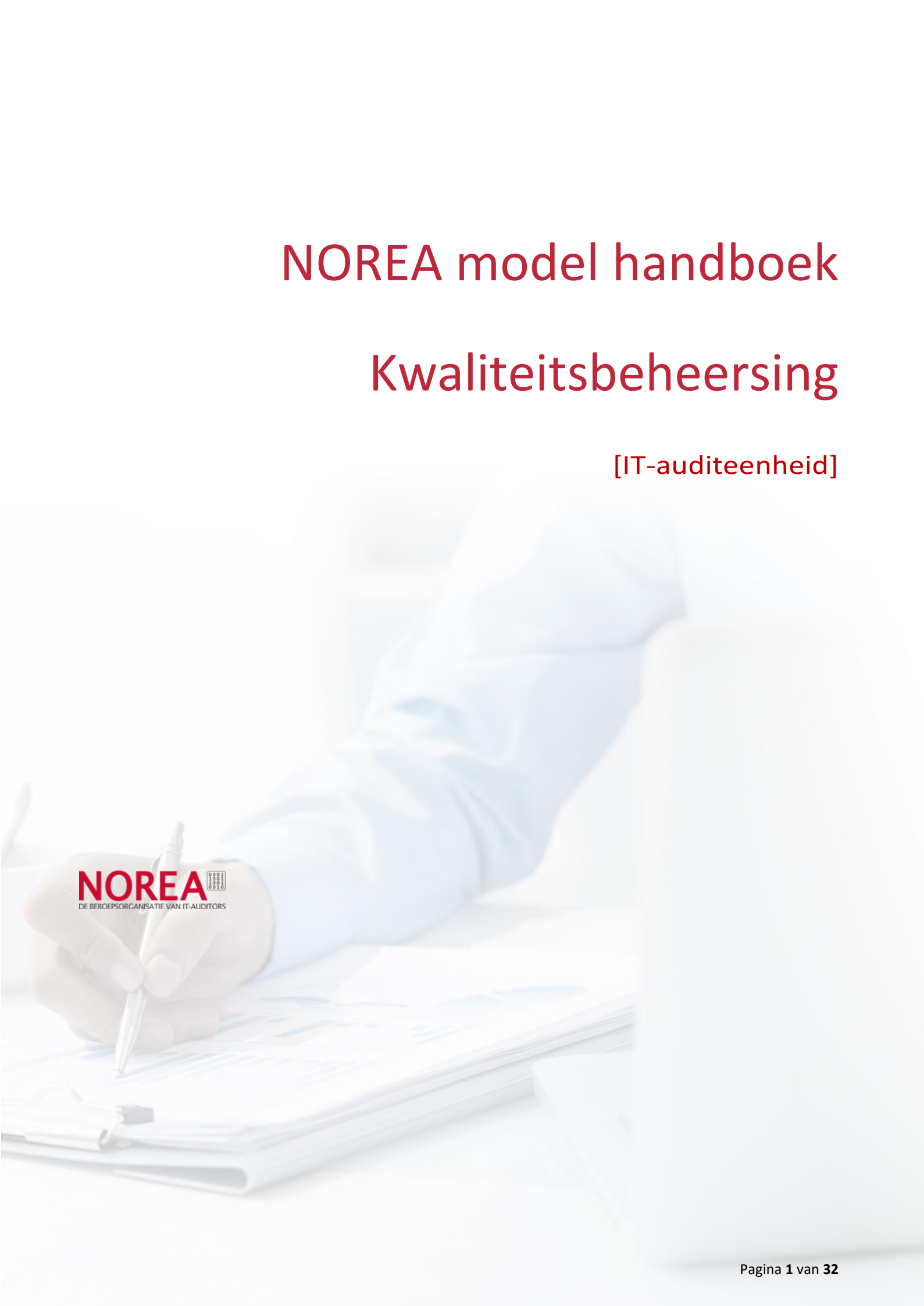
NOREA model handboek

Kwaliteitsbeheersing

[IT-auditeenheid]



Versiebeheer[1]				
Versie	Datum	Status	Naam	Omschrijving
0.1-0.8	05-08-2013	Werkversies	Frank Kossen	Template Handboek KITA opgesteld in opdracht van NOREA.
0.9	08-09-2013	Conceptversie	Frank Kossen	Om commentaar voorgelegd aan CKO.
0.99	09-10-2013	Conceptversie	Frank Kossen	Commentaar CKO (H. de Zwart) verwerkt. Versie om commentaar voorgelegd aan Commissie Beroepsregels en Vaktechnische Commissie.
1.0	01-11-2013	Definitieve versie	Frank Kossen	Commentaar Commissie Beroepsregels en Vaktechnische Commissie verwerkt en definitief exemplaar beschikbaar voor NOREA leden.
2.0	05-02-2020	Definitieve versie	Jan de Heer	Aanpassen aan actualiteit en vaktechnische verbeteringen aangebracht.
2.1	23-06-2025	Conceptversie	Mohamed El Aarbaoui Frank Kossen	Aanpassingen naar aanleiding van RKBN 2025. Versie om commentaar voorgelegd aan CKO.
2.2	30-06-2025	Conceptversie	Mohamed El Aarbaoui Frank Kossen	Commentaar CKO verwerkt en versie beschikbaar gesteld voor consultatieronde (voor NOREA leden).
3.0	16-07-2025	Definitieve versie	Mohamed El Aarbaoui Frank Kossen	Commentaar uit consultatieronde verwerkt en definitief exemplaar beschikbaar voor NOREA leden.

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-auditeenheden (KITA's) hier behoefte aan hebben.

Nadrukkelijk merkt NOREA op dat de IT-auditeenheid 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 beperkt aantal IT-auditor (RE) en een beperkt aantal personeelsleden, die al dan niet zijn ingeschreven als RE.

Ook andere (grotere) IT-auditeenheden kunnen (delen van) dit model-handboek gebruiken bij het opzetten van een dergelijk systeem.

[1] Dit is het versiebeheer van het model-handboek. De IT-auditeenheid dient zelf ook versiebeheer toe te passen voor het eigen specifiek gemaakte handboek.

