

WERKPROGRAMMA Kwaliteitsonderzoek	
INLEIDING	
A.	Dit standaardwerkprogramma is gericht op het uitvoeren van de kwaliteitsonderzoeken van NOREA vanaf 2020.
B.	De onderzoekers kunnen tijdens hun werkzaamheden concluderen dat dit standaardwerkprogramma niet toepasbaar is dan wel moet worden aangevuld met aanvullende of andere activiteiten. Indien zich een dergelijke situatie voordoet, wordt overlegd met het CKO-lid vermeld onder de identificerende kenmerken
C.	De onderzoeken hebben betrekking op in het voorgaande jaar uitgevoerde werkzaamheden; ook afgeronde opdrachten in het huidige jaar kunnen worden onderzocht.
D.	Het kwaliteitsonderzoek wordt onderscheiden op basis van de door de IT-auditorganisatie verrichte opdrachten in: • Opdrachten: alle opdrachten exclusief assurance-opdrachten (zie kolom O) • Richtlijn 4400-opdrachten (zie kolom 4). • Assurance-opdrachten (zie kolom A) In de kolommen van het werkprogramma is doormiddel van een kruisje aangegeven of een activiteit van toepassing op het onderzoek.
E.	Het werkprogramma is gebaseerd op het aanleggen van een elektronisch dossier. NOREA beschikt over faciliteiten om elektronische dossiers te ondersteunen en maakt gebruik van ClientOnline waarin het dossier wordt aangemaakt en gevuld.
F.	Het dossier is opgebouwd volgens de standaardindeling (zie doc.10 Dossierindeling). Dit werkprogramma kan daarin als eerste worden opgenomen.

WERKPROGRAMMA	
Naam IT-auditorganisatie:	
Soort onderzoek: Regulier / Vervolgonderzoek verbeterplan / Heronderzoek (doorhalen wat n.v.t. is)	
Teamleider:	Onderzoeker:

Regel	Activiteit voor toelichting: zie einde paragraaf	Dos- sierstuk	O	4	A	Uitgevoerd initiaal/d.d.
1	Identificerende kenmerken:					
1	Naam CKO-lid belast met de begeleiding:					
2	Naam contactpersoon IT-auditorganisatie:					
3	Telefoon / e-mail contactpersoon:					
4	Korte beschrijving van de IT-auditorganisatie:					
2	Correspondentie / e-mails					
1	Neem kennis van de generieke selectiebrief en de door de IT-auditorganisatie ondertekende opdrachtbevestiging		x	x	x	
2	Documenteer de afspraken met de IT-auditorganisatie bij de uitwerking en Invulling van het onderzoek		x	x	x	
3	Neem kennis van de in het dossier opgenomen relevante e-mails en andere correspondentie		x	x	x	
4	Voeg tijdens het onderzoek aangetroffen relevante e-mails en andere correspondentie toe aan het dossier		x	x	x	
5	Bevestig via e-mail de ontvangst van documentatie en neem deze e-mail op in het dossier		x	x	x	
3	Elektronisch dossier (in gangbaar (Word)-formaat – zie model)					
1	Leg het dossier aan conform document 10 – zie A en B in de toelichting		x	x	x	
2	Aanvullen van het van Bureau NOREA ontvangen dossier		x	x	x	
3	Afronding dossiervastlegging – zie N in de toelichting		x	x	x	

