NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Self assessment kwaliteitsonderzoek IT-auditorganisatie

INTRODUCTIE

Achtergrond self assessment

Ingevolge artikel 8 van het Reglement Kwaliteitsonderzoek NOREA, dient jaarlijks door alle IT-auditorganisaties een self assessment te worden ingevuld ten behoeve van het kwaliteitsonderzoek.

De door het College Kwaliteitsonderzoek (CKO) uit te voeren kwaliteitsonderzoeken zullen zich – ingevolge artikel 3 van het Reglement Kwaliteitsonderzoek NOREA – richten op de beoordeling of het door de IT-auditorganisatie gehanteerde stelsel van kwaliteitsbeheersingsmaatregelen voldoet aan de normen, zoals afgeleid uit het Reglement Kwaliteitsbeheersing NOREA (RKBN), de Statuten, Reglementen en Richtlijnen van NOREA. Deze vragenlijst zal bij dat kwaliteitsonderzoek worden betrokken.

De kwaliteitsbeheersingsmaatregelen moeten zijn uitgewerkt in een handboek. Dit handboek moet de beschrijving bevatten van alle maatregelen die het RKBN voorschrijft zodat niet alleen de kwaliteit van de uitgevoerde professionele diensten wordt beheerst, maar ook is voorzien in de opzet van de kwaliteitsbeheersing voor eventueel in de toekomst te leveren andere professionele diensten waartoe de IT-auditor is bevoegd op grond van zijn inschrijving in het Register.

Gebruik maken andere kwaliteitstoetsingen

Bij IT-auditorganisaties die onderdeel zijn van / gelieerd zijn aan een auditpraktijk, die op haar beurt onderworpen is aan de kwaliteitstoetsing van:

- de Autoriteit Financiële Markten (AFM)
- de Nederlandse Beroepsorganisatie van Accountants (NBA),
- het Institute of Internal Auditors (IIA) of
- het samenwerkingsverband Kwaliteitstoets OverheidsAuditors (KOA)

wordt een deel van het kwaliteitsonderzoek namens het NOREA/CKO uitgevoerd door deze instanties. Voor alle overige IT-auditorganisaties en de professionele diensten die niet vallen onder de toetsing door de hiervoor genoemde organisaties, zal de toetsing door het NOREA/CKO worden uitgevoerd.

Begrippen

- Advies: een besluitvormende mening over een of meer elementen of aspecten in de toekomst (ontleend aan ‘Studie Adviesdiensten’ – januari 2012).
- Adviesdienst: de werkzaamheden die benodigd zijn om een advies te formuleren en te uiten (ontleend aan ‘Studie Adviesdiensten’ – januari 2012).
- Assurance-opdracht: een opdracht waarbij een IT-auditor een conclusie formuleert die is bedoeld om het vertrouwen van beoogde gebruikers, niet zijnde de partij die zich verantwoordt, in de uitkomst van een evaluatie of de toetsing van het object van onderzoek ten opzichte van de toetsingsnormen te versterken.
- IT-auditor: de Register EDP-auditor (RE), ingeschreven in het register van NOREA.
- IT-auditorganisatie: de organisatorische eenheid waarbinnen één of meer IT-auditors op grond van een onderzoek met betrekking tot de situatie ten aanzien van de informatietechnologie een oordeel of advies geven.
- Professionele dienst: de werkzaamheden die een IT-auditor uitvoert binnen een IT-auditorganisatie, waarvoor IT-auditdeskundigheid en deskundigheid op

aanverwante terreinen is vereist.

TOELICHTING OP ENKELE IN RELATIE TOT KWALITEITSONDERZOEKEN RELEVANTE ONDERWERPEN

1. IT-auditorganisatie
De definitie van dit begrip geeft aan dat een IT-auditorganisatie in omvang kan variëren. Het begrip omvat derhalve ook IT-auditorganisaties met één of slechts een zeer beperkt aantal IT-auditors. IT-auditors kunnen zelfstandig zijn gevestigd (bijvoorbeeld de ZZP-er) of in dienstverband werkzaam zijn. Kenmerkend voor de IT-auditors in een IT-auditorganisatie is, dat zij professionele diensten leveren.

2. Kleinschalige IT-auditorganisatie (afgekort: KITA)
De inrichting van een kwaliteitsstelsel wordt mede beïnvloed door de omvang van de IT-auditorganisatie. De IFAC-normen, waarop het Reglement Kwaliteitsbeheersing NOREA (RKBN) is gebaseerd, houdt geen rekening met de omvang van een organisatie. Immers de afnemer van de professionele diensten moet er op kunnen vertrouwen dat de kwaliteit van de dienst gelijkwaardig is, ongeacht de omvang van de IT-auditorganisatie.

Het toepassen van de normen op kleinschalige IT-auditorganisaties vergt de nodige inventiviteit bij het realiseren daarvan. Ook zijn sommige normen in bepaalde situaties niet van toepassing. Daarom is in dit document, als **subset** van het begrip 'IT-auditorganisatie', het begrip 'kleinschalige IT-auditorganisatie' (KITA) geïntroduceerd. In de kolom 'Toelichting / voorbeelden' van onderstaande tabel is in relatie tot de KITA bij een aantal normen een kanttekening geplaatst. Verder is voor de KITA door NOREA een model Handboek Kwaliteitsbeheersing KITA's ontwikkeld.
Voor de goede orde wordt opgemerkt, dat de in deze kolom geplaatste kanttekeningen een KITA **niet** ontslaan van het beschikken over een kwaliteitsstelsel dat voorziet in het uitvoeren van alle professionele diensten.

3. Detachering
Een IT-auditor kan door een IT-auditorganisatie (tijdelijk) worden ingehuurd voor het leveren van professionele diensten. In die situatie richt het kwaliteitsonderzoek van NOREA zich op de wijze waarop de detacherende IT-auditorganisatie het naleven van de beroepsreglementering contractueel heeft geregeld in de dienstenovereenkomst tussen de betreffende IT-auditor(s) en de inhurende IT-auditorganisatie. Detachering is een wijze waarop professionele diensten kunnen worden geleverd. Van detachering **alleen** sprake is indien de opdrachtgever valt onder het kwaliteitstoezicht van organisaties waarmee door NOREA afspraken zijn gemaakt over het uitvoeren van kwaliteitstoezicht.
De IT-auditorganisatie moet in situaties waarin sprake is van enkel detachering, toch beschikken over een eigen kwaliteitshandboek, bijvoorbeeld op basis van het model Handboek Kwaliteitsbeheersing KITA's. Een RE is immers bevoegd om zelfstandig alle professionele diensten te verlenen en dient te beschikken over een kwaliteitsstelsel dat deze dienstverlening mogelijk maakt.
De vaktechnische aspecten van de verleende diensten worden in geval van detachering beoordeeld bij het kwaliteitsonderzoek naar de IT-auditorganisatie bij wie de IT-auditor is gedetacheerd. Voor het geval de IT-auditor uitingen ondertekent, moet dat worden gedaan onder de naam van de IT-auditorganisatie waar hij/zij is gedetacheerd. Indien een norm niet door de organisatie van de opdrachtgever is gerealiseerd, moet de IT-auditorganisatie deze norm alsnog zelf realiseren. Er

is in die situatie niet sprake van detachering, maar van een assurance-opdracht of adviesdienst.
De IFAC-normering houdt geen rekening met detachering. Een aantal normen is op die situatie niet van toepassing. In de kolom 'Toelichting / voorbeelden' van onderstaande tabel is bij een aantal normen daarom een kanttekening geplaatst in relatie tot detachering.