Vastgesteld door	[IT-auditeenheid]
Goedgekeurd door	
Handtekening	
Versie	x.x
Status	[status]
Datum	[datum vastgesteld door directie]
Aantal bladzijden	

Inhoudsopgave

1 Inleiding

1.1 Context

Op 1 januari 2009 is het Reglement Kwaliteitsbeheersing NOREA (hierna: RKBN) in werking getreden. Het RKBN is van toepassing op alle IT-auditors van [IT-auditeenheid] die assurance, aan assurance verwante en overige diensten[2] (hierna: professionele diensten) verrichten. Met de invoering van ISQM 1 en 2 vanuit de International Federation of Accountants (IFAC) heeft NOREA besloten om het bestaande RKBN aan te passen. De aangepaste ISQM 1 en 2 zijn opgenomen als deel 2 en deel 3 van het RKBN 2025. De delen 2 en 3 van het RKBN 2025 zijn van toepassing op IT-auditeenheden die assurance of aan assurance verwante onderzoeken (zoals opdrachten tot het verrichten van overeengekomen specifieke werkzaamheden) uitvoeren. Het RKBN 2025 is van kracht voor opdrachten die aanvangen op of na 1 juli 2025. In dit Handboek Kwaliteitsbeheersing (hierna: Handboek) zijn de aanpassingen naar aanleiding van de invoering van het RKBN 2025 doorgevoerd. RKBN 2025 wordt in dit Handboek verder aangeduid als RKBN.

1.2 Doelstelling

De doelstelling van dit Handboek is het vaststellen van grondbeginselen en procedures en het geven van aanwijzingen met betrekking tot de verantwoordelijkheden van [IT-auditeenheid] voor haar kwaliteitsbeheersingssysteem ten aanzien van assurance-, aan assurance verwante en andere opdrachten zoals adviesopdrachten. Het kwaliteitsbeheersingssysteem van [IT-auditeenheid] 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 en dat de door [IT-auditeenheid] of haar voor opdrachten verantwoordelijke professional afgegeven rapporten onder de gegeven omstandigheden voldoen aan de reglementen, richtlijnen en handreikingen die door NOREA zijn uitgevaardigd.

1.3 Verklaring van uitgifte

In dit Handboek beschrijft [IT-auditeenheid] de gedragslijnen en procedures van het kwaliteitsbeheersingssysteem. De Directie van [IT-auditeenheid] aanvaardt met de goedkeuring en ondertekening van dit Handboek de eindverantwoordelijkheid voor het kwaliteitsbeheersingssysteem van [IT-auditeenheid].

Het kwaliteitsbeheersingssysteem van [IT-auditeenheid] is gericht op het onderhouden en beheersen van alle processen welke vereist zijn om professionele diensten uit te kunnen voeren onder de beroepsregels en het toezicht van NOREA. Het systeem is gebaseerd op het RKBN. Het systeem omvat aspecten zoals risico-inschattingsproces, governance, ethische voorschriften, opdrachtuitvoering, middelen, communicatie en monitoring.

Dit Handboek moet als geheel worden gezien met de samenhangende documenten (o.a. richtlijnen en handreikingen van NOREA). Het beschrijft het Kwaliteitsbeheersingssysteem en hoe uitvoering wordt gegeven aan de eisen uit het RKBN. Het doel van het Handboek is inzicht te geven in de wijze waarop binnen [IT-auditeenheid] het beleid en bedrijfsprocessen zijn geborgd. Dit Handboek wordt bekend gemaakt aan de medewerkers van [IT-auditeenheid] en anderen die namens [IT-auditeenheid] professionele diensten uitvoeren, o.a. door bijvoorbeeld publicatie op het interne netwerk of het meesturen met samenwerkingsovereenkomsten.

[2] Let op: indien de IT-auditeenheid assurance-opdrachten inzake het IT-Jaarverslag uitvoert, dienen hiervoor de nodige richtlijnen en procedures te worden opgesteld en te worden verwerkt in het Handboek van [IT-auditeenheid]. Deze zijn nu (nog) niet in dit model-handboek opgenomen (zie hiervoor ook: *Deel 2 - Richtlijn KwaliteitsBeheersing NOREA (RKBN).*

1.4 Opbouw van het Handboek kwaliteitsbeheersing

Dit Handboek omschrijft de wijze waarop [IT-auditeenheid] de professionele diensten uitvoert in relatie tot het 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 [IT-auditeenheid] geconcretiseerde richtlijnen en werkinstructies worden opgesteld. De effectiviteit van het kwaliteitsbeheersingssysteem wordt geborgd door monitoring en remediëring welke nader zijn beschreven in hoofdstuk 9.

1.5 Reikwijdte van het Handboek kwaliteitsbeheersing

De reikwijdte van dit Handboek betreft alle professionele diensten, zoals assurance, aan assurance verwante en overige diensten, uitgevoerd door [IT-auditeenheid].

1.6 Beheer van het Handboek kwaliteitsbeheersing

Het beheer van dit Handboek en bijbehorende documenten ligt bij de Directie of bij een door de Directie aan te wijzen medewerker van [IT-auditeenheid]. Voor de inhoud van het Handboek draagt de Directie de eindverantwoordelijkheid. Om deze verantwoordelijkheid gestalte te geven, wordt het Handboek vastgesteld door de Directie. Het Handboek kan om diverse redenen worden gewijzigd. De Directie 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 NOREA en het praktisch functioneren van [IT-auditeenheid]. Als dit niet het geval is, worden aanpassingen doorgevoerd. Ook kunnen opmerkingen worden gemaakt door andere partijen die in overweging worden genomen door [IT-auditeenheid]. Ook grote wijzigingen zoals bijvoorbeeld in processen, procedures, bedrijfsvoering, technologieën en/of wet- en regelgeving kunnen leiden tot wijziging van het Handboek.

1.7 Organisatiestructuur [IT-auditeenheid]

De organisatiestructuur is dusdanig opgezet dat risico's op het gebied van integriteit, objectiviteit[3], deskundigheid en zorgvuldigheid, geheimhouding en professioneel gedrag (de grondbeginselen van de Gedrag- en Beroepsregels RE) worden geminimaliseerd. Het kleinschalige karakter van [IT-auditeenheid] 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 kunnen[4] worden ondervangen door de inzet van [samenwerkingsorganisatie], een vaktechnisch deskundige organisatie op het gebied van IT-audit, waarmee (schriftelijke) afspraken zijn gemaakt voor samenwerking op het gebied van het kwaliteitsbeheersingssysteem.

Geef hier een beschrijving van de organisatie:

- *Rechtsvorm: bijvoorbeeld eenmanszaak, VOF, BV, NV, CV, etc.*
- *Gegevens Kamer van Koophandel.*
- *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(s);*

[3] Afgeleid van integriteit en objectiviteit is onafhankelijkheid. Sinds de herziening van de gedragscode voor IT-auditors (Code of Ethics) neemt dit een prominentere plaats in. Daarom dient dit expliciet te worden benoemd in het Handboek als de IT-auditeenheid assurance of aan assurance verwante diensten levert (zie paragraaf 4.1.2).

[4] Dit is (mede) afhankelijk van het wel of niet uitvoeren van assurance (of daaraan verwante) opdrachten; een KITA zonder dit type opdrachten hoeft dit niet op te zetten.

