ALGEMENE VOORWAARDEN VOOR DIENSTVERLENING

Artikel 1 Algemeen

1. In deze algemene voorwaarden wordt verstaan onder:
a. Opdrachtgever: de partij die opdracht geeft.
b. Opdrachtnemer: besloten vennootschap BKBO.

2. Deze algemene voorwaarden zijn van toepassing op alle overeenkomsten voor werkzaamheden tussen Opdrachtnemer en Opdrachtgever, respectievelijk hun rechtsopvolgers. Hierna wordt hetgeen moet worden uitgevoerd, aangeduid als "de opdracht".

3. De algemene voorwaarden worden bij de het verstrekken van de offerte toegezonden aan Opdrachtgever en zijn te raadplegen op www.bkbo.nl en liggen ter inzage ten kantore van BKBO B.V. en zijn in december 2024 gedeponeerd bij de Kamer van Koophandel onder inschrijvingsnummer 67738516.

Artikel 2 Toepasselijkheid

1. Deze algemene voorwaarden zijn van toepassing op alle rechtsverhoudingen tussen Opdrachtnemer en Opdrachtgever, behoudens wijzigingen in deze voorwaarden welke door beide partijen uitdrukkelijk en schriftelijk dienen te zijn bevestigd.

2. Voor alle overeenkomsten met Opdrachtnemer wordt de werking van de artikelen 7:404 en 7:407 BW uitgesloten.

3. De gedrags en beroepsregels (zie bijlage) zijn van toepassing op alle medewerkers van de Opdrachtnemer en maken deel uit van de overeenkomst. Het betreft de “Code of Ethics voor IT-auditors” welke is gebaseerd op de Code of Ethics van de International Federation of Accountants (IFAC).

4. De Opdrachtgever verklaart de daaruit voor Opdrachtnemer voortvloeiende verplichtingen steeds volledig te zullen respecteren. De “Code of Ethics voor IT-auditors” is ook als Reglement Gedragscode te raadplegen op www.norea.nl.

Artikel 3 Totstandkoming van de overeenkomst

1. Teneinde de tussen partijen te sluiten overeenkomst een deugdelijke basis te geven, staat Opdrachtgever er voor in, dat hij naar beste weten alle essentiële informatie over de uit te voeren opdracht heeft verstrekt. De Opdrachtnemer zal op die basis de door hem te verrichten opdracht naar beste inzicht en vermogen en overeenkomstig de eisen van goed vakmanschap uitvoeren.

2. De overeenkomst komt tot stand op het moment dat de door Opdrachtnemer en Opdrachtgever ondertekende opdrachtbevestiging door Opdrachtnemer retour is ontvangen. De opdrachtbevestiging is gebaseerd op de ten tijde daarvan door Opdrachtgever aan Opdrachtnemer verstrekte informatie. De opdrachtbevestiging wordt geacht de overeenkomst juist en volledig weer te geven.

3. Het Code of Ethics voor IT-auditors staat partijen vrij te bewijzen dat de overeenkomst op andere wijze tot stand is gekomen.

4. De overeenkomst wordt aangegaan voor bepaalde tijd tenzij uit de inhoud, aard of strekking van de verleende opdracht voortvloeit dat deze voor een onbepaalde tijd is aangegaan.

Artikel 4 Terbeschikkingstelling

1. De Opdrachtgever verstrekt tijdig en in de gewenste vorm alle documentatie en gegevens die de Opdrachtnemer nodig heeft. De Opdrachtgever staat in voor de juistheid, volledigheid en tijdigheid van de door hem verstrekte informatie.

2. Dit geldt ook voor de terbeschikkingstelling van medewerkers van de eigen organisatie van de Opdrachtgever, die bij de werkzaamheden van de Opdrachtnemer betrokken (zullen) zijn.

3. Wanneer de Opdrachtnemer daarom verzoekt, verschaft de Opdrachtgever op de locatie waar de opdracht moet worden uitgevoerd een ter zake adequaat uitgeruste werkplek.

4. Indien en voor zover Opdrachtgever zulks verzoekt, worden de ter beschikking gestelde bescheiden aan deze geretourneerd.

Artikel 5 Het betrekken van derden bij de opdracht

1. Het betrekken of inschakelen van een derde bij de opdrachtuitvoering door Opdrachtgever of door de Opdrachtnemer geschiedt uitsluitend in onderling overleg.
2. Opdrachtnemer zal de rol en betrokkenheid van eventuele derden vermelden in de offerte voor de door Opdrachtgever gevraagde dienstverlening.

Artikel 6 Geheimhouding

1. Opdrachtnemer is, tenzij hij een wettelijke plicht dan wel beroepsplicht tot bekendmaking heeft, verplicht tot geheimhouding tegenover derden.

2. Opdrachtnemer is niet gerechtigd de informatie die aan hem door Opdrachtgever ter beschikking wordt gesteld aan te wenden ten behoeve van een ander doel dan waarvoor zij werd verkregen. Hierop wordt echter een uitzondering gemaakt in het geval Opdrachtnemer voor zichzelf optreedt in een tucht, civiele, of strafprocedure waarbij deze informatie of de desbetreffende stukken van belang kunnen zijn.

3. Opdrachtnemer zal zijn verplichtingen op grond van dit artikel opleggen aan medewerkers en eventueel ingeschakelde derden.

4. De Opdrachtgever zal zonder toestemming van de Opdrachtnemer aan derden geen mededelingen doen over de aanpak van de Opdrachtnemer, zijn werkwijze en dergelijke.

5. Tenzij daartoe door Opdrachtnemer voorafgaande schriftelijke toestemming is verleend, zal Opdrachtgever de inhoud van rapporten, adviezen of andere al of niet schriftelijke uitingen van Opdrachtnemer, die niet zijn opgesteld of gedaan met de strekking derden van de daarin neergelegde informatie te voorzien, niet openbaar maken. De Opdrachtgever zal er tevens voor zorgdragen dat derden niet van de in de vorige zin bedoelde inhoud kennis kunnen nemen.

Artikel 7 Intellectuele eigendommen

1. Het is Opdrachtgever uitdrukkelijk verboden die producten, waaronder mede begrepen computerprogramma's, systeemontwerpen, werkwijzen, adviezen, (model)contracten en andere geestesproducten die eigendom zijn en blijven van Opdrachtnemer, een en ander in de ruimste zin des woords, al dan niet met inschakeling van derden te verveelvoudigen, te openbaren of te exploiteren.
Openbaarmaking kan derhalve alleen geschieden na verkregen toestemming van de Opdrachtnemer.

2. De Opdrachtgever heeft het recht geestesproducten van de Opdrachtnemer te vermenigvuldigen uitsluitend voor gebruik in zijn eigen organisatie voorzover passend binnen het doel van de opdracht. Ingeval van tussentijdse beëindiging van de opdracht, is het voorgaande ook van toepassing.

Artikel 8 Personeel

1. De Opdrachtnemer kan in overleg met de Opdrachtgever de samenstelling van het team wijzigen, indien hij meent dat dit voor de uitvoering van de opdracht noodzakelijk is. Een wijziging van het team kan ook op verzoek van de Opdrachtgever in overleg met de Opdrachtnemer plaatsvinden.

2. Geen van de partijen mag tijdens de uitvoering van de opdracht en binnen één jaar na beëindiging van de opdracht personeel van de wederpartij in dienst nemen of met dit personeel over indiensttreding onderhandelen, zonder overleg met de wederpartij.

Artikel 9 Honorarium

1. Het honorarium van Opdrachtnemer is niet afhankelijk van de uitkomst van de verleende opdracht.

2. Indien na de totstandkoming van de overeenkomst, doch voordat de opdracht geheel is uitgevoerd, lonen en/of prijzen een wijziging ondergaan, is Opdrachtnemer gerechtigd het overeengekomen tarief dienovereenkomstig aan te passen, tenzij Opdrachtgever en Opdrachtnemer hierover andere afspraken hebben gemaakt.

3. Het honorarium van Opdrachtnemer, zo nodig vermeerderd met voorschotten en declaraties van ingeschakelde derden, wordt direct na opdrachtverlening in rekening gebracht door Opdrachtgever, tenzij Opdrachtgever en Opdrachtnemer hierover andere afspraken hebben gemaakt. Over alle door Opdrachtgever aan Opdrachtnemer verschuldigde bedragen wordt -indien van toepassing de omzetbelasting afzonderlijk in rekening gebracht.

4. Met betrekking tot de tarieven en de daarop gebaseerde kostenramingen staat in de offerte van Opdrachtnemer aangegeven, of daarin zijn begrepen de secretariaatskosten, reisuren, reis en verblijfkosten en eventuele andere opdrachtgebonden kosten. Voor zover deze kosten niet zijn inbegrepen, kunnen ze afzonderlijk worden berekend.

5. In het honorarium worden geen rentekosten opgenomen, tenzij in de opdracht anders is aangegeven.

Artikel 10 Betaling

1. Betaling door Opdrachtgever dient, zonder aftrek, korting of schuldverrekening te geschieden binnen 14 kalenderdagen na factuurdatum. Betaling dient te geschieden in euro's door middel van overmaking ten gunste van een door Opdrachtnemer aan te wijzen bankrekening.

2. Indien Opdrachtgever niet binnen de onder 10.1 genoemde termijn heeft betaald, is Opdrachtnemer gerechtigd, nadat hij Opdrachtgever ten minste eenmaal heeft aangemaand te betalen, zonder nadere ingebrekestelling en onverminderd de overige rechten van Opdrachtnemer, vanaf de vervaldag Opdrachtgever de wettelijke rente in rekening te brengen tot op de datum van algehele voldoening.

3. Alle in redelijkheid gemaakte gerechtelijke en buitengerechtelijke (incasso) kosten, die Opdrachtnemer maakt als gevolg van de niet nakoming door Opdrachtgever van diens betalingsverplichtingen, komen ten laste van Opdrachtgever.

4. Indien de financiële positie of het betalingsgedrag van Opdrachtgever naar het oordeel van Opdrachtnemer daartoe aanleiding geeft, is Opdrachtnemer gerechtigd van Opdrachtgever te verlangen, dat deze onverwijld (aanvullende) zekerheid stelt in een door Opdrachtnemer te bepalen vorm. Indien Opdrachtgever nalaat de verlangde zekerheid te stellen is Opdrachtnemer gerechtigd, onverminderd zijn overige rechten, de verdere uitvoering van de overeenkomst onmiddellijk op te schorten en is al hetgeen Opdrachtgever aan Opdrachtnemer uit welke hoofde ook verschuldigd is, direct opeisbaar.

Artikel 11 Reclames

1. Reclames met betrekking tot het uitvoeren van de opdracht en/of het factuurbedrag dienen schriftelijk binnen 60 dagen na de verzenddatum van de stukken of informatie waarover Opdrachtgever reclameert, dan wel binnen 60 dagen na de ontdekking van het gebrek indien Opdrachtgever aantoont dat hij het gebrek redelijkerwijs niet eerder kon ontdekken, aan Opdrachtnemer te worden kenbaar gemaakt.

2. Reclames als in het eerste lid bedoeld, schorten de betalingsverplichting van Opdrachtgever niet op.

3. In geval van een terecht uitgebrachte reclame heeft Opdrachtnemer de keuze tussen aanpassing van het in rekening gebrachte honorarium, het kosteloos verbeteren of opnieuw verrichten van de afgekeurde werkzaamheden of het geheel of gedeeltelijk niet (meer) uitvoeren van de opdracht tegen een restitutie naar evenredigheid van door Opdrachtgever reeds betaald honorarium.

Artikel 12 Wijziging van de opdracht c.q. meerwerk

1. De Opdrachtgever aanvaardt dat de tijdsplanning van de opdracht kan worden beïnvloed, indien partijen tussentijds overeenkomen de aanpak, werkwijze of omvang van de opdracht uit te breiden of te wijzigen.

2. Indien de tussentijdse wijziging het overeengekomen honorarium of de kostenvergoedingen beïnvloedt, zal de Opdrachtnemer dit de Opdrachtgever zo spoedig mogelijk melden.

3. Indien een tussentijdse wijziging in de opdrachtuitvoering ontstaat door toedoen van de Opdrachtgever, zal de Opdrachtnemer de noodzakelijke aanpassingen aanbrengen, indien de kwaliteit van de dienstverlening dit vergt. Indien een dergelijke aanpassing leidt tot meerwerk, zal dit als een aanvullende opdracht aan de Opdrachtgever worden bevestigd.

4. Opdrachtnemer kan slechts meerwerk verrichten en aan Opdrachtgever in rekening brengen als vooraf toestemming is verleend door Opdrachtgever.

Artikel 13 Afsluiting van de opdracht

1. Het moment van afsluiten van de opdracht kan behalve door de inspanning van het team dat met de uitvoering van de opdracht is belast, worden beïnvloed door allerlei factoren, zoals de kwaliteit van de informatie die de Opdrachtnemer verkrijgt en de medewerking die wordt verleend. De Opdrachtnemer kan dan ook niet altijd van tevoren exact aangeven hoe lang de doorlooptijd voor uitvoeren van de opdracht zal zijn.

2. In financiële zin is de opdracht afgesloten, zodra de eindafrekening door de Opdrachtgever is goedgekeurd. Binnen een termijn van 14 dagen na dagtekening van deze eindafrekening dient de Opdrachtgever de Opdrachtnemer hierover

te berichten. Indien de Opdrachtgever niet binnen deze termijn reageert, wordt de eindafrekening geacht te zijn goedgekeurd.

Artikel 14 Aansprakelijkheid

1. Opdrachtnemer zal de opdracht naar beste kunnen uitvoeren en daarbij de zorgvuldigheid in acht nemen die van een gecertificeerd RE en/of CISA auditor mag worden verwacht. Indien een fout wordt gemaakt doordat de Opdrachtgever hem onjuiste of onvolledige informatie heeft verstrekt, is Opdrachtnemer voor de daardoor ontstane schade niet aansprakelijk. Indien de Opdrachtgever aantoont dat hij schade heeft geleden door een fout van Opdrachtnemer die bij zorgvuldig handelen zou zijn vermeden, is Opdrachtnemer voor die schade slechts aansprakelijk tot een maximum van het bedrag van het honorarium voor de desbetreffende opdracht over het laatste kalenderjaar met een maximum van € 250.000,-.

2. Opdrachtgever vrijwaart Opdrachtnemer voor vorderingen van derden wegens schade die veroorzaakt is doordat de Opdrachtgever aan Opdrachtnemer onjuiste of onvolledige informatie heeft verstrekt, tenzij Opdrachtgever aantoont dat de schade geen verband houdt met verwijtbaar handelen of nalaten zijnerzijds dan wel veroorzaakt is door opzet of grove schuld van Opdrachtnemer.

Artikel 15 Vervaltermijn

Voor zover in deze algemene voorwaarden niet anders is bepaald, vervallen vorderingsrechten en andere bevoegdheden van Opdrachtgever uit welken hoofde ook jegens Opdrachtnemer in verband met het uitvoeren van de opdracht door Opdrachtnemer in ieder geval na één jaar na het moment waarop Opdrachtgever bekend werd of redelijkerwijs bekend kon zijn met het bestaan van deze rechten en bevoegdheden.

Artikel 16 Toepasselijk recht en forumkeuze

1. Op alle overeenkomsten tussen Opdrachtgever en Opdrachtnemer waarop deze algemene voorwaarden van toepassing zijn, is Nederlands recht van toepassing.

2. Alle geschillen die verband houden met overeenkomsten tussen Opdrachtgever en Opdrachtnemer, waarop deze voorwaarden van toepassing zijn, worden beslecht door de bevoegde rechter in het arrondissement waarin Opdrachtnemer is gevestigd.

3. In afwijking van het bepaalde in lid 2 zijn Opdrachtgever en Opdrachtnemer bevoegd om geschillen aan een college voor geschillen voor te leggen.

Artikel 17 Deponering Algemene Voorwaarden

Deze algemene voorwaarden zijn in december 2024 gedeponeerd onder inschrijvingsnummer 677 385 16 bij de Kamer van Koophandel.

Bijlage

Tijdens de Algemene Vergadering van de NOREA op 13 juli 2006 is ingestemd met de 'Code of Ethics voor IT-auditors' ter vervanging van het Reglement Gedrags en Beroepsregels Register EDP-Auditors (GBRE). Deze gedragscode is gebaseerd op de Code of Ethics van de IESBA (International Ethics Standards Board for Accountants). NOREA heeft zich als (geassocieerd) lid van de International Federation of Accountants (IFAC) verbonden om haar best te doen de regels van de IESBA om te zetten in nationale regelgeving indien relevant en van toepassing op de werkzaamheden van de le-den van NOREA.

Op 7 januari 2021 is door de Algemene Vergadering een herzieningsvoorstel van de Gedragscode vastgesteld in overeenstemming met de meest recente IESBA Code of Ethics, waarvan onderdeel 4B is toegevoegd aan de voor NOREA relevante delen omdat hierin de onafhankelijkheidsvereisten in verband met assurance-opdrachten zijn opgenomen. Daarnaast is in deze Code een onderdeel opgenomen uit deel 4A van de Code: de definiëring van Netwerkonderdeel (450) zoals genoemd in artikel 900.14, alsmede een onderdeel uit deel 3 van de IESBA -Code: de invulling van omgang met geschenken en gastvrijheid (340) als uitwerking van de vereisten die zijn opgenomen in sectie 906 (Geschenken en Gastvrijheid). Bovendien zijn enkele specifieke artikelen opgenomen over de onafhankelijkheid van interne IT-auditors en IT-auditors werkzaam bij de overheid bij de uitvoering van assuranceopdrachten (911 T5).

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')	
INHOUDSOPGAVE	**Artikel / blz.**

TOELICHTING

Tijdens de Algemene Vergadering van de NOREA op 13 juli 2006 is ingestemd met de 'Code of Ethics voor IT-auditors' ter vervanging van het Reglement Gedrags en Beroepsregels Register EDP Auditors (GBRE). Deze gedragscode is gebaseerd op de Code of Ethics van de IESBA (International Ethics Standards Board for Accountants). NOREA heeft zich als (geassocieerd) lid van de International Federation of Accountants (IFAC) verbonden om haar best te doen de regels van de IESBA om te zetten in nationale regelgeving indien relevant en van toepassing op de werkzaamheden van de le den van NOREA.

Op 7 januari 2021 is door de Algemene Vergadering een herzieningsvoorstel van de Gedragscode vastgesteld in overeenstemming met de meest recente IESBA Code of Ethics, waarvan onderdeel 4B is toegevoegd aan de voor NOREA relevante delen omdat hierin de onafhankelijkheidsvereisten in verband met assurance-opdrachten zijn opgenomen. Daarnaast is in deze Code een onderdeel op genomen uit deel 4A van de Code: de definiëring van Netwerkonderdeel (450) zoals genoemd in artikel 900.14, alsmede een onderdeel uit deel 3 van de IESBA -Code: de invulling van omgang met geschenken en gastvrijheid (340) als uitwerking van de vereisten die zijn opgenomen in sectie 906 (Geschenken en Gastvrijheid). Bovendien zijn enkele specifieke artikelen opgenomen over de onaf hankelijkheid van interne IT-auditors en IT-auditors werkzaam bij de overheid bij de uitvoering van assurance-opdrachten (911 T5).

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')	
Art./Par.	**Omschrijving**
	INLEIDING
	Reikwijdte reglement
1	Dit reglement is van toepassing op iedere in het RE-register ingeschreven IT-auditor.
B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')	

Art./Par.	Omschrijving
	Ingangsdatum
2	Dit reglement geldt met ingang van 1 juli 2021.
	Doelstelling
3	De doelstelling van dit reglement is het stellen van algemeen geldende gedragsregels voor IT-auditors die in het RE-register zijn ingeschreven, die in acht moeten worden ge nomen bij het uitoefenen van het beroep en daarbuiten.
	Definities
4	Zie het definitieoverzicht (woordenlijst, inclusief lijst van afkortingen, blz. 69)
Sectie 100	**NALEVING VAN DE CODE (VEREISTEN)**
100.1	Een onderscheidend kenmerk van het IT-auditberoep is de aanvaarding van de verantwoordelijkheid om te handelen in het algemeen belang.
100.2	Vertrouwen in het IT-auditberoep is een reden waarom bedrijven, overheden en andere organisaties IT-auditors betrekken bij een breed scala van terreinen, waaronder IT adviesopdrachten, IT-assurance-opdrachten en andere professionele diensten. IT-auditors begrijpen en erkennen dat een dergelijk vertrouwen is gebaseerd op de vaar digheden en waarden die IT-auditors bieden bij de professionele diensten die ze uitvoeren, waaronder: (a) Naleving van ethische beginselen en professionele standaarden; (b) Gebruik van zakelijk inzicht; (c) Toepassing van expertise op technische en andere zaken; en (d) Uitoefening van professionele oordeelsvorming. De toepassing van deze vaardigheden en waarden stelt IT-auditors in staat om advies te geven of anderszins in de behoefte te voorzien die voldoet aan het doel waarvoor ze dient en waarop kan worden vertrouwd door de beoogde gebruikers van dergelijke dienstverlening.
100.3	De Code bevat hoge kwaliteitsstandaarden voor ethisch gedrag dat van IT-auditors mag worden verwacht en dient ter adoptie door professionele beroepsorganisaties die lid zijn van de International Federation of Accountants (IFAC). De Code kan ook worden gebruikt of aangenomen door degenen die verantwoordelijk zijn voor het vaststellen van ethische normen voor IT-auditors in bepaalde sectoren of rechtsgebieden en door bedrijven bij het ontwikkelen van hun ethiek en onafhankelijkheidsbeleid.

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	Omschrijving

100.4	De Code stelt vijf fundamentele beginselen vast die door alle IT-auditors moeten worden nageleefd. Het bevat ook een conceptueel kader dat kan worden toegepast om bedreigingen voor de naleving van de fundamentele beginselen te identificeren, evalueren en te behandelen, evenals bedreigingen voor de onafhankelijkheid van assurance-opdrachten. De Code past ook de fundamentele beginselen en het conceptuele kader toe bij een reeks van feiten en omstandigheden die IT-auditors kunnen tegenkomen, zowel in het zakenle ven als in de openbare praktijk.
100.5 T1	De vereisten in de Code, aangeduid met de letter 'V', leggen verplichtingen op.
100.5 T2	Het toepassingsmateriaal, aangeduid met de letter 'T', geeft context, uitleg, suggesties voor acties, zaken ter overweging, illustraties en andere duidingen die relevant zijn voor het juiste begrip van de code. Het toepassingsmateriaal is in het bijzonder bedoeld om de IT-auditor te helpen begrijpen hoe het conceptueel kader bij een bepaalde reeks van omstandigheden dient te worden toegepast. Hoewel dergelijk toepassingsmateriaal op zichzelf geen vereiste oplegt, is overweging van het materiaal noodzakelijk voor de juiste toepassing van de vereisten van de Code, inclusief de toepassing van het conceptuele kader.
V 100.6	Een IT-auditor dient de Code na te leven.
100.6 T1	Handhaving van de fundamentele beginselen en naleving van de specifieke vereisten van de Code stelt IT-auditors in staat hun verantwoordelijkheid te nemen om in het algemeen belang te handelen.
100.6 T2	Het naleven van de Code omvat het geven van gepaste aandacht aan het doel en de uitleg van de specifieke vereisten.
100.6 T3	Naleving van de eisen van de Code betekent niet dat IT-auditors altijd hun verantwoorde lijkheid hebben genomen om in het algemeen belang te handelen. Er kunnen zich onge bruikelijke of uitzonderlijke omstandigheden voordoen, waarbij een IT-auditor van me ning is dat het voldoen aan een vereiste of vereisten van de Code mogelijk niet in het al gemeen belang is of zouden leiden tot een onevenredig resultaat. In die omstandigheden wordt de IT-auditor aangemoedigd om overleg te plegen met een geschikte instantie, zo als een professionele of regelgevende instantie.
100.6 T4	Bij het handelen in het algemeen belang houdt een IT-auditor niet alleen rekening met de voorkeuren of eisen van een individuele cliënt of werkgever, maar ook met de belangen van andere belanghebbenden bij het uitvoeren van professionele diensten.
V 100.7	Indien er omstandigheden zijn waarin wet of regelgeving een IT-auditor verhinderen om bepaalde delen van de Code na te leven, prevaleren die wet en regelgeving, en zal de IT auditor alle overige onderdelen van de Code naleven.