4. Overige professionele diensten

Binnen organisaties kan door de aard van een functie(benaming) of een gezagsverhouding onduidelijkheid bestaan over het al dan niet sprake zijn van wel of niet leveren van een professionele diensten. Voorbeelden van dergelijke situaties zijn toezichthoudende of adviserende functies. De introductie van het begrip 'Overige professionele diensten' beoogt, **binnen de context van de bestaande definities**, een eventuele onduidelijkheid over de verplichting tot het naleven van de voor IT-auditors geldende regelgeving op te heffen. Die regelgeving is ook op de 'Overige professionele diensten' van toepassing.
Het kwaliteitstoezicht richt zich bij deze activiteiten op de wijze waarop de IT-auditor heeft geborgd dat de kwaliteit van de werkzaamheden voldoet aan de beroepsreglementering en vaktechnische aspecten.
De IFAC-normering houdt geen rekening met het begrip 'Overige professionele diensten'. Sommige normen zijn op die situatie niet van toepassing. In de kolom 'Toelichting / voorbeelden' van onderstaande tabel is bij een aantal normen daarom een kanttekening geplaatst in relatie tot de overige professionele diensten.

5. RE die zich niet bezig houdt met professionele diensten (wegens ontheffing of vrijstelling van PE of gepensioneerd lidmaatschap)

Het kwaliteitsonderzoek richt zich op het onderzoeken van IT-auditorganisaties en professionele diensten. Een RE valt niet onder het kwaliteitsonderzoek omdat hij/zij werkzaamheden uitvoert die zich niet richten op het leveren van een professionele dienst, zoals bedoeld in artikel 4 van de NOREA-Richtlijn Opdrachtaanvaarding, d.w.z. werkzaamheden op het brede terrein van IT-Governance, -Risk, -Compliance en/of -Audit. Voor de goede orde: de RE die zich niet bezig houdt met het leveren van professionele diensten moet zich wel houden aan de fundamentele beginselen inzake integriteit en professioneel gedrag. De fundamentele beginselen objectiviteit, deskundigheid en zorgvuldigheid, geheimhouding zijn echter niet op deze functie van toepassing omdat deze beginselen zijn gericht op het leveren van professionele diensten als RE.

OPBOUW SELF ASSESSMENT

- Het self assessment wordt voorafgegaan door een aantal identificerende kenmerken.
- Het self assessment is gebaseerd op onder meer de grondslagen uit het Reglement voor de Kwaliteitsbeheersing NOREA (RKBN), waar nodig aangevuld met toelichtingen.
- Het self assessment is opgebouwd uit 19 deelgebieden.
- De tweede kolom bevat de **norm**.
  - De norm is ontleend aan het RKBN en good practices afkomstig uit diverse stelsels voor kwaliteitsonderzoeken.
  - Het RKBN bevat – in vetgedrukte tekst – de grondslagen en de noodzakelijk te verrichten werkzaamheden, met daarna in het normale lettertype nadere aanwijzingen en uiteenzettingen. Om de grondslagen en de noodzakelijk te verrichten werkzaamheden, samen met de daarbij behorende aanwijzingen, te kunnen begrijpen en toepassen moet de tekst van het RKBN, inclusief de daarin opgenomen nadere toelichtingen en uiteenzettingen, integraal in aanmer-

Self assessment kwaliteitsonderzoek IT-auditorganisatie

king worden genomen en niet slechts datgene wat vetgedrukt is. Het RKBN is beschikbaar is op de website van NOREA.
  - ➢ De definities van de in de onderstaande vragenlijst gehanteerde begrippen zijn ontleend aan diverse reglement, richtlijnen, etc. en aangevuld met de begrippen 'Detachering' en 'Overige professionele diensten'.
- De derde kolom (**Antw. – antwoord)** is bestemd voor het vastleggen van de resultaten van de self-assessment, het aangeven of al dan niet in opzet, bestaan en werking aan de norm is voldaan.
- De laatste kolom (**Toelichting / voorbeelden**) bevat toelichtingen / voorbeelden in relatie tot een de soort werkzaamheden en/of een bepaald type IT-auditorganisatie.

WIJZE INVULLEN SELF ASSESSMENT

De IT-auditorganisatie dient de self assessment in de kolom zeven door middel van de terminologie:
- GC = Geheel Compliant;
- DC = Deels Compliant;
- NC = Niet Compliant;
- NVT – Niet Van Toepassing

aan te geven of de organisatie voldoet aan de regelgeving.
In combinatie met het invullen van kolom zeven moet de IT-auditorganisatie in kolom acht beknopt (bijvoorbeeld door het verwijzen naar paragrafen uit een handboek) en rekening houdend met standaard toelichting vermelden op welke wijze de norm is gerealiseerd zodat de onderzoekers zich een beeld kunnen vormen over de inrichting van het kwaliteitsstelsel.

REACTIE OP VRAGENLIJST

Vragen en opmerkingen over deze lijst kunnen worden gericht aan het College Kwaliteitsonderzoek, p/a bureau NOREA.

INHOUDSOPGAVE	**Vraag**
Identificerende kenmerken	1
Uitgangspunten	2 t/m 4
Elementen kwaliteitsbeheersingssysteem	5 en 6
Verantwoordelijkheid leiding IT-auditorganisatie voor kwaliteit	7 t/m 10

Self assessment kwaliteitsonderzoek IT-auditorganisatie	
Ethische normen	11
Objectiviteit	12
Aanvaarden en voortzetten van relaties en specifieke opdrachten	13 t/m 19
Personeelsbeleid	20 en 21
Samenstelling opdrachtteams	22 t/m/ 25
Uitvoering van opdrachten	26 en 27
Consultatie	28 t/m/ 32
Verschillen van inzicht	33 t/m 35
Opdrachtgerichte kwaliteitsbeoordeling	36 t/m 39
Aard, tijdstip en omvang opdrachtgerichte kwaliteitsbeoordeling	40 en 41
Criteria voor opdrachtgerichte kwaliteitsbeoordelaar	42 t/m 44
Documentatie opdrachtgerichte kwaliteitsbeoordeling	45
Monitoren	46 t/m 57
Klachten en beschuldigingen	58 t/m 61
Dossiervorming	62 en 63

Self assessment kwaliteitsonderzoek IT-auditorganisatie – ingedeeld naar werkzaamheden en omvang organisatie			
IDENTIFICERENDE KENMERKEN			
1	a. Datum invulling vragenlijst		
	b. Naam IT-auditorganisatie		
	c. Leiding IT-auditorganisatie		
	d. Contactpersoon kwaliteitsonderzoek		
	e. Rechtsvorm en handelsnaam (KvK)		
	f. Relatie met een auditpraktijk	Ja / nee	Zo ja met …
	g. Onderworpen aan kwaliteitsonderzoek door en zo ja, datum laatste onderzoek: • NIVRA/NBA • IIA • KOA	Ja / nee • Ja / nee • Ja / nee • Ja / nee	Zo ja: d.d. d.d. d.d.
	h. Omvang IT-auditorganisatie in FTE's		
	i. Aantal leden RE		
	j. Aantal locaties		
	k. Beknopte omschrijving organisatiestructuur		
	l. Verdeling aard van de opdrachten: • Assurance-opdrachten • Advies • Detachering	In %: • ? • ?	