- *Aard van de uitgevoerde werkzaamheden.*

2 Risico-inschattingsproces

2.1.1 Algemeen

Het risico-inschattingsproces binnen [IT-auditeenheid] is een fundamenteel onderdeel van het Kwaliteitsbeheersingssysteem. Dit proces helpt om kwaliteitsrisico's te identificeren, te evalueren en passende maatregelen te treffen. Het doel van het risico-inschattingsproces is om kwaliteitsdoelstellingen vast te stellen, het identificeren en inschatten van kwaliteitsrisico's, het implementeren van beheersmaatregelen en het continu evalueren en aanpassen van het risico-inschattingsproces. Binnen [IT-auditeenheid] wordt een risicoanalyse-methodiek gebruikt om risico's te identificeren, te graderen en te reduceren tot een aanvaardbaar risico. De uitkomsten van deze risicoanalyse worden jaarlijks geactualiseerd (zie bijlage 2).

2.1.2 Wettelijke en contractuele risico's

[IT-auditeenheid] is een opzichzelfstaande juridische entiteit ([*rechtsvorm opnemen*]) die is ingeschreven bij de Kamer van Koophandel. Er zal een contract met geldende voorwaarden worden afgesloten met cliënten voor wie professionele diensten worden uitgevoerd. Voordat een contractuele overeenkomst wordt opgemaakt, zal de opdracht door [IT-auditeenheid] worden geanalyseerd op haalbaarheid en integriteits-/ objectiviteits-/ vertrouwelijkheids-/ 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.

2.1.3 Aansprakelijkheden en financiën

Financiële- en aansprakelijkheidsrisico's worden meengenomen in de risicoanalyse van [IT-auditeenheid]. Deze risicoanalyse wordt jaarlijks geactualiseerd.

3 Governance en leiderschap

De component governance en leiderschap van het Kwaliteitsmanagementsysteem schept de omgeving die de opzet, implementatie en werking van het kwaliteitsmanagementsysteem ondersteunt.

Hiervoor heeft [IT-auditeenheid] de volgende kwaliteitsdoelstellingen en -verantwoordelijkheden vastgesteld:

1. [IT-auditeenheid] hecht veel waarde aan commitment ten aanzien van kwaliteit binnen de gehele IT-auditeenheid. Hiertoe wordt de nadruk gelegd op de volgende aspecten:
    a. De rol van [IT-auditeenheid] bij het dienen van het openbaar belang door het consistent uitvoeren van opdrachten gekenmerkt door kwaliteit.
    b. Het belang van beroepsethiek, -waarden en -attitudes.
    c. De verantwoordelijkheid van alle medewerkers, alsook de samenwerkingsorganisatie(s) van [IT-auditeenheid] voor de kwaliteit van opdrachten of van activiteiten in het kader van het kwaliteitsbeheersingssysteem en het van hen verwachte gedrag.
    d. Het belang van de kwaliteit van de strategische beslissingen en acties van [IT-auditeenheid], met inbegrip van de financiële en operationele prioriteiten van het kantoor.
2. De Directie is eindverantwoordelijk voor kwaliteit en legt daar verantwoording over af.
3. De Directie geeft door haar handelingen en gedragingen blijk van commitment ten aanzien van kwaliteit.
4. De organisatiestructuur en de toewijzing van taken, verantwoordelijkheden en bevoegdheden zijn zodanig ingericht dat het Kwaliteitsbeheersingssysteem van [IT-auditeenheid] in werking is gesteld.
5. De behoeften aan bronnen, met inbegrip van financiële middelen, zijn gepland en middelen zijn verkregen, gealloceerd en toegewezen in lijn met commitment van [IT-auditeenheid] ten aanzien van kwaliteit.

[IT-auditeenheid] is een kleine IT-auditeenheid en zoals eerder genoemd is de eindverantwoordelijkheid bij de Directie belegd, maar dat laat niet onverlet dat alle medewerkers, alsook de samenwerkingsorganisatie(s) verantwoordelijk zijn voor de kwaliteit binnen [IT-auditeenheid]. Hoewel de Directie de toon aan de top zet door haar handelingen en gedragingen, dragen duidelijke, consistente en frequente handelingen en communicaties op alle niveaus van [IT-auditeenheid] bij tot de cultuur en tonen zij een commitment ten aanzien van kwaliteit. De relevante ethische vereisten stellen in het algemeen de beginselen van de beroepsethiek vast en worden meer in detail besproken in hoofdstuk 4 Relevante ethische voorschriften. Professionele waarden en attitudes die binnen [IT-auditeenheid] bijdragen aan het commitment ten aanzien van kwaliteit betreffen:

- professioneel gedrag (stiptheid, beleefdheid, respect, en het belang inzien van het afleggen van verantwoording, reactievermogen en betrouwbaarheid);
- commitment ten aanzien van teamwork en de IT-auditeenheid als geheel;
- openstaan voor nieuwe ideeën of andere perspectieven;
- het streven naar uitmuntendheid (bijv. ‘first time right’);
- voortdurende verbetering, bijvoorbeeld verwachtingen stellen die verder gaan dan de minimumvereisten en de nadruk leggen op voortdurend leren;
- sociale verantwoordelijkheid.

4 Relevante ethische voorschriften

4.1 Toepassing ethische normen

Het kwaliteitsbeheersingssysteem is gebaseerd op de vijf fundamentele beginselen uit de Gedragscode Register IT-auditors. [IT-auditeenheid] onderkent de noodzaak van deze grondbeginselen binnen haar professionele diensten. 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-auditeenheid] 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.

4.1.1 Integriteit

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

4.1.2 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 objectiviteit ten opzichte van de cliënt en andere belanghebbenden (bijvoorbeeld: nagegaan wordt of geen familiaire en/of financiële relaties bestaan, het niet verstrekken van aanbrengpremies). Als uitgangspunt geldt dat de aanvaarding van een assurance-opdracht kan niet worden gecombineerd met een adviesopdracht bij dezelfde cliënt.

De maatregelen zijn gericht op onder andere het nagaan:

- bij het aanvaarden van een opdracht of de relatie met de cliënt niet leidt tot een belangenverstrengeling met andere cliënten wier belangen worden behartigd;
- 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.

4.1.3 Vakbekwaamheid en zorgvuldigheid

Voor een geloofwaardige, effectieve en juiste beoordeling/ uitvoering van opdrachten zijn de juiste competenties van de IT-auditors binnen [IT-auditeenheid] van groot belang. De IT-auditors binnen [IT-auditeenheid] volgen zowel gestructureerde als ongestructureerde educatie. Minimaal wordt voldaan aan de eisen gesteld in de NOREA Richtlijn Permanente Educatie. De directie van [IT-auditeenheid] ziet hierop 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. Verder is het van belang om zorgvuldig te handelen en in overeenstemming met toepasselijke technieken en professionele standaarden.