Regel	Activiteit voor toelichting: zie einde paragraaf	Dos- sierstuk	O	4	A	Uitgevoerd initiaal/d.d.
4	Onderzoek kwaliteitsstelsel					
	1 Beoordeel documenten opgevraagd in de bijlage van de Opdrachtbevestiging aan de hand van document 17 –zie C in de toelichting		x	x	x	
	2 Beoordelen scope van het onderzoek – zie D t/m J in de toelichting		x	x	x	
	3 Beoordeel de ontvangen Self-assessment door de onderbouwing c.q. de evidence te controleren. Daartoe wordt additionele informatie opgevraagd zoals in ieder geval een lijst met de in de voorafgaande periode tot het kwaliteitsonderzoek uitgevoerde opdrachten (over het jaar van onderzoek en eventueel ook recenter, zie inleiding punt C.). Leg de bevindingen en conclusie vast. Zie K in de toelichting		x	x	x	
	4 Beoordeel het handboek Kwaliteitsbeheersing aan de hand van VK01 Vragenlijst kwaliteitsbeheersingssysteem en leg de bevindingen en conclusie vast – zie L in de toelichting		x	x	x	
	5a Beoordeel de werking hiervan door beoordeling van een of meer dossiers aan de hand van VK02. Vragenlijst dossierreview Assurance-opdrachten				x	
	5b Beoordeel de werking hiervan door beoordeling van een of meer dossiers aan de hand van VK03 Vragenlijst dossierreview Professionele diensten anders dan assurance		X			
	5c Beoordeel de werking hiervan door beoordeling van een of meer dossiers aan de hand van VK04 Vragenlijst Richtlijn 4400-opdrachten			x		
	6 Leg de bevindingen vast en formuleer een conclusie over de opzet en de werking van het kwaliteitsbeheersingssysteem		x	x	x	
5	Onderzoek dossiers					
	1 Selecteer aan de hand van het overzicht met uitgevoerde opdrachten minimaal twee recente opdrachten. Bepaal de nadere omvang van het aantal en de soort te onderzoeken opdrachten voor verkrijgen van een representatief beeld voor het oordeel over de werking van het kwaliteitsstelsel op basis van de volgende criteria: • het risico / de aard / het belang van de opdrachten; • de omzet; • het aantal uitgevoerde opdrachten; • de verhouding assurance-advies-detachering-overige professionele diensten; • de aard van de opdrachten; Bij een kleinschalige IT-Audit organisaties (KITA) zal het onderzoek tenminste één en maximaal twee dossiers betreffen. Bij grootschalige IT-auditorganisaties moet het aantal voldoende zijn om het oordeel te onderbouwen. Dat aantal zal zich veelal kunnen beperken tot vijf dossiers.		x	x	x	
6	Afstemming bevindingen					
	1 Bespreek de vastgelegde feitelijke bevindingen per hiervoor genoemd onderdeel met de contactpersoon van de IT- auditorganisatie en leg de uitkomsten hiervan vast in het dossier – zie M in de toelichting.		x	x	x	
7	Verslaglegging					
	1 Formuleer de afgestemde bevindingen en definitieve conclusies per deelgebied ten behoeve van het verslag		x	x	x	
	2 Stel Bevindingenrapport (indien van toepassing) of het Conceptrapport op binnen één week na afronding van het onderzoek		x	x	x	
	3 Bespreek het Conceptrapport of het Bevindingenrapport met de IT-Auditorganisatie. Let hierbij op het (nog) niet vermelden van conclusies.		x	x	x	
	4 Besprek binnen één week na de bespreking met de IT-Auditorganisatie van het Conceptrapport of het Bevindingenrapport het rapport met het CKO-lid. Geef in een mail aan het CKO-lid door dat de volgende documenten		x	x	x	