Self assessment kwaliteitsonderzoek IT-auditorganisatie – ingedeeld naar werkzaamheden en omvang organisatie		
IDENTIFICERENDE KENMERKEN		
	• Overige professionele diensten	• ? • ?
HANDTEKENING		
Met het beantwoorden van onderstaande vragen verklaart de leiding van de IT-auditorganisatie deze vragenlijst volledig en naar waarheid te hebben ingevuld.		
Handtekening		
Naam:		Functie:
Plaats:		Datum:

Self assessment kwaliteitsonderzoek IT-auditorg. – ingedeeld naar functies			
Vraag	**Norm**	**Antwoord [1]**	**Toelichting / voorbeeld**
UITGANGSPUNTEN			
2	De IT-auditorganisatie heeft een zodanig systeem van kwaliteitsbeheersing opgezet dat een redelijke mate van zekerheid wordt geboden, dat de organisatie en haar personeel voldoen aan de vaktechnische richtlijnen en de door wet- en regelgeving gestelde eisen en dat de door de organisatie of haar voor opdrachten verantwoordelijke professional afgegeven rapporten onder de gegeven omstandigheden voldoen aan de reglementen, richtlijnen en handreikingen die door NOREA zijn uitgevaardigd.		KITA: het systeem kan bestaan uit een handboek dat enkele A-4tjes omvat.

[1] Te hanteren terminologie: GC = Geheel Compliant; DC = Deels Compliant; NC = Niet Compliant; NVT – Niet Van Toepassing

Self assessment kwaliteitsonderzoek IT-auditorg. – ingedeeld naar functies			
Vraag	**Norm**	**Antwoord [1]**	**Toelichting / voorbeeld**
3	De leiding van de IT-auditorganisatie is verantwoordelijk voor het aangaan van de overeenkomst met NOREA voor het uitvoeren van het kwaliteits-onderzoek		De IT-auditor met een arbeidsrelatie waarbij het manage-ment geen RE is, moet overleggen wie deze overeenkomst aangaat.
4	De antwoorden zijn gebaseerd op versie 1.0 van het RKON en het RKBN versie met ingang van 01-01-2009		
STELSEL GERELATEERDE NORMEN			
	ELEMENTEN KWALITEITSBEHEERSINGSSYSTEEM		
5	Het kwaliteitsbeheersingssysteem van de IT-auditorga-nisatie bevat ge-dragslijnen en procedures gericht op de volgende aspecten:		
	1. Verantwoordelijkheid van de leiding voor kwaliteit binnen de IT-auditorganisatie.		
	2. Ethische normen.		
	3. Aanvaarden en voortzetten van de relatie met opdrachtgevers en van specifieke opdrachten.		Indien opdrachten worden aanvaard / voortgezet door een niet-IT-auditor moet de IT-auditor nagaan of zich daarbij op grond van de beroepsreglementering onaanvaardbare situa-ties voordoen.
	4. Personeelsbeleid.		Indien sprake is van een arbeidsrelatie mag het beleid van de werkgever niet opgespannen voet staan met de regelge-ving van NOREA.
	5. Uitvoering van de opdrachten.		Detachering: moet in zijn voorzien bij de opdrachtgever. Als de opdrachtgever geen RE is, moet de gedetacheerde RE

Self assessment kwaliteitsonderzoek IT-auditorg. – ingedeeld naar functies			
Vraag	**Norm**	**Antwoord [1]**	**Toelichting / voorbeeld**
			deze voorwaarden opnemen in zijn contract.
	6. Het monitoren.		• KITA: moet voor het monitoren een voorziening treffen, bijvoorbeeld door het inschakelen van een andere IT-auditor. • Detachering: moet in zijn voorzien bij de opdrachtgever.
6	De gedragslijnen voor kwaliteitsbeheersing en de kwaliteitsbeheersingsprocedures worden vastgelegd en bekend gemaakt aan het personeel van de IT-auditorganisatie. Dit omvat een toelichting, de te bereiken doelen, ieders persoonlijke verantwoordelijkheid voor kwaliteit en de terugkoppeling door het personeel over het kwaliteitsbeheersingssysteem.		• KITA: gedragslijn kan bestaan uit een paar A-4tjes. • Detachering: moet in zijn voorziening bij de opdrachtgever.
	VERANTWOORDELIJKHEID LEIDING IT-AUDITORGANISATIE VOOR KWALITEIT		
7	De IT-auditorganisatie heeft gedragslijnen en procedures die zijn opgezet om een interne bedrijfscultuur te bevorderen, gebaseerd op de erkenning dat kwaliteit essentieel is bij de uitvoering van opdrachten. Dergelijke gedragslijnen en procedures bevatten als eis dat het de leiding van de IT-auditorganisatie (ic het bestuur) de eindverantwoordelijkheid aanvaardt voor het kwaliteitsbeheersingssysteem van de IT-auditorganisatie.		• KITA: moet naar voren komen in de geformuleerde gedragslijn. • Detachering: moet in zijn voorzien bij de opdrachtgever.
8	De leiding van de IT-auditorganisatie heeft kwaliteitsbeheersingsprocedures ingericht die waarborgen dat:		
	1. Werkzaamheden worden verricht in overeenstemming zijn met de vaktechnische richtlijnen en de door wet- en regelgeving gestelde eisen; en		De: moet in zijn voorzien bij de opdrachtgever.
	2. Sprake is van een bedrijfscultuur waarin werkzaamheden van hoge kwaliteit worden gewaardeerd en beloond.		• KITA: moet naar voren komen in de geformuleerde gedragslijn.

Self assessment kwaliteitsonderzoek IT-auditorg. – ingedeeld naar functies			
Vraag	**Norm**	**Antwoord [1]**	**Toelichting / voorbeeld**
			• Detachering: IT-auditor moet nagaan of de overeenkomst met een niet-IT-auditor als zodanig wordt ervaren. • De IT-auditor met een arbeidsrelatie moet nagaan of de werkgever aan deze norm voldoet.
9	De leiding van de IT-auditorganisatie heeft gewaarborgd dat de zakelijke strategie van de organisatie ondergeschikt is aan de kwaliteit bij de uitvoering van al haar opdrachten.		De IT-auditor met een arbeidsrelatie moet nagaan of de werkgever aan deze norm voldoet.
10	Elk van de personen aan wie operationele verantwoordelijkheid voor het kwaliteitsbeheersingssysteem van de IT-auditorganisatie is opgedragen door de leiding van de organisatie, heeft toereikende ervaring en bekwaamheid, alsmede de noodzakelijke bevoegdheid en het gezag om die verantwoordelijkheid te kunnen dragen.		• KITA: moet voor deze norm een voorziening treffen, bijvoorbeeld door het organiseren van een review door een andere IT-auditor. • Detachering: moet in zijn voorzien bij de opdrachtgever.
	ETHISCHE NORMEN		
11	De IT-auditorganisatie heeft gedragslijnen en procedures die zijn opgezet om een redelijke mate van zekerheid te verkrijgen dat de IT-auditorganisatie en haar personeel voldoen aan de van kracht zijnde ethische normen. De grondbeginselen van deze ethische normen zijn: a. Integriteit; b. Objectiviteit; c. Vakbekwaamheid en zorgvuldigheid; d. Geheimhouding; en e. Professioneel gedrag.		