4.1.4 Vertrouwelijkheid

Tijdens de uitvoering van de professionele diensten kan toegang tot vertrouwelijke informatie van de cliënt noodzakelijk zijn. Binnen [IT-auditeenheid] zijn interne afspraken hierover vastgelegd, gecommuniceerd naar medewerkers (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.

4.1.5 Professionaliteit

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

- het auditberoep niet in diskrediet brengt bij het aanprijzen van zichzelf of haar werk;
- 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;
- geen afkeurende verwijzingen maakt naar het werk van een andere IT-auditor of IT-auditeenheid of hier niet onderbouwde vergelijkingen naar doet.

[IT-auditeenheid] borgt het professioneel gedrag binnen de organisatie door periodiek aandacht te besteden aan dit onderwerp, cursussen te organiseren of te volgen, et cetera.

In sommige gevallen (te denken valt o.a. aan het verbieden van het aannemen of geven van geschenken en gastvrijheid van een cliënt en de vaste roulatieperioden voor alle opdrachtpartners) kunnen de aangelegenheden die in het Kwaliteitsbeheersingssysteem van [IT-auditeenheid] aan de orde komen, specifieker zijn dan, of een aanvulling vormen op, de bepalingen van de desbetreffende ethische vereisten. In dit geval worden in overleg met de Directie de nodige stappen bepaald.

4.2 Verantwoordelijkheid

Het is de verantwoordelijkheid van [IT-auditeenheid] 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 doorgaans is 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 beoordelings- en rapportage-eisen per type beoordeling vastgelegd, op basis van de richtlijnen van NOREA. De geauditeerde organisatie is verantwoordelijk voor het voldoen aan de eisen vanuit de getoetste norm(en).

5 Middelen

5.1 Human resources

5.1.1 Competentie en beschikbaarheid van management en personeel

Om geloofwaardige professionele diensten te kunnen uitvoeren bepaalt [IT-auditeenheid] 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.

5.1.2 Personeel betrokken bij professionele diensten

Bij de selectie van personeel stelt [IT-auditeenheid] vast dat bij betrokkene gevoel aanwezig is voor eisen die samenhangen met het Kwaliteitsbeheersingssysteem. Het personeel van [IT-auditeenheid] 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-auditeenheid] beschikt over overzichten/matrices waar competenties zijn beschreven. Op basis van uitgevoerde opdrachten worden vaardigheden geëvalueerd. Indien vanuit de evaluaties trainingbehoeften worden geïdentificeerd wordt hierop geanticipeerd. Door middel van de activiteitenplanning wordt geborgd dat de juiste personen de werkzaamheden bij de cliënt uitvoeren. De uitkomst van deze evaluatie wordt in het Opdrachtdossier opgenomen.

5.1.3 Gebruik van externe auditors en materiedeskundigen

Indien binnen een opdrachtteam gebruik wordt gemaakt van externen, dienen deze zich te committeren aan de gedragsregels van [IT-auditeenheid]. Er wordt een contract opgesteld tussen [IT-auditeenheid] en de externe dienstverlener/ samenwerkingsorganisatie waarin alle eisen zijn vastgelegd m.b.t. de dienstverlening.
Indien de externe wordt ingezet voor een specifieke opdracht, maakt dit contract onderdeel uit van het Opdrachtdossier.

5.1.4 Personeelsdossiers

[IT-auditeenheid] houdt van het eigen personeel dossiers bij met aantoonbare registraties van competenties, kwalificaties, uitgevoerde diensten en werkervaring. Personeelsdossiers kunnen zowel digitaal als fysiek worden bewaard. [IT-auditeenheid] verkrijgt jaarlijks een gedocumenteerde bevestiging van de naleving van de onafhankelijkheidsvoorschriften van de medewerkers die op grond van relevante ethische voorschriften vereist zijn onafhankelijk te zijn.

5.1.5 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 vertrouwelijkheid en professionaliteit. [IT-auditeenheid] erkent dat zij als eindverantwoordelijke partij richting de cliënt zal optreden. De afspraken maken onderdeel uit van het Opdrachtdossier.

5.2 Technologische middelen

[IT-auditeenheid] beschikt over passende technologische middelen om het uitvoeren van opdrachten mogelijk te maken en de werking van het Kwaliteitsbeheersingssysteem aan te tonen. Dit betreffen de netwerkomgeving waarin de

Opdrachtdossiers en de interne documenten (Handboek, procedures, richtlijnen etc.) zijn opgeslagen, de e-mailtoepassing en de mogelijkheid voor het veilig uitwisselen van documentatie met cliënten (zoals het creëren van zipbestanden met een (veilig) wachtwoord).

5.3 Intellectuele middelen

Relevante intellectuele middelen, zoals schriftelijk vastgelegde beleidslijnen, procedures en handleidingen, worden door [IT-auditeenheid] beschikbaar gesteld aan alle medewerkers. Het doel van deze intellectuele middelen is om de werking van het kwaliteitsbeheersingssysteem op consistente wijze uit te voeren. Deze intellectuele middelen zijn consistent met professionele standaarden en, in voorkomend geval, met van toepassing zijnde vereisten uit wet- en regelgeving.

5.4 Service providers

Note: In bepaalde omstandigheden kan een IT-auditeenheid gebruik maken van middelen die door een service provider ter beschikking worden gesteld. Te denken valt hierbij aan o.a. aan Clouddiensten zoals Microsoft 365. Mocht dit het geval zijn, dient in deze paragraaf te worden beschreven welke middelen van welke service provider worden afgenomen en wordt benadrukt dat [IT-auditeenheid] zelf verantwoordelijk blijft voor het eigen Kwaliteitsbeheersingssysteem.

6 Informatie en communicatie

Het proces van informatie en communicatie is over het algemeen een continu proces, gericht op het mogelijk maken van de werking van het kwaliteitsbeheersingssysteem.

6.1 Algemeen

In het kader van informatie en communicatie zijn binnen [IT-auditeenheid] de volgende zaken aanwezig:

- een informatiesysteem voor het identificeren, vastleggen, verwerken en bewaren van relevante en betrouwbare informatie die het kwaliteitsbeheersingssysteem ondersteunt, ongeacht of die informatie van interne of externe bronnen afkomstig is;
- de cultuur binnen [IT-auditeenheid] en het erkennen en versterken van de verantwoordelijkheid van het personeel om informatie uit te wisselen met het kantoor en met elkaar;
- het uitwisselen van relevante en betrouwbare informatie binnen het kantoor en met de opdrachtteams.