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	**Omschrijving**
100.7 T1	Het beginsel professionaliteit vereist dat een IT-auditor handelt in overeenstemming met relevante wet en regelgeving. Sommige rechtsgebieden hebben mogelijk bepalingen die afwijken van of verder gaan dan deze Code. IT-auditors in deze rechtsgebieden moeten zich bewust zijn van die verschillen en voldoen aan de strengere bepalingen, tenzij deze strijdig zijn met wet of regelgeving.

100.8	**Overtreding van de Code**
V 100.8	De paragrafen V900.50 t/m V900.55 behandelen een overtreding van de onafhankelijk heidsstandaarden. Een IT-auditor die een overtreding van een andere bepaling van de Code vaststelt, zal de ernst en de impact van de overtreding beoordelen op het vermogen van de IT-auditor om aan de fundamentele beginselen te voldoen. De IT-auditor zal ook: a) zo snel als mogelijk de vereiste acties ondernemen om de gevolgen van de over treding van de code aan te pakken; en b) bepalen of de overtreding aan de relevante partijen moet worden gemeld.
100.8 T1	Relevante partijen aan wie een dergelijke overtreding zou kunnen worden gemeld, zijn onder meer degenen die er mogelijk door beïnvloed worden, een professionele of regel gevende instantie of een toezichthoudende autoriteit.
Sectie 110	**DE FUNDAMENTELE BEGINSELEN**
110.1 T1	ALGEMEEN Er zijn vijf fundamentele ethische beginselen voor IT-auditors: (A) Integriteit: oprecht en eerlijk optreden in professionele en zakelijke relaties. (B) Objectiviteit – het beoefenen van professionele of zakelijke oordeelsvorming, zonder in gevaar te komen door: (i) tendentie; (ii) belangenverstrengeling; of (iii) ongepaste beïnvloeding door of ongepast vertrouwen in individuen, organisaties, technologie of andere factoren. (C) Vakbekwaamheid en zorgvuldigheid om: (I) vakkennis en vaardigheid te verwerven en behouden op het niveau dat vereist is om de cliënt of werkgever bekwame en professionele diensten te verlenen, gebaseerd op de huidige vaktechnische en professionele standaarden en relevante wetgeving, en;

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	**Omschrijving**

	(II) zorgvuldig te handelen en in overeenstemming met toepasselijke technieken en pro fessionele standaarden. (D) Vertrouwelijkheid: het respecteren van het vertrouwelijk karakter van de verkregen in formatie als gevolg van de professionele en zakelijke relaties. (E) Professionaliteit om: (i) te voldoen aan relevante wet en regelgeving; (ii) zich te gedragen op een manier die in overeenstemming is met de verantwoordelijk heid van het beroep om te handelen in de algemeen belang bij alle professionele diensten en zakelijke relaties; en (iii) het vermijden van gedrag waarvan de IT-auditor weet of zou moeten weten dat het beroep in diskrediet wordt gebracht.
V 110.2	Een IT-auditor houdt zich aan elk van de fundamentele beginselen.
110.2 T1	De fundamentele ethische beginselen bepalen de gedragsnorm die van een IT-auditor wordt verwacht. Het conceptueel kader bepaalt de aanpak die een IT-auditor moet toe passen om te voldoen aan de fundamentele beginselen. Paragrafen 111 tot en met 115 bevatten vereisten en toepassingsmateriaal met betrekking tot elk van de fundamentele beginselen.
110.2 T2	Een IT-auditor kan te maken krijgen met een situatie waarin het naleven van een funda menteel beginsel in strijd is met een of meer andere fundamentele beginselen. In derge lijke situaties kan de IT-auditor overwegen om, zo nodig op anonieme basis, in overleg te treden met: • Anderen binnen de IT-auditeenheid of de werkgever; • De met Governance belaste personen; • Een professioneel orgaan; • Een regelgevende instantie; of • De juridische vertegenwoordiging. Een dergelijk overleg ontslaat de IT-auditor echter niet van de verantwoordelijkheid om professionele oordeelsvorming toe te passen om het conflict op te lossen of -zo nodig afstand te nemen van de aangelegenheid waardoor het conflict is veroorzaakt, tenzij wet of regelgeving dat verhinderen.

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	**Omschrijving**
110.2 T3	De IT-auditor wordt aanbevolen om de inhoud van de kwestie, de details van eventuele discussies, de genomen beslissingen en de onderbouwing daarvan te documenteren.
Sectie 111	**INTEGRITEIT**

V 111.1	Een IT-auditor dient het integriteitsbeginsel na te leven, dat vereist dat een IT-auditor in alle professionele en zakelijke relaties recht door zee en eerlijk is.
111.1 T1	Integriteit omvat eerlijk, oprecht handelen, op grond van de eigenschap en overtuiging om waarheidsgetrouw en gepast op te treden, zelfs wanneer men onder druk staat om iets anders te doen of wanneer dit mogelijk nadelige persoonlijke of organisatorische ge volgen kan hebben.
111.1 T2	Passend handelen houdt in: a) stand te houden wanneer men geconfronteerd wordt met dilemma's en moeilijke situaties; of b) anderen uitdagen als en wanneer de omstandigheden dit rechtvaardigen, op een wijze die past bij de omstandigheden.
V 111.2	Een IT-auditor wordt niet bewust in verband gebracht met rapportages, bevindingen, mededelingen of andere informatie die: (a) een materieel onjuiste of misleidende verklaring of informatie bevat; (b) verklaringen of informatie bevat die roekeloos is verstrekt; of (c) de vereiste informatie weglaat of verdoezelt wanneer een dergelijke weglating of verdoezeling misleidend zou zijn.
111.2 T1	Indien een IT-auditor ter zake van een dergelijke melding, mededeling of andere infor matie een aangepaste rapportage verstrekt, handelt de IT-auditor niet in strijd met artikel V111.2.
V 111.3	Wanneer een IT-auditor ontdekt dat hij in verband is gebracht met informatie zoals be schreven in artikel V111.2, zal de IT-auditor stappen ondernemen om afstand te nemen van die informatie.
Sectie 112	**OBJECTIVITEIT**
V 112.1	Een IT-auditor dient zich te houden aan het objectiviteitsbeginsel, wat vereist dat een iT auditor het zakelijk of professioneel oordeel niet in gevaar brengt door: (a) Vooringenomenheid (tendentie); (b) Belangenverstrengeling; of (c) Ongepaste invloed van of ongepast vertrouwen op individuen, organisaties,

Art./Par.	**Omschrijving**
	technologie of andere factoren.
V 112.2	Een IT-auditor verricht geen beroepsactiviteiten als een omstandigheid of relatie het pro fessioneel oordeel van de IT-auditor over die activiteit ongepast beïnvloedt.
Sectie 113	**VAKBEKWAAMHEID EN ZORGVULDIGHEID**

V 113.1	Een IT-auditor dient het beginsel van vakbekwaamheid en zorgvuldigheid in acht te ne men, hetgeen van een IT-auditor vereist om: (I) vakkennis en vaardigheid te verwerven en behouden op het niveau dat vereist is om de cliënt of werkgever bekwame en professionele diensten te verlenen, gebaseerd op de huidige vaktechnische en professionele normen en relevante wetgeving, en; (II) zorgvuldig te handelen en in overeenstemming met toepasselijke vaktechnische en professionele standaarden.
113.1 T1	Het bedienen van cliënten en werkgevers met professionele vakbekwaamheid vereist de toepassing van een gezond beoordelingsvermogen bij het toepassen van professionele vakkennis en vaardigheden bij het uitvoeren van professionele diensten.
113.1 T2	Het op peil houden van vakbekwaamheid vereist een voortdurend bewustzijn van en in zicht in relevante technische, professionele, zakelijke en technologie gerelateerde ont wikkelingen. Permanente Educatie stelt een IT-auditor in staat het vermogen te ontwikke len en behouden om vakbekwaam op te treden binnen de professionele omgeving.
113.1 T3	Zorgvuldigheid omvat de verantwoordelijkheid om zorgvuldig, grondig en tijdig te han delen in overeenstemming met de vereisten van een opdracht.
V 113.2	Bij het naleven van het beginsel van vakbekwaamheid en zorgvuldigheid neemt een IT auditor redelijke maatregelen om ervoor te zorgen dat degenen die beroepshalve onder het gezag van de IT-auditor werken, een passende training hebben en toezicht krijgen.
V 113.3	Indien van toepassing zal een IT-auditor de cliënten, werkgevers, of andere gebruikers van de professionele diensten of activiteiten van de IT-auditor bewust maken van de be perkingen die inherent zijn aan de diensten of activiteiten.
Sectie 114	**VERTROUWELIJKHEID**
V 114.1	Een IT-auditor dient het beginsel van vertrouwelijkheid in acht te nemen. Dat vereist dat een IT-auditor de vertrouwelijkheid respecteert van informatie die is verkregen als gevolg van professionele en zakelijke relaties. Een IT-auditor moet: (a) Alert zijn op de mogelijkheid van onbedoelde openbaarmaking, ook in een sociale omgeving en in het bijzonder aan een zakenrelatie, gezinslid of familielid; c) De vertrouwelijkheid behouden van informatie, verkregen binnen de IT- auditeenheid of werkgever; (c) De vertrouwelijkheid behouden van informatie die wordt verstrekt door een po tentiële cliënt of werkgever; (d) Géén vertrouwelijke informatie openbaar te maken die is verkregen als resultaat van professionele en zakelijke relaties buiten de IT-auditeenheid of werkgever, zonder instemming van het bevoegd gezag van de betreffende organisatie, tenzij er een wettelijke of professionele plicht of het recht bestaat om de informatie openbaar te maken; (e) Geen vertrouwelijke informatie te gebruiken die is verkregen als gevolg van professionele en zakelijke relaties voor het persoonlijke voordeel van de IT-auditor of het voordeel van een derde partij;

	(f) Geen vertrouwelijke informatie te gebruiken of openbaar te maken, ongeacht of deze is verkregen of ontvangen als resultaat van een professionele of zakelijke relatie, nadat die relatie is beëindigd; en (b) Redelijke maatregelen te nemen om ervoor te zorgen dat het personeel onder toezicht van de IT-auditor en de personen van wie advies en hulp wordt verkregen, de vertrouwelijkheidsplicht van de IT-auditor respecteren.
B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')	
Art./Par.	**Omschrijving**
	(g)
114.1 T1	Vertrouwelijkheid dient het algemeen belang omdat het de vrije informatieverstrekking van de cliënt of werkgever aan de IT-auditor bevordert in de wetenschap dat de informa tie niet aan derden wordt verstrekt. Desalniettemin zijn de volgende omstandigheden te onderscheiden waarin IT-auditors verplicht zijn of zouden kunnen zijn om vertrouwelijke informatie te verstrekken of waarin een dergelijke openbaarmaking passend zou kunnen zijn: (a) Openbaarmaking is wettelijk verplicht, bijvoorbeeld: • Overleggen van documenten of andere bewijsvoering in de loop van een ge rechtelijke procedure; of • Openbaarmaking aan de betreffende overheidsinstanties van overtredingen van de wet die aan het licht komen; (b) Openbaarmaking is wettelijk toegestaan en is geautoriseerd door de cliënt of werkgever; en (c) Er is een professionele plicht of het recht om openbaar te maken, tenzij dit bij wet verboden is: • Om te voldoen aan de kwaliteitsbeoordeling van een beroepsorganisatie (NO REA): Om te reageren op een vraag of onderzoek door een professional of regelge vende instantie;

	• Om de professionele belangen van een IT-auditor in een gerechtelijke proce dure te beschermen, of • Om te voldoen aan technische en professionele standaarden, inclusief ethische vereisten.
B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')	
Art./Par.	**Omschrijving**

114.1 T2	Bij de beslissing om vertrouwelijke informatie al dan niet openbaar te maken zijn de vol gende factoren, afhankelijk van de omstandigheden, te overwegen:
	• Of de belangen van eventuele partijen, ook van derden, kunnen worden geschaad als de cliënt of werkgever instemt met de openbaarmaking van de informatie door de IT-auditor;
	• Of alle relevante informatie bekend en onderbouwd is, voor zover praktisch uit voerbaar. Factoren die van invloed zijn op de beslissing om openbaar te maken zijn:
	  • Niet-onderbouwde feiten.
	  • Onvolledige informatie.
	  • Niet-onderbouwde conclusies.
	• Het voorgestelde soort communicatie en aan wie deze is gericht.
	• Of de partijen aan wie de communicatie is gericht, geschikte ontvangers zijn.

V 114.2	Een IT-auditor blijft het beginsel van vertrouwelijkheid in acht nemen, ook na het beëin digen van de relatie tussen de IT-auditor en een cliënt of werkgever. Bij het veranderen van het dienstverband of het verwerven van een nieuwe cliënt heeft de IT-auditor het recht om eerdere ervaringen te gebruiken, maar hij zal geen vertrouwelijke informatie die is verkregen of ontvangen als gevolg van een professionele of zakelijke relatie gebruiken of openbaar maken.

Sectie 115	**PROFESSIONALITEIT**
V115.1	Een IT-auditor houdt zich aan het principe van professionaliteit, dat vereist dat een IT auditor: (a) De relevante wet en regelgeving naleeft; (b) Zich gedraagt op een manier die in overeenstemming is met de verantwoordelijkheid van het beroep om bij alle professionele diensten en zakelijke relaties in het algemeen belang te handelen; en (c) Elk gedrag vermijdt waarvan de IT-auditor weet of zou moeten weten dat het beroep in diskrediet gebracht zou kunnen worden.
B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')	
Art./Par.	**Omschrijving**
	Een IT-auditor mag niet willens en wetens een bedrijf, beroep of activiteit uitoefenen dat de integriteit, objectiviteit of goede reputatie van het beroep aantast of zou kunnen aan tasten, en als gevolg daarvan onverenigbaar zou zijn met de fundamentele beginselen.
115.1 T1	Gedrag dat het beroep in diskrediet kan brengen, is gedrag waarvan een objectieve, re delijke en geïnformeerde derde partij waarschijnlijk zou concluderen dat het de goede reputatie van het beroep nadelig beïnvloedt.
V 115.2	Bij het ondernemen van marketing of promotieactiviteiten mag een IT-auditor het be roep niet in diskrediet brengen. Een IT-auditor is eerlijk en waarheidsgetrouw en ont houdt zich van: (a) Het wekken van overdreven verwachtingen voor de diensten die worden aangebo den door, of de kwalificaties of ervaring van de IT-auditor; of (b) Het maken van afkeurende verwijzingen naar of niet onderbouwde vergelijkingen met het werk van een derde.
115.2 T1	Indien een IT-auditor twijfelt of een vorm van reclame of marketing passend is, wordt de IT-auditor aangemoedigd om overleg te plegen met NOREA.
Sectie 120	**HET CONCEPTUEEL KADER**
120.1	**Inleiding** De omstandigheden waarin IT-auditors opereren kunnen een bedreiging vormen voor de naleving van de fundamentele beginselen. Sectie 120 bevat vereisten en toepassingsma teriaal, inclusief een conceptueel kader, om IT-auditors te helpen bij het naleven van de fundamentele beginselen en het nakomen van hun verantwoordelijkheid om in het alge meen belang te handelen. Dergelijke vereisten en toepassingsmateriaal zijn afgestemd op het brede scala aan feiten en omstandigheden, inclusief de verschillende professionele diensten, belangen en relaties, die een bedreiging vormen voor de naleving van de fundamentele beginselen. Bovendien ontmoedigen ze de IT-auditors om te concluderen dat een situatie is toegestaan omdat die situatie niet specifiek is verboden door de Code.

120.2	Het conceptueel kader specificeert een aanpak voor een IT-auditor om: a) Bedreigingen voor de naleving van de fundamentele beginselen te identificeren; b) De geïdentificeerde bedreigingen te evalueren; en c) De bedreigingen te behandelen door ze te elimineren of terug te brengen tot een aanvaardbaar niveau.
	VEREISTEN EN TOEPASSINGSMATERIAAL
V 120.3	De IT-auditor past het conceptueel kader toe om bedreigingen voor de naleving van de

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	**Omschrijving**
	fundamentele beginselen, uiteengezet in sectie 110, te identificeren, evalueren en te be handelen
120.3 T1	Aanvullende eisen en toepassingsmateriaal die relevant zijn voor de toepassing van het conceptueel kader zijn uiteengezet in: • deel 4B Onafhankelijkheid voor assurance-opdrachten (delen 2, 3 en 4A gelden niet voor de NOREA, met uitzondering van 340 en 400).
V 120.4	Bij de behandeling van een ethische kwestie houdt de IT-auditor rekening met de context waarin de kwestie is ontstaan of kan ontstaan. Indien een natuurlijke persoon die IT auditor is in het openbare beroep, beroepsactiviteiten uitoefent uit hoofde van de relatie van de IT-auditor met de IT-auditeenheid, hetzij als aannemer, werknemer of eigenaar, dient hij te voldoen aan de bepalingen in deze Code.
V 120.5	Bij de toepassing van het conceptueel kader dient de IT-auditor: (a) Een onderzoekende geest te hebben; (b) Professionele oordeelsvorming toe te passen; en (c) De objectieve, redelijke en geïnformeerde derde partij toets te gebruiken, zoals beschreven in artikel 120.5 T6.
120.5 T1	*Een onderzoekende geest hebben* Een onderzoekende geest is een eerste vereiste om inzicht te krijgen in bekende feiten en omstandigheden die nodig zijn voor de juiste toepassing van het conceptuele kader. Een onderzoekende geest hebben houdt in: (a) Het overwegen van de bron, relevantie en toereikendheid van de verkregen informatie, daarbij rekening houdend met de aard, reikwijdte en output van de professionele activiteit die wordt ondernomen; en (b) Openstaan en alert zijn op de noodzaak van verder onderzoek of andere actie.

120.5 T2	Bij het beschouwen van de bron, relevantie en toereikendheid van de verkregen informatie kan de IT-auditor onder meer overwegen of: • Nieuwe informatie naar voren is gekomen of dat er veranderingen zijn geweest in feiten en omstandigheden; • De informatie of de bron ervan kan worden beïnvloed door tendentie(s) of eigenbelang; • Er reden tot bezorgdheid is dat mogelijk relevante informatie ontbreekt in de feiten en omstandigheden die bij de IT-auditor bekend zijn; • Er een inconsistentie is tussen de bekende feiten en omstandigheden en de verwachtingen van de IT-auditor;

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	Omschrijving
	• De informatie een redelijke basis biedt om tot een conclusie te komen; • Andere redelijke conclusies kunnen worden getrokken uit de verkregen in formatie.
120.5 T3	Artikel V 120.5 vereist dat alle IT-auditors een onderzoekende geest hebben bij het identificeren, evalueren en behandelen van bedreigingen voor de fundamentele beginselen. Deze voorwaarde voor het toepassen van het conceptuele kader geldt voor alle IT auditors, ongeacht de uitgeoefende beroepsactiviteit. Op grond van de RKBN moeten IT auditors ook een professioneel kritische instelling hebben, waaronder een kritische beoordeling van bewijsmateriaal.
120.5 T4	Professionele oordeelsvorming omvat de toepassing van relevante training, professionele kennis, vaardigheid en ervaring die in overeenstemming zijn met de feiten en omstandigheden, inclusief de aard en de reikwijdte van specifieke professionele diensten en de betrokken belangen en relaties.
120.5 T5	Professionele oordeelsvorming is vereist wanneer de IT-auditor het conceptuele kader toepast om onderbouwde beslissingen te nemen over de beschikbare handelwijzen en om te bepalen of dergelijke beslissingen in de gegeven omstandigheden passend zijn. Bij het maken van deze afweging kan de IT-auditor overwegen of: • De vakbekwaamheid en ervaring van de IT-auditor voldoende zijn om tot een conclusie te komen; • Er behoefte is aan overleg of consultatie met anderen met relevante expertise of ervaring; • De eigen vooroordelen of tendentie(s) van de IT-auditor van invloed kunnen zijn op de professionele oordeelsvorming van de IT-auditor.

120.5 T6	*Objectieve, Redelijke en Geïnformeerde Derde Partij Toets* De objectieve, redelijke en geïnformeerde derde partij toets is een afweging door de IT auditor of dezelfde conclusies waarschijnlijk ook door een andere partij zouden worden bereikt. Een dergelijke afweging wordt gemaakt vanuit het perspectief van een objectieve, redelijke en geïnformeerde derde partij, die alle relevante feiten en omstandigheden weegt die de IT-auditor kent of redelijkerwijs zou kunnen weten op het moment dat de conclusies worden getrokken. De objectieve en redelijk geïnformeerde derde partij hoeft geen IT-auditor te zijn, maar zou over de relevante kennis en ervaring beschikken om de toepasselijkheid van de conclusie van de IT-auditor op een onpartijdige manier te begrijpen en evalueren.
V 120.6	**Bedreigingen identificeren** De IT-auditor signaleert bedreigingen voor de naleving van de fundamentele beginselen.

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	**Omschrijving**
120.6 T1	Inzicht in de feiten en omstandigheden, inclusief eventuele professionele diensten, be langen en relaties die de naleving van de fundamentele beginselen in gevaar kunnen brengen, is een voorwaarde voor het onderkennen van bedreigingen voor een dergelijke naleving door de IT-auditor. Het bestaan van bepaalde voorwaarden, beleidslijnen en procedures die zijn vastgesteld door het beroep, de wet, regelgeving, de IT-auditeenheid of de werkgever, die het ethisch handelen van de IT-auditor kunnen versterken, kan ook helpen voor het identificeren van bedreigingen en voor de naleving van de fundamentele beginselen. Artikel 120.8 A2 bevat algemene voorbeelden van dergelijke omstandigheden, beleidslijnen en procedures die ook factoren zijn die relevant zijn bij het evalueren van het niveau van bedreigingen.
120.6 T2	Bedreigingen voor de naleving van de fundamentele beginselen kunnen worden veroor zaakt door een breed scala aan feiten en omstandigheden. Het is niet mogelijk om elke situatie te definiëren die bedreigingen veroorzaakt. Bovendien kan de aard van opdrachten en taken verschillen en kunnen er bijgevolg verschillende soorten bedreigingen ont staan.
120.6 T3	Bedreigingen voor het naleven van de fundamentele beginselen vallen in één of meer van de volgende categorieën: a) Eigenbelang -de dreiging dat een financieel of ander belang het oordeel of het gedrag van een IT-auditor op ongepaste wijze zal beïnvloeden; b) Zelftoetsing -de dreiging dat een IT-auditor de resultaten van een eerder oordeel niet naar behoren zal evalueren; of een activiteit uitgevoerd door de IT-auditor, of andere persoon binnen de IT-auditeenheid of de werkgever, waarop de IT-auditor zal vertrouwen bij het vormen van een oordeel als onderdeel van het uitoefenen van een lopende activiteit; c) Belangenbehartiging -de dreiging dat een IT-auditor de positie van een cliënt of werkgever zodanig behartigt dat de objectiviteit van de IT-auditor in het gedrang komt; d) Vertrouwdheid – de dreiging dat een IT-auditor als gevolg van een langdurige of nauwe relatie met een cliënt of werkgever te sympathiek staat tegenover zijn belangen of zijn werk te veel accepteert; en e) Intimidatie – de dreiging dat een IT-auditor zal worden verhinderd om objectief te handelen vanwege feitelijke of vermeende druk, waaronder pogingen om ongepaste invloed uit te oefenen op de IT-auditor.