Regel	Activiteit voor toelichting: zie einde paragraaf	Dos- sierstuk	O	4	A	Uitgevoerd initiaal/d.d.
	in het dossier beschikbaar zijn: • uren- / omzetverantwoording met conclusie t.a.v. scope van het onderzoek • Bevindingen beoordeling handboek Kwaliteitsbeheersing • Bevindingen VK01 Vragenlijst kwaliteitsbeheersingssysteem • Bevindingen VK02 Vragenlijst dossierreview Assurance-opdrachten • Bevindingen VK03 Vragenlijst dossierreview Professionele diensten anders dan assurance • Bevindingen VK04 Vragenlijst dossierreview Richtlijn 4400-opdracht • Conceptrapport inclusief conclusie ter bespreking met lid CKO					
5	Bepaal met het CKO-lid of de uitkomst van het onderzoek aanleiding geeft tot het geven van aanwijzingen of aanbevelingen in combinatie met het realiseren van een Verbeterplan. ➔ Dit in het geval van een 'Voldoet niet'-conclusie (zie punt 13).		x	x	x	
6	Voer de aanpassingen in het Conceptrapport door naar aanleiding van het overleg met het CKO-lid.		x	x	x	
7	Zend het Conceptrapport binnen één week na overleg met het CKO-lid aan de contactpersoon van de IT-auditorganisatie.		x	x	x	
8	Bespreek het Conceptrapport met de contactpersoon van de IT-auditorganisatie.		x	x	x	
9	Leg de uitkomst van deze bespreking vast in het dossier.		x	x	x	
10	Stel vast of de IT-auditorganisatie binnen vier weken na het toezenden van het (bijgestelde) conceptrapport bezwaar maakt tegen de inhoud.		x	x	x	
11	Verwerk de reactie(s) van de IT-auditorganisatie – indien relevant – binnen één week na ontvangst van het bezwaar.		x	x	x	
12	Eventueel: stem met het CKO-lid af over het bezwaar, het naar aanleiding daarvan bijgestelde Conceptrapport en de afwikkeling van het rapport.		x	x	x	
13	Indien conclusie "Voldoet niet": de IT-auditorganisatie stelt het Verbeterplan op. Dat wordt beoordeeld door de (oorspronkelijke) onderzoeker: Deze beoordeling heeft tot doel te onderzoeken of het door de IT-auditorganisatie uitgebrachte Verbeterplan voldoende waarborgen in zich heeft om het stelsel van kwaliteitsbeheersingsmaatregelen te laten voldoen aan het RKBN, de Statuten, Reglementen en Richtlijnen van NOREA.		x	x	x	
14	Eventueel: stel de termijn voor het Verbeterplan vast (maximaal zes maanden)		x	x	x	
15	Eventueel: stel vast dat de IT-auditorganisatie de afspraken over de beoordeling van het Verbeterplan en het heronderzoek heeft ondertekend.		x	x	x	
16	Draag na het vervallen van de vierweekstermijn voor bezwaar het dossier over aan het bureau: • het Conceptrapport; • de aanwijzingen aan het bureau voor het definitief maken van het rapport; • het dossier. Zie N in de toelichting		x	x	x	

Ondertekening			
a.	(eventueel) Dossierreview teamleider	Datum:	Paraaf:
b.	Dossierbeoordeling lid CKO	Datum:	Paraaf:

Toelichting op het werkprogramma

A. 3.1: dossier op ClientOnline in te richten door het Bureau. Dit moet ten minste bevatten:

- selectiebrief.
- ondertekende opdrachtbevestiging.
- Ingevulde self-assessment
- Eventueel: kopie correspondentie n.a.v. opdracht zoals bezwaren en reacties daarop.
- De PE-registratie van NOREA van de bij de IT-auditorganisatie werkzame RE's

B. 3.1: dossier aanleggen – zie document 10 Dossierindeling

C. 4.1: documenten opgevraagd in bijlage bij Opdrachtbevestiging.

- Volledigheid vaststellen
- Vaststellen ondertekening van de Opdrachtbevestiging door opdrachtgever en -nemer; let ook op datering hiervan
- Eventueel ontbrekende documenten opvragen, of vastleggen dat document terecht ontbreekt.
- Documenten vastleggen op inhoudsopgave dossier.

