijke redden waarom de toekomstige cliënt kiest voor deze IT-auditorganisatie[3] • Betrokken bij omstreden politieke kwesties • Op andere wijze negatief in de publiciteit door de activiteiten of eigenaarschap	

Eventuele toelichting (Hoofdstuk 2)

[2] Alleen voor OOB organisaties

[3] Alleen voor toekomstige klanten

Hoofdstuk 3 – Geassocieerde risico's – relatie met andere IT-auditorganisaties

3.0	Is er kans op reputatieschade bij andere IT-auditorganisaties indien de toekomstige cliënt wordt geaccepteerd of de bestaande relatie wordt gecontinueerd? *[Indien 'Ja' vul dan in de onderstaande textbox de aard van de mogelijke reputatieschade in]*	Ja/Nee
3.1.1	Is de (toekomstige) cliënt (of de moeder organisatie) ook cliënt bij een andere IT-auditorganisatie?	Ja/Nee
3.1.2	Selecteer uit onderstaande lijst de van belang zijnde risico-indicatoren bij de (toekomstige) cliënt: • de toekomstige cliënt is recent geweigerd door onze of een andere IT-auditorganisatie • een aan de toekomstige cliënt gelieerde organisatie is recent geweigerd door onze of een andere IT-auditorganisatie. • wij hebben eerder discussies gehad met de cliënt of moederorganisatie. • een andere IT-auditorganisatie heeft specifieke risico's geïdentificeerd bij de (toekomstige) cliënt. • De relatie met de (toekomstige) cliënt roept bij anderen vragen oproepen over de integriteit van onze organisatie.	

Eventuele toelichting (Hoofdstuk 3)

Hoofdstuk 4 – Geassocieerde risico's – reputatie- of imagoschade

4.0	Is er een (verhoogde) kans op reputatieschade indien de toekomstige cliënt wordt geaccepteerd of de relatie met de cliënt wordt gecontinueerd? *[Indien 'Ja' vul dan in de onderstaande textbox de aard van de mogelijke reputatieschade in]*	Ja/Nee

Eventuele toelichting (Hoofdstuk 4)

Hoofdstuk 5 – Financiële risico's

5.0	Is er sprake van financiële of andere problemen bij de (toekomstige) cliënt die een bedreiging vormen voor het voortbestaan van de cliënt of vermogen om onze facturen te betalen? *[Indien 'Ja' geef dan in de onderstaande textbox aan waarop dit is gebaseerd]*	Ja/Nee
5.1.1	Selecteer uit onderstaande lijst de van belang zijnde risico-indicatoren bij de (toekomstige) cliënt: • verzuim bij contracten, leningen e.d. • verzuim bij betaling leveranciers/adviseurs e.a. • slechte liquiditeit • Faillissement of soortgelijke status • slechte krediet positie • dalende operationele en financiële resultaten • actief in een financieel economisch ongunstig bekend staande branche	

Eventuele toelichting (Hoofdstuk 5)

Bijlage 2 Voorbeeld risk assessment audit- en adviesdiensten KITA

Risk Assessment audit- en adviesdiensten [IT-audit organisatie]

Processtap	Risicoinventarisatie	Kans	Impact	Risico	Maatregel(en)	Kans	Impact	Risico	Borging
Algemeen	Medewerkers zijn niet op de hoogte van de richtlijnen m.b.t. interne procedures.	H	H	**H**	introductie training, informeren bij wijzigingen, evaluatie via functioneringsgesprekken	L	H	**M**	Introductietraining bij aanvang van nieuwe medewerkers. Borging door monitoring van medewerkers
Algemeen	Uitlekken en comprimeren van vertrouwelijke informatie	H	H	**H**	Security baseline opstellen (maatregelen treffen zoals encryptie, toegangscontrole, autorisatie, beleid)	L	H	**M**	Permanente sociale controle
Algemeen	Niet naleving interne procedures/richtlijnen	M	H	**M**	Discipline beleid, interne controle (o.a. technische review)	L	M	**L**	Binnen beleid zijn sancties bepaald voor het niet naleven van procedures en richtlijnen. Technische review controleert op een aantal belangrijke aspecten betreffende procedurele maatregelen.

Processtap	Risicoinventarisatie	Kans	Impact	Risico	Maatregel(en)	Kans	Impact	Risico	Borging
Aanvraag/aanvraag evaluatie	Juiste competenties auditor niet aanwezig	H	H	**H**	Aanname beleid, competentie tabel, opleidingen, raamcontract i.g.v. extern	L	H	**M**	Monitoring van auditors
Aanvraag/aanvraag evaluatie	Onterechte toezeggingen naar de klanten	M	M	**M**	Functiescheiding, goedkeuring door management kritische informatie, Procedure 'communicatie'	L	M	**L**	Contracten, offertes en andere externe communicatiemiddelen gaan via directie. Rolprofielen met TBV's.
Aanvraag/ aanvraag evaluatie	Solvabilitiet aanvrager onvoldoende	M	H	**M**	Controle in KvK register (insolventie)	M	H	**M**	
Aanvraag/ aanvraag evaluatie	Klant verstrekt onjuiste informatie	M	M	**M**	Opgegeven informatie controleren	L	M	**L**	Gegevensverificatie tijdens eerste bezoek
Algemeen	Onpartijdigheidrisico	M	H	**M**	Opdracht evaluatie t.o.v. geidentifceerde risico's en gerichte maatregelen	L	M	**L**	
Algemeen	Onvolledigheid Dossier(s) (intergriteit en juistheid)	M	H	**M**	Interne audits, procedure 'dossiervorming'	M	H	**M**	
Algemeen	Beschikbaarheid van gegevens	H	H	**H**	Backup procedures	L	H	**M**	Periodiek toetsing of restore mogelijk is