120.6 T4	Een omstandigheid kan meer dan één bedreiging creëren, en een bedreiging kan de nale ving van meer dan één fundamenteel beginsel aantasten.

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')	
Art./Par.	**Omschrijving**
V 120.7	**Bedreigingen evalueren** Wanneer de IT-auditor een bedreiging constateert voor de naleving van de fundamentele grondbeginselen, beoordeelt de IT-auditor of een dergelijke bedreiging van een aanvaardbaar niveau is.
120.7 T1	*Acceptabel niveau* Een acceptabel niveau is een niveau waarop een IT-auditor die de objectieve, redelijke en geïnformeerde derde-partijtoets gebruikt, waarschijnlijk zou concluderen dat de IT-auditor de fundamentele beginselen naleeft.
120.8 T1	*Factoren die relevant zijn bij het evalueren van het niveau van bedreigingen* De afweging door de IT-auditor van zowel kwalitatieve als kwantitatieve factoren is relevant bij de beoordeling van bedreigingen, evenals het gecombineerde effect van meerdere bedreigingen, indien van toepassing.
120.8 T2	Het bestaan van voorwaarden, beleidslijnen en procedures beschreven in artikel 120.6 1 kunnen ook factoren zijn die relevant zijn bij de evaluatie en het niveau van bedreiging voor de naleving van de fundamentele beginselen. Voorbeelden van dergelijke voorwaarden, beleidslijnen en procedures zijn onder meer: • Corporate governance vereisten. • Kennis, opleidings en ervaringseisen voor het beroep. • Effectieve klachtensystemen waarmee de IT-auditor en het maatschappelijk verkeer aandacht kunnen vragen voor onethisch gedrag. • Een expliciet verklaarde plicht om overtredingen op ethische vereisten te melden. • Professionele of regelgevende bewaking en disciplinaire procedures.
V120.9	*In overweging nemen van nieuwe informatie of wijzigingen in feiten en omstandigheden* Indien de IT-auditor kennis krijgt van nieuwe informatie of wijzigingen in feiten en omstandigheden die van invloed kunnen zijn op de vraag of een bedreiging is geëlimineerd of tot een aanvaardbaar niveau is teruggebracht, zal de IT-auditor die dreiging opnieuw evalueren en behandelen.

120.9 T1	Alert blijven gedurende de beroepsactiviteit helpt de IT-auditor bij het bepalen of er nieuwe informatie naar voren is gekomen dan wel wijzigingen in feiten en omstandighe den hebben plaatsgevonden die: (a) Invloed hebben op het niveau van een bedreiging; of (b) De conclusie van de IT-auditor beïnvloeden over de vraag of waarborgen toege past blijven die geschikt zijn om geïdentificeerde bedreigingen te behandelen.

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	Omschrijving
120.9 T2	Indien nieuwe informatie leidt tot de identificatie van een nieuwe bedreiging, is de IT auditor verplicht deze bedreiging te evalueren en eventueel te behandelen (zie artikelen V120.7 en V120.10).
V120.10	**Bedreigingen behandelen** Indien de IT-auditor vaststelt dat de geïdentificeerde bedreigingen voor de naleving van de fundamentele beginselen niet van een acceptabel niveau zijn, zal de IT-auditor de be dreigingen behandelen door deze weg te nemen of terug te brengen tot een acceptabel niveau. De IT-auditor doet dit door: a) Het elimineren van de omstandigheden, inclusief belangen of relaties, die de be dreiging vormen; b) Waarborgen toepassen, indien beschikbaar en mogelijk toegepast, om de bedrei gingen tot een acceptabel niveau terug te brengen; of c) Het weigeren of beëindigen van de specifieke beroepsactiviteit.
120.10 T1	*Acties om bedreigingen te elimineren* Afhankelijk van de feiten en omstandigheden kan een bedreiging worden aangepakt door de omstandigheid die de dreiging veroorzaakt weg te nemen. Er zijn echter situaties waarin bedreigingen alleen kunnen worden aangepakt door de specifieke professionele activiteit te weigeren of beëindigen. De reden hiervoor is dat de omstandigheden die de bedreiging hebben gecreëerd niet kunnen worden weggenomen en er geen maatregelen kunnen worden genomen om de bedreiging tot een acceptabel niveau terug te brengen.
120.10 T2	*Waarborgen* Waarborgen zijn acties, afzonderlijk of in combinatie, die de IT-auditor neemt om be dreigingen voor de naleving van de fundamentele beginselen effectief terug te brengen tot een acceptabel niveau.

V 120.11	*Overweging van significante oordelen en bereikte algemene conclusies* De IT-auditor dient zich een algemene conclusie te vormen over de vraag of de acties die de IT-auditor onderneemt of voornemens is te ondernemen om de gecreëerde bedreigin gen te behandelen, deze bedreigingen zullen elimineren of tot een acceptabel niveau zul len terugbrengen. Bij het vormen van de algehele conclusie dient de IT-auditor: (a) Alle significante oordeelsvormingen of getrokken conclusies te beoordelen; en (b) De objectieve, redelijke en geïnformeerde derde partij toets te gebruiken.
120.12 T1	**Andere overwegingen bij de toepassing van het conceptuele kader** *Vooringenomenheid (tendentie)* Bewuste of onbewuste tendentie beïnvloedt de uitoefening van de professionele oor-

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	Omschrijving
	deelsvorming bij het identificeren, beoordelen en behandelen van bedreigingen voor de naleving van de fundamentele beginselen.
120.12 T2	Voorbeelden van mogelijke tendentie(s) waarvan men zich bewust moet zijn bij de uitoe fening van professionele oordeelsvorming zijn: – Verankerde tendentie, dat wil zeggen de neiging om een initiële informatie te gebruiken als een anker waaraan latere informatie onvoldoende wordt getoetst. – Automatiseringstendentie, dat wil zeggen de neiging om de voorkeur te geven aan output die door geautomatiseerde systemen wordt gegenereerd, zelfs wanneer menselijke redeneringen of tegenstrijdige informatie vragen doen rijzen over de betrouw baarheid of geschiktheid van die output. – Beschikbaarheidstendentie, dat wil zeggen de neiging om gebeurtenissen of ervaringen die onmiddellijk in je opkomen of gemakkelijk beschikbaar zijn, zwaarder te laten wegen dan gebeurtenissen of ervaringen die dat niet zijn. – Bevestigingstendentie, dat wil zeggen de neiging om meer belang te hechten aan in formatie die een bestaande overtuiging bevestigt dan aan informatie die die overtuiging tegenspreekt of in twijfel trekt. – Groepsdenken, dat wil zeggen de neiging van een groep individuen om individuele creativiteit en verantwoordelijkheid te ontmoedigen en als gevolg daarvan tot een besluit te komen zonder kritisch te redeneren of alternatieven in overweging te nemen. – Overschatte tendentie, dat wil zeggen de neiging tot overschatting van het eigen vermogen om risico's of andere oordelen of beslissingen juist in te schatten. – Representatietendentie, dat wil zeggen de neiging om een begrip te baseren op een patroon van ervaringen, gebeurtenissen of overtuigingen die als representatief wordt aangenomen. – Selectieve perceptie, dat wil zeggen de neiging van een persoon om zijn verwachtingen te laten meewegen bij de manier waarop hij tegen een bepaalde kwestie of persoon aankijkt.

120.12 T3	Acties die het effect van tendenties kunnen verzachten, zijn onder meer: • Advies inwinnen bij deskundigen om extra input te verkrijgen; • Overleg plegen met anderen om ervoor te zorgen dat het evaluatieproces op de juiste manier wordt uitgedaagd; • Het ontvangen van training met betrekking tot het herkennen van vooroordelen als onderdeel van de professionele ontwikkeling.
120.13 T1	*Organisatiecultuur* De effectieve toepassing van het conceptueel kader door een IT-auditor wordt bevorderd

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	Omschrijving
	wanneer het belang van ethische waarden die aansluiten bij de fundamentele beginselen en andere bepalingen die in de code zijn opgenomen, worden bevorderd via de interne cultuur van de organisatie van de IT-auditor.
120.13 T2	De bevordering van een ethische cultuur binnen een organisatie is het meest effectief wanneer: a) Leiders en leidinggevenden het belang van de ethische waarden van de organisatie onder de aandacht brengen en zichzelf en anderen verantwoordelijk houden voor het uitdragen van deze waarden; b) Er passende opleidings en trainingsprogramma's, managementprocessen en prestatiebeoordelings en beloningscriteria voorhanden zijn die een ethische cultuur bevorderen; c) Er doeltreffende beleidslijnen en procedures bestaan om personen die feitelijk of vermoedelijk illegaal of onethisch gedrag melden, met inbegrip van klokkenlui ders, aan te moedigen en te beschermen; en d) De organisatie zich houdt aan ethische waarden in haar omgang met derden.
120.13 T3	Van professionele IT-auditors wordt verwacht dat zij een op ethiek gebaseerde cultuur in hun organisatie aanmoedigen en bevorderen, rekening houdend met hun positie en ancienniteit.
120.14 A1	**Overwegingen met betrekking tot assurance-opdrachten** *Bedrijfscultuur* RKBN bevat voorschriften en toepassingsbepalingen met betrekking tot de bedrijfscultuur in het kader van de verantwoordelijkheden van een kantoor voor het opzetten, invoeren en toepassen van een kwaliteitsbeheersingssysteem voor assurance-opdrachten of opdrachten voor aanverwante diensten.

120.15 T1	*Onafhankelijkheid* IT-auditors, werkzaam in de openbare praktijk, zijn verplicht onafhankelijk te zijn bij het uitvoeren van assurance-opdrachten. Onafhankelijkheid bestaat uit: a. Onafhankelijkheid in wezen De geesteshouding die het tot uitdrukking bren gen van een conclusie toestaat zonder beïnvloed te worden door invloeden die professionele oordeelsvorming in gevaar brengen, waardoor een individu met integriteit kan handelen, alsmede objectiviteit en een professioneel-kritische instelling kan uitoefenen; b. Onafhankelijkheid in schijn. Het vermijden van feiten en omstandigheden die dermate significant zijn dat een objectieve, redelijke en geïnformeerde derde partij waarschijnlijk zou concluderen, alle feiten en omstandigheden afwegend, inclusief toegepaste maatregelen, dat de integriteit, objectiviteit of professioneel-kritische instelling van een IT-auditeenheid of van een lid van het assurance-team in gevaar is gebracht.
B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')	
Art./Par.	**Omschrijving**
120.15 T2	Deze Code bevat vereisten en toepassingsmateriaal over hoe het conceptuele kader moet worden toegepast om onafhankelijkheid te behouden bij het uitvoeren van assurance opdrachten. IT-auditors en IT-auditeenheden zijn verplicht om aan deze standaarden te voldoen om onafhankelijk te zijn bij het uitvoeren van dergelijke opdrachten. Het conceptuele kader voor het identificeren, evalueren en behandelen van bedreigingen voor de naleving van de fundamentele beginselen is op dezelfde manier van toepassing op de na leving van de onafhankelijkheidsvereisten. De categorieën bedreigingen voor de naleving van de fundamentele beginselen beschreven in artikel 120.6 T3 zijn ook de categorieën bedreigingen voor de naleving van de onafhankelijkheidsvereisten.
120.16 T1	*Professioneel-kritische instelling* Op grond van het RKBN en de assurance-standaarden, zijn IT-auditors werkzaam in het openbare beroep verplicht om een professioneel-kritische instelling te hanteren bij het plannen en uitvoeren van opdrachten. De professioneel-kritische instelling en de fundamentele beginselen die worden beschreven in sectie 110 zijn onderling gerelateerde concepten.

120.16 T2	Bij een assurance-opdracht ondersteunt de naleving van de grondbeginselen, afzonder lijk en collectief, de uitoefening van professioneel-kritische instelling, zoals blijkt uit de volgende voorbeelden: • Integriteit vereist dat de IT-auditor recht door zee en eerlijk is. Zo voldoet de IT auditor bijvoorbeeld aan het principe van integriteit door: a) Recht-door-zee en eerlijk te zijn wanneer hij zijn bezorgdheid uit over een door een cliënt ingenomen standpunt. b) Onderzoek te doen naar inconsistente informatie en verder assurance informatie te zoeken om zorgen weg te nemen over verklarin gen/vermeldingen die materieel onjuist of misleidend zouden kunnen zijn, om weloverwogen beslissingen te nemen over de juiste handelwijze in de omstan digheden. c) De wilskracht te hebben om juist te handelen, zelfs wanneer men onder druk staat om anders te handelen of wanneer dit mogelijk nadelige persoonlijke of organisatorische gevolgen kan hebben. Juist handelen houdt in: • Op eigen benen staan wanneer men geconfronteerd wordt met di lemma's en moeilijke situaties; of
B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')	
Art./Par.	**Omschrijving**

	• Anderen uitdagen als en wanneer de omstandigheden dat recht vaardigen, op een manier die bij de omstandigheden past. Daarbij geeft de IT-auditor blijk van een kritische beoordeling van assurance-informatie die bijdraagt tot de uitoefening van een professioneel-kritische instelling. • Objectiviteit vereist dat de professionele IT-auditor een professioneel of zakelijk oor deel uitoefent zonder in het gedrang te komen door: a) Vooringenomenheid (tendentie); b) Belangenconflict; of c) Ongepaste beïnvloeding van, of ongepast vertrouwen in, personen, organisaties, technologie of andere factoren. Bijvoorbeeld, de IT-auditor voldoet aan het principe van objectiviteit door: a) Het onderkennen van omstandigheden of relaties, zoals vertrouwdheid met de cliënt, die het professionele of zakelijke oordeel van de IT-auditor in gevaar kunnen brengen; en b) Rekening te houden met de invloed van dergelijke omstandigheden en relaties op het oordeel van de IT-auditor bij het beoordelen van de toereikendheid en geschiktheid van controle-informatie met betrekking tot een aangelegenheid die van materieel belang is voor de financiële overzichten van de cliënt. Door dit te doen, gedraagt de IT-auditor zich op een wijze die bijdraagt tot de uitoefening van een professioneel-kritische instelling. • Vakbekwaamheid en zorgvuldigheid vereisen dat de IT-auditor beschikt over vakkennis en vakbekwaamheid op het niveau dat vereist is om een deskundige professionele dienstverlening te waarborgen, en dat de IT-auditor zorgvuldig handelt in overeenstemming met de toepasselijke standaarden, wet en regelgeving. De IT-auditor vol doet bijvoorbeeld aan het beginsel van vakbekwaamheid en zorgvuldigheid door: a) Kennis toe te passen die relevant is voor de bedrijfstak en bedrijfsactiviteiten van een bepaalde cliënt om risico's op afwijkingen van materieel belang naar behoren te onderkennen; b) Passende controleprocedures op te zetten en uit te voeren; en c) Het toepassen van relevante kennis bij het kritisch beoordelen of assurance informatie toereikend is en passend in de omstandigheden. Daarbij gedraagt de IT-auditor zich op een wijze die bijdraagt aan de uitoefening van een professioneel-kritische instelling.
SECTIE 340	**AANMOEDIGINGEN, INCLUSIEF GESCHENKEN EN GASTVRIJHEID**
340.1	**Introductie**

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	**Omschrijving**
	IT-auditors zijn verplicht de fundamentele beginselen in acht te nemen en het in hoofd stuk 120 beschreven conceptueel kader toe te passen om bedreigingen te onderkennen, te evalueren en aan te pakken.

340.2	Het aanbieden of aanvaarden van aanmoedigingen zou een bedreiging kunnen vormen voor eigenbelang, vertrouwdheid of intimidatie met betrekking tot de naleving van de fundamentele beginselen, met name de beginselen van integriteit, objectiviteit en profes sioneel gedrag.
340.3	In deze sectie worden vereisten en toepassingsmateriaal beschreven die relevant zijn voor de toepassing van het conceptueel kader met betrekking tot het aanbieden en aanvaar den van aanmoedigingen bij de uitvoering van professionele diensten die geen niet naleving van wet en regelgeving inhouden. Deze sectie schrijft ook voor dat een IT auditor zich bij het aanbieden of aanvaarden van aanmoedigingen aan de relevante wet en regelgeving moet houden.
	Vereisten en toepassingsmateriaal
340.4 T1	**Algemeen** Een aanmoediging is een voorwerp, situatie of handeling die wordt gebruikt als middel om het gedrag van een andere persoon te beïnvloeden, maar niet noodzakelijk met de bedoeling om het gedrag van die persoon op ongepaste wijze te beïnvloeden. Aanmoedigingen kunnen variëren van kleine gastvrijheidsacties tussen IT-auditors en bestaande of potentiële cliënten tot handelingen die resulteren in niet-naleving van wet en regelgeving. Een aanmoediging kan veel verschillende vormen aannemen, bijvoorbeeld: • Geschenken; • Gastvrijheid; • Amusement; • Politieke of liefdadige giften; • Beroepen op vriendschap en loyaliteit; • Werkgelegenheid of andere commerciële kansen; • Voorkeursbehandeling, rechten of privileges.
V340.5	**Aanmoedigingen verboden door wet en regelgeving** In veel rechtsgebieden bestaat wet en regelgeving, zoals die met betrekking tot omkoping en corruptie, die het aanbieden of accepteren van aanmoedigingen in bepaalde omstandigheden verbiedt. De IT-auditor dient inzicht te verkrijgen in de relevante wet en regelgeving en deze na te leven wanneer de IT-auditor met dergelijke omstandigheden te maken krijgt.

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	Omschrijving
340.6 T1	**Aanmoediging niet verboden door wet en regelgeving** Het aanbieden of aanvaarden van aanmoedigingen die niet bij wet en regelgeving ver boden zijn, kan toch een bedreiging vormen voor de naleving van de fundamentele beginselen.
V340.7	**Aanmoedigingen met de bedoeling gedrag op ongepaste wijze te beïnvloeden** Een IT-auditor mag geen aanmoedigingen aanbieden, of anderen aanmoedigen dit te doen, die worden aangeboden, of waarvan de IT-auditor van mening is dat een objectieve, redelijke en geïnformeerde derde partij waarschijnlijk zou concluderen dat ze worden aangeboden, met de bedoeling het gedrag van de ontvanger of van een ander individu op ongepaste wijze te beïnvloeden.

V340.8	Een IT-auditor mag geen enkele aanmoediging aanvaarden, of anderen ertoe aanzetten dit te aanvaarden, waarvan de IT-auditor concludeert dat het is gedaan, of waarvan een objectieve, redelijke en geïnformeerde derde partij waarschijnlijk concludeert dat het is gedaan, met het oogmerk het gedrag van de ontvanger of van een andere persoon op ongepaste wijze te beïnvloeden.
340.9 T1	Een aanmoediging wordt beschouwd als ongepaste beïnvloeding van het gedrag van een persoon als zij ertoe leidt dat die persoon op een onethische manier handelt. Een derge lijke ongepaste beïnvloeding kan gericht zijn op de ontvanger of op een andere persoon die een relatie met de ontvanger heeft. De fundamentele beginselen vormen een passend referentiekader voor een IT-auditor bij de beoordeling van wat onethisch gedrag is van de kant van de IT-auditor en, zo nodig naar analogie, van andere personen.
340.9 T2	Er is sprake van schending van het fundamentele beginsel van integriteit wanneer een IT auditor een aanmoediging aanbiedt of aanvaardt, of anderen ertoe aanzet een aanmoediging aan te bieden of aan te nemen, met de bedoeling het gedrag van de ontvanger of van een andere persoon op ongepaste wijze te beïnvloeden.
340.9 T3	De vaststelling of er sprake is van een werkelijke of gepercipieerde intentie om gedrag op ongepaste wijze te beïnvloeden, vereist de toepassing van een professionele oordeelsvorming. Relevante factoren om in overweging te nemen kunnen zijn: • De aard, frequentie, waarde en cumulatief effect van de aanmoediging. • De timing van het moment waarop de aanmoediging wordt aangeboden in ver houding tot een actie of beslissing die ze zou kunnen beïnvloeden. • Of de aanmoediging gebruikelijk is in de cultuur in de gegeven omstandigheden, bijvoorbeeld het aanbieden van een geschenk ter gelegenheid van een religieuze feestdag of huwelijk. • Of de aanmoediging een bijkomstig onderdeel is van een professionele dienst, bijvoorbeeld het aanbieden of aanvaarden van een lunch in verband met een za-

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	Omschrijving
	kenbijeenkomst. • Of het aanbod van de aanmoediging beperkt is tot een individuele ontvanger of beschikbaar is voor een bredere groep. De bredere groep kan intern of extern zijn, zoals andere leveranciers van de cliënt. • De functies en posities van de personen in het kantoor of bij de cliënt die de aan moediging aanbieden of krijgen aangeboden. • Of de IT-auditor weet, of redenen heeft om aan te nemen, dat het aanvaarden van de aanmoediging het beleid en de procedures van de cliënt zou schenden. • De mate van transparantie waarmee de aanmoediging wordt aangeboden. • Of de stimulans vereist was of gevraagd werd door de ontvanger. • Het gekende eerdere gedrag of de reputatie van de aanbieder.

340.10 T1	**Overweging van verdere acties** Indien de IT-auditor kennis krijgt van een aanmoediging die wordt aangeboden met de werkelijke of vermoede bedoeling het gedrag op ongepaste wijze te beïnvloeden, kunnen er nog steeds bedreigingen voor de naleving van de fundamentele beginselen ontstaan, zelfs indien aan de vereisten van de punten V340.7 en V340.8 is voldaan.
340.10 T2	Voorbeelden van acties die als voorzorgsmaatregel kunnen dienen om dergelijke bedreigingen aan te pakken, zijn onder meer: • Het informeren van het senior management van de onderneming of degenen die belast zijn met het bestuur van de cliënt over het aanbod. • Het wijzigen of beëindigen van de zakelijke relatie met de cliënt.
340.11 T1	**Aanmoedigingen zonder de intentie het gedrag op ongepaste wijze te beïnvloeden** De in het conceptueel kader opgenomen vereisten en toepassingsmateriaal zijn van toepassing wanneer een IT-auditor heeft geconcludeerd dat geen sprake is van een werkelijke of gepercipieerde intentie om het gedrag van de ontvanger of van een andere persoon op ongepaste wijze te beïnvloeden.
340.11 T2	Indien een dergelijke stimulans triviaal en onbeduidend is, zullen de bedreigingen die er van uitgaan, van een aanvaardbaar niveau zijn.
340.11 T3	Voorbeelden van omstandigheden waarin het aanbieden of aanvaarden van een dergelijke stimulans bedreigingen zou kunnen creëren, zelfs als de IT-auditor tot de conclusie is gekomen dat er geen sprake is van een werkelijke of gepercipieerde intentie om gedrag op ongepaste wijze te beïnvloeden, zijn onder meer: • Bedreigingen uit eigenbelang o Een IT-auditor wordt gastvrijheid aangeboden door de kandidaat-

Art./Par.	**Omschrijving**
	overnemer van een cliënt terwijl hij diensten op het gebied van bedrijfsfinanciering verleent aan de cliënt. • Bedreigingen door vertrouwdheid o Een IT-auditor neemt regelmatig een bestaande of potentiële cliënt mee naar sportevenementen. • Intimidatiebedreigingen o Een IT-auditor aanvaardt gastvrijheid van een cliënt waarvan de aard on gepast zou kunnen worden geacht indien deze publiekelijk bekend zou worden gemaakt.
340.11 T4	Relevante factoren bij de beoordeling van de omvang van dergelijke bedreigingen als ge volg van het aanbieden of aanvaarden van een dergelijke stimulans zijn onder meer de zelfde factoren als die welke in punt 340.9 T3 zijn beschreven om de intentie vast te stel len.