Self assessment kwaliteitsonderzoek IT-auditorg. – ingedeeld naar functies			
Vraag	**Norm**	**Antwoord [1]**	**Toelichting / voorbeeld**
	OBJECTIVITEIT		
12	De IT-auditorganisatie heeft gedragslijnen en procedures die zijn opgezet om een redelijke mate van zekerheid te verkrijgen dat de IT-auditorganisatie, haar medewerkers en indien van toepassing anderen, voldoen aan de objectiviteitsvoorschriften (op grond van de Gedragscode en nationale ethische normen). Dergelijke gedragslijnen en procedures stellen de IT-auditorganisatie in staat om:		
	1. Haar grondbeginselen bekend te maken aan het personeel en indien van toepassing aan anderen die aan die eisen moeten voldoen; en		• KITA: moet zijn opgenomen in bijvoorbeeld een handboek. • Detachering: moet in zijn voorzien bij de opdrachtgever.
	2. Omstandigheden en relaties te onderkennen en te onderzoeken die de objectiviteit bedreigen en de juiste maatregelen te treffen om deze bedreigingen weg te nemen dan wel terug te brengen tot een aanvaardbaar niveau door het inbouwen van waarborgen of, indien dit juist wordt geacht, door de opdracht terug te geven.		• Vereist rechte rug van de IT-auditor indien de werkgever niet met deze norm rekening houdt. • Kan arbeidsrelatie beïnvloeden.
	AANVAARDEN EN VOORTZETTEN VAN RELATIES EN SPECIFIEKE OPDRACHTEN		
13	De IT-auditorganisatie heeft gedragslijnen en procedures voor het aanvaarden en voortzetten van de relatie met opdrachtgevers en specifieke opdrachten, die zijn opgezet om een redelijke mate van zekerheid te verkrijgen dat zij alleen relaties en specifieke opdrachten zal aanvaarden en voortzetten indien zij: a. De integriteit van de opdrachtgever heeft beoordeeld en geen informatie heeft verkregen die tot de conclusie leidt dat de opdrachtgever onvoldoende integer is; b. De deskundigheid bezit om de opdracht uit te voeren en de capacitei-		• De IT-auditor moet bij een arbeidsrelatie met een niet-IT-auditor nagaan of bij het aanvaarden of voortzetten van een opdracht aan deze norm kan worden voldaan. • Bij een arbeidsrelatie is deze norm niet van toepassing op werkzaamheden binnen de eigen organisatie.

Self assessment kwaliteitsonderzoek IT-auditorg. – ingedeeld naar functies			
Vraag	**Norm**	**Antwoord [1]**	**Toelichting / voorbeeld**
	ten, tijd en middelen daartoe bezit; en c. Kan voldoen aan de ethische normen.		
14	Alvorens een opdracht van een nieuwe opdrachtgever te aanvaarden, bij het beslissen of een bestaande opdracht zal worden voortgezet en bij het overwegen of een nieuwe opdracht voor een bestaande opdrachtgever zal worden aanvaard, verzamelt de IT-auditorganisatie de informatie die zij in de gegeven omstandigheden noodzakelijk acht. Indien knelpunten zijn onderkend en de IT-auditorganisatie toch besluit de relatie met de opdrachtgever of de specifieke opdracht te aanvaarden of voort te zetten, moet de organisatie vastleggen hoe de knelpunten zijn opgelost		• Indien deze situatie zich voordoet bij een arbeidsrelatie met een niet-IT-auditor moet de IT-auditor vastleggen op welke wijze de knelpunten zijn opgelost. • Bij een arbeidsrelatie is deze norm niet van toepassing op werkzaamheden binnen de eigen organisatie.
15	De IT-auditorganisatie beoordeelt de opdrachtgever op de volgende aspecten: • De identiteit en de zakelijk reputatie van de belangrijkste eigenaren van de huishouding van de opdrachtgever. • De leidinggevende functionarissen op sleutelposities, de verbonden partijen en de organen belast met governance. • De aard van de bedrijfsactiviteiten, alsmede de bedrijfscultuur. Deze bedrijfscultuur moet mede zijn gericht op het voorkomen van IT-fraude • De informatie over de houding van de belangrijkste eigenaren van de huishouding, leidinggevende functionarissen op sleutelposities en de organen belast met governance inzake onderwerpen als het niet te goeder trouw optreden in de interne beheersingsomgeving. • De vraag of de opdrachtgever overdreven aandacht heeft voor het zo laag mogelijk houden van de declaraties van de IT-auditorganisatie. • De aanwijzingen dat onaanvaardbare beperkingen in de audit voorkomen.		• De IT-auditor moet bij een arbeidsrelatie met een niet-IT-auditor nagaan of bij het aanvaarden of voortzetten van een opdracht aan deze norm kan worden voldaan. • Bij een arbeidsrelatie is deze norm niet van toepassing op werkzaamheden voor de eigen organisatie.

Self assessment kwaliteitsonderzoek IT-auditorg. – ingedeeld naar functies			
Vraag	**Norm**	**Antwoord [1]**	**Toelichting / voorbeeld**
	• De aanwijzingen dat de opdrachtgever betrokken zou kunnen zijn bij computerfraude of andere criminele activiteiten. • De redenen om de IT-auditorganisatie aan te stellen en geen gebruik meer te maken van de diensten van de voorgaande IT-auditorganisatie. De informatie die nodig is om de voorgenoemde aspecten te kunnen beoordelen wordt verkregen uit betrouwbare bronnen. Hierbij wordt de betrouwbaarheid van elke bron geadresseerd. .		
16	Bij het overwegen of de IT-auditorganisatie de capaciteiten, bekwaamheid, tijd en middelen bezit om een nieuwe opdracht te aanvaarden van een nieuwe of bestaande opdrachtgever, onderzoekt de organisatie de specifieke eisen van de opdracht en de bestaande profielen van de professionals op elk relevant niveau. Hierbij wordt tevens onderzocht of de IT-auditorganisatie voldoende capaciteit heeft om de opdracht binnen de gestelde rapporteringstermijn uit te voeren.		De IT-auditor moet bij een arbeidsrelatie met een niet-IT-auditor nagaan of bij het aanvaarden of voortzetten van een opdracht aan deze norm kan worden voldaan.
17	De IT-auditorganisatie overweegt ook of het accepteren van een opdracht van een nieuwe of bestaande opdrachtgever een belangentegenstelling in wezen of schijn kan doen ontstaan. Als een potentiële belangentegenstelling wordt gesignaleerd, overweegt de IT-auditorganisatie of het juist is om de opdracht te aanvaarden.		De IT-auditor moet bij een arbeidsrelatie met een niet-IT-auditor nagaan of bij het aanvaarden of voortzetten van een opdracht of deze situatie zich niet voordoet.
18	Bij het nemen van de beslissing om een relatie met een opdrachtgever voort te zetten wordt rekening gehouden met belangrijke zaken die zich hebben voorgedaan tijdens de lopende of vorige opdrachtperioden en hun gevolgen voor de voortzetting van de relatie.		De IT-auditor moet bij een arbeidsrelatie met een niet-IT-auditor nagaan of bij het aanvaarden of voortzetten van een opdracht of deze situatie van toepassing is.
19	Indien de IT-auditorganisatie informatie verkrijgt die haar genoodzaakt zou hebben om de opdracht te weigeren als die informatie eerder beschikbaar was geweest, bepalen de gedragslijnen en procedures aangaande voort-		De IT-auditor moet bij een arbeidsrelatie met een niet-IT-auditor zijn werkgever wijzen op de genoemde punten.

