NOREA Webinar Herziening Gedragscode

Commissie Beroepsregels

18 november 2021

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Inhoud Webinar

- Toelichting wijzigingen in de Code of Ethics
- Herhaling enkele kernelementen
- Introductie nieuwe begrippen
- Introductie nieuwe onderwerpen
- Introductie Casuïstiek

Achtergrond aanleiding wijziging Code of Ethics

- De voorgaande Code of Ethics (CoE) van NOREA dateert uit 2006
- De voorgaande CoE omvat geen duidelijke definitie van het begrip Onafhankelijkheid
- De IFAC Code of Ethics is aangepast
- NOREA is lid van IFAC
- Het aantal IT Auditors dat assurance–opdrachten uitvoert is sterk gegroeid
- De discussie omtrent Onafhankelijkheid wordt steeds indringender

Aanleiding voor dit webinar

- Invoering herziene Code of Ethics (1 juli 2021)
- Aanbeveling Raad voor Beroepsethiek: neem voldoende tijd voor:
  - Voorbeelden
  - Casuïstiek
  - Voorlichting en trainingen

Voor wie is de kennistoets herziening Gedragscode verplicht

In 2021 verplicht voor alle RE's.

Vrijstelling:

- Indien de verplichte NBA–Kennistoets(en) VGBA/VIO en COS–standaarden 2019/2020 met goed gevolg zijn afgelegd.

PE punten:

- 1–2 PE punten voor dit webinar (afhankelijk van de duur);
- 2 PE punten voor de e–learning & kennistoets.

Doelstelling Webinar CoE

- Doelstelling is een introductie te geven op de nieuwe elementen in de gewijzigde CoE.
  - Daarnaast komen in de vragen ook dilemma's terug.

Deel 1 Terugblik – begrippen – casus

René Ewals - ACS

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Inleiding structuur nieuwe CoE

- De gehele IFAC CoE bestaat uit de volgende onderdelen: deel 1, 2, 3, 4A en 4B.
- Voor NOREA gelden straks de volgende secties.
- Deel 1:
  - Sectie 100 : Naleving van de Code (Vereisten) ;
  - Sectie 110: De fundamentele beginselen;
  - Sectie 111: Integriteit;
  - Sectie 112: Objectiviteit;
  - Sectie 113: Vakbekwaamheid en zorgvuldigheid;
  - Sectie 114: Vertrouwelijkheid;
  - Sectie 115: Professionaliteit;
  - Sectie 120: Het conceptueel kader.
  - *Sectie 340 : Aanmoedigingen, inclusief geschenken en gastvrijheid*
  - *Sectie 400 : Netwerkonderdelen*
- Deel 4B:
  - Sectie 900: Toepassing van het conceptueel kader voor de onafhankelijkheid van assurance–opdrachten
  - Sectie 905: Vergoedingen
  - Sectie 906: Geschenken en Gastvrijheid
  - Sectie 907: Feitelijke of Dreigende Juridische Procedures
  - Sectie 910: Financiële Belangen
  - Sectie 911: Leningen en Garantiestellingen
  - Sectie 920: Zakelijke Relaties
  - Sectie 921: Familie en Persoonlijke Relaties
  - Sectie 922: Recent Dienstverband bij een Verantwoordelijke Partij
  - Sectie 923: Bekleden van de positie van Bestuurder of Verantwoordelijke van een assurance–cliënt
  - Sectie 924: Dienstverband bij een Verantwoordelijke Partij
  - Sectie 940: Langdurige betrokkenheid van personeel bij een Verantwoordelijke partij
  - Sectie 950: Verlenen van Non–Assurance–opdrachten aan een Verantwoordelijke partij
  - Sectie 990: Assurance–rapporten waarin een gebruiks– en verspreidingsbeperking is opgenomen

Nieuwe begrippen in de CoE

- **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:**
  - een individuele IT–auditor, IT–auditmaatschap of IT–auditkantoor;
  - een entiteit die de zeggenschap uitoefent over deze partijen, door het bezit of het beheer ervan of op andere wijze; en
  - een entiteit die onder de zeggenschap staat van deze partijen, door het bezit of het beheer ervan of op andere 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 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 opdrachten.
- **IT–auditpraktijk:** het IT–auditkantoor.

Sectie 110 – De fundamentele beginselen

Integriteit: oprecht en eerlijk optreden in professionele en zakelijke relaties.

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.

Vakbekwaamheid en zorgvuldigheid: (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 (II) zorgvuldig te handelen en in overeenstemming met toepasselijke technieken en professionele standaarden.

Vertrouwelijkheid: het respecteren van het vertrouwelijk karakter van de verkregen informatie als gevolg van de professionele en zakelijke relaties.

Professionaliteit: (i) te voldoen aan relevante wet- en regelgeving; (ii) zich te gedragen op een manier die in overeenstemming is met de verantwoordelijkheid 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.

