NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS
College Kwaliteitsonderzoek

WERKPROGRAMMA 2020	
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 collegelid dat is vermeld onder de identificerende kenmerken
C.	De onderzoeken hebben betrekking op in het voorgaande jaar uitgevoerde werkzaamheden
D.	Het kwaliteitsonderzoek wordt onderscheiden op basis van de door de IT-auditorganisatie verrichte opdrachten in: • **O**pdrachten: alle opdrachten exclusief assurance-opdrachten. • **A**ssurance-opdrachten 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 niet over faciliteiten om elektronische dossiers te ondersteunen. Daarom wordt uitgegaan van het aanleggen van elektronische map in waarin alle documenten, ongeacht het bestandsformaat, worden opgeslagen.
F.	Het dossier is opgebouwd volgens standaardindeling – zie doc.10 – werkprogramma als eerste in dossier opnemen
WERKPROGRAMMA	

Naam IT-auditorganisatie:							**2014**
Soort onderzoek: Regulier / Vervolgonderzoek verbeterplan / Heronderzoek (doorhalen wat is n.v.t.)							
Teamleider:		**Onderzoeker:**					
Regel		Activiteit voor toelichting: zie einde paragraaf		Dos-sierstuk	**O**	**A**	Uitgevoerd init. / d.d.
1		**Identificerende kenmerken:**					
	1	Naam lid CKO belast met de begeleiding					
	2	Naam contactpersoon IT-auditorganisatie.					
	3	Telefoon / e-mail contactpersoon					
	4	Type onderzoek (doorhalen wat niet van toepassing is)	**O**pdracht / **A**ssurance				
	5	Maak een korte beschrijving van de IT-auditorganisatie			x	x	
2		**Correspondentie / e-mails**					
	1	Neem kennis van de generieke selectiebrief en de door de ITauditorganisatie getekende opdrachtbevestiging			x	x	
	2	Betrek de afspraken met de IT-auditorganisatie bij de uitwerking en invulling onderzoek			x	x	
	3	Neem kennis van de in het dossier opgenomen relevante e-mails en andere correspondentie			x	x	
	4	Voeg tijdens het onderzoek aangetroffen relevante e-mails en andere correspondentie toe aan het dossier			x	x	
	5	Bevestig via e-mail de ontvangst van documentatie en neem deze mail op in het dossier			x	x	
3		**Elektronisch dossier** (in gangbaar (Word)-formaat – zie model)					
	1	Leg het dossier aan conform document 10 – zie A en B hierna			x	x	
	2	Aanvullen van het Bureau NOREA ontvangen dossier			x	x	
	3	Afwerken dossier – zie N hierna			x	x	
4		**Onderzoek kwaliteitsstelsel**					
	1	Beoordeel documenten opgevraagd in opdrachtbevestiging aan de hand van document 17 –zie C hierna			x	x	
	2	Beoordelen scope van het onderzoek – zie D t/m J hierna			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 periode tot de toetsing uitgevoerde opdrachten (minimaal een jaar terug). Leg de bevindingen en conclusie vast. Zie K hierna		x	x	
	4	Beoordeel het ontvangen handboek aan de hand van vragenlijst B4.3 en leg de bevindingen en conclusie vast – zie L hierna		x	x	
	5	Beoordeel het bestaan aan de hand van een of meer dossiers		x	x	

Naam IT-auditorganisatie:						**2020**
Soort onderzoek: Regulier / Vervolgonderzoek verbeterplan / Heronderzoek (doorhalen wat is n.v.t.)						
Teamleider:		**Onderzoeker:**				
Regel		Activiteit voor toelichting: zie einde paragraaf	Dos-sierstuk	**O**	**A**	Uitgevoerd init. / d.d.
		aan de hand van vragenlijst B.4.4.				
	6	Leg de bevindingen vast en formuleer een conclusie over de opzet en het bestaan van het stelsel		x	x	
5		**Onderzoek dossiers**				
	1	Selecteer aan de hand van het ontvangen 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 KITA zal het onderzoek tenminste 1 en maximaal 2 dossiers betreffen. Bij grootschalige IT-auditorganisaties moet het aantal voldoende zijn om het oordeel te onderbouwen. Dat aantal zal zich veelal kunnen beperken tot, stel, 5 dossiers.			x	
	2	Leg onderbouwing van de geselecteerde opdrachten vast in dossier			x	
	3	Voer dossierbeoordeling uit voor geselecteerde opdrachten aan de hand van vragenlijst B4.4			x	
	4	Formuleer de conclusie met bevindingen over de werking van het stelsel op basis van de dossier beoordeling			x	
6		**Afstemming bevindingen**				
	1	Bespreek de vastgelegde feitelijke bevindingen per hiervoor genoemd onderdeel met de contactpersoon van de IT-auditorganisatie en legt uitkomsten vast in dossier – zie M hierna.		x	x	
7		**Verslaglegging**				
	1	Formuleer de afgestemde bevindingen en definitieve conclusies per deelgebied ten behoeve van het verslag		x	x	
	2	Stel het conceptverslag op binnen 1 week na afronden van het onderzoek		x	x	

	3	Bespreek binnen 1 week na het opstellen het conceptverslag met het lid CKO. Mail daartoe de volgende documenten in Word aan het CKO-lid: • uren- / omzetverantwoording met conclusie t.a.v. scope onderzoek • Bevindingen beoordeling handboek • Bevindingen vragenlijst B4.3 =bijlage18 (opzet kwalitetissysteem) • Bevindingen vragenlijst B4.4 = bijlage 19 (andere dan assurance-opdrachten, als hulpmiddel voor het vaststellen van het bestaan • Bevindingen vragenlijst B4.4 = bijlage 19 (dossierreview alleen bij assurance-opdrachten) • Conceptversie rapport ter bespreking met lid CKO		x	x	
	4	Bepaal met het lid CKO of de uitkomst van het onderzoek aanleiding is de vier jaartermijn in te korten		x	x	
	5	Voer de aanpassingen door naar aanleiding van het overleg met het lid CKO		x	x	
	6	Zend het conceptverslag binnen 1 week na overleg met lid CKO toe aan de contactpersoon van de IT-auditorganisatie		x	x	
	7	Bespreek het conceptverslag met de contactpersoon van de ITauditorganisatie		x	x	