Self assessment kwaliteitsonderzoek IT-auditorg. – ingedeeld naar functies			
Vraag	**Norm**	**Antwoord [1]**	**Toelichting / voorbeeld**
	zetting van de opdracht en de relatie met de opdrachtgever dat in aanmerking dienen te worden genomen: a. De vaktechnische en juridische verantwoordelijkheden die onder deze omstandigheden gelden, alsmede of er een verplichting voor de IT-auditorganisatie bestaat om aan de persoon of personen, die de IT-audit-organisatie hebben benoemd verslag uit te brengen of in bepaalde gevallen aan regelgevende instanties te melden; en b. De mogelijkheid om de opdracht terug te geven, eventueel in combinatie met het verbreken van de relatie met de opdrachtgever.		
	PERSONEELSBELEID		
20	De IT-auditorganisatie heeft gedragslijnen en procedures die zijn opgezet om een redelijke mate van zekerheid te verkrijgen dat zij voldoende personeel in dienst heeft met de capaciteiten, bekwaamheid en binding met ethische grondslagen, die noodzakelijk zijn om haar opdrachten uit te kunnen voeren in overeenstemming met de vaktechnische richtlijnen en de door wet- en regelgeving gestelde eisen en om de organisatie, of de voor opdrachten verantwoordelijke professional, in staat te stellen rapporten af te geven die onder de gegeven omstandigheden juist zijn. Dergelijke gedragslijnen en procedures richten zich op de volgende aspecten van het personeelsbeleid: • Personeelswerving • Prestatiebeoordeling • Capaciteiten • Deskundigheid • Loopbaanontwikkeling		• Bij een KITA met één medewerker die tevens de eigenaar is, is het beschikken over een personeelsbeleid niet aan de orde. • Indien een IT-auditor een arbeidsrelatie heeft met een niet-IT-audit-organisatie mag het personeelsbeleid de bij de norm genoemde aspecten niet belemmeren.

Self assessment kwaliteitsonderzoek IT-auditorg. – ingedeeld naar functies			
Vraag	**Norm**	**Antwoord [1]**	**Toelichting / voorbeeld**
	• Promotie • Salariëring • Inschatting van de personeelsbehoefte		
21	Adequate methoden zijn ingericht binnen de IT-auditorganisatie om capaciteiten en bekwaamheden van het personeel te ontwikkelen.		Indien een IT-auditor een arbeidsrelatie heeft met een niet-IT-audit-organisatie mag het personeelsbeleid de bij de norm genoemde aspecten niet belemmeren.
	SAMENSTELLING OPDRACHTTEAMS		
22	De IT-auditorganisatie draagt de verantwoordelijkheid voor elke opdracht op aan een voor de opdracht verantwoordelijke professional.		Detachering: is belegd bij de opdrachtgever.
23	De IT-auditorganisatie heeft gedragslijnen en procedures, die voorschrijven dat:.		
	1. De identiteit en de rol van de voor de opdracht verantwoordelijke professional worden bekendgemaakt aan leidinggevende functionarissen op sleutelposities van de huishouding van de opdrachtgever en de organen belast met governance.		• Bij een KITA wordt veelal van nature aan deze norm voldaan omdat de sprake is van een zeer beperkt aantal It-auditors. • Detachering: is belegd bij de opdrachtgever.
	2. De voor de opdracht verantwoordelijke professional over de juiste capaciteiten, bekwaamheden, bevoegdheid en het gezag beschikt en voldoende tijd heeft om zijn taak uit te voeren.		De IT-auditor die arbeidsrelatie heeft met een niet-IT-auditorganisatie moet bij zijn werkgever begrip ervaren indien hij aangeeft een opdracht niet met een voldoende professionaliteit te kunnen uitvoeren.
	3. De verantwoordelijkheden van de voor de opdracht verantwoordelijke professionals duidelijk worden gedefinieerd en besproken met die professionals		• Deze norm is niet van toepassing op de KITA. • Detachering: is belegd bij de opdrachtgever.

Self assessment kwaliteitsonderzoek IT-auditorg. – ingedeeld naar functies			
Vraag	**Norm**	**Antwoord [1]**	**Toelichting / voorbeeld**
24	De IT-auditorganisatie stelt geschikte professionals aan met de noodzakelijke capaciteiten, bekwaamheden en voldoende tijd om opdrachten in overeenstemming met de vaktechnische richtlijnen en de door wet- en regelgeving gestelde eisen uit te voeren en om de organisatie of haar voor opdrachten verantwoordelijke professionals in staat te stellen rapporten af te geven die onder de gegeven omstandigheden juist zijn.		Een KITA moet in relatie tot elke opdracht nagaan of de IT-auditor(s) aan deze norm kan (kunnen) voldoen.
25	De IT-auditorganisatie stelt procedures vast om de capaciteiten en bekwaamheden van de overige beroepsbeoefenaren te beoordelen. De capaciteiten en bekwaamheden die in aanmerking worden genomen bij het samenstellen van opdrachtteams en bij het bepalen hoe zwaar het toezicht moet zijn, zijn de volgende: • Het inzicht in en praktische ervaring met soortgelijke opdrachten qua aard en complexiteit verkregen door de juiste training en deelname aan dergelijke opdrachten. • Het inzicht in de vaktechnische richtlijnen en de door wet- en regelgeving gestelde eisen. • De juiste vaktechnische kennis, met name kennis van de van belang zijnde informatietechnologie. • Het vermogen om vakkundige oordeelsvorming toe te passen. • Het inzicht in de gedragslijnen en procedures van de IT-auditorganisatie met betrekking tot kwaliteitsbeheersing.		• Bij de KITA is deze norm slechts beperkt van toepassing omdat het aantal overige beroepsbeoefenaren nul of zeer gering is. • Detachering: is belegd bij de opdrachtgever.
	UITVOERING VAN OPDRACHTEN		
26	De IT-auditorganisatie heeft gedragslijnen en procedures die zijn opgezet om een redelijke mate van zekerheid te verkrijgen dat de opdrachten worden uitgevoerd in overeenstemming met de vaktechnische richtlijnen en de door wet- en regelgeving gestelde eisen, en dat de organisatie of haar		• Bij de KITA vergt met name het toezicht (derde bullet), de belangrijke beoordelingen en vorm van het rapport (vierde bullet) om extra voorzieningen, bijvoorbeeld door de in-

Self assessment kwaliteitsonderzoek IT-auditorg. – ingedeeld naar functies			
Vraag	**Norm**	**Antwoord [1]**	**Toelichting / voorbeeld**
	voor opdrachten verantwoordelijke professionals rapporten afgeven die onder de gegeven omstandigheden juist zijn. Zaken waaraan aandacht moet worden besteed, zijn: • De wijze waarop opdrachtteams worden geïnstrueerd ten aanzien van de opdracht waarbij zij worden ingezet, om inzicht te verkrijgen in het doel van hun werkzaamheden. • De maatregelen ter naleving van de voor de opdracht van toepassing zijnde richtlijnen. • De maatregelen op het gebied van toezicht binnen de opdracht, training van de overige beroepsbeoefenaren en begeleiding. • De methoden om de uitgevoerde werkzaamheden, de belangrijke beoordelingen die het opdrachtteam heeft ingenomen en de vorm van het rapport dat wordt afgegeven, te beoordelen. • Een juiste vastlegging van de uitgevoerde werkzaamheden en van de tijdsfasering en de omvang van de kwaliteitsbeoordeling. • De maatregelen om alle gedragslijnen en procedures actueel te houden.		schakeling van een andere IT-auditor. • In de situatie van solistische opererende IT-auditor die een werkrelatie heeft bij een niet-IT-auditorganisatie, moet voor relevante onderzoeken een beroep kunnen worden gedaan op een beoordeling door de benoemde andere auditor. • Detachering: is belegd bij de opdrachtgever.
27	De reviewverantwoordelijkheden worden zo geregeld dat meer ervaren leden van het opdrachtteam, waaronder de voor de opdracht verantwoordelijke professional, een review uitvoeren op de werkzaamheden die zijn uitgevoerd door minder ervaren teamleden. In het kader van de review wordt vastgesteld of: 1. De werkzaamheden zijn uitgevoerd overeenkomstig de vaktechnische richtlijnen en de door wet- en regelgeving gestelde eisen. 2. Zich belangrijke zaken hebben voorgedaan die nadere beschouwing noodzakelijk maken.		• Bij de KITA vergt de review extra voorzieningen omdat door de beperkte omvang van de organisatie de review veelal niet binnen de organisatie op een objectieve wijze kan worden uitgevoerd. Een voorbeeld voor het uitvoeren van een objectieve review is het inschakelen van een andere IT-auditor. • Detachering: is belegd bij de opdrachtgever.