340.11 T5	Voorbeelden van acties die bedreigingen wegnemen die ontstaan door het aanbieden of aanvaarden van een dergelijke aanmoediging zijn: • Het weigeren of niet aanbieden van de aanmoediging. • De verantwoordelijkheid voor het leveren van professionele diensten aan de cliënt overdragen aan een andere persoon van wie de IT-auditor geen reden heeft om aan te nemen dat hij ongepast zou worden beïnvloed bij het leveren van de diensten, of dat dit zou worden opgevat als ongepast.
340.11 T6	Voorbeelden van acties die kunnen dienen als voorzorgsmaatregelen om dergelijke bedreigingen die ontstaan door het aanbieden of aanvaarden van een dergelijke aanmoediging aan te pakken, zijn onder meer: • Transparant zijn tegenover het senior management van de onderneming of van de cliënt over het aanbieden of aanvaarden van een aanmoediging. • Het registreren van de aanmoediging in een logboek dat wordt bijgehouden door het senior management van de onderneming of een andere persoon die verantwoordelijk is voor de ethische compliance van de onderneming, of dat wordt bijgehouden door de cliënt. • Het laten beoordelen door een geschikte beoordelaar, die niet anderszins betrokken is bij het verlenen van de professionele dienst, van alle door de professionele IT auditor verrichte werkzaamheden of genomen beslissingen met betrekking tot de client van wie de IT-auditor de aanmoediging heeft aanvaard. • Het doneren van de aanmoediging aan een goed doel na ontvangst en het op gepaste wijze bekendmaken van de donatie, bijvoorbeeld aan een lid van het senior manage ment van het kantoor of de persoon die de aanmoediging heeft aangeboden. • De kosten van de ontvangen aanmoediging, zoals gastvrijheid, terugbetalen. • Het zo snel mogelijk teruggeven van de beloning, zoals een geschenk, nadat het initieel werd aanvaard.

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	Omschrijving
V340.12	**Directe of naaste familieleden** Een IT-auditor moet alert blijven op mogelijke bedreigingen voor de naleving van de fundamentele beginselen door de IT-auditor die ontstaan door het aanbieden van een aanmoediging door een direct of naast familielid van de IT-auditor aan een bestaande of potentiële cliënt van de IT-auditor.
V340.13	Wanneer de IT-auditor kennis krijgt van een aanmoediging die wordt aangeboden aan of wordt uitgeoefend door een direct of naast familielid en tot de conclusie komt dat sprake is van opzet om het gedrag van de IT-auditor of van een bestaande of potentiële cliënt van de IT-auditor ongepast te beïnvloeden, of van mening is dat een objectieve, redelijke en geïnformeerde derde partij waarschijnlijk tot de conclusie zou komen dat een dergelijke opzet bestaat, adviseert de IT-auditor het directe of naaste familielid om de aanmoediging niet aan te bieden of te accepteren.

340.13 T1	De in artikel 340.9 T3 uiteengezette factoren zijn relevant om te bepalen of sprake is van een werkelijke of gepercipieerde intentie om het gedrag van de IT-auditor of van de bestaande of potentiële cliënt op ongepaste wijze te beïnvloeden. Een andere factor die re levant is, is de aard of de hechtheid van de relatie, tussen: a) De IT-auditor en het directe of naaste familielid; b) Het directe of indirecte familielid en de bestaande of potentiële cliënt; en c) De IT-auditor en de bestaande of potentiële cliënt. Zo zou bijvoorbeeld het aanbod van een dienstbetrekking, buiten de normale wervingsprocedure om, aan de echtgenoot van de IT-auditor door een cliënt voor wie de IT auditor een assurance-opdracht uitvoert, op een dergelijke bedoeling kunnen wijzen.
340.13 T2	Het toepassingsmateriaal van punt 340.10 T2 is ook relevant voor de aanpak van bedrei gingen die kunnen ontstaan wanneer sprake is van een werkelijke of gepercipieerde in tentie om het gedrag van de IT-auditor of van de bestaande of potentiële cliënt op onge paste wijze te beïnvloeden, ook al heeft het naaste familielid het overeenkomstige punt V340.13 gegeven advies opgevolgd.
340.14 T1	**Toepassing van het conceptueel kader** Wanneer de IT-auditor kennis krijgt van een aanmoediging die wordt aangeboden in de omstandigheden die in artikel V340.12 aan de orde komen, kunnen bedreigingen voor de naleving van de fundamentele beginselen ontstaan wanneer: a) Het directe of naaste familielid de aanmoediging aanbiedt of aanvaardt in strijd

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	Omschrijving
	met het advies van de IT-auditor op grond van artikel V340.13; of b) De IT-auditor geen reden heeft om aan te nemen dat er een werkelijke of gepercipieerde bedoeling om het gedrag van de IT-auditor of van de bestaande of potentiële cliënt op ongepaste wijze te beïnvloeden bestaat.
340.14 T2	Het toepassingsmateriaal in de artikelen 340.11 T1 tot en met 340.11 T6 is van belang voor de vaststelling, beoordeling en aanpak van dergelijke bedreigingen. Factoren die van belang zijn bij de beoordeling van het niveau van bedreigingen in deze omstandigheden zijn onder meer ook de aard of de hechtheid van de in artikel 340.13 T1 beschreven relaties.
Sectie 400	**NETWERKONDERDELEN**
Definitie	Netwerkonderdeel: – een IT-auditeenheid of andere entiteit die behoort tot een netwerk.
400.50 T1	Ondernemingen vormen vaak grotere structuren met andere eenheden om hun professionele diensten te verbeteren. Of deze grotere structuren een netwerk creëren is afhankelijk van de specifieke feiten en omstandigheden. Het hangt niet af van het juridisch ge scheiden en te onderscheiden zijn van de ondernemingen en entiteiten.
V400.51	Een netwerkonderdeel moet onafhankelijk zijn van de assurance-cliënten van de andere kantoren binnen het netwerk zoals vereist in deze Code.

400.51 T1	De onafhankelijkheidsvereisten in deze Code voor een netwerkonderdeel gelden voor elk onderdeel dat aan de definitie van een netwerkonderdeel voldoet. Het is niet noodzakelijk dat de entiteit ook voldoet aan de definitie van een onderneming. Zo kan bijvoorbeeld een adviesbureau of een advocatenpraktijk een netwerkbedrijf zijn, maar geen onderneming.
V400.52	Wanneer een firma geassocieerd is met een grotere structuur van andere firma's en entiteiten, moet zij: a) Professionele oordeelsvorming uitoefenen om te bepalen of een netwerk wordt gecreëerd door een dergelijke grotere structuur; b) In overweging nemen of een objectieve, redelijke en geïnformeerde derde partij waarschijnlijk zou concluderen dat de andere kantoren en entiteiten in de grotere structuur op zodanige wijze verbonden zijn dat er een netwerk bestaat; en c) Dit oordeel consequent toepassen in de gehele grotere structuur.
V400.53	Bij het bepalen of een netwerk wordt gevormd door een grotere structuur van ondernemingen en andere entiteiten, moet een onderneming concluderen dat er sprake is van een netwerk wanneer een dergelijke grotere structuur gericht is op samenwerking en: a) Het duidelijk gericht is op winst of kostendeling tussen de onderdelen binnen de structuur (zie artikel 400.53 T2); b) De onderdelen binnen de structuur gemeenschappelijk eigendom, zeggenschap of beheer hebben (zie artikel 400.53 T3); c) De onderdelen binnen de structuur een gemeenschappelijk beleid en procedures voor kwaliteitscontrole delen (zie artikel 400.53 T4); d) De onderdelen binnen de structuur een gemeenschappelijke bedrijfsstrategie de len (zie artikel 400.53 T5); e) De onderdelen binnen de structuur gezamenlijk een gemeenschappelijke merk naam gebruiken (zie artikelen 400.53 A6, 400.53 T7); of f) De onderdelen binnen de structuur een aanzienlijk deel van de professionele mid delen delen (zie artikelen 400.53 A8, 400.53 T9).

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	**Omschrijving**
400.53 T1	Er kunnen andere regelingen zijn tussen ondernemingen en onderdelen binnen een gro tere structuur die een netwerk vormen, in aanvulling op de regelingen die in artikel V400.53 worden beschreven. Een grotere structuur kan echter alleen gericht zijn op het vergemakkelijken van de doorverwijzing van werk, hetgeen op zichzelf niet voldoet aan de criteria om een netwerk te vormen.
400.53 T2	Het delen van immateriële kosten leidt op zichzelf niet tot een netwerk. Indien het delen van de kosten beperkt blijft tot de kosten die verband houden met de ontwikkeling van audit methodologieën, handboeken of trainingen, zou dit op zich bovendien geen net werk tot stand brengen. Voorts leidt een relatie tussen een kantoor en een anderszins niet-verbonden onderdeel om gezamenlijk een dienst te verlenen of een product te ont wikkelen, op zich niet tot een netwerk. (zie artikel R400.53(a)).

400.53 T3	Gemeenschappelijke eigendom, zeggenschap of beheer kan bij overeenkomst of op andere wijze worden geregeld. (zie artikel R400.53(b)).
400.53 T4	Gemeenschappelijke beleidslijnen en procedures voor kwaliteitscontrole zijn die welke in de grotere structuur worden ontworpen, uitgevoerd en gecontroleerd (zie artikel R400.53(c)).
400.53 T5	Het delen van een gemeenschappelijke bedrijfsstrategie omvat een overeenkomst tussen de onderdelen om gemeenschappelijke strategische doelstellingen te verwezenlijken. Een onderdeel is geen netwerkonderneming louter en alleen omdat zij met een ander onder deel samenwerkt om gezamenlijk te reageren op een verzoek om een offerte voor het verlenen van een professionele dienst. (zie artikel R400.53(d)).
400.53 T6	Een gemeenschappelijke merknaam omvat gemeenschappelijke initialen of een gemeen schappelijke naam. Een IT-auditkantoor gebruikt een gemeenschappelijke merknaam als het bijvoorbeeld de gemeenschappelijke merknaam als onderdeel van, of samen met, zijn kantoornaam vermeldt wanneer een partner van het kantoor een rapport ondertekent.

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	**Omschrijving**
	(zie artikel R400.53(e)).
400.53 T7	Zelfs wanneer een onderneming niet tot een netwerk behoort en geen gemeenschappelij ke merknaam als onderdeel van haar bedrijfsnaam gebruikt, kan het lijken alsof zij tot een netwerk behoort indien in haar briefpapier of promotiemateriaal wordt vermeld dat de onderneming lid is van een vereniging van ondernemingen. Indien een onderneming dit lidmaatschap niet met de nodige zorgvuldigheid beschrijft, kan de indruk worden ge wekt dat de onderneming tot een netwerk behoort. (zie artikel R400.53(e)).
400.53 T8	Professionele hulpmiddelen omvatten: • Gemeenschappelijke systemen die ondernemingen in staat stellen informatie uit te wisselen zoals cliëntgegevens, facturering en tijdregistraties. • Partners en ander personeel. • Vaktechnische afdelingen die advies geven over vaktechnische of sectorspeci fieke kwesties, transacties of gebeurtenissen voor assurance-opdrachten. • Auditmethodologie of audithandleidingen. • Opleidingen, cursussen en faciliteiten (zie artikel R400.53(f)).

400.53 T9	Of de gedeelde beroepsmiddelen significant zijn, hangt af van de omstandigheden. Bij voorbeeld: • De gedeelde middelen kunnen beperkt blijven tot een gemeenschappelijke auditmethodologie of audithandleidingen, zonder uitwisseling van personeel of cliënt of marktinformatie. In dergelijke omstandigheden is het onwaar schijnlijk dat de gedeelde middelen significant zouden zijn. Hetzelfde geldt voor een gemeenschappelijke opleidingsinspanning. • De gedeelde middelen zouden de uitwisseling van personeel of informatie kunnen inhouden, zoals wanneer personeel wordt geput uit een gemeen schappelijke pool, of wanneer een gemeenschappelijke vaktechnische afde ling wordt opgericht binnen de grotere structuur om de deelnemende onder nemingen vaktechnisch advies te verstrekken dat de ondernemingen verplicht zijn op te volgen. In dergelijke omstandigheden is het waarschijnlijker dat een objectieve, redelijke en geïnformeerde derde partij tot de conclusie komt dat de gedeelde middelen aanzienlijk zijn. (Ref: Para. R400.53(f)).
V400.54	Indien een IT-auditkantoor of een netwerk een onderdeel van zijn praktijk verkoopt, en het onderdeel gedurende een beperkte tijd de naam van het kantoor of netwerk geheel of gedeeltelijk blijft gebruiken, moeten de betrokken onderdelen bepalen hoe zij bij de pre sentatie aan externe partijen bekend moeten maken dat zij geen netwerkkantoor zijn.
400.54 T1	In de overeenkomst tot verkoop van een onderdeel van een praktijk kan worden bepaald dat het verkochte onderdeel gedurende een beperkte periode de naam van het kantoor of

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	**Omschrijving**
	het netwerk geheel of gedeeltelijk mag blijven gebruiken, ook al is het niet langer ver bonden met het kantoor of het netwerk. In dergelijke omstandigheden oefenen de twee entiteiten weliswaar onder een gemeenschappelijke naam hun bedrijf uit, maar zijn de feiten van dien aard dat zij niet tot een grotere op samenwerking gerichte structuur be horen. De twee entiteiten zijn derhalve geen netwerkondernemingen.
4B	**ONAFHANKELIJKHEID VOOR ASSURANCE-OPDRACHTEN**
Sectie 900	**TOEPASSING VAN HET CONCEPTUEEL KADER VOOR DE ONAFHANKELIJKHEID VAN ASSU RANCE-OPDRACHTEN** **Inleiding** **Algemee** **n**
900.1	Dit deel is van toepassing op assurance-opdrachten. Voorbeelden van dergelijke opdrachten zijn: • assurance ten aanzien van interne beheersing van operationele of financiële processen; • assurance ten aanzien van de General IT Controls; • assurance ten aanzien van de kernprestatie-indicatoren van een entiteit; • assurance ten aanzien van de naleving van de wet en regelgeving door een entiteit; • assurance ten aanzien van door een organisatie van openbaar belang te be halen prestatiecriteria, zoals prijskwaliteitverhouding; • assurance ten aanzien van de doelmatigheid van het interne beheersingssysteem van een entiteit.

900.2	Waar in dit deel de term "IT-auditor" wordt gebruikt, verwijst dit zowel naar afzonderlijke IT-auditors werkzaam in een openbare praktijk als naar hun IT-auditeenheid.
900.3	Een IT-auditeenheid is op grond van RKBN verplicht beleidsmaatregelen en procedures vast te stellen waarmee met redelijke zekerheid de onafhankelijkheid van de IT auditeenheid, het personeel ervan en waar van toepassing anderen waarop onafhan kelijkheidseisen van toepassing zijn, gewaarborgd wordt, waar dit op grond van de toe passelijke ethische normen is voorgeschreven. Daarnaast schrijven Richtlijnen verant woordelijkheden voor aan opdrachtpartners en opdrachtteams op het niveau van de op dracht. De toewijzing van verantwoordelijkheden binnen een IT-auditeenheid hangt af van de omvang, structuur en organisatie daarvan. Veel van de bepalingen van deel 4B schrijven geen specifieke verantwoordelijkheid voor aan individuele personen binnen de IT-auditeenheid voor handelingen gericht op de instandhouding van de onafhankelijk heid, maar verwijzen in plaats daarvan gemakshalve naar "IT-auditeenheid". De verant woordelijkheid voor een bepaalde handeling wordt door de IT-auditeenheid en conform RKBN toegewezen aan een persoon of een groep van personen (bijvoorbeeld een assu- rance-team). Elke individuele IT-auditor blijft daarnaast verantwoordelijk voor het nale ven van de op de handelingen, belangen en relaties van die IT-auditor toepasselijke be-

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	Omschrijving
	palingen.
900.4	Onafhankelijkheid hangt samen met de beginselen van objectiviteit en integriteit. Het omvat: a) Onafhankelijkheid in wezen – De geesteshouding die het tot uitdruk king brengen van een conclusie toestaat zonder beïnvloed te worden door invloeden die professionele oordeelsvorming in gevaar brengen, waardoor een individu met integriteit kan handelen, alsmede objectiviteit en een professioneel-kritische instelling kan uitoefenen. b) Onafhankelijkheid in schijn – Het vermijden van feiten en omstandig heden die dermate significant zijn dat een objectieve, redelijke en ge informeerde derde partij waarschijnlijk zou concluderen, alle feiten en omstandigheden afwegend, inclusief toegepaste maatregelen, dat de integriteit, objectiviteit of professioneel-kritische instelling van een IT auditeenheid of van een lid van het assurance-team in gevaar is ge bracht. Waar in dit deel wordt verwezen naar de "onafhankelijkheid" van een persoon of IT auditeenheid, betekent dit dat die persoon of die IT-auditeenheid voldoet aan de bepalingen van dit deel.
900.5	De Code schrijft voor dat IT-auditeenheden bij de uitvoering van assurance opdrachten de fundamentele beginselen dienen na te leven en onafhankelijk moeten zijn. In dit deel worden de specifieke vereisten en toepassingsmateriaal uiteengezet die van wezenlijk belang zijn bij de toepassing van het conceptuele kader om ervoor te zorgen dat bij het uitvoeren van assurance-opdrachten, de voortdurende onafhan kelijkheid gewaarborgd wordt. Het in sectie 120 opgenomen conceptuele kader is zowel van toepassing op de onafhankelijkheid als op de in sectie 110 vermelde fundamentele beginselen.

900.6	In dit deel wordt beschreven: a) de feiten en omstandigheden, waaronder professionele diensten, belangen en relaties, die (mogelijk) bedreigingen voor de onafhankelijkheid creëren; b) mogelijke handelingen, inclusief waarborgen, om aan deze bedreigimgen te behandelen; en

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	Omschrijving
	c) bepaalde situaties waarin het niet mogelijk is de bedreigingen te elimi neren of waarin er geen waarborgen zijn voor het terugbrengen van de bedreigingen tot een aanvaardbaar niveau.
900.7	Een assurance-opdracht houdt in dat de IT-auditeenheid tracht voldoende geschikte assurance-informatie te verzamelen om een conclusie te kunnen afgeven gericht op het vergroten van het vertrouwen van de beoogde gebruikers, uitgezonderd de ver antwoordelijke partij, ten aanzien van het onderzoeksobject van de informatie. In de (herziene) Richtlijn 3000 (A en D) worden de elementen en doelstellingen beschreven van een op basis van die Richtlijn uitgevoerde assurance-opdracht; het assurance stramien geeft een algemene omschrijving van assurance-opdrachten. Een assurance-opdracht kan een attest opdracht of een directe opdracht zijn.
900.8	Vervalt, niet relevant voor NOREA
900.9	**Rapporten die een gebruiks en verspreidingsbeperking bevatten** In een assurance-rapport kan een beperking ten aanzien van het gebruik en de versprei ding ervan worden opgenomen. Wanneer dit het geval is, en aan de voorwaarden van sectie 990 is voldaan, kunnen de in onderhavig deel opgenomen onafhankelijkheidseisen overeenkomstig het bepaalde in Artikel 990 worden aangepast.
	Controle en beoordelingsopdrachten
900.10	Vervalt, niet relevant voor NOREA
	Vereisten en toepassingsmateriaal **Algemeen**
V 900.11	Een IT-auditeenheid die assurance-opdrachten uitvoert dient onafhankelijk te zijn van de degene die de assurance-opdracht verstrekt (de "verantwoordelijke partij").
900.11 T1	Voor de strekking van dit deel is de assurance-cliënt degene die de assurance-opdracht verstrekt, is ook de verantwoordelijke partij en tevens, in het geval van een attestop dracht, de partij die verantwoordelijkheid aanvaardt voor de informatie over het onder zoeksobject (welke partij dezelfde als de verantwoordelijke partij kan zijn).

900.11 T2	De rollen van de partijen die zijn betrokken bij een assurance-opdracht kunnen verschillen, wat van invloed kan zijn op de toepassing van de in dit deel opgenomen onafhankelijkheidseisen. Ten aanzien van de meeste attestopdrachten (attest) zijn de verantwoordelijke partij en de partij die verantwoordelijkheid aanvaardt voor de informatie over het onderzoeksobject dezelfde. Hiertoe behoren ook situaties waarin de verantwoordelijke partij een andere partij inschakelt om het onderzoeksobject te meten of te evalueren op

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	Omschrijving
	basis van de criteria (de evalueerder) en waarbij de verantwoordelijke partij de verantwoordelijkheid aanvaardt voor de informatie over het onderzoeksobject. De verantwoordelijke partij of cliënt kunnen echter ook een andere partij opdracht geven om de informatie over het onderzoeksobject op te stellen, waarbij deze partij de verantwoordelijkheid aanvaardt voor de informatie over het onderzoeksobject. In dat geval zijn voor de toepassing van dit deel zowel de verantwoordelijke partij als de partij die verantwoorde lijk is voor de informatie over het onderzoeksobject de assurance cliënt.
900.11 T3	Naast de verantwoordelijke partij en, ten aanzien van een attestopdracht, de partij die verantwoordelijkheid aanvaardt voor de informatie over het onderzoeksobject, kunnen nog andere partijen bij de opdracht betrokken zijn. Zo kan er, afgezien van de partij die verantwoordelijkheid aanvaardt voor de informatie over het onderzoeksobject, sprake zijn van een afzonderlijke cliënt of van een evalueerder. In die gevallen schrijft het conceptuele kader voor dat de IT-auditor de door de belangen van of relaties met deze par tijen veroorzaakte bedreigingen voor de fundamentele beginselen identificeert en evalueert en vaststelt of er sprake is van belangenverstrengeling.
900.11 T4	1. Onafhankelijkheid bij een assurance-opdracht met een niet-nader bepaalde kring van gebruikers geldt ten opzichte van het onderzoeksobject, de verantwoordelijke persoon en de verantwoordelijke entiteit. 2. Onafhankelijkheid bij een assurance-opdracht ten behoeve van een nader bepaalde kring van gebruikers geldt ten opzichte van het onderzoeksobject en de verantwoordelijke persoon, mits: a. het assurance-rapport: 1. geadresseerd is aan de nader bepaalde kring van gebruikers; 2. duidelijk de beperking in gebruik en verspreidingskring vermeldt; 3. duidelijk de toepassing van dit artikellid vermeldt; b. alle gebruikers van buiten de verantwoordelijke entiteit en haar verbonden derde vooraf instemmen met de toepassing van dit lid. Hierbij worden het Rijk, de provincies en de gemeenten geacht onderdeel te zijn van één verantwoordelijke entiteit en haar verbonden derde. 3. Onafhankelijkheid bij een assurance-opdracht ten behoeve van een nader bepaalde kring van gebruikers geldt ten opzichte van het onderzoeksobject, de verantwoordelijke persoon en de verantwoordelijke entiteit als niet voldaan wordt aan de voorwaarden in het tweede lid, onderdelen a en b. Indien het assurance-rapport openbaar wordt gemaakt op grond van de Wet openbaarheid van bestuur, wordt