D. 4.2: bepalen scope van het onderzoek

Basis: het overzicht van de in het afgelopen jaar uitgevoerde opdrachten / werkzaamheden. Attentiepunten:

- Kijk op website naar informatie die relevant is voor scope onderzoek. Mogelijk staat die informatie niet in de overlegde stukken.
- Volledigheid vaststellen door aansluiting met grootboek of urenverantwoording (aantal verantwoorde uren versus normaantal van circe 1.600 werkbare uren per jaar).
- Bepalen aard van de opdrachten werkzaamheden:
 - Assurance –zie E en F in de toelichting
 - Richtlijn 4400-opdrachten – zie I
 - Advies – zie G
 - Detachering – zie G
 - Overige professionele diensten – zie G en H.
- Indien de conclusie luidt, dat de opdrachten / werkzaamheden niet passen binnen de hiervoor genoemde categorieën het onderzoek staken: er is sprake van 'in business' of 'niet actief'.
- De CKO-begeleider gaat na of deze conclusie terecht is getrokken.

E. 4.2 Begrip assurance

Bij de onderzoeken worden veel begrippen gebruikt waarvan niet duidelijk is of het wel of niet assurance-opdrachten betreft. Begrippen die de revue zijn gepasseerd zijn: GBA-audit (zie I), schouw en uitvoeringstoets.

IT-auditorganisaties hanteren het begrip assurance, waar dat niet altijd assurance-opdrachten zijn in de context van de NOREA-definitie.

Het CKO heeft besloten om voor classificeren van werkzaamheden als assurance-opdracht uit te gaan van de definitie:

'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'.

In de opdracht en het rapport moeten dus de volgende begrippen naar voren komen:

- conclusie;
- vertrouwen;
- versterken;
- gebruikers zijn derden (uitzondering: [3000, art. 25A]: alleen Opdrachtgever en -nemer) en
- toetsingsnormen

De centrale onderzoeksvraag kan met ja/nee, voldoet wel/niet worden beantwoord.

De benaming van de opdracht kan tot onduidelijkheid leiden en is niet doorslaggevend.

Als aan de bovenstaande criteria wordt voldaan is sprake van een assurance opdracht en dienen de regels daarvoor te worden toegepast. Denk hierbij aan de 3000 of 3402 standaard.

Als niet aan deze criteria wordt voldaan kan er sprake zijn van een Richtlijn 4400-opdracht (overeengekomen specifieke werkzaamheden). Dit soort opdrachten verdient extra aandacht omdat er geen conclusie in de rapportage mag worden opgenomen om de schijn van assurance geven te vermijden. Voor dit soort opdrachten is een aparte vragenlijst beschikbaar.

Ook in geval van Adviesopdrachten zal niet aan deze criteria worden voldaan. Alleen het opnemen van een conclusie in een Adviesrapportage betekent niet dat het daarmee een Assurance opdracht wordt, dat is afhankelijk van de criteria. Het is wel verstandig om hier terughoudend mee om te gaan om niet ten onrechte de schijn van assurance op te roepen. Vaak zal in de opdrachtbevestiging en de rapportage worden opgenomen dat er geen sprake is van een assurance opdracht.

F. 4.2 Werkzaam als RE, maar soms niet bijdragend aan/ resulterend in een (schriftelijk eind-)rapport

Door het College Kwaliteitsonderzoek (CKO) is vastgesteld dat er veel onduidelijkheid bestaat over de interpretatie en uitleg van het begrip 'professionele dienst' in relatie tot de RE-titel.

Sommige RE's geven aan dat ze '*uitsluitend als consultant werkzaam zijn*' of '*advieswerkzaamheden doen, maar dan niet als RE*'. In dat verband heeft het bestuur de volgende interpretatie van de regels m.b.t. de RE-beroepskwalificatie bevestigd, gebaseerd op (IFAC-)uitgangspunten en eisen die aan de beroepsbeoefening en het opleidingsniveau van auditors worden gesteld (o.a. zoals bedoeld in artikel 6 van de Richtlijn 2006/43/EG). **Deze regels zijn van toepassing op alle RE's die zijn ingeschreven in het NOREA-register:**

Men treedt op als RE zodra professionele diensten worden uitgevoerd op het brede terrein van IT-audit, -Risk, -Compliance en/of -Governance (artikel 10 Statuten 'optreden als RE'). Wanneer professionele diensten door RE's worden uitgevoerd moeten deze voldoen aan de eisen van deskundigheid en zorgvuldigheid conform de Gedragscode. Kwaliteitsonderzoek is er op gericht om vast te stellen dat de RE voldoet aan het zorgvuldigheidsprincipe, zoals geformuleerd in de Gedragscode (artikel 113).