Self assessment kwaliteitsonderzoek IT-auditorg. – ingedeeld naar functies			
Vraag	**Norm**	**Antwoord [1]**	**Toelichting / voorbeeld**
	3. De juiste consultaties hebben plaatsgevonden en de daaruit voortvloeiende eindoordelen / adviezen zijn vastgelegd en overgenomen. 4. De noodzaak bestaat om de aard, tijdsfasering en omvang van de uitgevoerde werkzaamheden te herzien. 5. De eindoordelen / adviezen die zijn gevormd / gegeven, worden onderbouwd met de uitgevoerde werkzaamheden en op de juiste wijze zijn vastgelegd. 6. De verkregen informatie toereikend genoeg is om het rapport te onderbouwen. 7. Het doel van de in het kader van de opdracht uitgevoerde werkzaamheden is bereikt.		
	CONSULTATIE		
28	De IT-auditorganisatie heeft gedragslijnen en procedures die zijn opgezet om een redelijke mate van zekerheid te verkrijgen dat: 1. Over moeilijke of omstreden zaken de juiste consultaties hebben plaatsgevonden. 2. Voldoende middelen ter beschikking zijn, zodat de juiste consultaties kunnen plaatsvinden. 3. De aard en reikwijdte van dergelijke consultaties worden vastgelegd. 4. De eindoordelen voortkomend uit consultaties worden vastgelegd en overgenomen.		• Bij de KITA vergt de consultatie extra voorzieningen omdat door de beperkte omvang van de organisatie de consultatie veelal niet binnen de organisatie op een objectieve wijze kan worden uitgevoerd. Een voorbeeld voor het uitvoeren van een objectieve consultatie is het inschakelen van een andere IT-auditor. • Detachering: is belegd bij de opdrachtgever.
29	De IT-auditorganisatie tracht een cultuur tot stand te brengen waarin consultatie wordt gezien als een kracht en die het personeel stimuleert om advies in te winnen in moeilijke of omstreden zaken.		• Detachering: is belegd bij de opdrachtgever.

Self assessment kwaliteitsonderzoek IT-auditorg. – ingedeeld naar functies			
Vraag	**Norm**	**Antwoord [1]**	**Toelichting / voorbeeld**
30	De procedures betreffende consultatie stellen als eis dat consultatie plaatsvindt bij personen die de juiste kennis, senioriteit en ervaring bezitten binnen de IT-auditorganisatie (of indien van toepassing daarbuiten) over belangrijke vaktechnische, ethische en andere zaken en dat de eindoordelen voortkomend uit consultaties op de juiste wijze worden vastgelegd en overgenomen.		• Detachering: is belegd bij de opdrachtgever.
31	Indien gebruikt wordt gemaakt van extern advies, heeft de IT-auditorganisatie vastgesteld dat de externe dienstaanbieder voldoende gekwalificeerd is.		• Detachering: is belegd bij de opdrachtgever.
32	De vastlegging van consultaties bij andere beroepsgenoten over moeilijke of omstreden zaken wordt goedgekeurd door zowel de persoon op wiens verzoek consultatie plaatsvond als de persoon die is geconsulteerd. De vastlegging is voldoende compleet en gedetailleerd om inzicht te verkrijgen in: 1. De kwestie waarvoor consultatie plaatsvond. 2. De resultaten van de consultatie, waaronder alle genomen beslissingen, de basis daarvoor en de wijze waarop de beslissingen zijn uitgevoerd.		• Detachering: is belegd bij de opdrachtgever.
	VERSCHILLEN VAN INZICHT		
33	De IT-auditorganisatie heeft gedragslijnen en procedures voor het behandelen en het oplossen van verschillen van inzicht binnen het opdrachtteam, met de personen bij wie advies is ingewonnen en indien van toepassing tussen de voor de opdracht verantwoordelijke professional en de opdrachtgerichte kwaliteitsbeoordelaar. De eindoordelen die zijn gevormd, worden vastgelegd en overgenomen.		• Bij de KITA moet het afwikkelen van verschillen van inzicht worden gezien in relatie tot de vragen 26 tot en met 32. • Detachering: is belegd bij de opdrachtgever.

Self assessment kwaliteitsonderzoek IT-auditorg. – ingedeeld naar functies			
Vraag	**Norm**	**Antwoord [1]**	**Toelichting / voorbeeld**
34	Het assurance rapport wordt niet afgegeven voordat de verschillen van inzicht zijn opgelost.		• Ad: gezien het aandeel van adviezen in het werkpakket van IT-auditororganisaties is het logisch dat deze regel ook voor rapportages over adviezen geldt. • Detachering: is belegd bij de opdrachtgever. • Ov: hoewel deze werkzaamheden niet formeel zijn aan te merken als assurance, is het gezien het belang voor de naam en faam van de beroepsgroep logisch deze norm ook toe te passen op overige professionele diensten.
35	Een IT-auditorganisatie die gebruikmaakt van de diensten van een voldoende gekwalificeerde externe persoon om een opdrachtgerichte kwaliteitsbeoordeling uit te voeren, realiseert zich dat verschillen van inzicht kunnen ontstaan en stelt procedures vast om dergelijke verschillen van inzicht op te lossen.		• Bij de KITA moet het afwikkelen van verschillen van inzicht worden gezien in relatie tot de vragen 26 tot en met 32. • Detachering: is belegd bij de opdrachtgever.
DOSSIER GERELATEERDE NORMEN			
	OPDRACHTGERICHTE KWALITEITSBEOORDELING		
36	De IT-auditorganisatie heeft gedragslijnen en procedures die als eis stellen dat voor daarvoor in aanmerking komende opdrachten een opdrachtgerichte kwaliteitsbeoordeling plaatsvindt, waarin een objectieve evaluatie plaatsvindt van de belangrijke standpunten die het opdrachtteam heeft ingenomen en de eindoordelen / het advies die zijn gevormd bij het formuleren van het rapport. Dergelijke gedragslijnen omvatten: 1. De criteria te aan de hand waarvan alle andere opdrachten worden geëvalueerd om te beoordelen of een opdrachtgerichte kwaliteitsbeoordeling dient te worden uitgevoerd. 2. Een opdrachtgerichte kwaliteitsbeoordeling voor te schrijven voor alle		• Bij de KITA vergt deze norm aanvullende voorzieningen, bijvoorbeeld door het inschakelen van een andere IT-auditor. • Detachering: is belegd bij de opdrachtgever. • Voor een voorbeeld van de opdrachtgerichte kwaliteitsbeoordeling (OKB) wordt onder andere verwezen naar het document ‘Werkprogramma (beperkte) OKB’ op de website van NOREA