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')	
Art./Par.	**Omschrijving**
	dit voor de toepassing van dit artikel niet gezien als een assurance-opdracht voor een niet-nader bepaalde kring van gebruikers.
900.11 T5	In afwijking van 900.11 T4, eerste tot en met derde lid, is sprake van een onafhankelijke uitvoering van een assurance-opdracht door een overheids-IT-auditor of een interne IT auditor werkzaam bij een financiële instelling als: a. de overheids-IT-auditor of interne IT-auditor bij of krachtens wet deze assurance-opdracht kan uitvoeren; b. deze assurance-opdracht zowel in wezen als in schijn onafhankelijk wordt uitgevoerd van het onderzoeksobject en de verantwoordelijke persoon; en c. de overheids-IT-auditor of interne IT-auditor voldoet aan eventuele bij of krachtens die wet gestelde voorwaarden aan de onafhankelijke uitvoering van de assurance-opdracht.
V900.12	Een IT-auditeenheid dient het in artikel 120 omschreven conceptuele kader toe te passen teneinde bedreigingen voor de onafhankelijkheid ten aanzien van een assurance opdracht te signaleren, evalueren en behandelen.
900.13 T1	Bij bepaalde assurance-opdrachten, hetzij een attestopdracht of een rechtstreekse op dracht, kan er sprake zijn van verschillende verantwoordelijke partijen of, ten aanzien van een attestopdracht, van verschillende partijen die verantwoordelijkheid aanvaarden voor de informatie over het onderzoeksobject. De IT-auditeenheid kan bij het vaststellen of het noodzakelijk is om de bepalingen van dit deel toe te passen op elke afzonderlijke verantwoordelijke partij of elke afzonderlijke partij die verantwoordelijkheid aanvaardt voor de informatie over het onderzoeksobject van deze opdrachten, verschillende zaken in overweging nemen. Deze zaken betreffen onder andere of de IT-auditeenheid of een lid van het assurance-team een belang heeft in of een relatie met een specifieke verant woordelijke partij of partij die verantwoordelijkheid aanvaardt voor de informatie over het onderzoeksobject, hetgeen een bedreiging kan vormen voor de onafhankelijkheid die, in de context van de informatie over het onderzoeksobject, niet kan worden aangemerkt als verwaarloosbaar of onbeduidend. Bij deze vaststelling dient o.a. rekening te worden ge houden met de volgende factoren: (a) de materialiteit van het onderzoeksobject of de informatie over het on derzoeksobject waarvoor de betreffende partij verantwoordelijk is in de context van de assurance-opdracht als geheel; (b) het openbare belang van de assurance-opdracht. Wanneer de IT-auditeenheid vaststelt dat de door een dergelijk belang in of dergelijke relatie met een specifieke partij ontstane bedreiging verwaarloosbaar en onbeduidend is, is het wellicht niet noodzakelijk alle bepalingen van dit artikel op die partij toe te passen.
B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')	
Art./Par.	**Omschrijving**
	Netwerken

V 900.14	Wanneer een IT-auditeenheid weet of vermoedt dat belangen in en relaties van een net werk een bedreiging kunnen vormen voor de onafhankelijkheid van de IT-auditeenheid, dient de IT-auditeenheid die bedreiging te evalueren en te behandelen.
900.14 T1	Netwerken van IT-auditeenheden worden nader besproken in artikel 400.50 T1 tot en met 400.54 T1 (blz. 26)
	Verbonden entiteiten
V 900.15	Wanneer het assurance-team weet of vermoedt dat een relatie of situatie waarbij een ver bonden entiteit van de assurance-cliënt is betrokken relevant kan zijn voor het vaststellen of de IT-auditeenheid onafhankelijk is van de cliënt, dient het assurance-team die verbonden entiteit op te nemen bij het signaleren, evalueren en behandelen van bedreigingen voor de onafhankelijkheid.
	[Artikel 900.16 tot en met 900.29 zijn opzettelijk blanco gelaten]
V 900.30	De in dit deel voorgeschreven onafhankelijkheid dient te worden gewaarborgd geduren de: (a) de opdrachtperiode; en (b) de periode waarop de informatie over het onderzoeksobject betrekking heeft.
900.30 T1	De opdrachtperiode vangt aan op het moment waarop het assurance-team begint met het uitvoeren van de assurance-taken met betrekking tot de betreffende opdracht. De opdrachtperiode eindigt op het moment waarop het assurance-rapport wordt uitgebracht. Wanneer de opdracht van wederkerende aard is, eindigt deze op het moment waarop een der partijen de andere partij in kennis stelt dat deze de professionele relatie beëindigt of bij het uitbrengen van het laatste assurance-rapport, afhankelijk welk moment later is.
V900.31	Wanneer een entiteit tijdens of na de periode waarop de informatie over het onder zoeksobject waarover de IT-auditeenheid een conclusie zal verstrekken betrekking heeft, een verantwoordelijke partij wordt, dient de IT-auditeenheid vast te stellen of de onafhankelijkheid wordt bedreigd door: (a) financiële of zakelijke relaties met de verantwoordelijke partij tijdens of na de periode waarop de informatie over het onderzoeksobject betrekking heeft maar voordat de assurance-opdracht wordt aanvaard; of (b) eerder aan de verantwoordelijke partij verleende diensten.

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	**Omschrijving**

V 900.32	Bedreigingen voor de onafhankelijkheid ontstaan wanneer tijdens of na de periode waarop de informatie over het onderzoeksobject betrekking heeft maar voordat het assurance-team de assurance-taak begint uit te voeren een non-assurance dienst was verleend aan de verantwoordelijke partij, en het verlenen van deze dienst niet zou zijn toegestaan gedurende de opdrachtperiode. In dat geval dient de IT auditeenheid elke bedreiging die door deze dienst ontstaat te evalueren en te behandelen. Indien de bedreigingen onaanvaardbaar groot zijn, mag de IT-auditeenheid de assurance-opdracht uitsluitend aanvaarden wanneer de bedreigingen tot een aanvaardbaar niveau worden teruggebracht.
900.32 T1	Handelingen die waarborgen kunnen bieden tegen deze bedreigingen zijn onder andere: • de dienst laten uitvoeren door medewerkers die geen lid zijn van het assurance-team. • een gepaste beoordelaar laten beoordelen of de assurance en non assurance werkzaamheden gepast zijn.
V 900.33	Indien een non-assurance-opdracht die niet zou zijn toegestaan gedurende de op drachtperiode niet is voltooid en het is praktisch niet mogelijk deze opdracht te voltooien of te beëindigen voor aanvang van professionele dienstverlening in het kader van de assurance-opdracht, mag de IT-auditeenheid de assurance-opdracht uitsluitend aanvaarden indien: (a) tot tevredenheid van de IT-auditeenheid is vastgesteld dat: **(i)** de non-assurance-opdracht binnen afzienbare tijd zal zijn voltooid; of **(ii)** de cliënt maatregelen heeft getroffen om de opdracht binnen afzienbare tijd over te dragen aan een ander; (b) de IT-auditeenheid voor zover noodzakelijk waarborgen toepast gedurende de opdrachtperiode; en (c) de IT-auditeenheid de kwestie onder de aandacht brengt van de met governance belaste personen.

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	**Omschrijving**
	[Artikel 900.34 tot en met 900.39 zijn opzettelijk blanco gelaten]
	Algemene documentatie met betrekking tot de onafhankelijkheid voor assurance opdrachten

V 900.40	Een IT-auditeenheid is verplicht alle conclusies ten aanzien van de naleving van dit deel en de inhoud van relevante besprekingen ter onderbouwing van deze conclusies vast te leggen. De IT-auditeenheid is in het bijzonder verplicht: (a) voor zover waarborgen worden toegepast tegen een bedreiging, de aard van de bedreiging en de aanwezige of toegepaste waarborgen vast te leggen; en (b) voor zover een bedreiging grondig is geanalyseerd en de IT auditeenheid concludeert dat de bedreiging al van aanvaardbaar niveau was, de aard van de bedreiging en de reden(en) voor die conclusie vast te leggen.
900.40 T1	Documentatie levert bewijs van het oordeel van de IT-auditeenheid bij het komen tot conclusies ten aanzien van naleving van dit deel. Een gebrek aan documentatie houdt echter niet in dat een IT-auditeenheid een specifieke aangelegenheid heeft overwogen of dat de IT-auditeenheid onafhankelijk is.
	[Artikel 900.41 tot en met 900.49 zijn opzettelijk blanco gelaten]
	Overtreding van een onafhankelijkheidsbepaling met betrekking tot assurance opdrachten *Wanneer een IT-auditeenheid een overtreding signaleert*
V 900.50	Wanneer een IT-auditeenheid een overtreding signaleert van een van de bepalingen van dit deel, dient de IT-auditeenheid: (a) het belang dat of de relatie die verantwoordelijk is voor de overtreding te beëindigen, op te schorten of ongedaan te maken; (b) de omvang van de overtreding en de gevolgen daarvan voor de objectiviteit van de IT-auditeenheid en diens vermogen om een assu rance-rapport uit te brengen te evalueren; en (c) vast te stellen of en zo ja, welke maatregelen genomen kunnen worden om de gevolgen van de overtreding op bevredigende wijze weg te nemen of verminderen tot een acceptabel niveau.

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	**Omschrijving**
	Bij het maken van deze vaststelling dient de IT-auditeenheid haar professionele oordeelsvorming toe te passen en zich af te vragen of een objectieve, redelijke en geïnformeerde derde waarschijnlijk tot de conclusie zou komen dat de objectiviteit van de IT-auditeenheid in het geding is en dat de IT-auditeenheid derhalve niet in staat zou zijn een assurance-rapport uit te brengen.

V 900.51	Wanneer de IT-auditeenheid vaststelt dat het niet mogelijk is om maatregelen te ne men om de gevolgen van de overtreding op bevredigende wijze weg te nemen of te verminderen tot een acceptabel niveau, dient de IT-auditeenheid zo snel mogelijk de partij die de IT-auditeenheid opdracht heeft gegeven of de met governance belaste personen daarvan in kennis te stellen. De IT-auditeenheid dient verder alle noodzakelijke stappen te nemen om de assurance-opdracht te beëindigen In overeenstemming met toepasselijke bepalingen van wet of regelgeving voor het beëindigen van assurance-opdrachten.
V 900.52	Wanneer de IT-auditeenheid vaststelt dat het wel mogelijk is om maatregelen te ne men om de gevolgen van de overtreding op bevredigende wijze ongedaan te maken, dient de IT-auditeenheid de overtreding en de stappen die het heeft genomen of denkt te nemen te bespreken met de partij die de IT-auditeenheid opdracht heeft ge geven of met degenen die zijn belast met governance. De IT-auditeenheid dient de overtreding en de voorgenomen maatregelen tijdig ter sprake te brengen, rekening houdend met de omstandigheden van de opdracht en de overtreding.
V 900.53	Indien de partij die de opdracht heeft verstrekt aan de IT-auditeenheid of de met governance belaste personen van mening zijn dat de door de IT-auditeenheid overeenkomstig het bepaalde in artikel R900.50(c) voorgestelde maatregelen de gevolgen van de overtreding niet op bevredigende wijze ongedaan maken, dient de IT-auditeenheid de benodigde stappen te nemen om de assurance-opdracht te beëindigen In overeenstemming met toepasselijke bepalingen van wet of regelgeving voor het beëindigen van assurance-opdrachten.
V 900.54	*Vastlegging* De IT-auditeenheid dient ter naleving van de bepalingen van artikel V900.50 tot en met V900.53: (a) de overtreding;

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	**Omschrijving**
	(b) de getroffen maatregelen; (c) de belangrijkste genomen besluiten; en (d) alle zaken die zijn besproken met de partij die de IT-auditeenheid opdracht heeft gegeven of de met governance belaste personen, vast te leggen.

V 900.55	Indien de IT-auditeenheid verder gaat met het uitvoeren van de assurance-opdracht, dient zij het volgende te documenteren: (a) de conclusie dat naar het professionele oordeel van de IT auditeenheid de objectiviteit niet in het geding is; en (b) de reden waarom de IT-auditeenheid van mening is dat de getroffen maatregelen op bevredigende wijze de gevolgen van de over treding ongedaan hebben gemaakt, zodat de IT-auditeenheid in staat was een assurance-rapport te verstrekken.
Sectie 905	**VERGOEDINGEN** **Inleiding**
905.1	IT-auditeenheden zijn verplicht de fundamentele beginselen na te leven, onafhanke lijk te zijn en het in sectie 120 opgenomen conceptuele kader toe te passen teneinde bedreigingen voor de onafhankelijkheid te signaleren, evalueren en te behandelen.
905.2	De aard en het niveau van de vergoedingen of andere vormen van beloning kan een bedreiging als gevolg van eigenbelang of intimidatie vormen. In deze sectie worden de specifieke vereisten en het toepassingsmateriaal beschreven die relevant zijn voor het in die situaties toepassen van het conceptuele kader.
	Vereisten en toepassingsmateriaal *Relatieve omvang van de vergoedingen*
905.3 T1	Wanneer de totale inkomsten die de IT-auditeenheid, die in het kader van een assurance-opdracht een conclusie afgeeft genereert bij de betreffende verantwoordelijke partij een groot deel van de totale inkomsten van die IT-auditeenheid vertegenwoordigen, kan de afhankelijkheid van die cliënt en zorgen over het verliezen van die client een bedreiging als gevolg van eigenbelang of intimidatie vormen.
905.3 T2	Factoren die relevant zijn bij het beoordelen van de omvang van de bedreiging zijn onder andere:

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	**Omschrijving**
	• de bedrijfsstructuur van de IT-auditeenheid; • of de IT-auditeenheid al langer bestaat of recentelijk is gevestigd; • de betekenis van de cliënt voor de IT-auditeenheid in zowel kwalitatief als kwantitatief opzicht.
905.3 T2	Bedreigingen als gevolg van eigenbelang of intimidatie kunnen bijvoorbeeld worden aangepakt door het vergroten van het aantal cliënten van de IT-auditeenheid om zo de afhankelijkheid van de verantwoordelijke partij te verkleinen.

905.3 T4	Van een bedreiging als gevolg van eigenbelang of intimidatie kan verder sprake zijn wanneer de inkomsten die de IT-auditeenheid genereert bij één verantwoordelijke partij een aanzienlijk deel vormt van de omzet die wordt gegenereerd bij de cliënten van één afzonderlijke partner.
	Achterstallige vergoedingen
905.4 T1	Een bedreiging als gevolg van eigenbelang kan ontstaan wanneer een aanzienlijk deel van de vergoeding met betrekking tot de komende periode niet vóór het uitbrengen van het eventuele assurance-rapport wordt voldaan. Gewoonlijk wordt verwacht dat de IT-auditeenheid betaling van deze vergoeding verlangt voordat het rapport wordt uitgebracht. De vereisten en het toepassingsmateriaal met betrekking tot leningen en garantstellingen als bedoeld in artikel 911 kunnen eveneens van toepassing zijn op situaties waarin sprake is van achterstallige vergoedingen.
905.4 T2	Een bedreiging als gevolg van eigenbelang kan onder meer ongedaan worden gemaakt door: • het verkrijgen van gedeeltelijke betaling van achterstallige vergoedingen; • het beoordelen van de uitgevoerde werkzaamheden door een ge schikte beoordelaar die niet betrokken was bij de uitvoering van de assurance-opdracht.
V 905.5	Wanneer een aanzienlijk deel van de door een verantwoordelijke partij verschuldigde vergoeding langere tijd niet is voldaan, dient de IT-auditeenheid vast te stellen: **(a)** of de achterstallige betaling beschouwd kan worden als een lening aan de cliënt; en
B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')	
Art./Par.	**Omschrijving**
	(b) of het gepast is dat de IT-auditeenheid opnieuw wordt aangesteld of doorgaat met het uitvoeren van de assurance-opdracht.
	Resultaatafhankelijke vergoeding
905.6 T1	Resultaatafhankelijke vergoedingen zijn vergoedingen die worden vastgesteld op ba sis van een vooraf overeengekomen resultaat van een transactie of van de verleende diensten. Een resultaatafhankelijke vergoeding die in rekening wordt gebracht via een tussenpersoon is een voorbeeld van een indirecte resultaatafhankelijke vergoeding. Voor de strekking van dit artikel wordt een vergoeding niet beschouwd als resultaat afhankelijk indien deze is vastgesteld door een rechter of andere overheidsinstelling.
V 905.7	Het is een IT-auditeenheid niet toegestaan een directe of indirecte resultaatafhankelijke vergoeding in rekening te brengen voor een assurance-opdracht.

V 905.8	Het is een IT-auditeenheid niet toegestaan een directe of indirecte resultaatafhankelijke vergoeding in rekening te brengen voor een non-assurancedienst uitgevoerd voor een verantwoordelijke partij indien de uitkomst van de non-assurancedienst en derhalve de omvang van de vergoeding afhankelijk is van een toekomstig of gelijktijdig oordeel met betrekking tot het object dat van materieel belang is voor de assurance-opdracht.
905.9 T1	Het is een IT-auditeenheid op grond van artikel R905.7 en R905.8 niet toegestaan bepaalde resultaatafhankelijke vergoedingsregelingen overeen te komen met een verantwoordelijke partij. Ook als het overeenkomen van een resultaatafhankelijke vergoedingsregeling niet uitgesloten is ten aanzien van het verlenen van een non assurancedienst aan een verantwoordelijke partij, kan evengoed een bedreiging als gevolg van eigenbelang ontstaan.
905.9 T2	Factoren die relevant zijn bij het beoordelen van de omvang van de bedreiging zijn onder andere: • de hoogte van de mogelijke vergoedingen; • of de uitkomst waarvan de resultaatafhankelijke vergoeding afhankelijk is, wordt vastgesteld door een bevoegde autoriteit; • of de door de IT-auditeenheid uitgevoerde werkzaamheden worden gedeeld met de betreffende gebruikers en de basis van de beloning; • de aard van de dienstverlening; • de gevolgen die het voorval of de transactie heeft op de informatie over het onderzoeksobject.
B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')	
Art./Par.	**Omschrijving**
905.9 T3	Dergelijke bedreigingen als gevolg van eigenbelang kunnen bijvoorbeeld worden voor komen door: • de betreffende assurance-werkzaamheden te laten beoordelen door een geschikte beoordelaar die niet bij het verlenen van de non-assurancedienst was betrokken; • van tevoren schriftelijke afspraken te maken met de cliënt over de basis van de beloning.
Sectie 906	**GESCHENKEN EN GASTVRIJHEID (zie ook sectie 340, blz. 20)** **Inleiding**
906.1	IT-auditeenheden zijn verplicht de fundamentele beginselen na te leven, onafhankelijk te zijn en het in sectie 120 opgenomen conceptuele kader toe te passen ten einde bedreigingen voor de onafhankelijkheid te signaleren, evalueren en te behandelen.
906.2	Het aanvaarden van geschenken en gastvrijheid van een verantwoordelijke partij kan een bedreiging als gevolg van eigenbelang, vertrouwdheid of intimidatie doen ontstaan. In dit artikel worden de specifieke vereisten en het toepassingsmateriaal om schreven die relevant zijn voor het in die situaties toepassen van het conceptuele kader.

	Vereisten en toepassingsmateriaal
V 906.3	Een IT-auditeenheid of een lid van het assurance-team mag geen geschenken en gastvrijheid aanvaarden van een verantwoordelijke partij, tenzij de waarde ervan verwaarloosbaar en onbeduidend is.
906.3 T1	Voor zover een IT-auditeenheid of een lid van het assurance-team een aansporing aanbiedt aan of aanvaardt van een verantwoordelijke partij, zijn daarop de in sectie 340 bedoelde voorschriften en het toepassingsmateriaal van toepassing; het niet na leven van deze voorschriften kan een bedreiging voor de onafhankelijkheid doen ontstaan.
906.3 T2	De in sectie 340 bedoelde voorschriften met betrekking tot het aanbieden of aanvaarden van aansporingen houden in dat het een IT-auditeenheid of een lid van het assurance-team niet is toegestaan geschenken en gastvrijheid te aanvaarden indien deze erop zijn gericht om ongepaste invloed uit te oefenen op het gedrag, ook al is de waarde ervan verwaarloosbaar en onbeduidend.

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	Omschrijving
Sectie 907	**FEITELIJKE OF DREIGENDE JURIDISCHE PROCEDURES** **Inleiding**
907.1	IT-auditeenheden zijn verplicht de fundamentele beginselen na te leven, onafhankelijk te zijn en het in sectie 120 opgenomen conceptuele kader toe te passen teneinde bedreigingen voor de onafhankelijkheid te signaleren, evalueren en te behandelen.
907.2	Indien sprake is van (dreigende) juridische procedure van of tegen een verantwoordelijke partij, kan dit een bedreiging als gevolg van eigenbelang en intimidatie doen ontstaan. In deze sectie wordt het specifieke toepassingsmateriaal beschreven dat re levant is voor het in die situaties toepassen van het conceptuele kader.
	Toepassingsmateriaal **Algemeen**
907.3 T1	De relatie tussen cliëntenbeheer en leden van het assurance-team dient gekenmerkt te worden door volledige openheid en openbaarmaking van alle aspecten van de activiteiten van de cliënt. Meningsverschillen kunnen leiden tot feitelijke of dreigende juridische procedures tussen een assurance-cliënt en de IT-auditeenheid of een lid van het assurance-team. Dergelijke meningsverschillen kunnen de bereidheid beïnvloeden van het management om over te gaan tot volledige openbaarmaking en bedreigingen als gevolg van eigenbelang en intimidatie doen ontstaan.
907.3 T2	Factoren die relevant zijn bij het beoordelen van de omvang van dergelijke bedreigingen zijn onder andere: • het materieel belang bij de juridische procedure; • of de juridische actie betrekking heeft op een voorgaande assurance opdracht.

907.3 T3	Indien bij de juridische procedure een lid van het assurance-team is betrokken, kan het verwijderen van de betreffende persoon uit het assurance-team ervoor zorgen dat dergelijke bedreigingen als gevolg van eigenbelang en intimidatie worden geëlimineerd.
907.3 T4	Een bedreiging als gevolg van eigenbelang of intimidatie kan bijvoorbeeld worden aangepakt door de uitgevoerde werkzaamheden te laten beoordelen door een geschikte beoordelaar.

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	**Omschrijving**
Sectie 910	**FINANCIËLE BELANGEN** **Inleiding**
910.1	IT-auditeenheden zijn verplicht de fundamentele beginselen na te leven, onafhankelijk te zijn en het in sectie 120 opgenomen conceptuele kader toe te passen teneinde bedreigingen voor de onafhankelijkheid te signaleren, evalueren en ongedaan te maken.
910.2	Het bezitten van een financieel belang in een verantwoordelijke partij kan leiden tot een bedreiging als gevolg van eigenbelang. In deze sectie worden de specifieke vereisten en het toepassingsmateriaal omschreven die relevant zijn voor het in die situaties toepassen van het conceptuele kader.
	Vereisten en toepassingsmateriaal
910.3 T1	Er kan zowel sprake zijn van een direct financieel belang als van een indirect financieel belang via een tussenpersoon, bijvoorbeeld een collectief investeringsvehikel, boedel of trust. Wanneer de beschikkingsmacht over een tussenpersoon wordt uitgeoefend door een economisch eigenaar of deze is in staat de beleggingsbeslissingen ervan te sturen, bepaalt de Code dat er sprake is van een direct financieel belang. Andersom, wanneer de economisch eigenaar niet de beschikkingsmacht uitoefent over een tussenpersoon of niet in staat is de beleggingsbeslissingen ervan te sturen, bepaalt de Code dat er sprake is van een indirect financieel belang.
910.3 T2	Deze sectie bevat verwijzingen naar de "materialiteit" van een financieel belang. Bij het vaststellen of een belang materieel is voor een persoon kan het netto vermogen van de betreffende persoon en van zijn gezinsleden in overweging worden genomen.
910.3 T3	Factoren die relevant zijn bij het beoordelen van de omvang van een bedreiging als gevolg van eigenbelang veroorzaakt door het bezitten van een financieel belang in een verantwoordelijke partij zijn onder andere: • de rol van de persoon die het financieel belang bezit; • of er sprake is van een direct of een indirect financieel belang; • de materialiteit van het financieel belang.