Processtap	Risicoinventarisatie	Kans	Impact	Risico	Maatregel(en)	Kans	Impact	Risico	Borging
Offerte opstellen	Onjuiste uitgebrachte offertecalculatie	M	M	**M**	Controle van offertegegevens. Escape clausule in voorwaarden vastleggen als de aangeleverde informatie onjuist / onvolledig is.	M	M	**M**	
Offerte opstellen	Beschikbaarheid van de auditors/materiedeskundige	H	M	**M**	Interne trainingen, externe middelen inhuren	L	M	**L**	Offerte evaluatie of opdracht kan worden uitgevoerd ,Inhuren van extern personeel, Uitbesteden van diensten
Offerte opstellen	Voorwaarden van dienstverlening zijn onvoldoende overeengekomen met de klant	M	H	**M**	Informatiebronnen voor klanten identificeren en beschikbaar stellen	L	M	**L**	Algemene voorwaarden
Aanvraag/ aanvraag evaluatie	Vereiste competenties zijn niet binnen het auditteam aanwezig	M	H	**M**	Inhuren extern, Opdracht niet aanvaarden	L	L	**L**	Competentie management, Permanente educatie, Inhuren extern, Opdracht niet aanvaarden

Processtap	Risicoinventarisatie	Kans	Impact	Risico	Maatregel(en)	Kans	Impact	Risico	Borging
Selectie externe auditor	Niet bekend met interne procedures/richtlijnen	H	H	**H**	Uitbesteding beschrijven, competentie eisen extern personeel beschrijven, Beleid / richtlijnen en procedures beschikbaar stellen. Competentie toetsing	L	M	**L**	Raamcontract, beschikbaar stellen interne procedures. Borging door Periodiek evaluatie audits (monitoring), functioneringsgesprekken, technische review van rapporten
Algemeen	Vereiste resources niet beschikbaar (MAPGOOD)	M	M	**M**		M	M	**M**	
Contract opstellen	Contract voldoet niet aan de wetgeving en/of externe c.q. interne richtlijnen	M	M	**M**	Periodiek contract templates evalueren.	L	M	**L**	Contracten, offertes en andere externe communicatiemiddelen (met rechtmatige binding) gaan via directie en vallen onder documentbeheersing
Contract opstellen	Onbevoegden tekenen het contract (vanuit de klant)	L	M	**L**	Geaccepteerd risico	L	L	**L**	
Audit uitvoeren	Onverwachte uitval van personeel	L	M	**L**	Geaccepteerd risico	L	L	**L**	Mogelijkheid tot inhuren extern personeel
Algemeen	Onafhankelijkheid risico's	M	H	**M**	opdracht evaluatie t.o.v. geïdentificeerde risico's en gerichte maatregelen	L	L	**L**	

Processtap	Risicoinventarisatie	Kans	Impact	Risico	Maatregel(en)	Kans	Impact	Risico	Borging
Algemeen	Aansprakelijkheid bij het niet nakomen van contractverplichtingen	M	M	**M**	Kleine financiële aansprakelijkheden -> uit kas, Grotere -> limiteren in algemene voorwaarden (deze nimmer laten uitsluiten!) en buffer in financiële middelen, geen tijdig personeel -> inhuren extern.	M	L	**L**	Financiële buffer ter grootte van het gemiddelde verzekeringsbedrag en conform algemene voorwaarden: de maximale omzet bij een klant in het afgelopen jaar. Jaarlijkse forecast vaststellen in januari.
Algemeen	Afhankelijkheid van één eigen auditor	M	H	**H**		M	L	**L**	
Samenwerking met andere auditorganisatie	Verlies van klanten doordat andere auditorganisaties een breder pakket aanbieden of goedkoper zijn	H	H	**H**	Alleen samenwerking met auditorganisaties die inhoudelijk andere diensten leveren	L	H	**M**	Onderlinge afspraken maken met andere auditorganisaties
Samenwerking met andere auditorganisatie	Samenwerking betekent samen plannen met de andere auditorganisaties en in gecombineerde teams werken om (voor de klant) tijd te besparen. Risico met afstemming planning.	M	M	**M**	Afspraken hierover dienen geformaliseerd te worden	L	M	**L**	Overleg met andere auditorganisatie en afstemmen van een goede borging