6.2 Interne communicatie

Interne communicatie binnen [IT-auditeenheid] betreft:

- informatie voor medewerkers en opdrachtteams, die hen in staat stelt hun verantwoordelijkheden voor de uitvoering van activiteiten in het kader van het kwaliteitsbeheersingssysteem of van opdrachten te begrijpen en uit te voeren;
- informatie van medewerkers en opdrachtteams aan [IT-auditeenheid] bij de uitvoering van activiteiten in het kader van het kwaliteitsbeheersingssysteem dan wel in het kader van opdrachten.

[IT-auditeenheid] is een kleine organisatie waar binnen en buiten de opdrachtsfeer regelmatig contact is tussen de medewerkers (en de Directie). Voorliggend Handboek (en de samenhangende documenten o.a. richtlijnen en handreikingen van NOREA) wordt met alle medewerkers gecommuniceerd en opgeslagen in de netwerkomgeving. Formele communicatie vanuit de Directie vindt schriftelijk plaats en wordt eveneens opgeslagen in de netwerkomgeving.

6.3 Externe communicatie

Binnen [IT-auditeenheid] worden de navolgende onderwerpen geschaard onder externe communicatie.

6.3.1 Publiekelijk toegankelijke informatie

De website van [IT-auditeenheid] wordt als belangrijkste communicatiemiddel richting de cliënt gebruikt. Op de website is beschreven hoe [IT-auditeenheid] 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.

6.3.2 Rapportage

Van haar auditwerkzaamheden stelt [IT-auditeenheid] een rapport op. Het rapport voldoet aan de door NOREA vastgestelde richtlijnen voor het betreffende onderzoek (zie o.a. Richtlijn 3000, 3402 en 4400). 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 eisen die zijn gesteld in de hiervoor geldende richtlijn(en).

6.3.3 Geheimhouding

Geheimhouding tussen [IT-auditeenheid] en de cliënt is contractueel vastgelegd. De richtlijnen met betrekking tot geheimhouding zijn vastgelegd in arbeidscontracten, het personeelshandboek en de overeenkomst met de samenwerkingsorganisatie(s). Eén van de maatregelen in dit kader is het tekenen van een geheimhoudingsverklaring door

[IT-auditeenheid] en/of bij de opdracht betrokken medewerker(s). 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.

6.3.4 Informatie-uitwisseling tussen [IT-auditeenheid] en cliënt

De cliënt zal geïnformeerd worden betreffende alle activiteiten (en wijzigingen daarin) binnen de professionele diensten. Kritische afspraken zullen juridisch worden vastgelegd in een contract dat voldoet aan Richtlijn Opdrachtaanvaarding 210. Deze contracten worden opgenomen in het Opdrachtdossier.

6.3.5 Reactie op klachten

Klachten welke bekend zijn gemaakt richting [IT-auditeenheid] 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 inachtneming van contractuele, organisatorische en/of wettelijke verplichtingen. De kleinschaligheid van [IT-auditeenheid] brengt met zich mee dat een op de kleinschalige situatie toegespitste procedure is ingericht. Die bestaat uit het wijzen van de cliënt in de algemene leveringsvoorwaarden op de mogelijkheid om:

- te reclameren over de uitgevoerde diensten (art. XXX Algemene voorwaarden [IT-auditeenheid]);
- gebruik te maken van het tuchtrecht van NOREA (art. YYY Algemene voorwaarden [IT-auditeenheid]).

7 Aanvaarding en continuering van cliëntrelaties en specifieke opdrachten en opdrachtuitvoering

Het primaire werkproces binnen [IT-auditeenheid] is het uitvoeren van assurance, aan assurance verwant en overige diensten op verzoek van de cliënt. Samengevat vallen deze diensten onder de noemer 'professionele diensten'. Het uitvoeren van professionele diensten 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 en regelgeving van NOREA. In dit hoofdstuk is beschreven hoe de achtereenvolgende fasen van een opdracht worden ingevuld. De uitvoering is steeds gericht op het adequaat, professioneel en efficiënt kunnen beantwoorden van de onderzoeksvragen van de cliënt (opdrachtgever). In alle opdrachten worden de volgende processtappen onderkend:

1. Cliëntacceptatie
2. Opdrachtaanvaarding en -bevestiging
3. Uitvoering van de opdracht
4. Kwaliteitsbewaking uitvoering
5. Opdrachtgerichte kwaliteitsbeoordeling (in hoofdstuk 8 nader uitgewerkt)
6. Dossiervorming en documentatie
7. Rapportage en (verplichte formulering inzake) oordelen
8. Monitoren kwaliteitsbeheersingsprocedure (in hoofdstuk 9 opgenomen)

7.1 Cliënt- en/of opdrachtacceptatie

Voordat een organisatie als klant (of een nieuwe opdracht bij een bestaande klant) door [IT-auditeenheid] wordt geaccepteerd, vindt een afweging van de hiermee verbonden risico's plaats. Deze afweging wordt gemaakt aan de hand van een Checklist Cliënt Acceptatie (zie bijlage 1). De Checklist wordt gedurende de 'levenscyclus' van de klant gebruikt en kan meerdere opdrachten bevatten. Bij elke volgende opdracht wordt de actualiteit van de eerder uitgevoerde cliëntacceptatie gevalideerd. De afwegingen worden door de verantwoordelijke IT-auditor gemaakt en door het bestuur bekrachtigd. Bij de afwegingen 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 social media. De uitkomsten van dit proces worden vastgelegd in de Checklist Cliënt Acceptatie (bijlage 1).

7.2 Opdrachtaanvaarding en -bevestiging

Teneinde misverstanden met betrekking tot de opdrachtaanvaarding te vermijden, hebben zowel de opdrachtgever als de IT-auditor er belang bij dat de IT-auditor de opdracht schriftelijk bevestigt. [IT-auditeenheid] 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[5]) wordt

[5] Indien de opdracht wordt aanvaard onder verwijzing naar algemene voorwaarden van de cliënt of brancheverenigingwaaraan deze verbonden is, dienen deze voorwaarden verwijzingen te bevatten naar de wet- en regelgeving waaraan de IT-auditor gehouden is. Indien deze verwijzingen niet in de Algemene Voorwaarden zijn opgenomen, dient de verwijzing naar de wet- en regelgeving te worden opgenomen in de brief waarmee de opdracht wordt aanvaard.

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. De opdrachtbevestiging is vereist voor het opstarten van de opdracht. [IT-auditeenheid] heeft door middel van de Checklist in bijlage 1 geborgd dat een opdrachtbevestiging in het dossier aanwezig dient te zijn alvorens wordt gestart met de opdracht. Voor de aanvaarding van professionele diensten geldt de Richtlijn Opdrachtaanvaarding (210) van NOREA. [IT-auditeenheid] volgt de aanwijzingen in deze richtlijn voor alle professionele diensten.