	Financiële belangen gehouden door de IT-auditeenheid, leden van het assurance-team en gezinsleden
B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')	
Art./Par.	**Omschrijving**
V 910.4	Het is de volgende personen niet toegestaan een direct financieel belang of een ma terieel indirect financieel belang te bezitten in de verantwoordelijke partij: (a) de IT-auditeenheid; of (b) een lid van het assurance-team of een gezinslid.
	Financiële belangen in een entiteit die de zeggenschap uitoefent over een verantwoorde lijke partij
V 910.5	Voor zover een entiteit de zeggenschap uitoefent over een verantwoordelijke partij en de laatste is van materieel belang voor de entiteit, is het de IT-auditeenheid, noch een lid van het assurance-team of een van diens gezinsleden toegestaan een direct of materieel indirect financieel belang in die entiteit te bezitten.
	Financiële belangen gehouden als trustee
V 910.6	Artikel V910.4 is van overeenkomstige toepassing op een financieel belang in een verantwoordelijke partij dat wordt gehouden door een trust ten aanzien waarvan de IT-auditeenheid of een persoon optreedt als trustee, tenzij: (a) geen van de navolgende personen een begunstigde is van de trust: de trustee, het lid van het assurance-team of een van diens gezinsleden, of de IT-auditeenheid; (b) het belang dat de trust in de verantwoordelijke partij bezit niet van materieel belang is voor de trust; (c) de trust geen aanmerkelijke invloed kan uitoefenen op de verantwoordelijke partij; en (d) geen van de navolgende personen aanmerkelijke invloed kan uitoefenen op beleggingsbeslissingen waarbij een financieel belang van de verantwoordelijke partij is betrokken: de trustee, het lid van het assurance-team of een van diens gezinsleden, of de IT-auditeenheid.
	Onbedoeld verkregen financiële belangen
V 910.7	Wanneer een IT-auditeenheid, een lid van het assurance-team of een van diens ge zinsleden een direct financieel belang of een materieel indirect financieel belang ver krijgt in een verantwoordelijke partij als gevolg van een erfenis, gift, fusie, of verge-
B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')	

Art./Par.	Omschrijving
	lijkbare omstandigheden en het anderszins niet toegestaan zou zijn het belang te be zitten op grond van deze sectie, dient: (a) het financieel belang, voor zover het is verkregen door de IT auditeenheid, onmiddellijk te worden afgestoten, en van een indirect financieel belang een groot genoeg deel daarvan dat het resterend belang niet langer materieel is; of (b) het financieel belang, voor zover het is verkregen door een lid van het assurance-team of een van zijn gezinsleden, door de persoon die het heeft verkregen onmiddellijk te worden afgestoten, en van een indirect financieel belang een groot genoeg deel daarvan dat het resterend belang niet langer materieel is.
	Financiële belangen – Overige situaties *Familieleden*
910.8 T1	Een bedreiging als gevolg van eigenbelang kan ontstaan wanneer een lid van het assurance-team weet dat een familielid een direct financieel belang of een materieel in direct financieel belang bezit in de verantwoordelijke partij.
910.8 T2	Factoren die relevant zijn bij het beoordelen van de omvang van de bedreiging zijn onder andere: • de aard van de relatie tussen het lid van het assurance-team en het familielid; • of er sprake is van een direct of een indirect financieel belang; • de materialiteit van het financieel belang van het familielid.
910.8 T3	Dergelijke bedreigingen als gevolg van eigenbelang kunnen onder meer ongedaan worden gemaakt door: • het familielid over te halen het gehele financiële belang zo snel mogelijk af te stoten dan wel zoveel van het indirecte financiële belang dat het resterende belang niet langer materieel is; • het verwijderen van het betreffende lid uit het assurance-team.
910.8 T4	Een bedreiging als gevolg van eigenbelang of intimidatie kan bijvoorbeeld ongedaan worden gemaakt door de werkzaamheden van het betreffende lid van het assurance team te laten beoordelen door een geschikte beoordelaar.
B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')	
Art./Par.	**Omschrijving**

910.8 T5	*Overige Personen* Een bedreiging als gevolg van eigenbelang kan ontstaan wanneer een lid van het as surance-team weet dat een van de volgende personen een financieel belang bezit in de verantwoordelijke partij: • partners en professionele werknemers van de IT-auditeenheid, naast degenen die het op grond van artikel R910.4 uitdrukkelijk niet is toegestaan dergelijke financiële belangen te bezitten, dan wel hun gezinsleden; • personen die een nauwe persoonlijke relatie onderhouden met een lid van het assurance-team.
910.8 T6	Een bedreiging als gevolg van eigenbelang kan onder meer worden geëlimineerd door het lid dat een nauwe persoonlijke relatie onderhoudt te verwijderen uit het assurance-team.
910.8 T7	Het ontstaan van een bedreiging als gevolg van eigenbelang kan onder meer worden voorkomen door: • het lid van het assurance-team uit te sluiten van belangrijke besluitvorming ten aanzien van de assurance-opdracht; • de werkzaamheden van het lid van het assurance-team laten te beoordelen door een geschikte beoordelaar.
Sectie 911	**LENINGEN EN GARANTSTELLINGEN** **Inleiding**
911.1	IT-auditeenheden zijn verplicht de fundamentele beginselen na te leven, onafhanke lijk te zijn en het in sectie 120 opgenomen conceptuele kader toe te passen teneinde bedreigingen voor de onafhankelijkheid te signaleren, evalueren en ongedaan te maken.
911.2	Een lening of een garantstelling voor een lening van een verantwoordelijke partij kan aanleiding geven tot een bedreiging als gevolg van eigenbelang. In deze sectie worden de specifieke vereisten en het toepassingsmateriaal omschreven die relevant zijn voor het in die situaties toepassen van het conceptuele kader.
	Vereisten en toepassingsmateriaal

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	**Omschrijving**
911.3 T1	Deze sectie bevat verwijzingen naar de "materialiteit" van een lening of garantstelling. Bij het vaststellen of een lening of garantstelling materieel is voor een persoon kan het netto vermogen van de betreffende persoon en van zijn gezinsleden in overweging worden genomen.
	Leningen en garantstellingen bij een verantwoordelijke partij

V 911.4	Een IT-auditeenheid, lid van het assurance-team of gezinsleden van dat lid mogen geen garantstelling of lening verstrekken aan een assurance-cliënt partij tenzij de le ning of garantstelling niet van materieel belang is voor zowel: (a) de IT-auditeenheid en de persoon die de lening of garantstelling ver strekken; als (b) de cliënt.
	Leningen en garantstellingen bij een verantwoordelijke partij die een bank of vergelijkbare instelling is
V 911.5	Een IT-auditeenheid, lid van het assurance-team of gezinsleden van dat lid mogen geen garantstelling of lening aanvaarden van een verantwoordelijke partij die een bank of vergelijkbare instelling is, tenzij de lening of garantstelling wordt verstrekt met inachtneming van de gebruikelijke procedures en tegen de gebruikelijke voor waarden.
911.5 T1	Voorbeelden van leningen zijn hypotheken, roodstandfaciliteiten, autoleningen en credit cardschulden.
911.5 T2	Ook als een IT-auditeenheid een lening verkrijgt van een verantwoordelijke partij die een bank of vergelijkbare instelling is, met inachtneming van de gebruikelijke procedures en tegen de gebruikelijke voorwaarden, kan de lening, indien deze van materi eel belang is voor zowel de verantwoordelijke partij als de IT-auditeenheid die de lening verkrijgt, desalniettemin een bedreiging als gevolg van eigenbelang vormen.
911.5 T3	Een bedreiging als gevolg van een eigenbelang kan bijvoorbeeld ongedaan worden gemaakt door de werkzaamheden te laten beoordelen door een geschikte beoordelaar die geen lid is van het assurance-team, van een ander onderdeel van het netwerk dat geen begunstigde is van de lening.
V 911.6	*Deposito of makelaarsrekening*

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')	
Art./Par.	**Omschrijving**
	Een IT-auditeenheid, lid van het assurance-team of gezinsleden van dat lid mogen geen deposito of makelaarsrekening aanhouden bij een verantwoordelijke partij die een bank, makelaar of vergelijkbare instelling is, tenzij de deposito of makelaarsrekening wordt aangehouden onder de gebruikelijke marktvoorwaarden.
	Leningen en garantstellingen van een verantwoordelijke partij die geen bank of ver gelijkbare instelling is.

V 911.7	Een IT-auditeenheid, lid van het assurance-team of naaste familieleden van dat lid mogen geen lening of garantstelling daarvoor aanvaarden van een verantwoordelijke partij die geen bank of vergelijkbare instelling is, tenzij de lening of garantstelling niet van materieel belang is voor zowel: (a) de IT-auditeenheid of de persoon die de lening of garantie ontvangt; als (b) de cliënt.
Sectie 920	**ZAKELIJKE RELATIES** **Inleiding**
920.1	IT-auditeenheden zijn verplicht de fundamentele beginselen na te leven, onafhankelijk te zijn en het in sectie 120 opgenomen conceptuele kader toe te passen teneinde bedreigingen voor de onafhankelijkheid te signaleren, evalueren en ongedaan te maken.
920.2	Een nauwe zakelijke relatie met een verantwoordelijke partij of diens management kan een bedreiging als gevolg van eigenbelang of intimidatie opleveren. In deze sec tie worden de specifieke vereisten en het toepassingsmateriaal omschreven die relevant zijn voor het in die situaties toepassen van het conceptuele kader.
	Vereisten en toepassingsmateriaal **Algemeen**
920.3 T1	Deze sectie bevat verwijzingen naar de "materialiteit" van een financieel belang en het "belang" van een zakelijke relatie. Bij het vaststellen of een financieel belang materieel is voor een persoon kan het netto vermogen van de betreffende persoon en van zijn gezinsleden in overweging worden genomen.
920.3 T2	Voorbeelden van een nauwe zakelijke relatie voortvloeiend uit een commerciële rela tie of gezamenlijk financieel belang zijn onder meer:
B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')	
Art./Par.	**Omschrijving**

	• het bezitten van een financieel belang in een joint venture met de assurance-cliënt of met een eigenaar met beschikkingsmacht, bestuurder of functionaris daarvan of met een ander persoon die managementtaken voor die cliënt uitvoert; • regelingen op grond waarvan een of meer diensten of producten van de IT-auditeenheid worden samengevoegd met een of meer diensten of producten van de cliënt en dit pakket gezamenlijk, on der de naam van beide partijen, op de markt wordt gebracht; • distributie of marketingregelingen op grond waarvan de IT auditeenheid de producten of diensten van de cliënt distribueert of op de markt brengt of de cliënt de producten of diensten van de IT-auditeenheid distribueert of op de markt brengt.
	Zakelijke relaties van de IT-auditeenheid, leden van het assurance-team of gezinsleden
V 920.4	Het is een IT-auditeenheid of een lid van het assurance-team niet toegestaan een nauwe zakelijke relatie te onderhouden met een assurance-cliënt of diens manage ment, met uitzondering van immateriële financiële belangen of wanneer de zakelijke relatie van geen belang is voor de cliënt c.q. diens management en de IT auditeenheid c.q. het lid van het assurance-team.
920.4 T1	Wanneer sprake is van een nauwe zakelijke relatie tussen de verantwoordelijke partij of diens management en de gezinsleden van een lid van het assurance-team kan een bedreiging als gevolg van eigenbelang of intimidatie ontstaan.
	Afname van goederen of diensten
920.5 T1	Het afnemen van goederen en diensten van een verantwoordelijke partij door een IT auditeenheid of een lid van het assurance-team of door een van de gezinsleden daar van vormt gewoonlijk geen bedreiging voor de onafhankelijkheid, mits de transactie plaatsvindt als onderdeel van de gewone bedrijfsuitoefening en tegen marktconforme voorwaarden. Dergelijke transacties kunnen echter van zodanige aard en omvang zijn dat zij toch een bedreiging als gevolg van zelfbelang kunnen vormen.
920.5 T2	Dergelijke bedreigingen als gevolg van eigenbelang kunnen onder andere worden voor komen door: • het elimineren of verkleinen van de omvang van de transactie;
B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')	
Art./Par.	**Omschrijving**
	• het verwijderen van het betreffende lid uit het assurance-team.
Sectie 921	**FAMILIE EN PERSOONLIJKE RELATIES** **Inleiding**

921.1	IT-auditeenheden zijn verplicht de fundamentele beginselen na te leven, onafhankelijk te zijn en het in sectie 120 opgenomen conceptuele kader toe te passen teneinde bedreigingen voor de onafhankelijkheid te signaleren, evalueren en ongedaan te maken.
921.2	Familie of persoonlijke relaties met personeel van de cliënt kunnen een bedreiging als gevolg van eigenbelang, vertrouwdheid of intimidatie vormen. In deze sectie worden de specifieke vereisten en het toepassingsmateriaal omschreven die relevant zijn voor het in die situaties toepassen van het conceptuele kader.
	Vereisten en toepassingsmateriaal **Algemeen**
921.3 T1	Indien sprake is van een familie of persoonlijke relatie tussen een lid van het assurance-team en een bestuurder of functionaris of, afhankelijk van hun functie, bepaal de werknemers van de assurance-cliënt, kan er een bedreiging als gevolg van eigenbelang, vertrouwdheid of intimidatie ontstaan.
921.3 T2	Factoren die relevant zijn bij het beoordelen van de omvang van de bedreiging zijn onder andere: • de taken die de betreffende persoon vervult in het assurance-team; • de functie die het gezins of familielid of ander persoon bekleedt bij de verantwoordelijke partij, en de aard van de relatie.
	Gezinsleden van een lid van het assurance-team
921.4 T1	Indien een gezinslid van een lid van het assurance-team een werknemer is die een functie bekleedt waarin deze aanzienlijke invloed kan uitoefenen op het object van de assurance-opdracht, kan er een bedreiging als gevolg van eigenbelang, vertrouwd- heid of intimidatie ontstaan.
921.4 T2	Factoren die relevant zijn bij het beoordelen van de omvang van dergelijke bedreigingen zijn onder andere: • de door het gezinslid beklede functie;

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')	
Art./Par.	**Omschrijving**
	• de door het lid van het assurance-team uitgevoerde taken.
921.4 T3	Een bedreiging als gevolg van een eigenbelang, vertrouwdheid of intimidatie kan on der meer worden geëlimineerd door het lid dat een nauwe persoonlijke relatie onderhoudt te verwijderen uit het assurance-team.

921.4 T4	Een voorbeeld van een handeling die kan dienen als waarborg tegen een bedreiging als gevolg van eigenbelang, vertrouwdheid of intimidatie is het zodanig inrichten van de taken van het assurance-team dat het lid van het assurance-team zich niet bezighoudt met zaken die ook tot de taken behoren van het gezinslid.
V 921.5	Een persoon kan geen deel uitmaken van het assurance-team wanneer een van de gezinsleden van die persoon: (a) een bestuurder of functionaris van de verantwoordelijke partij is; (b) in geval van een attestopdracht, een werknemer is die een functie bekleedt waarbij deze aanzienlijke invloed kan uitoefenen op de informatie over het onderzoeksobject; of (c) deze functie bekleedde gedurende de periode waarop de opdracht of de informatie over het onderzoeksobject betrekking heeft.
	Familieleden van een lid van het assurance-team
921.6 T1	Er ontstaat een bedreiging als gevolg van eigenbelang, vertrouwdheid of intimidatie wanneer een familielid van een lid van het assurance-team: (a) een bestuurder of functionaris van de verantwoordelijke partij is; of (b) een werknemer die een functie bekleedt waarbij deze aanzienlijke invloed kan uitoefenen op het onderliggende object of, in geval van een attestopdracht, op de informatie over het onderzoeksobject.
921.6 T2	Factoren die relevant zijn bij het beoordelen van de omvang van dergelijke bedreigingen zijn onder andere: • de aard van de relatie tussen het lid van het assurance-team en het familielid; • de door het familielid beklede functie; • de door het lid van het assurance-team uitgevoerde taken.

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	**Omschrijving**
921.6 T3	Een voorbeeld van een handeling waarmee een bedreiging als gevolg van eigenbe lang, vertrouwdheid of intimidatie ongedaan kan worden gemaakt, is het verwijderen van het lid uit het assurance-team.
921.6 T4	Een voorbeeld van een handeling die kan dienen als waarborg tegen een bedreiging als gevolg van eigenbelang, vertrouwdheid of intimidatie is het zodanig inrichten van de taken van het assurance-team dat het lid van het assurance-team zich niet bezig houdt met aangelegenheden die tot de verantwoordelijkheid behoren van het familielid.

	Overige nauwe relaties van een lid van het assurance-team
V 921.7	Een lid van het assurance-team dient overeenkomstig het beleid en de procedures van de IT-auditeenheid advies in te winnen wanneer deze een nauwe relatie onder houdt met een persoon die, hoewel geen gezinslid of familielid: (a) een bestuurder of functionaris is van de verantwoordelijke partij; of (b) een werknemer die een functie bekleedt waarbij deze aanzienlijke invloed kan uitoefenen op het onderliggende object of, in geval van een attestopdracht, op de informatie over het onderzoeksobject.
921.7 T1	Factoren die relevant zijn bij het beoordelen van de mate van een bedreiging als ge volg van eigenbelang, vertrouwdheid of intimidatie veroorzaakt door een dergelijke relatie zijn onder andere: o de aard van de relatie tussen de persoon en het lid van het assurance team; o de functie die deze persoon bekleedt bij de cliënt; o de door het lid van het assurance-team uitgevoerde taken.
921.7 T2	Een voorbeeld van een handeling waarmee een bedreiging als gevolg van eigenbelang, vertrouwdheid of intimidatie ongedaan kan worden gemaakt, is het verwijderen van het lid uit het assurance-team.
921.7 T3	Een voorbeeld van een handeling die kan dienen als waarborg tegen een bedreiging als gevolg van eigenbelang, vertrouwdheid of intimidatie is het zodanig inrichten van de taken van het assurance-team dat het lid van het assurance-team zich niet bezighoudt met aangelegenheden die tot de verantwoordelijkheden behoren van de persoon met wie het lid een nauwe relatie onderhoudt.
B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')	
Art./Par.	**Omschrijving**
	Relaties van partners en werknemers van de IT-auditeenheid
921.8 T1	Er kan een bedreiging als gevolg van eigenbelang, vertrouwdheid of intimidatie ont staan wanneer er sprake is van een persoonlijke of familierelatie tussen: (a) een partner of werknemer van de IT-auditeenheid die geen lid is van het assurance-team; en (b) elk van de volgende personen bij de verantwoordelijke partij: i. een bestuurder of functionaris; ii. een werknemer die een functie bekleedt waarbij deze aanzien lijke invloed kan uitoefenen op het onderliggende object of, in geval van een attestopdracht, op de informatie over het onderzoeksobject.

921.8 T2	Factoren die relevant zijn bij het beoordelen van de omvang van dergelijke bedreigingen zijn onder andere: o de aard van de relatie tussen de partner of werknemer van de IT auditeenheid en de bestuurder of functionaris of werknemer van de cliënt; o de mate van interactie tussen de partner of werknemer van de IT auditeenheid en het assurance-team; o de functie die de partner of werknemer bekleedt binnen de IT auditeenheid; o de functie die de persoon bekleedt bij de cliënt.
921.8 T3	Dergelijke bedreigingen als gevolg van eigenbelang, vertrouwdheid of intimidatie kunnen onder meer ongedaan worden gemaakt door: o de taken van de partner of werknemer zodanig te structureren dat elke potentiële invloed op de assurance-opdracht wordt verkleind; o de betreffende uitgevoerde assurance-werkzaamheden te laten beoor delen door een geschikte beoordelaar.
Sectie 922	**RECENT DIENSTVERBAND BIJ EEN VERANTWOORDELIJKE PARTIJ** **Inleiding**
922.1	IT-auditeenheden zijn verplicht de fundamentele beginselen na te leven, onafhankelijk te zijn en het in sectie 120 opgenomen conceptuele kader toe te passen teneinde bedreigingen voor de onafhankelijkheid te signaleren, evalueren en ongedaan te maken.
B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')	
Art./Par.	**Omschrijving**
922.2	Indien een lid van het assurance-team recentelijk als bestuurder of functionaris of werknemer in dienst was van de verantwoordelijke partij, kan er sprake zijn van een bedreiging als gevolg van eigenbelang, zelftoetsing of vertrouwdheid. In deze sectie worden de specifieke vereisten en het toepassingsmateriaal omschreven die relevant zijn voor het in die situaties toepassen van het conceptuele kader.
	Vereisten en toepassingsmateriaal **Dienstverband gedurende de periode waarop het assurance-rapport betrekking heeft**
V922.3	Van het assurance-team mogen geen personen deel uitmaken die gedurende de periode waarop het assurance rapport betrekking heeft: (a) een bestuurder of functionaris waren van de assurance-cliënt; of (b) een werknemer in een functie waarin deze aanzienlijke invloed konden uitoefenen op het onderzoeksobject of, in geval van een attestopdracht, op de informatie over het onderzoeksobject.

	Dienstverband voorafgaand aan de periode waarop het assurance-rapport betrekking heeft
922.4 T1	Er kan sprake zijn van een bedreiging als gevolg van eigenbelang, zelftoetsing of vertrouwdheid indien een lid van het assurance-team voorafgaand aan de periode waar op het assurance-rapport betrekking heeft: (a) een bestuurder of functionaris was van de assurance-cliënt; of (b) een werknemer die een functie bekleedde waarbij deze aanzienlijke invloed kon uitoefenen op het onderliggende onderzoeksobject of, in geval van een attestopdracht, op de informatie over het onder zoeksobject. Er kan bijvoorbeeld sprake zijn van een bedreiging indien een door deze persoon in de voorafgaande periode, toen hij nog in dienst was van de cliënt, genomen besluit of uitgevoerde werkzaamheden in de huidige periode worden geëvalueerd als onderdeel van de huidige assurance-opdracht.
922.4 T2	Factoren die relevant zijn bij het beoordelen van de omvang van dergelijke bedreigingen
B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')	
Art./Par.	**Omschrijving**
	zijn onder andere: • de functie die deze persoon bekleedde bij de cliënt; • de tijd die is verstreken sinds de persoon het dienstverband met de cli ent beëindigde; • de door het lid van het assurance-team uitgevoerde taken.
922.4 T3	Een voorbeeld van een handeling die kan dienen als waarborg tegen een bedreiging als gevolg van een eigenbelang, zelftoetsing of vertrouwdheid is het laten beoordelen van de werkzaamheden van het lid van het assurance-team door een geschikte be oordelaar.
Sectie 923	**BEKLEDEN VAN DE POSITIE VAN BESTUURDER OF FUNCTIONARIS BIJ EEN ASSURANCE CLI ENT** **Inleiding**
923.1	IT-auditeenheden zijn verplicht de fundamentele beginselen na te leven, onafhankelijk te zijn en het in sectie 120 opgenomen conceptuele kader toe te passen teneinde bedreigingen voor de onafhankelijkheid te signaleren, evalueren en ongedaan te maken.
923.2	Het bekleden van de positie van bestuurder of functionaris bij een assurance-cliënt kan aanleiding geven tot bedreigingen als gevolg van zelftoetsing en eigenbelang. In deze sectie worden de specifieke vereisten en het toepassingsmateriaal omschreven die relevant zijn voor het in die situaties toepassen van het conceptuele kader.