Sectie 120 – Het conceptueel kader

- Het conceptueel kader specificeert een aanpak voor een IT–auditor om (120.2):
  - Bedreigingen voor de naleving van de fundamentele beginselen te identificeren;
  - De geïdentificeerde bedreigingen te evalueren; en
  - De bedreigingen te behandelen door ze te elimineren of terug te brengen tot een aanvaardbaar niveau.
- Bij de toepassing van het conceptueel kader dient de IT–auditor: (V 120.5)
  - Een onderzoekende geest te hebben;
  - Professionele oordeelsvorming toe te passen; en
  - De objectieve, redelijke en geïnformeerde derde partij toets te gebruiken, zoals beschreven in artikel 120.5 T6.

- *Objectieve, Redelijke en Geïnformeerde Derde Partij Toets (120.5 T6):*
- 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.

Sectie 120 Bedreigingen van onafhankelijkheid

- Bedreigingen voor het naleven van de fundamentele beginselen vallen in één of meer van de volgende categorieën:
  - Eigenbelang –de dreiging dat een financieel of ander belang het oordeel of het gedrag van een IT–auditor op ongepaste wijze zal beïnvloeden;
  - 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;
  - 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;
  - 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
  - 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.

Sectie 120 - Onafhankelijkheid

- R120.15 T1 bevat de definitie van onafhankelijkheid.

- IT–auditors, werkzaam in de openbare praktijk, zijn verplicht onafhankelijk te zijn bij het uitvoeren van assurance–opdrachten.

- Onafhankelijkheid bestaat uit:
  - Onafhankelijkheid in wezen – De geesteshouding die het tot uitdrukking 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;
  - 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.

Sectie 120 Het conceptuele kader – tendenties (1)

- Op basis van de laatste aanpassingen in de CoE vanuit IFAC 2020 zijn artikelen 120.12 T1, 2 en 3 opgenomen.
- 120.12 T1
- *Vooringenomenheid (tendentie)*
  - Bewuste of onbewuste tendentie beïnvloedt de uitoefening van de professionele oordeelsvorming 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 uitoefening 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 betrouwbaarheid 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 informatie die een bestaande overtuiging bevestigt dan aan informatie die die overtuiging tegenspreekt of in twijfel trekt.

Sectie 120 Het conceptueel kader – tendenties (2)

- 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.

Sectie 120 Het conceptueel kader – tendenties (3)

- 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.

Sectie 120 Het conceptueel kader – organisatiecultuur

- *120.13 T1 Organisatiecultuur*
- De effectieve toepassing van het conceptueel kader door een IT–auditor wordt bevorderd 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:
  - 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;
  - Er passende opleidings– en trainingsprogramma's, managementprocessen en prestatiebeoordelings– en beloningscriteria voorhanden zijn die een ethische cultuur bevorderen;
  - Er doeltreffende beleidslijnen en procedures bestaan om personen die feitelijk of vermoedelijk illegaal of onethisch gedrag melden, met inbegrip van klokkenluiders, aan te moedigen en te beschermen; en
  - 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 anciënniteit.

Sectie 120 Het conceptuele kader – organisatiecultuur

- *120.14 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.

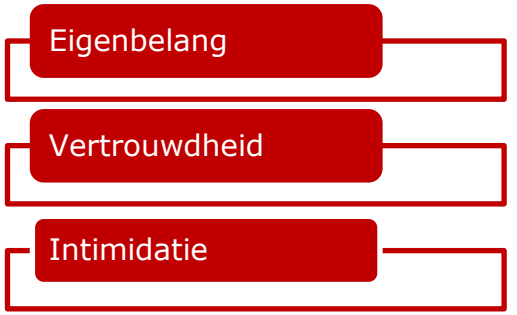
Deel 2 Sectie 340 – Aanmoedigingen, inclusief geschenken en gastvrijheid

Jan Matto - Mazars

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

SECTIE 340: AANMOEDIGINGEN, INCLUSIEF GESCHENKEN EN GASTVRIJHEID

- Bedreiging: Het aanvaarden of aanbieden van aanmoedigingen van een assurance client kan leiden tot eigenbelang, vertrouwdheid of intimidatie met betrekking tot de naleving van de fundamentele beginselen, met name de beginselen van integriteit, objectiviteit en professioneel gedrag.



- Aanmoedigingen kunnen in vele vormen voorkomen. Enkele voorbeelden:
  - Geschenken;
  - Gastvrijheid;
  - Amusement;
  - Politieke of liefdadige giften;
  - Beroepen op vriendschap en loyaliteit;
  - Werkgelegenheid of andere commerciële kansen;
  - Voorkeursbehandeling, rechten of privileges.

- Indien een dergelijke stimulans triviaal en onbeduidend is, zullen de bedreigingen die ervan uitgaan, van een aanvaardbaar niveau zijn.

SECTIE 340: AANMOEDIGINGEN, INCLUSIEF GESCHENKEN EN GASTVRIJHEID

- Het gaat zowel om de inschatting van de werkelijke als de gepercipieerde intentie om het gedrag te beïnvloeden. Daarbij speelt ook hoe de perceptie van de intentie om gedrag te beïnvloeden valt bij een geïnformeerde derde partij.