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-auditeenheid] uitgevoerd met inachtneming van de geldende NOREA richtlijnen en regelgeving. Conform Paragraaf 36 Richtlijn 3000 ‘Assurance-opdrachten door IT-auditors’ dient, als onderdeel van de kwaliteitsbeheersing, de overweging of het voorgestelde assurance-rapport passend is te worden geëvalueerd. Voorafgaand aan het uitbrengen van een voorstel (offerte) wordt overwogen welke Richtlijn voor het onderzoek zal worden gehanteerd (3000(A of D), 3402 of 4400). In bepaalde gevallen kan minder duidelijk zijn welke Richtlijn zal worden gehanteerd (de zgn. ‘grijze gebieden’). In deze gevallen zal de opdrachtpartner de overweging(en) in het dossier vastleggen. Bij de uitvoering van de opdracht past [IT-auditeenheid] de volgende principes toe:

- de medewerkers begrijpen en vervullen hun verantwoordelijkheden met betrekking tot opdrachten, met inbegrip van algemene verantwoordelijkheid van opdrachtpartners voor het beheer en het bereiken van kwaliteit op het niveau van de opdracht en voor het op voldoende en passende wijze betrokken blijven voor de gehele duur van de opdracht;
- de aard, timing en omvang van de aansturing van, en van het toezicht op, de opdrachtteams en de beoordeling van de uitgevoerde werkzaamheden passen bij de aard en omstandigheden van de opdrachten en de middelen die aan de opdrachtteams zijn toegewezen of ter beschikking zijn gesteld, en de door minder ervaren opdrachtteamleden uitgevoerde werkzaamheden, worden geleid, gesuperviseerd en beoordeeld door meer ervaren opdrachtteamleden;
- de medewerkers passen een passende professionele oordeelsvorming toe en, indien van toepassing op het soort opdracht, geven blijk van een professioneel kritische houding;
- raadpleging over moeilijke of omstreden kwesties komt tot stand en de overeengekomen conclusies worden geïmplementeerd;
- meningsverschillen binnen een opdrachtteam, of tussen het opdrachtteam en de opdrachtgerichte kwaliteitsbeoordelaar of de personen die binnen het kwaliteitsbeheersingssysteem van het kantoor activiteiten uitvoeren, worden onder de aandacht van [IT-auditeenheid] gebracht en worden opgelost;
- motivatie en vastlegging van de keuze of bij een opdracht OKB uitgevoerd dient te worden, conform de criteria/ richtlijnen van [IT-auditeenheid];
- opdrachtdocumentatie wordt tijdig verzameld (na de datum van het opdrachtrapport) en wordt op passende wijze bijgehouden en bewaard om te voldoen aan de behoeften van [IT-auditeenheid] om in overeenstemming te zijn met wet- en regelgeving, relevante ethische voorschriften of professionele standaarden.

7.4 Kwaliteitsbewaking uitvoering

Binnen [IT-auditeenheid] gelden de eigen periodieke kwaliteitscontroles, het self-assessment, de OKB en het Kwaliteitsonderzoek conform het RKON door het CKO, 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, 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 Opdrachtdossier.

7.5 Opdrachtgerichte kwaliteitsbeoordeling (OKB)

Voor sommige opdrachten dient een Opdrachtgerichte Kwaliteitsbeoordeling door een voldoende gekwalificeerde (externe) persoon te worden uitgevoerd. Om te bepalen of een OKB moet worden uitgevoerd, wordt de *Handreiking Opdrachtgerichte kwaliteitsbeoordeling* gebruikt. Voor aanvang van elke opdracht wordt aantoonbaar bepaald of een OKB nodig is. In ieder geval wordt een OKB uitgevoerd bij:

- Assurance-opdrachten[6];
- Opdrachten met een grotere fee dan XXX euro[7];
- Opdrachten voor beursgenoteerde ondernemingen;
- Opdrachten voor financiële instellingen;
- Opdrachten tot controle van het IT-Jaarverslag;
- Opdrachten waarbij een externe deskundige wordt ingeschakeld;
- Opdrachten buiten de landsgrenzen;
- Rapporten voor brede verspreidingskring.

Bij de OKB wordt gekeken naar onder andere:

- de deskundigheid van het opdrachtteam;
- de onafhankelijkheid van het opdrachtteam ten opzichte van de opdrachtgever;
- de afbakening van verantwoordelijkheden van [IT-auditeenheid] 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;
- aanwezigheid audittrail (norm - bevinding - conclusie - (en aanbeveling) - rapportage).

[6] Vermeld hier de eventuele uitzonderingen zoals de assurance-opdrachten die binnen een vastgesteld stramien worden uitgevoerd (zoals DigiD).

[7] De IT-auditeenheid dient zelf te bepalen vanaf welke bedrag een OKB is verplicht. Hiervoor kunnen verschillende overwegingen worden gehanteerd: zoals de omvang van de opdrachtfee t.a.v. de totale (jaar)omzet van de KITA en eventuele andere zaken die de onafhankelijkheid kunnen beïnvloeden.

De rapportage wordt niet aan de opdrachtgever verzonden voordat de OKB en de afhandeling van de bevindingen is afgerond.

Om te voorkomen dat de OKB 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. Het proces inzake de OKB is in hoofdstuk 8 nader uitgewerkt.

7.6 Dossiervorming en documentatie

Tenzij anders vermeld vindt dossiervorming digitaal plaats. Alle aangemaakte (werk)documenten, offertes, audit-evidence en (concept-)rapportages worden opgeslagen binnen de netwerkomgeving. 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;
- verklaring dat de opdrachtnemer onafhankelijk is van de opdrachtgever c.q. auditee in geval van een assurance opdracht of aan assurance verwante werkzaamheden
- overzicht van de mogelijke dreigingen en maatregelen ten aanzien van de fundamentele beginselen;
- de gehanteerde normering;
- het controleplan;
- de uitvoering van het onderzoek;
- de bevindingen;
- de conclusies;
- het oordeel/ advies/ de bevindingen, et cetera;
- de rapportage.

Voor de documentatie van opdrachten waarbij sprake is van een (eind)rapport, geldt de Richtlijn Documentatie (230) van NOREA. [IT-auditeenheid] volgt de aanwijzingen in deze richtlijn voor alle professionele diensten, ook bij opdrachten waarbij geen sprake is van een (eind)rapport.

De volgende functionarissen hebben toegang tot de dossiers (limitatief):

- Controleleider/ Lead-auditor, verantwoordelijk voor de opdracht;
- Auditor(s), betrokken bij de opdracht;
- Auditor met de QA-functie t.a.v. de opdracht;
- OKB professional;
- Directie (generiek t.a.v. alle (cliënt)mappen).