Hieruit vloeit voort dat een Register IT-auditor de 'RE-titel' **niet** naar believen kan voeren. Men is te allen tijde RE zodra IT-auditdeskundigheid **wordt of kan worden** aangewend. Het uitvoeren van adviesopdrachten of verlenen van professionele diensten (ook 'als consultant') impliceert het aanwenden van RE-deskundigheid en dus is de gedragscode en het Reglement Kwaliteitsbeheersing van toepassing.

Indien de feitelijke werkzaamheden niet bijdragen aan of resulteren in een schriftelijk rapport, zal het onderzoek zich slechts beperken tot het vaststellen van de organisatorische randvoorwaarden (ic het kwaliteitsstelsel) omdat geen rapportage of documentatie kan worden gereviewd.

G. 4.2 Detachering

Detachering kan aanleiding vormen voor vrijstelling van kwaliteitsonderzoek mits kan worden aangegeven welke persoon (RE) namens de organisatie waarbij de detacheringswerkzaamheden plaatsvinden de verantwoordelijkheid draagt voor het kwaliteitsstelsel waaronder de werkzaamheden plaatsvinden

H. 4.2 Opnemen passage over beroepsregels in opdrachtbevestiging

Grote opdrachtgevers hanteren veelal standaard leveringsvoorwaarden die een IT-auditorganisatie in het kader van de opdrachtverstrekking moet accepteren. Dergelijke voorwaarden bevatten veelal geen passage waarin is geregeld dat de RE in staat wordt gesteld om de verplichtingen na te leven die NOREA heeft vastgelegd in de beroepsreglementering.

Het CKO heeft ten aanzien van deze situatie het volgende bepaald:

- a. Als uitgangspunt geldt, dat in de algemene leveringsvoorwaarden van een IT-auditorganisatie en/of de offerte een passage wordt opgenomen die kan luiden als volgt: 'Op het uitvoeren van deze opdracht is het Reglement Gedragscode van NOREA (zie bijlage) van toepassing. De opdrachtgever verklaart de daaruit voor de opdrachtnemer voortvloeiende verplichtingen steeds volledig te zullen respecteren.' Woorden van gelijke strekking zijn vanzelfsprekend toegestaan. Voor de goede orde: in artikel 12, lid 1 van de Statuten staat vermeld dat de leden verplicht zijn tot naleving van de Statuten en alle op hen van toepassing zijnde regels van de Orde. Tot deze regels behoort onder meer de regelgeving die door de ALV is goedgekeurd en is gepubliceerd op de website. Daaronder valt het kwaliteitsbeheersingssysteem en alles wat daarmee samenhangt. Door de verwijzing naar het Reglement Gedragscode kan een opdrachtgever kennis nemen van de eisen die NOREA stelt aan haar leden.
- b. Indien de in de aanhef van dit punt geschetste situatie zich voordoet, zal in de bevestigingsbrief van de IT-auditorganisatie aan de opdrachtgever de onder a. vermelde passage moten worden opgenomen.
De ervaring leert, dat een dergelijke oplossing in de praktijk niet leidt tot problemen.

I. Richtlijn 4400 – Opdrachten overeengekomen specifieke werkzaamheden

De werkzaamheden en rapportage, uitgevoerd op basis van deze richtlijn, voldoen niet aan de criteria van punt 1. De opdracht heeft de kenmerken van een 'aan assurance verwante opdracht' maar de rapportage bevat bevindingen (de feitelijke uitkomsten van de uitgevoerde overeengekomen specifieke werkzaamheden en geen oordeel.