Naam IT-auditorganisatie:						**2014**
Soort onderzoek: Regulier / Vervolgonderzoek verbeterplan / Heronderzoek (doorhalen wat is n.v.t.)						
Teamleider:		**Onderzoeker:**				
Regel		Activiteit voor toelichting: zie einde paragraaf	Dos-sierstuk	**O**	**A**	Uitgevoerd init. / d.d.
	8	Leg de uitkomst van de bespreking vast in het dossier		x	x	
	9	Bepaal of de IT-organisatie binnen 4 weken na het toezenden van het bijgestelde verslag bezwaar maakt tegen de inhoud		x	x	
	10	Verwerk de reacties IT-auditorganisatie – indien relevant – binnen 1 week na ontvangst van het bezwaar		x	x	
	11	Eventueel: stem met het lid CKO af over het bezwaar, het naar aanleiding daarvan bijgestelde conceptverslag en de afwikkeling van het verslag		x	x	
	12	Eventueel: stel de termijn voor het verbeterplan vast bij een oordeel ‘voldoet niet’ (maximaal 12 maanden)		x	x	
	13	Eventueel: bij het onderzoek naar het verbeterplan: stem de bevindingen af met de onderzoekers in eerste aanleg		x	x	
	14	Eventueel: stel vast dat de IT-auditorganisatie de afspraken over het verbeterplan heeft ondertekend		x	x	
	15	Draag na vervallen van 4-wekentermijn over aan het bureau: • het conceptverslag; • de aanwijzingen aan bureau voor afwikkelen van verslag; • het dossier. Zie N hierna		x	x	
8		**Evaluatie en afronding onderzoek**				
	1	Overhandig de contactpersoon van de IT-auditorganisatie het evaluatieformulier		x	x	
	2	Onderteken de urenverantwoording van de onderzoeker en zend de verantwoording aan het bureau:		x	x	

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

Toelichting op het werkprogramma

A. 3.1: dossier te ontvangen van het Bureau.
Dit moet ten minste bevatten:
- Kopie selectiebrief.
- Kopie getekende opdrachtbevestiging.
- 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: inhoudsopgave dossier aanleggen – zie document 10:
- Kop invullen. Voettekst aanpassen.

C. 4.1: documenten opgevraagd in bijlage opdrachtbevestiging – zie document 17 Volledigheid vaststellen.
- Eventueel ontbrekende documenten opvragen, dan wel 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 F hierna ○ Advies – zie G hierna ○ Detachering – zie H hierna ○ Overige professionele diensten – zie G en H hierna.
- Indien de conclusie luidt, dat de opdrachten / werkzaamheden niet passen binnen de hiervoor genoemde categorieën het onderzoek staken: er is sprak van 'in business' of 'niet actief'.
- Dossier via de CKO-begeleider naar het Bureau zenden. De CKO-begeleider gaat na of de 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.
Verder hanteren IT-auditorganisaties het begrip assurance, terwijl dat geen 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 en toetsingsnormen.

Als niet aan deze criteria wordt voldaan is sprake van een adviesopdracht. De benaming in de opdracht doet door deze benadering niet ter zake. De feitelijke inhoud van de opdracht bepaalt derhalve of al dan niet sprake is van assurance.

Let op: een door een IT-auditorganisatie gehanteerd begrip 'advies' kan op basis van deze analyse worden gekenmerkt als zijnde 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 130). Hieruit vloeit voort dat een Register IT-auditor de IT-auditpet (d.w.z. de 'RE-titel') **niet** naar believen op of af kan zetten. Men is te allen tijde RE, dus 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 kwaltetsstelsel waaronder de werkzaamheden plaatsvinden

H. 4.2 Opnemen passage over beroepsregels in opdrachtbevestiging

Grote opdrachtgevers hanteren veelal standaard leveringsvoorwaarden die een ITauditorganisatie 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 ITauditorganisatie 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 kwaliteitstoezicht en alles wat daarmee samenhangt. Door de verwijzing naar het Reglement Gedragscode kan een opdrachtgever derhalve kennis nemen van de eisen die de beroepsorganisatie 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 4401 – 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 en geen oordeel.
Het CKO concludeert dat dergelijke opdrachten worden aangemerkt als advies

J. 4.3 Beoordeel de self assessment:
 Stel ondertekening vast. Ga na of invulling '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 een herstelplan en een heraudit.

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 hiervoor vermelde conclusie worden afgestemd met de IT-auditorganisatie, het rapport worden opgesteld en het onderzoek worden 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 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.

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, zeker in de aanloopperiode, nog consensus over de inhoud van oordelen moet worden gevormd.

Het is logisch dat de onderzochte IT-auditorganisatie na afloop van het onderzoek, en vooruitlopend op het verstrekken van het conceptrapport, wil weten wat de conclusie van de onderzoeker is.
Ik stel voor om dan te verwijzen naar de hiervoor genoemde procedure en alleen met de nodige slagen om de arm een globale indicatie te geven van de eigen mening OP DAT MOMENT. Het kan namelijk ook zo zijn dat je als onderzoeker de bevindingen nog op je wilt laten inwerken en daarom zelfs nog geen globale uitspraak kunt 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.

***