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

Het Opdrachtdossier heeft bijvoorbeeld de volgende standaard sub-mappen:

Naar behoefte kan het Opdrachtdossier nog andere submappen bevatten (bijvoorbeeld 'OKB').

De 'Checklist cliënt acceptatie' dient worden ingevuld voordat de offerte wordt verzonden, en wordt in de map offertetrajecten bewaard. Deze wordt gedurende de verschillende processtappen tijdens de audit zo nodig bijgewerkt. Als de offerte door de cliënt wordt afgewezen (expliciet of zonder verdere kennisgeving) wordt de /map naam cliëntorganisatie met daarin de offerte overgebracht naar de map Niet gegund, een submap van de map offertetrajecten. Wanneer mogelijk wordt de cliënt gevraagd aan te geven waarom de offerte niet is geaccepteerd. Dit wordt vastgelegd in een korte notitie en onder de aandacht van de directie gebracht. Als het definitieve rapport is opgesteld en ondertekend en in digitale en 'papieren' vorm aan de opdrachtgever is gezonden, worden de toegangsrechten (schrijfrechten) tot het dossier ingetrokken. In geval er sprake is van bijzonder vertrouwelijke gegevens, worden ook de leesrechten van medewerkers beperkt. Slechts in een uitzonderlijke situatie worden hierna nog (tijdelijke) toegangsrechten verleend.

7.7 Bewaren en vernietigen

Dossiers inzake professionele diensten waarbij sprake is van een (eind)rapport 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. Na de bewaartermijn worden digitale gegevens verwijderd van de betreffende systemen (netwerk e.d.). Papieren dossiers worden adequaat vernietigd door middel van shredders die (minimaal) voldoen aan DIN-norm 66399 DIN-P4, dan wel ter vernietiging aangeboden aan een gespecialiseerd archiefvernietiging bedrijf.

7.8 Rapportage en (verplichte formulering inzake) oordelen

Een belangrijk product van de diensten van [IT-auditeenheid] 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 professionele diensten zijn (worden) door NOREA verschillende templates ontwikkeld. In beginsel gebruikt [IT-auditeenheid] de templates van NOREA.

8 Opdrachtgerichte kwaliteitsbeoordeling (OKB)

8.1 Algemeen

De doelstelling van [IT-auditeenheid], door middel van de benoeming van een geschikte opdrachtgerichte Kwaliteitsbeoordelaar, is een objectieve evaluatie uit te voeren van de significante oordeelvormingen van het opdrachtteam en van de bereikte conclusies in dat verband. In dit hoofdstuk zijn de volgende aspecten van de OKB opgenomen:

- benoeming en geschiktheid van de Kwaliteitsbeoordelaar;
- uitvoering van de OKB;
- documentatie van de OKB.

8.2 Benoeming en geschiktheid van de opdrachtgerichte kwaliteitsbeoordelaar

[IT-auditeenheid] heeft ZZZZ aangewezen als opdrachtgerichte kwaliteitsbeoordelaars, te weten XXXX en YYYYY. Zij voldoen aan de volgende eisen:

- beschikken over de competentie en capaciteiten, met inbegrip van voldoende tijd, en over de passende autoriteit om de opdrachtgerichte kwaliteitsbeoordeling uit te voeren;
- voldoen aan de relevante ethische voorschriften, inclusief met betrekking tot bedreigingen voor de objectiviteit en de onafhankelijkheid van de opdrachtgerichte kwaliteitsbeoordelaar;
- voldoen aan de bepalingen van eventuele wet- en regelgeving, die van toepassing zijn op de geschiktheid van de opdrachtgerichte kwaliteitsbeoordelaar.

Daarnaast gelden de volgende uitgangspunten:

- de opdrachtgerichte kwaliteitsbeoordelaar is geen lid van het opdrachtteam, met uitzondering van een opdracht tot controle van het IT-Jaarverslag;
- een voormalig Opdrachtpartner mag tenminste twee jaren na vervanging niet de opdrachtgerichte kwaliteitsbeoordelaar zijn.
- de opdrachtgerichte Kwaliteitsbeoordelaar heeft de gehele verantwoordelijkheid voor de uitvoering van de OKB;
- indien de geschiktheid van de opdrachtgerichte Kwaliteitsbeoordelaar is aangetast, zal de Directie passende maatregelen treffen.

8.3 Uitvoering van de OKB

Voor de uitvoering van de OKB past de opdrachtgerichte Kwaliteitsbeoordelaar het volgende toe:

- de OKB vindt op gepaste tijdstippen plaats tijdens de uitvoering van de opdracht;
- de datering van het rapport geschiedt pas na afronding van de OKB;
- bij de uitvoering dient de opdrachtgerichte Kwaliteitsbeoordelaar informatie te lezen die is verstrekt door het opdrachtteam over de aard en de omstandigheden van de opdracht en entiteit;
- met de Opdrachtpartner (en leden van het team) significante aangelegenheden en oordeelsvormingen te bespreken die zijn toegepast;
- geselecteerde opdrachtdocumentatie te beoordelen en daarbij mee te nemen. De basis van deze documentatie en de professioneel-kritische houding door het opdrachtteam betreft;
    - of de documentatie de bereikte conclusies onderbouwt;

  - of de bereikte conclusies passend zijn;
  - of is voldaan aan de eisen van onafhankelijkheid;
  - of consultaties hebben plaatsgevonden over moeilijke of omstreden aangelegenheden en of de conclusies passend zijn;
  - of de Opdrachtpartner voldoende betrokken is geweest;
- de opdrachtgerichte Kwaliteitsbeoordelaar licht (indien het geval) de Opdrachtpartner in over enige bezorgdheid of bereikte conclusies die mogelijk niet passend zijn geweest. Als de bezorgdheden niet naar tevredenheid worden opgelost, wordt hiervan melding gemaakt aan een andere gepaste persoon (dat de OKB niet kan worden voltooid);
- de opdrachtgerichte Kwaliteitsbeoordelaar licht de Opdrachtpartner in, dat de OKB is voltooid.