Het CKO concludeert dat dergelijke opdrachten worden aangemerkt als een Richtlijn 4400-opdracht

J. 4.3 Beoordeel de Self-assessment:

- Stel de ondertekening vast.
- Ga na of de invulling van '1. Identificerende kenmerken' aansluit op de bevindingen uit punt 4 en/of D hiervoor.

L. 4.4 Ontbreken van een kwaliteitshandboek

Het CKO heeft bepaald dat het ontbreken van een kwaliteitshandboek moet leiden tot de conclusie 'Voldoet niet' in combinatie met maken van afspraken over het opstellen van een Verbeterplan en een Heronderzoek.

Het is zaak dat de onderzoeker in een zo vroeg mogelijk stadium nagaat of een kwaliteitshandboek aanwezig is. Als dat niet het geval blijkt te zijn moet de conclusie

eerst worden afgestemd met het CKO-lid, daarna met de IT-auditorganisatie. Het definitieve rapport wordt opgesteld en het onderzoek beëindigd.

In het kader van het overleg met de IT-auditorganisatie kan het onderdeel kwaliteitsbeheersing uit het handboek KITA worden verstrekt (zie document D). Dit model kan dienen als basis voor het inrichten van een kwaliteitshandboek.

Let op: de IT-auditorganisatie kan stellen dat de uitgevoerde werkzaamheden wel voldoen aan het RKBN. Om deze stelling te onderzoeken moet de relatie tussen het RKBN en de uitgevoerde werkzaamheden in dat geval door de onderzoeker worden gelegd. Het CKO is van mening dat een dergelijke stelling in theorie mogelijk is, maar dat een dergelijke analyse leidt tot interpretaties door de onderzoeker die ongewenst kunnen zijn en leiden tot extra werkzaamheden. Daarom heeft het CKO, conform het gestelde in de artikelen 5, 6 en 7 van het RKBN, het formele standpunt ingenomen dat gedragslijnen voor kwaliteitsbeheersing en de kwaliteitsbeheersingsprocedures dienen te worden vastgelegd, bijvoorbeeld in een handboek kwaliteitsbeheersing.

M. 6.1 Afstemming (voorlopige) bevindingen met IT-auditorganisatie

Volgens het Handboek mogen GEEN uitspraken worden gedaan over de conclusie van een kwaliteitsonderzoek VOORDAT het begeleidende CKO-lid het onderzoek en de conclusie heeft beoordeeld. Daarna kan de Conceptrapportage worden afgestemd met de IT-auditorganisatie. De reden voor deze afspraak is dat nog consensus over de inhoud van oordelen moet worden gevormd.

Het is logisch dat de onderzochte IT-auditorganisatie direct na afloop van het onderzoek, en vooruitlopend op het verstrekken van het Conceptrapport, wil weten wat de conclusie van de onderzoeker is.

Verwijs dan naar de hiervoor genoemde procedure en vermijdt het geven van een conclusie. Daarnaast wil je als onderzoeker de bevindingen nog op je wilt laten inwerken en daarom kun je nog geen globale uitspraak doen.

N. 3.3 en 7.15 Kenmerken goed controledossier (bron: toezichtbevindingen AFM)

- a. Kenmerk 1: een goed controledossier laat duidelijk alle relevante controlestappen en hun onderlinge samenhang zien.
- b. Kenmerk 2: een goed controledossier bevat voldoende motivering van de keuzes die de IT-auditor heeft gemaakt in het kader van zijn professionele oordeelsvorming.
- c. Kenmerk 3: in een goed controledossier zijn de uitgevoerde controlewerkzaamheden voldoende gedetailleerd vastgelegd.
- d. Kenmerk 4: een goed controledossier is compleet en overzichtelijk. Daarbij is een goede audit-trail aanwezig: van norm via bevindingen naar de analyse en oordeelsvorming, inclusief de conclusie en eventuele aanbevelingen in de rapportage. En ook weer terug.