	Vereisten en toepassingsmateriaal **Bekleden van de positie van bestuurder of functionaris**
V 923.3	Een partner of werknemer van de IT-auditeenheid mag niet de positie bekleden van bestuurder of functionaris van een assurance-cliënt van de IT-auditeenheid.
	Bekleden van de positie van Vennootschappelijk Secretaris
V923.4	Een partner of werknemer van de IT-auditeenheid mag niet de positie bekleden van Vennootschappelijk Secretaris van een assurance-cliënt van de IT-auditeenheid, ten zij: (a) dit uitdrukkelijk is toegestaan op grond van het toepasselijk recht, de beroepsregels of in de praktijk;

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	Omschrijving
	(b) alle besluiten worden genomen door het management; én (c) de uitgevoerde taken en activiteiten zijn beperkt tot die van routinematige of administratieve aard, zoals het opstellen van notulen en bijhouden van wettelijke aangiften.
923.4 T1	De invulling van de positie van vennootschappelijk secretaris kan per rechtsgebied verschillen. Diens taken kunnen variëren van administratieve taken (zoals personeelsbeheer en het bijhouden van de boeken en gegevens van de onderneming) tot zulke diverse taken als toezien dat de onderneming zich houdt aan de toepasselijke regelgeving of het adviseren over corporate governance kwesties. Deze positie wordt gewoonlijk geacht een nauwe verbondenheid met de entiteit in te houden. Derhalve ontstaat er een bedreiging wanneer een partner of werknemer van de IT-auditeenheid de positie bekleedt van vennootschappelijk secretaris bij de verantwoordelijke partij. (Zie sectie 950, *Verlenen van non-assurancediensten aan een verantwoordelijke partij* voor meer informatie over het verlenen van non-assurancediensten aan een verantwoordelijke partij)
Sectie 924	**DIENSTVERBAND BIJ EEN VERANTWOORDELIJKE PARTIJ** **Inleiding**
924.1	IT-auditeenheden zijn verplicht de fundamentele beginselen na te leven, onafhankelijk te zijn en het in sectie 120 opgenomen conceptuele kader toe te passen teneinde bedreigingen voor de onafhankelijkheid te signaleren, evalueren en ongedaan te maken.
924.2	Een dienstverband bij een verantwoordelijke partij kan leiden tot een bedreiging als gevolg van eigenbelang, vertrouwdheid of intimidatie. In deze sectie worden de specifieke vereisten en het toepassingsmateriaal omschreven die relevant zijn voor het in die situaties toepassen van het conceptuele kader.

	Vereisten en toepassingsmateriaal **Algemeen**
924.3 T1	Een bedreiging als gevolg van vertrouwdheid of intimidatie kan ontstaan wanneer een van de volgende personen lid van het assurance-team of partner van de IT auditeenheid zijn geweest: • een bestuurder of functionaris van de verantwoordelijke partij; • een werknemer die een functie bekleedde waarin deze aanzienlijke

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')	
Art./Par.	**Omschrijving**
	invloed kon uitoefenen op het onderliggende onderzoeksobject of, in geval van een attestopdracht, op de informatie over het onderzoeksobject.
V 924.4	*Beperkingen ten aanzien van voormalige partners of leden van het assurance-team* Indien een voormalig partner in dienst is getreden bij een verantwoordelijke partij of in dien een voormalig lid van het assurance-team in dienst is getreden van de verantwoordelijke partij als: **(a)** bestuurder of functionaris; of **(b)** werknemer in een functie waarin deze aanzienlijke invloed kan uit oefenen op het onderzoeksobject of, in geval van een attestop dracht, op de informatie over het onderzoeksobject, is het deze persoon niet toegestaan deel te blijven nemen aan de onderneming of professionele diensten van de IT-auditeenheid.
924.4 T1	Ook als een van de personen als bedoeld in artikel V924.4 in een dergelijke functie in dienst is getreden bij de verantwoordelijke partij en niet langer deelneemt aan de onderneming of professionele diensten van de IT-auditeenheid, kan er desalniettemin een bedreiging als gevolg van vertrouwdheid of intimidatie ontstaan.
924.4 T2	Een dergelijke bedreiging als gevolg van vertrouwdheid of intimidatie kan eveneens ontstaan wanneer de voormalige partner van de IT-auditeenheid in dienst is getreden van een entiteit in een van de functies als bedoeld in artikel 924.3 A1 en deze entiteit wordt vervolgens een assurance-cliënt van de IT-auditeenheid.

924.4 T3	Factoren die relevant zijn bij het beoordelen van de omvang van dergelijke bedreigingen zijn onder andere: • de functie die deze persoon is gaan bekleden bij de cliënt; • of deze persoon op enigerlei wijze betrokken zal zijn bij het assurance team; • de tijd die is verstreken sinds de persoon lid was van het assurance team of een partner van de IT-auditeenheid; • de functie die de persoon bekleedde bij het assurance team of de IT-auditeenheid. Een voorbeeld hiervan is of de persoon verantwoordelijk was voor het onderhouden van periodiek contact met het management van de cliënt of met degenen die zijn belast met governance.

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	Omschrijving
924.4 T4	Voorbeelden van handelingen die kunnen dienen als waarborgen tegen het ontstaan van een bedreiging als gevolg van vertrouwdheid of intimidatie zijn: • het vaststellen van regelingen op grond waarvan deze persoon niet langer recht heeft op uitkeringen of betalingen van de IT auditeenheid, behoudens voor zover deze plaatsvinden op grond van eerder vastgestelde regelingen; • het vaststellen van regelingen op grond waarvan de aan deze per soon verschuldigde bedragen niet van materieel belang zijn voor de IT-auditeenheid; • aanpassen van het plan voor de assurance-opdracht; • het toevoegen aan het assurance-team van personen die beschik ken over afdoende ervaring vergeleken met de persoon die in dienst is getreden van de assurance-cliënt; • de werkzaamheden van het voormalig lid van het assurance-team laten beoordelen door een geschikte beoordelaar.
V 924.5	*Leden van het assurance-team die gesprekken aangaan met een assurance-cliënt over een mogelijk dienstverband* Een IT-auditeenheid dient beleidsmaatregelen en procedures vast te stellen op grond waarvan leden van het assurance-team verplicht zijn de IT-auditeenheid in kennis te stellen wanneer zij gesprekken aangaan met een verantwoordelijke partij over een mogelijk dienstverband.
924.5 T1	Er is sprake van een bedreiging als gevolg van eigenbelang wanneer een lid van het assurance-team betrokken is bij de uitvoering van de assurance-opdracht terwijl hij weet dat hij op enig moment in de toekomst een dienstverband met de assurance cliënt aangaat of zou kunnen aangaan.

924.5 T2	Een voorbeeld van een handeling waarmee een bedreiging als gevolg van eigenbelang ongedaan kan worden gemaakt, is het verwijderen van het lid uit het assurance-team.
924.5 T3	Een voorbeeld van een handeling die kan dienen als waarborg tegen een bedreiging als gevolg van eigenbelang is het laten beoordelen door een geschikte beoordelaar van belangrijke beslissingen van de betreffende persoon toen deze in het assurance-

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	Omschrijving
	team zat.
Sectie 940	**LANGDURIGE BETROKKENHEID VAN PERSONEEL BIJ EEN VERANTWOORDELIJKE PARTIJ** **Inleiding**
940.1	IT-auditeenheden zijn verplicht de fundamentele beginselen na te leven, onafhankelijk te zijn en het in sectie 120 opgenomen conceptueel kader toe te passen teneinde bedreigingen voor de onafhankelijkheid te signaleren, evalueren en ongedaan te maken.
940.2	Wanneer een persoon gedurende langere tijd betrokken is bij de uitvoering van een wederkerende assurance-opdracht, kunnen bedreigingen als gevolg van vertrouwdheid en eigenbelang ontstaan. In deze sectie worden de voorschriften en het toepassingsmateriaal besproken die relevant zijn voor het in dergelijke situaties toepassen van het conceptueel kader.
	Vereisten en toepassingsmateriaal **algemeen**
940.3 T1	Een bedreiging als gevolg van vertrouwdheid kan ontstaan als gevolg van de langdurige betrokkenheid van een persoon bij: (a) de verantwoordelijke partij; (b) het hogere management van de verantwoordelijke partij; of (c) het onderliggende onderzoeksobject of, met betrekking tot een at testopdracht, de informatie over het onderzoeksobject.
940.3 T2	Er kan een bedreiging als gevolg van eigenbelang ontstaan wanneer een persoon zich zorgen maakt over het verliezen van een langdurige relatie met een verantwoordelijke partij of van een belang bij het in stand houden van een nauwe persoonlijke relatie met een lid van het hogere management of met de met governance belaste personen. Dergelijke bedreigingen kunnen het oordeel van deze persoon nadelig beïnvloeden.

940.3 T3	Factoren die relevant zijn bij het beoordelen van de omvang van de bedreiging als gevolg van vertrouwdheid of eigenbelang zijn onder andere: • de aard van de assurance-opdracht; • de tijd dat de persoon deel heeft uitgemaakt van het assurance team, de senioriteit van die persoon binnen het team en de aard van de door hem vervulde taken, waaronder of de relatie al bestond
B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')	
Art./Par.	**Omschrijving**
	toen de persoon nog verbonden was aan een andere IT auditeenheid; • de mate waarin de taken van de persoon worden gestuurd, beoor deeld of gecontroleerd door het hogere kader; • de mate waarin het voor die persoon, gezien diens senioriteit, mo gelijk is invloed uit te oefenen op de uitkomst van de assurance opdracht, bijvoorbeeld door het nemen van belangrijke beslissin gen of het sturen van de werkzaamheden van andere leden van het team; • de aard van de persoonlijke relatie die de persoon onderhoudt met de verantwoordelijke partij of, indien relevant, het hogere management daarvan; • de aard, frequentie en omvang van de interactie tussen de persoon en de verantwoordelijke partij; • in hoeverre de aard of complexiteit van het onderliggende onderzoeksobject of de informatie over het onderzoeksobject gewijzigd is; • of er recentelijk wijzigingen zijn opgetreden in de perso(o)n(en) bij de verantwoordelijke partij die verantwoordelijk is/zijn voor het object of, met betrekking tot een attestopdracht, de informatie over het onderzoeksobject of, indien relevant, het hogere management.
940.3 T4	De omvang van de bedreigingen kunnen verder worden vergroot of verkleind door een combinatie van twee of meer factoren. Zo kunnen bedreigingen als gevolg van vertrouwdheid die na verloop van tijd ontstaan door de voortdurende nauwe relatie tussen een lid van het assurance-team en een persoon bij de assurance-cliënt die een positie bekleedt waarin deze aanzienlijke invloed kan uitoefenen op het onderzoeks object of, met betrekking tot een attestopdracht, de informatie over het onderzoeks object, verminderen door het vertrek van deze persoon bij de cliënt.
940.3 T5	Een bedreiging als gevolg van vertrouwdheid kan bijvoorbeeld ongedaan worden gemaakt door het terugtreden van het lid uit het assurance-team.
940.3 T6	Voorbeelden van handelingen die kunnen dienen als waarborgen tegen het ontstaan
B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')	

Art./Par.	Omschrijving
	van een bedreiging als gevolg van vertrouwdheid of eigenbelang zijn: • het wijzigingen van de rol die de persoon bekleedt in het assurance-team of de aard en diepgang van de door deze persoon uitgevoerde taken; • de uitgevoerde werkzaamheden van de betreffende persoon laten beoordelen door een geschikte beoordelaar, die geen onderdeel was van het assurance-team. • de opdracht regelmatig onderwerpen aan onafhankelijke interne of externe kwaliteitsbeoordelingen.
V 940.4	Indien een IT-auditeenheid besluit dat de omvang van de ontstane bedreigingen uitsluitend kan worden verkleind door de betreffende persoon tijdelijk te laten terugtreden uit het assurance-team, dient de IT-auditeenheid een gepaste termijn vast te stellen gedurende welke het deze persoon niet is toegestaan: (a) deel uit te maken van het opdrachtteam met betrekking tot de betreffende assurance-opdracht; (b) een kwaliteitscontrole uit te voeren ten aanzien van de assurance opdracht; of (c) rechtstreeks invloed uit te oefenen op de uitkomst van de assurance opdracht. Deze termijn dient voldoende lang te zijn om bedreigingen als gevolg van vertrouwdheid en eigenbelang te elimineren.
Sectie 950	**VERLENEN VAN NON-ASSURANCEDIENSTEN AAN VERANTWOORDELIJKE PARTIJEN** **Inleiding**
950.1	IT-auditeenheden zijn verplicht de fundamentele beginselen na te leven, onafhankelijk te zijn en het in sectie 120 opgenomen conceptuele kader toe te passen teneinde bedreigingen voor de onafhankelijkheid te signaleren, evalueren en ongedaan te maken.
950.2	IT-auditeenheden kunnen, afhankelijk van hun vakbekwaamheid en expertise, hun cliënten een uitgebreid pakket aan non-assurance diensten aanbieden. Het verlenen van bepaalde non-assurance diensten aan cliënten kan bedreigingen voor de naleving van de fundamentele beginselen en de onafhankelijkheid opleveren. In deze sectie worden de specifieke vereisten en het toepassingsmateriaal omschreven die relevant zijn voor het in die situaties toepassen van het conceptuele kader.

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	Omschrijving

	Vereisten en toepassingsmateriaal **Algemeen**
V 950.3	Voordat een IT-auditeenheid een opdracht voor het verlenen van non assurancediensten aan een verantwoordelijke partij aanvaardt, dient de IT auditeenheid vast te stellen of deze diensten een bedreiging voor de onafhankelijkheid kunnen vormen.
950.3 T1	De in deze sectie opgenomen voorschriften en het toepassingsmateriaal kunnen IT auditeenheden ondersteunen bij het analyseren van bepaalde non-assurancediensten en de bedreigingen die in verband daarmee kunnen ontstaan wanneer een IT-auditeenheid non-assurancediensten verleent aan een verantwoordelijke partij.
950.3 T2	Nieuwe ondernemingspraktijken, doorlopende veranderingen op de financiële mark ten en wijzigingen in IT zijn slechts enkele factoren waardoor het niet mogelijk is een uitputtende lijst op te stellen van alle non-assurancediensten die aan een verantwoordelijke partij kunnen worden verleend. Deze Code omvat derhalve geen uitput tende lijst van alle non-assurancediensten die aan een verantwoordelijke partij kunnen worden verleend.
950.4 T1	*Beoordeling van bedreigingen* Bij het beoordelen van de omvang van bedreigingen die ontstaan door het verlenen van non-assurancediensten aan een verantwoordelijke partij zijn onder meer de volgende factoren van belang: • de aard, reikwijdte en het doel van de dienstverlening; • in hoeverre wordt vertrouwd op de uitkomst van de verleende dienst als onderdeel van de assurance-opdracht; • de wet en regelgevende omgeving waarin de dienstverlening plaatsvindt; • of de uitkomst van de verleende dienst invloed heeft op het onderzoeksobject en, ten aanzien van een attestopdracht, onderwerpen waarop de informatie over het onderzoeksobject van de assurance opdracht betrekking heeft, en indien dit het geval is:

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')	
Art./Par.	**Omschrijving**

	○ in hoeverre de uitkomst van de verleende dienst materiële of aanmerkelijke invloed heeft op het onderliggende onderzoeks object en, ten aanzien van een attestopdracht, de informatie over het onderzoeksobject; ○ de mate van betrokkenheid van de verantwoordelijke partij bij het vaststellen van wezenlijke zaken waarop het oordeel be trekking heeft; • de mate van expertise van het management en de werknemers van de verantwoordelijke partij ten aanzien van de soort verleende diensten.
	Materialiteit ten aanzien van de informatie van een verantwoordelijke partij
950.4 T2	Het concept van materialiteit ten aanzien van informatie over het onderzoeksobject wordt besproken in de Richtlijnen 3000A en 3000D. Het vaststellen van materialiteit betreft professionele oordeelsvorming en wordt mede bepaald door kwantitatieve en kwalitatieve factoren. Andere bepalende factoren zijn de ideeën over de financiële of andere informatiebehoeften van gebruikers.
	Levering meerdere non-assurancediensten aan één verantwoordelijke partij
950.4 T3	Een IT-auditeenheid kan aan een verantwoordelijke partij meerdere non assurancediensten verlenen. In die situatie is de samenloop van de bedreigingen die worden gevormd door dergelijke dienstverlening relevant voor de evaluatie van de bedreigingen door de IT-auditeenheid.
950.5 T1	*Terugbrengen van bedreigingen* In artikel 120.10 T2 wordt een beschrijving gegeven van de waarborgen. Ten aanzien van het verlenen van non-assurancediensten aan verantwoordelijke partijen wordt onder waarborgen verstaan handelingen die een IT-auditeenheid afzonderlijk of ge combineerd verricht om bedreigingen voor de onafhankelijkheid tot een aanvaardbaar niveau terug te brengen. Dergelijke waarborgen kunnen mogelijk niet in alle gevallen waarin een bedreiging ontstaat door het verlenen van een dienst aan een verantwoor delijke partij worden gegeven. In die gevallen dient de IT-auditeenheid, gezien het in sectie 120 bedoelde conceptuele kader, af te zien van het verlenen van de non-assurancedienst of de assurance-opdracht, of deze te beëindigen.
B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')	
Art./Par.	**Omschrijving**

V 950.6	*Verbod op het aanvaarden van bestuursverantwoordelijkheden* Het is een IT-auditeenheid niet toegestaan bestuursverantwoordelijkheid te aanvaar den ten aanzien van het onderliggende object en, ten aanzien van een attestopdracht, de door de IT-auditeenheid verstrekte informatie over het onderzoeksobject. Indien de IT-auditeenheid, als onderdeel van een andere aan de verantwoordelijke partij verleende dienst, bestuursverantwoordelijkheid aanvaardt, dient de IT-auditeenheid ervoor zorg te dragen dat deze verantwoordelijkheid niet ziet op het onderliggende object en, ten aanzien van een attestopdracht, de door de IT-auditeenheid verstrekte informatie over het onderzoeksobject.
950.6 T1	Tot bestuursverantwoordelijkheden behoren het toezicht houden op, leiding geven aan en sturen van een entiteit, en het nemen van besluiten ten aanzien van de aanschaf, inzet en het toezicht op personele, financiële, materiële en immateriële midd len.
950.6 T2	Door bestuursverantwoordelijkheid te aanvaarden als onderdeel van het verlenen van een non-assurancedienst aan een verantwoordelijke partij ontstaan bedreigingen als gevolg van zelftoetsing en eigenbelang. Ten aanzien van het verlenen van een met het onderliggende object verband houdende dienst en, ten aanzien van een attest opdracht, de door de IT-auditeenheid verstrekte informatie over het onderzoeksobject, ontstaat door het aanvaarden van bestuursverantwoordelijkheid een bedreiging als gevolg van vertrouwdheid en mogelijk een bedreiging als gevolg van belangenbehartiging, aangezien de IT-auditeenheid te nauw verbonden raakt aan de standpunten en belangen van het bestuur.
950.6 T3	Bij het vaststellen of een activiteit een bestuursverantwoordelijkheid vormt, dienen de omstandigheden van het geval in overweging te worden genomen, waarvoor een professioneel oordeel is vereist. Voorbeelden van activiteiten die tot bestuursverantwoordelijkheden gerekend kunnen worden zijn: • het vaststellen van het beleid en de strategische richting; • het aannemen of ontslaan van werknemers; • het sturen van en verantwoordelijkheid aanvaarden voor de hande lingen van werknemers ten aanzien van de door hen voor de enti teit verrichte werkzaamheden; • het goedkeuren van transacties;

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	Omschrijving
	• het toezicht houden op of beheren van bankrekeningen of investerin gen; • het besluiten welke aanbevelingen van de IT-auditeenheid of van der den overgenomen moeten worden; • het rapporteren aan degenen die namens het bestuur zijn belast met governance; • het nemen van verantwoordelijkheid voor het vaststellen, uitvoe ren, bewaken en in stand houden van interne beheersmaatregelen.

950.6 T4	Het adviseren en doen van aanbevelingen teneinde het bestuur van de verantwoorde lijke partij bij te staan bij het uitvoeren van diens verantwoordelijkheden wordt niet beschouwd als aanvaarding van bestuursverantwoordelijkheid (Ref: art. V950.6 tot en met 950.6 T3).
V 950.7	Om bij het verlenen van non-assurancediensten aan een assurance-cliënt die verband houden met het onderliggende object en, ten aanzien van een attestopdracht, de in formatie over het onderzoeksobject, de aanvaarding van bestuursverantwoordelijk heid te vermijden, dient de IT-auditeenheid naar tevredenheid vast te stellen dat alle oordelen en besluiten die deel uitmaken van de bestuursverantwoordelijkheid worden genomen door het bestuur van de assurance-cliënt. Hierbij dient erop te worden toe gezien dat het bestuur van de assurance-cliënt: **(a)** een persoon aanstelt die beschikt over voldoende vakbekwaam heid, kennis en ervaring om te allen tijde verantwoordelijkheid te kunnen nemen voor de besluiten van de cliënt en toezicht te hou den op de diensten. Deze persoon, die bij voorkeur een lid van het bestuur is, dient inzicht te hebben in: **(i)** de doelstellingen, aard en resultaten van de diensten; en **(ii)** de respectievelijke verantwoordelijkheden van de cliënt en de IT auditeenheid. Deze persoon hoeft echter niet te beschikken over de vakbe kwaamheid om deze diensten zelf (opnieuw) uit te voeren; **(b)** toezicht houdt op de dienstverlening en beoordeelt of de verleende diensten beantwoorden aan het door de cliënt gestelde doel; en
B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')	
Art./Par.	**Omschrijving**
	(c) verantwoordelijkheid aanvaardt voor de eventueel naar aanleiding van de resultaten van de verleende diensten te verrichten handelin gen.

950.8 T1	*Overige overwegingen ten aanzien van het verlenen van specifieke non assurancediensten* Er kan een bedreiging als gevolg van zelftoetsing ontstaan wanneer, ten aanzien van een assurance-opdracht, de IT-auditeenheid betrokken is bij het opstellen van infor matie over een object dat vervolgens informatie over het onderzoeksobject wordt. Voorbeelden van non-assurancediensten als gevolg waarvan bij het verlenen van diensten met betrekking tot de informatie over het onderzoeksobject dergelijke be dreigingen als gevolg van zelftoetsing kunnen ontstaan zijn: (a) het ontwikkelen en opstellen van mogelijke informatie en het ver volgens verstrekken van een assurance-rapport over deze informa tie; (b) het uitvoeren van een waardering met betrekking tot of die deel uitmaakt van de informatie over het onderzoeksobject.
Sectie 990	**ASSURANCE-RAPPORTEN WAARIN EEN GEBRUIKS EN VERSPREIDINGSBEPERKING IS OPGENOMEN** **Inleiding**
990.1	IT-auditeenheden zijn verplicht de fundamentele beginselen na te leven, onafhanke lijk te zijn en het in sectie 120 opgenomen conceptuele kader toe te passen teneinde bedreigingen voor de onafhankelijkheid te signaleren, evalueren en ongedaan te ma ken.
990.2	Deze sectie bevat bepaalde uitzonderingen op deel 4B die van toepassing zijn in be paalde situaties waarin in het rapport dat naar aanleiding van een assurance opdracht is opgesteld bepaalde gebruiks en verspreidingsbeperkingen zijn opgeno men. In deze sectie wordt een opdracht waarbij in de situaties als bedoeld in art. R990.3 beperkingen worden opgelegd aan het gebruik en de verspreiding van het as-surance-rapport aangeduid als een "in aanmerking komende assurance-opdracht."
	Vereisten en toepassingsmateriaal **Algemeen**
V 990.3	Wanneer een IT-auditeenheid voornemens is een rapport uit te brengen van een as-
B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')	
Art./Par.	**Omschrijving**

	surance-opdracht waarin een beperking op het gebruik en de distributie is opgeno men, dienen voor de in dit deel geoorloofde aanpassingen de onafhankelijkheidseisen als bedoeld in deel 4B in aanmerking te worden genomen, maar uitsluitend voor zo ver: a) de IT-auditeenheid de beoogde gebruikers van het rapport wijst op de aangepaste onafhankelijkheidseisen die op het verlenen van de dienst van toepassing zijn; en b) de beoogde gebruikers van het rapport inzicht hebben in het doel, de informatie over het object en de in het rapport opgelegde beper kingen en uitdrukkelijk met de aanpassingen akkoord gaan.
990.3 T1	De beoogde gebruikers van het rapport kunnen inzicht verkrijgen in het doel, de in formatie over het object en de beperkingen van het rapport door direct of indirect via een vertegenwoordiger die bevoegd is namens de beoogde gebruikers op te treden, betrokken te worden bij het vaststellen van de aard en de reikwijdte van de opdracht. Deze betrokkenheid helpt de IT-auditeenheid in ieder geval de beoogde gebruikers in kennis te stellen van de onafhankelijkheidseisen, zoals de voor de toepassing van het conceptuele kader relevante omstandigheden. Dit stelt de IT-auditeenheid tevens in staat het akkoord van de beoogde gebruikers te verkrijgen voor de aangepaste onafhankelijkheidseisen.
V 990.4	Voor zover de beoogde gebruikers een groep gebruikers is die op het moment van het vaststellen van de voorwaarden van de opdracht niet bij name geïdentificeerd kunnen worden, dient de IT-auditeenheid deze gebruikers vervolgens op de hoogte te stellen van de met hun vertegenwoordiger overeengekomen aangepaste onafhankelijkheidseisen.
990.4 T1	Voor zover de beoogde gebruikers bijvoorbeeld een groep gebruikers is zoals geld verstrekkers die deel uitmaken van een syndicaat, kan de IT-auditeenheid de aange paste onafhankelijkheidseisen omschrijven in een opdrachtbrief gericht aan de verte genwoordiger van de geldverstrekkers. De vertegenwoordiger kan deze opdrachtbrief vervolgens doen toekomen aan de leden van het syndicaat om zo te voldoen aan het voorschrift van de IT-auditeenheid dat de gebruikers op de hoogte moeten worden gesteld van de met de vertegenwoordiger overeengekomen aangepaste onafhankelijkheidseisen.
B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')	
Art./Par.	**Omschrijving**
V 990.5	Wanneer de IT-auditeenheid een in aanmerking komende assurance-opdracht uit voert, dienen de aanpassingen van deel 4B beperkt te worden tot de in artikel V 990.7 en V990.8 vermelde aanpassingen.
V 990.6	Indien de IT-auditeenheid tevens een assurance-rapport verstrekt dat ten aanzien van dezelfde cliënt geen beperking bevat op het gebruik en de verspreiding, dient de IT-auditeenheid deel 4B op die assurance-opdracht toe te passen.