8.4 Documentatie

De opdrachtgerichte Kwaliteitsbeoordelaar is verantwoordelijk voor de documentatie van de OKB. De documentatie van de OKB wordt vastgelegd in het Opdrachtdossier. De opdrachtgerichte Kwaliteitsbeoordelaar dient vast te stellen dat de documentatie van de OKB voldoende is om een ervaren beroepsbeoefenaar die niet eerder bij de opdracht betrokken was, in staat te stellen inzicht te verkrijgen in de aard, timing en omvang van de werkzaamheden die zijn uitgevoerd door de opdrachtgerichte Kwaliteitsbeoordelaar en in de conclusies die bij de uitvoering van de beoordeling zijn bereikt. De opdrachtgerichte Kwaliteitsbeoordelaar dient ook te bepalen dat de documentatie van de opdrachtgerichte kwaliteitsbeoordeling het volgende omvat:

- de namen van de opdrachtgerichte Kwaliteitsbeoordelaar en -indien van toepassing- de personen die assistentie hebben verleend bij de opdrachtgerichte Kwaliteitsbeoordeling;
- een identificatie van de beoordeelde opdrachtdocumentatie;
- de basis voor de vaststelling van de opdrachtgerichte Kwaliteitsbeoordelaar in overeenstemming met de vereisten;
- de kennisgevingen die vereist zijn in overeenstemming met de vereisten;
- de datum van voltooiing van de OKB.

9 Monitoren en remediëren

Het doel van monitoring en remediëren is:

- het monitoren van het kwaliteitssysteem zodat [IT-auditeenheid] en de daar waar relevante, betrouwbare en tijdige informatie heeft over het ontwerp, de implementatie en de werking van het Kwaliteitssysteem;
- het nemen van passende maatregelen om te reageren op geïdentificeerde tekortkomingen, zodat tekortkomingen tijdig worden verholpen en herhaling kan worden voorkomen. Het nemen van passende maatregelen kan ook het corrigeren van bevindingen omvatten die betrekking hebben op werkzaamheden wanneer blijkt dat procedures zijn weggelaten bij een lopende of voltooide opdracht, of een al uitgebracht rapport ongepast was.

Monitoring en herstel bevorderen de proactieve en voortdurende verbetering van de kwaliteit van de werkzaamheden en het kwaliteitssysteem. Het identificeren en verhelpen van tekortkomingen is opbouwend en een essentieel onderdeel van een effectief Kwaliteitssysteem. Het proces van monitoren en remediëren is binnen [IT-auditeenheid] opgedeeld in de volgende stappen:

- het opzetten en uitvoeren van monitoring activiteiten;
- het evalueren van bevindingen, identificeren van tekortkomingen en het evalueren van tekortkomingen;
- het reageren op geïdentificeerde tekortkomingen;
- communicatie.

In het kader van monitoren en remediëren voert de Directie, naast de OKB, de volgende activiteiten uit:

- Opdrachtevaluaties: elke opdracht wordt door het Opdrachtteam geëvalueerd nadat deze is voltooid. De evaluatie wordt inzichtelijk vastgelegd;
- Trendanalyses: de evaluaties worden elk kwartaal besproken zodat herhalingen van bevindingen en trends worden gesignaleerd;
- Opdrachtdossier reviews: de Opdrachtdossiers worden regelmatig onderzocht om vast te stellen dat de verplichte documentatie in het dossier aanwezig is. Van elke Opdrachtpartner wordt minimaal 1x per jaar één opdrachtdossier inhoudelijk gereviewd;
- Self-assessments: het self-assessment van NOREA wordt jaarlijks ingevuld en zo nodig wordt het Kwaliteitsbeheersingssysteem op basis van de uitkomsten van het assessment aangepast. Het self-assessment is voorzien van een cross reference naar verwijzingen waar staat hoe er aan voldaan wordt.
- Jaarlijkse reviews: jaarlijks wordt het self-assessment besproken en worden besluiten genomen over eventuele aanpassingen van dit Handboek.

Bijlage 1 Voorbeeld cliëntacceptatie formulier

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-auditeenheid? *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 cliënt acceptatie

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

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

VRAGENLIJST CLIËNT 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 witwas 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 witwassen, 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[8]. • Ontbreken van een duidelijke redden waarom de toekomstige cliënt kiest voor deze IT-auditeenheid[9]. • Betrokken bij omstreden politieke kwesties. • Op andere wijze negatief in de publiciteit door de activiteiten of eigenaarschap.	

Eventuele toelichting (Hoofdstuk 2)

[8] Alleen voor OOB organisaties

[9] Alleen voor toekomstige klanten

Bijlage 2 Voorbeeld risk assessment professionele diensten KITA

Risk Assessment professionele diensten [IT-auditeenheid]

Situatie vóór mitigerende maatregel(en)					Mitigerende Maatregel(en)	Situatie na mitigerende maatregel(en)			
Processtap	**Risico**	**Kans**	**Impact**	**Risico**		**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	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.
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	L	M	**L**	Contracten, offertes en andere externe communicatiemiddelen gaan via directie. Rolprofielen met Taken, Bevoegdheden en Verantwoordelijkheden (TBV's).

Situatie vóór mitigerende maatregel(en)					Mitigerende Maatregel(en)	Situatie na mitigerende maatregel(en)			
Processtap	**Risico**	**Kans**	**Impact**	**Risico**		**Kans**	**Impact**	**Risico**	**Borging**
					informatie, Procedure 'communicatie'.				
Aanvraag/aanvraag evaluatie	Solvabiliteit aanvrager onvoldoende	M	H	**M**	Controle in KvK register (insolventie).	M	H	**M**	
Aanvraag/aanvraag evaluatie	Klant verstrekt onjuiste en/of onvolledige informatie	M	M	**M**	Opgegeven informatie controleren.	L	M	**L**	Gegevensverificatie tijdens eerste bezoek
Algemeen	Onpartijdigheidrisico	M	H	**M**	opdracht evaluatie t.o.v. geïdentificeerde risico's en gerichte maatregelen.	L	M	**L**	
Algemeen	Onvolledigheid Dossier(s) (integriteit en juistheid)	M	H	**M**	Interne audits, procedure 'dossiervorming'.	M	H	**M**	
Algemeen	Beschikbaarheid van gegevens	H	H	**H**	Back-up procedures.	L	H	**M**	Periodiek toetsing of restore mogelijk is
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.

Situatie vóór mitigerende maatregel(en)					Mitigerende Maatregel(en)	Situatie na mitigerende maatregel(en)			
Processtap	**Risico**	**Kans**	**Impact**	**Risico**		**Kans**	**Impact**	**Risico**	**Borging**
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
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**	Gemiste resources beschikbaar stellen (of opdracht weigeren).	M	M	**L**	Borging dat resources gedurende de gehele looptijd van de opdracht beschikbaar blijven.
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

Situatie vóór mitigerende maatregel(en)					Mitigerende Maatregel(en)	Situatie na mitigerende maatregel(en)			
Processtap	**Risico**	**Kans**	**Impact**	**Risico**		**Kans**	**Impact**	**Risico**	**Borging**
Algemeen	Onafhankelijkheid risico's	M	H	**M**	opdracht evaluatie t.o.v. geïdentificeerde risico's en gerichte maatregelen.	L	L	**L**	
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