Self assessment kwaliteitsonderzoek IT-auditorg. – ingedeeld naar functies			
Vraag	**Norm**	**Antwoord [1]**	**Toelichting / voorbeeld**
	opdrachten die voldoen aan de vastgestelde criteria.		
37	De gedragslijnen en procedures van de IT-auditorganisatie stellen als eis dat de opdrachtgerichte kwaliteitsbeoordeling is afgerond voordat het rapport wordt afgegeven.		Detachering: is belegd bij de opdrachtgever.
38	De criteria die de IT-auditorganisatie in aanmerking neemt bij het bepalen van de opdrachten die onderwerp moeten zijn van een opdrachtgerichte kwaliteitsbeoordeling, zijn: • 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.		Detachering: is belegd bij de opdrachtgever.
39	De IT-auditorganisatie heeft gedragslijnen en procedures vastgesteld, waarin zijn opgenomen: 1. De aard, tijdsfasering en omvang van een opdrachtgerichte kwaliteitsbeoordeling. 2. De criteria om op te kunnen treden als opdrachtgerichte kwaliteitsbeoordelaar. 3. De vereisten voor dossiervorming voor een opdrachtgerichte kwaliteitsbeoordeling. De gedragslijnen en procedures bieden de mogelijkheid om nuanceringen voor advies en aanverwante diensten aan te brengen.		Detachering: is belegd bij de opdrachtgever.
	AARD, TIJDSTIP EN OMVANG OPDRACHTGERICHTE KWALITEITSBEOORDELING		

Self assessment kwaliteitsonderzoek IT-auditorg. – ingedeeld naar functies			
Vraag	**Norm**	**Antwoord [1]**	**Toelichting / voorbeeld**
40	Een opdrachtgerichte kwaliteitsbeoordeling omvat in het algemeen een bespreking met de voor de opdracht verantwoordelijk professional, een onderzoek van informatie dat object van het onderzoek is en van het rapport en in het bijzonder de juistheid daarvan. Het omvat ook het onderzoeken van geselecteerde dossierstukken die betrekking hebben op de belangrijke standpunten die het opdrachtteam heeft ingenomen en de eindoordelen adviezen die zijn gevormd.		Detachering: is belegd bij de opdrachtgever.
41	De opdrachtgerichte kwaliteitsbeoordelaar verricht het onderzoek tijdig op daartoe geschikte momenten tijdens de uitvoering van de opdracht, zodat belangrijke zaken onmiddellijk kunnen worden opgelost conform de wens van de kwaliteitsbeoordelaar en voordat het rapport / advies wordt afgegeven.		• Bij de KITA vergt deze norm aanvullende voorzieningen, bijvoorbeeld door het maken van afspraken over het tijdig uitvoeren van deze activiteit door een andere IT-auditor. Zie ook norm 44. • Detachering: is belegd bij de opdrachtgever.
	CRITERIA VOOR OPDRACHTGERICHTE KWALITEITSBEOORDELAAR		
42	De gedragslijnen en procedures van de IT-auditorganisatie richten zich op de benoeming van de opdrachtgerichte kwaliteitsbeoordelaar en bepalen onder welke voorwaarden zij kunnen worden benoemd. Hierbij worden in aanmerking genomen: 1. De vaktechnische kwalificaties die vereist zijn om deze rol te vervullen, alsmede de noodzakelijke ervaring, bevoegdheid en het gezag. 2. De mate waarin bij een opdrachtgerichte kwaliteitsbeoordelaar advies kan worden ingewonnen over de opdracht zonder dat de objectiviteit van de kwaliteitsbeoordelaar wordt aangetast.		Detachering: is belegd bij de opdrachtgever.
43	De kwaliteitsbeoordelaar is voldoende deskundig, ervaren en bevoegd en heeft voldoende gezag en is te allen tijde objectief.		Detachering: is belegd bij de opdrachtgever.

Self assessment kwaliteitsonderzoek IT-auditorg. – ingedeeld naar functies			
Vraag	**Norm**	**Antwoord [1]**	**Toelichting / voorbeeld**
44	Indien kleine IT-auditorganisaties opdrachten aanvaarden waarvoor kwaliteitsbeoordelingen moeten worden uitgevoerd, waarborgen zij dat zij hiervoor voldoende gekwalificeerde externe personen aantrekken indien zijn de kwaliteitsbeoordelingen door een andere auditorganisaties laat uitvoeren.		Detachering: is belegd bij de opdrachtgever.
	DOCUMENTATIE OPDRACHTGERICHTE KWALITEITSBEOORDELING		
45	De gedragslijnen en procedures betreffende de dossiervorming van de opdrachtgerichte kwaliteitsbeoordeling kennen als eis dat dossiervorming plaatsvindt waarin wordt vastgelegd dat: 1. De procedures, die zijn vereist op grond van de gedragslijnen van de IT-auditorganisatie met betrekking tot opdrachtgerichte kwaliteitsbeoordeling, zijn uitgevoerd. 2. De opdrachtgerichte kwaliteitsbeoordeling is afgerond voordat het rapport is afgegeven. 3. De kwaliteitsbeoordelaar geen onopgeloste zaken kent waarvan hij de indruk heeft dat de belangrijke standpunten die het opdrachtteam heeft ingenomen en de eindoordelen die zij hebben gevormd niet juist waren		Detachering: is belegd bij de opdrachtgever.
	MONITOREN		
46	De IT-auditorganisatie heeft gedragslijnen en procedures die zijn opgezet om een redelijke mate van zekerheid te verkrijgen dat de gedragslijnen en procedures met betrekking tot het systeem van kwaliteitsbeheersing relevant en adequaat zijn, effectief werken en binnen de beroepsuitoefening worden nageleefd. In dergelijke gedragslijnen en procedures is opgenomen dat voortdurend aandacht wordt besteed aan en evaluatie plaatsvindt		Detachering: is belegd bij de opdrachtgever.

Self assessment kwaliteitsonderzoek IT-auditorg. – ingedeeld naar functies			
Vraag	**Norm**	**Antwoord [1]**	**Toelichting / voorbeeld**
	van het systeem van kwaliteitsbeheersing, en dat een periodieke inspectie van een selectie uit afgeronde opdrachten plaatsvindt.		
47	De IT-auditorganisatie draagt de verantwoordelijkheid voor het bewakingsproces op aan een of meer verantwoordelijke professionals of andere personen met een zodanig toereikende ervaring en bevoegdheid binnen de organisatie dat zij die verantwoordelijkheid op zich kunnen nemen. De bewaking van het kwaliteitsbeheersingssysteem van de IT-auditorganisatie wordt uitgevoerd door bekwame personen en omvat zowel de juiste opzet als de effectiviteit van de werking van het kwaliteitsbeheersingssysteem.		• Bij de KITA vergt deze norm veelal aanvullende voorzieningen, bijvoorbeeld door het maken van afspraken over het invullen van deze norm door een andere IT-auditor. • Detachering: is belegd bij de opdrachtgever.
48	De IT-auditorganisatie evalueert periodiek het kwaliteitsbeheersingssysteem. Indien de IT-auditorganisatie tekortkomingen signaleert in het kwaliteitsbeheersingssysteem, worden adequate aanpassingen onmiddellijk doorgevoerd.		• De KITA moet overwegen deze evaluatie te realiseren via de op grond van andere normen reeds betrokken andere IT-auditor. Zie ook norm 50. • Detachering: is belegd bij de opdrachtgever.
49	Het kwaliteitstoezicht van een selectie uit afgeronde opdrachten wordt in het algemeen cyclisch uitgevoerd. Tot de opdrachten die worden geselecteerd voor kwaliteitstoezicht behoort tenminste een opdracht van elke voor opdrachten verantwoordelijke professionals per inspectiecyclus, die in het algemeen niet langer is dan vijf jaar.		Detachering: is belegd bij de opdrachtgever.
50	Kleine IT-auditorganisaties kunnen gebruik maken van voldoende gekwalificeerde externe personen of een andere IT-auditorganisatie om opdrachtgerichte inspecties en andere kwaliteitsbewakingsprocedures uit te voeren.		Detachering: is belegd bij de opdrachtgever.
51	De IT-auditorganisatie evalueert het effect van tekortkomingen die zijn opgemerkt als gevolg van het bewakingsproces en bepaalt of deze tekortkomingen:		• De KITA moet overwegen deze evaluatie te realiseren via de op grond van andere normen reeds betrokken andere IT-auditor.