	Financiële belangen, leningen en garantstellingen, nauwe zakelijke, familie of persoonlij ke relaties
V 990.7	Wanneer de IT-auditeenheid een in aanmerking komende assurance-opdracht uit voert: a) hoeven de relevante bepalingen van sectie 910, 911, 920, 921, 922 en 924 uitsluitend te worden toegepast op de leden van het op drachtteam en hun gezinsleden en familieleden; b) dient de IT-auditeenheid bedreigingen voor de onafhankelijkheid vast te stellen, te evalueren en te elimineren die ontstaan door de in sectie 910, 911, 920, 921, 922 en 924 bedoelde belangen en relaties tussen de verantwoordelijke partij en de volgende leden van het as surance-team: (i) degenen die adviseren over technische of sectorspecifieke zaken, transacties of gebeurtenissen; en (ii) degenen die verantwoordelijk zijn voor de kwaliteitscontrole van de opdracht, inclusief degene die de kwaliteitscontrole beoordeelt; en c) dient de IT-auditeenheid alle bedreigingen te evalueren en te elimi neren waarvan het opdrachtteam reden heeft om aan te nemen dat deze zijn ontstaan als gevolg van de belangen van en relaties tussen de verantwoordelijke partij en anderen binnen de IT-auditeenheid die rechtstreeks invloed kunnen uitoefenen op de uitkomst van de assu rance-opdracht, zoals bedoeld in sectie 910, 911, 920, 921, 922 en 924.
990.7 T1	Tot de anderen binnen de IT-auditeenheid die rechtstreeks invloed kunnen uitoefenen op de uitkomst van de assurance-opdracht behoren zij die aanbevelingen doen over de vergoeding en degenen die rechtstreeks toezicht uitoefenen op de engage ment partner van in het kader van de uitvoering van de assurance-opdracht bij een verantwoordelijke partij.

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	Omschrijving
V 990.8	De IT-auditeenheid mag, wanneer het een in aanmerking komende assurance opdracht uitvoert, geen materieel direct of een materieel indirect financieel belang bezitten in de verantwoordelijke partij.
	DEFINITIES, INCLUSIEF LIJST VAN AFKORTINGEN

	Aansporing: een financieel belang via een collectief investeringsvehikel, boedel of trust of een andere tussenpersoon op de beleggingsbeslissingen waarvan de betref fende persoon of entiteit geen invloed kan uitoefenen. Een voorwerp, situatie of han deling dat of die wordt aangewend om invloed uit te oefenen op het gedrag van an deren, doch niet noodzakelijkerwijs met de bedoeling om dat gedrag op oneigenlijke wijze te beïnvloeden. Aansporingen kunnen variëren van onschuldige vormen van gastvrijheid tussen zake lijke collega's (voor interne IT-auditors), of tussen IT-auditors en bestaande of po tentiële cliënten (voor IT-auditors), tot handelingen die kunnen leiden tot schending van wet of regelgeving. Een aansporing kan verschillende vormen aannemen, zoals: • Geschenken. • Gastvrijheid. • Entertainment. • Politieke giften of giften aan liefdadigheid. • Beroep doen op vriendschap of loyaliteit. • Het aanbieden van een dienstverband of andere za kelijke mogelijkheden. • Voorkeursbehandeling, voorrechten of privileges.
	Aanvaardbaar niveau: een niveau waarop de IT-auditor, onder toepassing van de objectieve, redelijke en geïnformeerde derde partijtoets, waarschijnlijk tot het oordeel zal komen dat de fundamentele beginselen zijn nageleefd.

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	Omschrijving
	Adverteren: bekendmakingen van IT-auditors van informatie over de diensten die zij verlenen en de vakbekwaamheden waarover zij beschikken met het oog op het ver krijgen van professionele opdrachten.
	Assurance-cliënt: de verantwoordelijke partij alsmede, ten aanzien van een attestop dracht, de partij die verantwoordelijkheid aanvaardt voor de informatie over het on derzoeksobject (en die dezelfde als de verantwoordelijke partij kan zijn).
	Assurance-opdracht: een opdracht waarbij een IT-auditor ernaar streeft voldoende deugdelijk bewijs te verkrijgen om een conclusie te kunnen verstrekken gericht op het vergroten van het vertrouwen van de beoogde gebruikers, uitgezonderd de verantwoordelijke partij, in de informatie over het object. In de Richtlijn 3000 (A en D) worden de elementen en doelstellingen omschreven van een op basis van die standaard uitgevoerde assurance-opdracht; het Stramien geeft een algemene omschrijving van assurance-opdrachten waarop de Richtlijnen zijn gebaseerd. In deel 4B wordt de term 'assurance-opdracht' gebruikt voor assurance-opdrachten.

	Assurance-team: (a) Alle leden van het opdracht-team dat de assurance opdracht uitvoert;` (b) Alle anderen binnen de IT-auditeenheid die rechtstreeks invloed kun nen uitoefenen op de uitkomst van de assurance-opdracht, waar onder: (I) degenen die aanbevelingen doen over de vergoeding en dege nen die rechtstreeks toezicht houden op de assurance opdrachtpartner in het kader van de uitvoering van de as surance-opdracht; (II) degenen die worden geconsulteerd over technische of sector specifieke zaken, transacties of gebeurtenissen; en (III) degenen die verantwoordelijk zijn voor de kwaliteitscontrole van de opdracht, inclusief degene die de kwaliteitscontrole beoordeelt.

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	Omschrijving
	Attest-opdracht: een assurance-opdracht waarbij een andere partij dan de IT-auditor het onderzoeksobject meet of evalueert ten opzichte van de criteria. Deze partij geeft ook vaak de resulterende informatie over het onderzoeksobject weer in een rapport of een overzicht. In bepaalde gevallen kan de informatie over het onderzoeksobject echter door de IT-auditor in het assurance-rapport worden weergegeven. Bij een at test-opdracht is de conclusie van de IT-auditor gericht op de vraag of de informatie over het onderzoeksobject geen afwijking van materieel belang bevat. De conclusie van de IT-auditor kan betrekking hebben op: i. Het onderzoeksobject en de van toepassing zijnde criteria; ii. De informatie over het onderzoeksobject en de van toepassing zijnde criteria; of iii. Een overzicht dat door de geschikte partij is gemaakt.
	Bedreigingen: zie betekenis in art. 120.6 T3 en omvat de volgende categorieën: ei genbelang, zelftoetsing, belangenbehartiging, vertrouwdheid en intimidatie.
	Beoogde IT-auditor: een IT-auditor die overweegt een assurance-opdracht of op dracht voor het verlenen van audit, advies of vergelijkbare professionele diensten te aanvaarden van een potentiële cliënt (of, in bepaalde gevallen, van een bestaande client).
	Bestuurder of functionaris: degenen die zijn belast met het bestuur van een entiteit, of die handelen in een vergelijkbare hoedanigheid, ongeacht hun titel, welke per rechtsgebied anders kan zijn.
	Cliënt: de natuurlijke persoon of rechtspersoon die, anders dan in het kader van een gezagsverhouding, aan een IT-auditor opdracht geeft tot het verrichten van een professionele dienst.
	Conceptueel kader: zie betekenis in sectie 120.

	Criteria: de benchmarks waartegen het object wordt gemeten of geëvalueerd. De "toepasselijke criteria" zijn de criteria die op de betreffende opdracht van toepassing zijn.
	Direct financieel belang: een financieel belang: (a) dat direct wordt gehouden of waarover de beschikkingsmacht direct wordt uitgeoefend door een persoon of entiteit (inclusief indien op discretionaire basis beheerd door anderen); of (b) dat het economisch eigendom is via een collectief investeringsvehikel, boedel of trust of andere tussenpersoon waarover de beschikkingsmacht wordt uitgeoefend door de persoon of entiteit, of op de beleggingsbeslissingen waarvan deze invloed kunnen uitoefenen.
	Directe opdracht: een assurance-opdracht in het kader waarvan een partij, niet zijnde de IT-auditor, het object meet of evalueert op basis van de criteria en de IT-auditor de resulterende informatie ten aanzien van het onderwerp verstrekt als onderdeel van of bijlage bij het assurance-rapport. In een directe opdracht heeft de conclusie van de IT-auditor betrekking op de weergegeven uitkomst van de waardering of evaluatie van het object afgezet tegen de criteria.
	Externe deskundige: een persoon (uitgezonderd een partner of medewerker, inclusief tijdelijke arbeidskrachten, van de IT-auditeenheid of een netwerk) of organisatie die beschikt over vakbekwaamheid, kennis en ervaring op een ander terrein dan de assurance-werkzaamheden en van wiens activiteiten op dat gebied gebruik wordt gemaakt om de IT-auditor behulpzaam te zijn bij het verkrijgen van voldoende geschikt bewijs.
	Familielid: een ouder, kind of broer/zus die geen gezinslid is.
	Filiaal: een onderscheiden subgroep, georganiseerd naar geografie of praktijk.
	Financieel belang: een belang in het vermogen of in andere effecten, schuldbrieven, leningen of andere schuldinstrumenten van een entiteit, inclusief rechten en verplichtingen tot het verkrijgen van dergelijk belang en rechtstreeks op dat belang betrekking hebbende derivaten.

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	Omschrijving

	Fundamentele beginselen: zie betekenis in art. 110.1 A1. Elk van deze fundamentele beginselen wordt vervolgens nader omschreven in de betreffende artikelen: Integriteit en Objectiviteit (111) Vakbekwaamheid en Zorgvuldigheid (112)
B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')	
Art./Par.	**Omschrijving**
	Vertrouwelijkheid en (113) Professioneel Gedrag (114)
	Geschikte beoordelaar: een beroepsbeoefenaar die beschikt over de benodigde ken nis, vakbekwaamheid, ervaring en bevoegdheid om op objectieve wijze de betreffen de uitgevoerde werkzaamheden of verleende diensten te beoordelen. Deze persoon kan een IT-auditor zijn.
	Gezinslid: een echtgeno(o)t(e) (of daarmee vergelijkbare partner) of (financieel) af hankelijke (bijvoorbeeld: kinderen).
	In aanmerking komende assurance-opdracht: heeft voor toepassing van sectie 990 de betekenis gegeven in art. 990.2.
	Indirect financieel belang: een financieel belang via een collectief investeringsvehikel, boedel of trust of een andere tussenpersoon op de beleggingsbeslissingen waarvan de betreffende persoon of entiteit geen invloed kunnen uitoefenen.
	Informatie over het onderzoeksobject: de informatie die het resultaat is van het toe passen van de criteria op het onderzoeksobject, dat wil zeggen de uitkomst van de meting of evaluatie van het onderzoeksobject ten opzichte van de criteria.
	Interne IT-auditor: de IT-auditor die werkzaam is bij of verbonden is aan een IT auditafdeling.
	IT-auditafdeling: de organisatorische eenheid, die behoort tot een onderneming, een instelling of de overheid en de daarmee gelijk te stellen dienst, waarbij één of meer IT-auditors werkzaam zijn die binnen die onderneming, instelling of overheid en daarmee gelijk te stellen dienst verbijzonderde toetsende activiteiten verrichten, waaronder begrepen onderzoek naar en de evaluatie en bewaking van de toereikendheid en effectiviteit van de administratieve organisatie en interne beheersing van de IT (processen).

	IT-auditeenheid: 1) een individuele IT-auditor, IT-auditmaatschap of IT auditkantoor; 2) een entiteit die de zeggenschap uitoefent over deze

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')	
Art./Par.	**Omschrijving**
	partijen, door het bezit of het beheer ervan of op ande re wijze; en 3) een entiteit die onder de zeggenschap staat van deze partijen, door het bezit of het beheer ervan of op ande re wijze. In artikel 900.3 wordt toegelicht hoe de term "IT-auditeenheid" wordt gebruikt om de verantwoordelijkheid van IT-auditors en IT-auditkantoren aan te geven in verband met de naleving van 4B.
	IT-auditor: een persoon die lid is van een bij de IFAC aangesloten of geassocieerde orga nisatie, zoals de NOREA in Nederland. In deel 1 verwijst de term "IT-auditor" naar individuele interne IT-auditors en naar IT auditors en hun praktijk. In Deel 4B verwijst de term "IT-auditor" naar IT-auditors en hun praktijk.
	IT-auditor in openbare praktijk: een IT-auditor, ongeacht zijn functionele aanduiding (zoals assurance-opdrachten, IT-onderzoek of advies) werkzaam in een IT-auditeenheid die professionele diensten verleent. De term "IT-auditor" verwijst tevens naar een IT auditeenheid van IT-auditors.
	IT-auditkantoor: hieronder wordt verstaan: de organisatorische eenheid waarbij een IT auditor werkzaam is of waaraan een IT-auditor verbonden is en waarbinnen één of meer IT-auditors voor een cliënt bedrijfsmatig professionele diensten verrichten, bestaande uit assurance-opdrachten of aan assurance verwante opdrachten en eventueel overige op drachten.
	IT-auditpraktijk: het IT-auditkantoor**.**
	Kan: deze term wordt in de Code gebruikt om toestemming voor een bepaalde han deling in bepaalde omstandigheden aan te geven, inclusief als afwijking op een voor schrift. Het wordt niet gebruikt om een mogelijkheid aan te geven.
	Met Governance belaste persoon: de perso(o)n(en) of organisatie(s) (bijvoorbeeld een zakelijke trustee) die verantwoordelijkheid is/zijn voor het uitoefenen van toezicht op de strategische richting van de entiteit en de verantwoordingsplicht van de entiteit. Dit omvat tevens het toezicht op het financiële rapportageproces. In sommige rechtsgebieden

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	Omschrijving
	kunnen ten aanzien van bepaalde entiteiten tot de met governance belaste personen ook bestuursleden behoren, zoals uitvoerende leden van het bestuur van een private sector organisatie of organisatie van openbaar belang of een eigenaar-directeur.
	Nauwe persoonlijke relatie: gezinslid of een persoon met wie intensief sociaal contact bestaat.
	Netwerk: een overkoepelende structuur: • gericht op samenwerking; en • die duidelijk is gericht op winst of kostendeling of gemeenschappelijk aandelenbezit, zeggenschap of bestuur, gezamenlijk beleid en procedures met betrekking tot kwaliteitsbeheersing, gezamenlijke bedrijfsstrategieën, een gemeenschappelijke merknaam of het delen van een aanzienlijk deel van bedrijfsmiddelen.
	Netwerkonderdeel: een IT-auditeenheid of andere entiteit die behoort tot een net werk. Voor meer informatie, zie art. 400.50 A1 tot en met 400.54 A1.
	Onafhankelijkheid: onafhankelijkheid omvat: (a) Onafhankelijkheid in wezen – De geesteshouding die het tot uit drukking brengen van een conclusie toestaat zonder beïnvloed te worden door invloeden die professionele oordeelsvorming in ge vaar brengen, waardoor een individu met integriteit kan handelen, alsmede objectiviteit en een professioneel-kritische instelling kan uitoefenen. (b) Onafhankelijkheid in schijn – Het vermijden van feiten en omstan digheden die dermate significant zijn dat een objectieve, redelijke en geïnformeerde derde partij waarschijnlijk zou concluderen, alle feiten en omstandigheden afwegend, inclusief toegepaste maatre gelen, dat de integriteit, objectiviteit of professioneel-kritische in stelling van een IT-auditeenheid of van een lid van het assurance team in gevaar is gebracht. Waar in artikel 900.4 wordt verwezen naar de "onafhankelijkheid" van een persoon of

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	Omschrijving
	IT-auditeenheid, betekent dit dat die persoon of die IT-auditeenheid voldoet aan de bepalingen van deel 4B.
	Onderzoeksobject: datgene dat wordt gewaardeerd of geëvalueerd door het toepassen van criteria.
	Opdrachtgerichte kwaliteitsbeoordeling (OKB): een procedure met als doel om bij of voorafgaand aan de verstrekking van het rapport een objectieve evaluatie te geven van de wezenlijke oordelen van het opdrachtteam en de conclusies die het heeft ge trokken bij het opstellen van het rapport.

	Opdrachtperiode: een opdrachtperiode vangt aan op het moment waarop het assurance team begint met het uitvoeren van de assurance-taken met betrekking tot de betreffende opdracht. De opdrachtperiode eindigt op het moment waarop het assurance-rapport wordt uitgebracht. Wanneer de opdracht van wederkerende aard is, eindigt deze op het moment waarop een der partijen de andere partij in kennis stelt dat deze de professionele relatie beëindigt of bij het uitbrengen van het laatste assurance-rapport, afhankelijk welk moment later is.
	Opdrachtpartner: de partner of een ander persoon van de IT-auditeenheid die ver antwoordelijk is voor de opdracht en de uitvoering daarvan en voor het namens de IT-auditeenheid uit te brengen rapport en aan wie, voor zover voorgeschreven, door een beroepsorganisatie, gerechtelijke instantie of toezichthouder de noodzakelijke bevoegdheid is verleend.
	Opdrachtteam: alle partners en medewerkers die de opdracht uitvoeren en alle perso nen die zijn aangesteld door de IT-auditeenheid of een netwerk die de assurance procedures voor de opdracht uitvoeren. Hiertoe behoren niet de door de IT auditeenheid of een netwerk aangestelde externe deskundigen. De term "opdrachtteam" omvat evenmin personen binnen de interne Audit Functie van de cliënt die rechtstreeks ondersteuning (direct assistance) verlenen bij een assuran ce-opdracht, voor zover de externe IT-auditor voldoet aan de vereisten van Handrei king 610 (gebruikmaken van het werk van de Interne Audit Functie). Noot: deze handreiking is ten tijde van de publicatie van de Code (juli 2021) nog niet definitief opgesteld binnen het kader van NOREA. Derhalve is dit nog niet van toepassing. Deze noot wordt verwijderd zodra de Handreiking 610 definitief is. Wel kunnen IT-auditors gebruik maken van de bestaande Standaard 610 zoals vastgesteld door het NBA.

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')

Art./Par.	Omschrijving
	Openbaar IT-auditor: de IT-auditor die werkzaam is bij of verbonden is aan een IT auditpraktijk.
	Overtreding van wet en regelgeving: overtreding van wet en regelgeving ("overtreding") omvat elke handeling of nalaten en het al dan niet opzettelijk verrichten van handelingen in strijd met de heersende wet en regelgeving door een van de volgende partijen: *(a)* een cliënt; *(b)* degenen die bij een cliënt zijn belast met governance; *(c)* het bestuur van een cliënt; of *(d)* andere personen die werkzaam zijn voor of anderszins onder toezicht staan van een cliënt.

	Professionele activiteit: activiteit(en) op het brede terrein van IT-Governance, -Risk, Compliance en/of – Audit.
	Professionele dienstverlening: professionele activiteiten uitgevoerd voor cliënten op het brede terrein van IT-Governance, -Risk, -Compliance en/of -Audit.
	Redelijke en geïnformeerde derde partij toets: de objectieve, redelijke en geïnformeerde derden partij-toets betreft de vraag van een IT-auditor of een derde waarschijnlijk tot dezelfde conclusies zou komen. Deze vraag dient beantwoord te worden vanuit het oog punt van een objectieve, redelijke en geïnformeerde derde partij, die daarbij rekening houdt met alle relevante feiten en omstandigheden waarmee de IT-auditor op het mo ment waarop de conclusies worden gemaakt bekend is of in redelijkheid bekend zou moeten zijn. De objectieve, redelijke en geïnformeerde derde hoeft zelf geen IT-auditor te zijn, maar moet wel beschikken over relevante kennis en ervaring om de gepastheid van de conclusies van de IT-auditor op onpartijdige wijze te begrijpen en beoordelen. Deze termen worden nader omschreven in art. R120.5 A4.
	Resultaatafhankelijke vergoeding: een vergoeding die wordt vastgesteld op basis van het behalen van een vooraf overeengekomen resultaat van een door de IT auditeenheid uitgevoerde transactie of verleende dienst. Een vergoeding wordt niet beschouwd als resultaatafhankelijk indien deze is vastgesteld door een rechter of andere overheidsinstelling.

BKBO bv

KVK 67738516
BTW NL 857155647B01
IBAN NL98INGB0006077440
Bezoekadres: Voorstraat 20 5251 CP Vlijmen
Telefoon: 073 211 03 37

B1 – Reglement Gedragscode Register IT-Auditors ('Code of Ethics')	
Art./Par.	**Omschrijving**
	Voorafgaande IT-auditor: een IT-auditor die meest recentelijk belast was met een as surance-opdracht of die advies of vergelijkbare professionele diensten verleende aan een cliënt, voor zover er geen huidige IT-auditor is.
	Verantwoordelijke partij: verantwoordelijke partij ten aanzien van een assurance opdracht: de partij die verantwoordelijk is voor het object.
	Waarborgen: individueel of samen met anderen door de IT-auditor verrichte hande lingen waardoor bedreigingen voor de naleving van de fundamentele beginselen tot een aanvaardbaar niveau worden gereduceerd. Deze term wordt nader omschreven in art. 120.10 A2.
	Zou kunnen: deze term wordt in de Code gebruikt om de mogelijkheid aan te geven dat een zaak of gebeurtenis zich voordoet, of dat een handeling plaatsvindt. Wanneer gebruikt in verband met een bedreiging geeft de term niet een bepaalde mate van mogelijkheid of waarschijnlijkheid weer, aangezien de beoordeling van het niveau van de bedreiging afhangt van feiten en omstandigheden van een bepaalde zaak, geval of handeling.