Self assessment kwaliteitsonderzoek IT-auditorg. – ingedeeld naar functies			
Vraag	**Norm**	**Antwoord [1]**	**Toelichting / voorbeeld**
	1. Losstaande gevallen zijn, die er niet noodzakelijk op wijzen dat het kwaliteitsbeheersingssysteem van de IT-auditorganisatie onvoldoende is om een redelijke mate van zekerheid te verschaffen, dat het voldoet aan de vaktechnische richtlijnen en de door wet- en regelgeving gestelde eisen en dat de door de organisatie of haar voor opdrachten verantwoordelijke professionals afgegeven rapporten onder de gegeven omstandigheden juist zijn. 2. Systematische, zich herhalende of andere belangrijke tekortkomingen zijn, die een snelle corrigerende actie vereisen.		• Detachering: is belegd bij de opdrachtgever.
52	De IT-auditorganisatie maakt tekortkomingen die zijn opgemerkt als bevinding van het bewakingsproces en aanbevelingen voor de adequate correctieactie bekend aan de desbetreffende professionals en ander personeel.		Detachering: is belegd bij de opdrachtgever.
53	De evaluatie door de IT-auditorganisatie van elke soort tekortkoming resulteert in aanbevelingen met betrekking tot een of meer van de volgende acties aanbevelingen: 1. Het treffen van corrigerende maatregelen met betrekking tot een bepaalde opdracht of een bepaald personeelslid. 2. Het bekendmaken van de bevindingen aan degenen, die verantwoordelijk zijn voor training en vaktechnische ontwikkeling. 3. Het aanbrengen van wijzigingen in de gedragslijnen voor kwaliteitsbeheersing en de kwaliteitsbeheersingsprocedures. 4. Het nemen van disciplinaire maatregelen tegen degenen, die niet voldoen aan de gedragslijnen en procedures van de IT-auditorganisatie, in het bijzonder tegen degenen die dat herhaaldelijk doen.		Detachering: is belegd bij de opdrachtgever.
54	In het geval dat de uitkomsten van de kwaliteitsbewakingsprocedures		Detachering: is belegd bij de opdrachtgever.

Self assessment kwaliteitsonderzoek IT-auditorg. – ingedeeld naar functies			
Vraag	**Norm**	**Antwoord [1]**	**Toelichting / voorbeeld**
	aangeven dat een rapport onjuist zou kunnen zijn of dat procedures ten onrechte niet zijn gehanteerd bij de uitvoering van de opdracht, bepaalt de IT-auditorganisatie welke verdere acties adequaat zijn om te kunnen voldoen aan de geldende vaktechnische richtlijnen en de door wet- en regelgeving gestelde eisen. Ook wordt het inwinnen van juridisch advies overwogen.		
55	Ten minste een keer per jaar maakt de IT-auditorganisatie de uitkomsten van de bewaking van haar kwaliteitsbeheersingssysteem bekend aan de voor opdrachten verantwoordelijke professionals en andere belangrijke personen binnen de organisatie, waaronder de leiding van de IT-auditorganisatie.		Detachering: is belegd bij de opdrachtgever.
56	De rapportage van gesignaleerde tekortkomingen aan andere personen dan de betrokken voor opdrachten verantwoordelijke professionals bevat in het algemeen niet de aanduiding van de desbetreffende specifieke opdrachten, tenzij een dergelijke aanduiding noodzakelijk is voor een correcte decharge van de verantwoordelijkheden van de andere personen.		Detachering: is belegd bij de opdrachtgever.
57	Er is sprake van adequate dossiervorming over de bewaking van de kwaliteitsprocedures en de gesignaleerde tekortkomingen.		Detachering: is belegd bij de opdrachtgever.
	KLACHTEN EN BESCHULDIGINGEN		
58	De IT-auditorganisatie heeft gedragslijnen en procedures die zijn opgezet om een redelijke mate van zekerheid te verkrijgen dat de volgende zaken op de juiste wijze worden behandeld: 1. Klachten en beschuldigingen dat de door de IT-auditorganisatie uitgevoerde werkzaamheden niet voldoen aan de vaktechnische richtlijnen en de door de wet- en regelgeving gestelde eisen. 2. Beschuldigingen dat niet wordt voldaan aan het kwaliteitsbeheersings-		Detachering: is belegd bij de opdrachtgever.

Self assessment kwaliteitsonderzoek IT-auditorg. – ingedeeld naar functies			
Vraag	**Norm**	**Antwoord [1]**	**Toelichting / voorbeeld**
	systeem van de IT-auditorganisatie.		
59	De IT-auditorganisatie stelt duidelijk omschreven communicatielijnen voor personeel van de organisatie vast waardoor alle bedenkingen kunnen worden gemeld op een wijze, waarbij personeelsleden zich kunnen uitspreken zonder angst voor represailles te hoeven hebben.		Detachering: is belegd bij de opdrachtgever.
60	De IT-auditorganisatie onderzoekt dergelijke klachten en beschuldigingen volgens de vastgestelde gedragslijnen en procedures. Op het onderzoek wordt toezicht gehouden door een professional met toereikende ervaring, bevoegdheid en het gezag binnen de IT-auditorganisatie die niet op andere wijze betrokken is bij de opdracht. Het onderzoek omvat indien noodzakelijk het inwinnen van juridisch advies. Kleine auditorganisaties kunnen gebruikmaken van de diensten van een voldoende gekwalificeerde externe persoon of een andere IT-auditorganisatie om het onderzoek uit te voeren. Er is sprake van adequate dossiervorming.		Detachering: is belegd bij de opdrachtgever.
61	Indien de resultaten van de onderzoeken duiden op tekortkomingen in de opzet of werking van de gedragslijnen voor kwaliteitsbeheersing en de kwaliteitsbeheersingsprocedures van de IT-auditorganisatie of het niet voldoen aan het kwaliteitsbeheersingssysteem van de organisatie door één of meer personen, neemt de IT-auditorganisatie gepaste maatregelen om de gedragslijnen en/of kwaliteitsbeheersingsprocedures aan te passen.		Detachering: is belegd bij de opdrachtgever.
	DOSSIERVORMING		
62	De IT-auditorganisatie heeft gedragslijnen en procedures die eisen dat adequate vastleggingen worden vervaardigd om aan te tonen dat elk onderdeel van haar kwaliteitsbeheersingssysteem op de juiste wijze werkt.		Detachering: is belegd bij de opdrachtgever.

Self assessment kwaliteitsonderzoek IT-auditorg. – ingedeeld naar functies			
Vraag	**Norm**	**Antwoord [1]**	**Toelichting / voorbeeld**
63	De IT-auditorganisatie bewaart haar dossiers zo lang, dat degenen die kwaliteitsbewakingsprocedures uitvoeren voldoende tijd krijgen om te evalueren dat de IT-auditorganisatie voldoet aan haar systeem van kwaliteitsbeheersing, of de dossiers worden voor een langere periode bewaard als de wet- of regelgeving dit voorschrijven.		Detachering: is belegd bij de opdrachtgever.