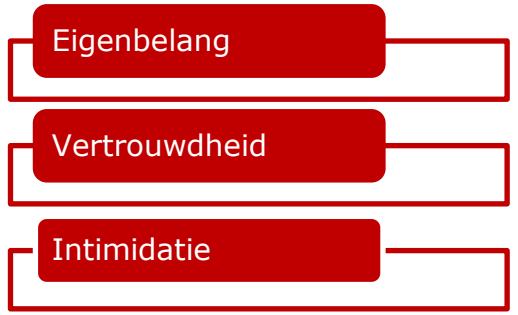
- Een IT–auditor mag *geen aanmoedigingen aanbieden*, of anderen aanmoedigen dit te doen, die worden aangeboden, of waarvan de IT–auditor van mening is dat een *objectieve, redelijke en geïnformeerde derde partij* waarschijnlijk zou concluderen dat ze worden aangeboden, met de bedoeling het gedrag van de ontvanger of van een ander individu op ongepaste wijze te beïnvloeden.

- 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.

- Eigenbelang
- Vertrouwdheid
- Intimidatie

SECTIE 340: AANMOEDIGINGEN, INCLUSIEF GESCHENKEN EN GASTVRIJHEID

- 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 dergelijke ongepaste beïnvloeding kan gericht zijn op de ontvanger of op een andere persoon die een relatie met de ontvanger heeft.

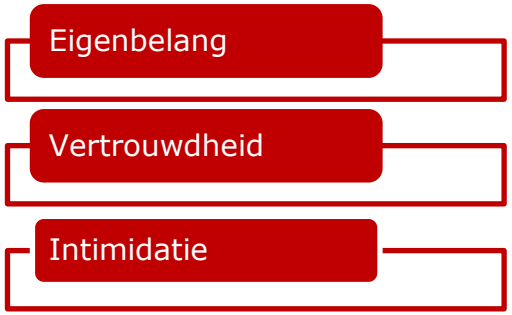


SECTIE 340: AANMOEDIGINGEN, INCLUSIEF GESCHENKEN EN GASTVRIJHEID

- Eigenbelang
- Vertrouwdheid
- Intimidatie

- Afhankelijk van de situatie en onderkende bedreigingen van aanmoedigingen zijn verschillende mitigerende maatregelen mogelijk (niet limitatief):

- 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.
- 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.
- Transparant zijn tegenover het senior management van de onderneming of van de cliënt over het aanbieden of aanvaarden van een aanmoediging.

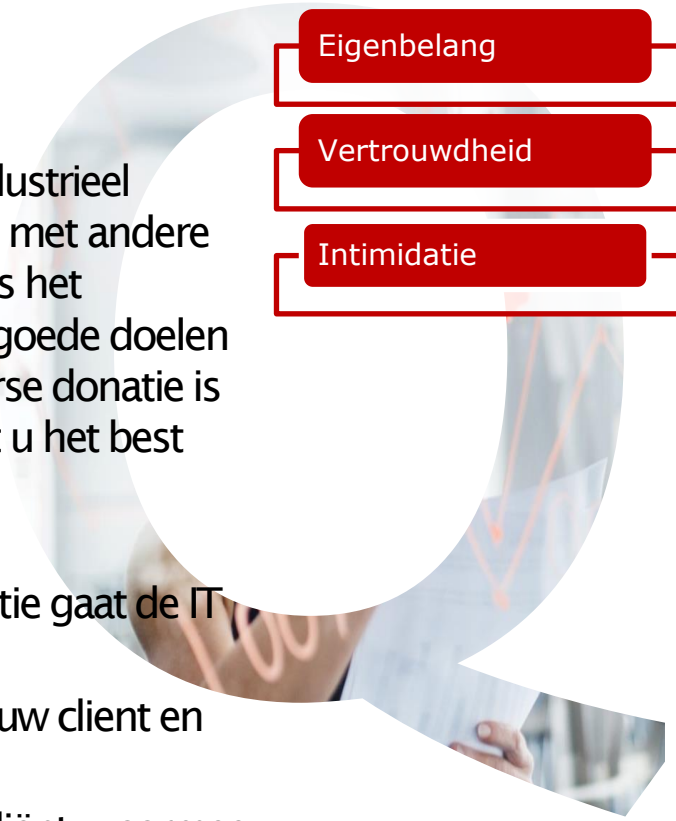


- Afhankelijk van de onderkende bedreigingen van aanmoedigingen zijn verschillende mitigerende maatregelen mogelijk (niet limitatief, vervolg):

- 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 management van het kantoor of de persoon die de aanmoediging heeft aangeboden.

SECTIE 340: AANMOEDIGINGEN, INCLUSIEF GESCHENKEN EN GASTVRIJHEID

Casuspositie:



De partner van een IT-auditor is actief lid in een goede doelen organisatie ter bescherming van industrieel erfgoed. De IT Auditor en zijn/haar partner worden uitgenodigd door een assurance client samen met andere relaties van de client voor het bijwonen van een Formule 1 evenement, inclusief after party. Tijdens het evenement raakt de cliënt in gesprek met de partner van de IT-auditor over de activiteiten van de goede doelen organisatie en raakt erg enthousiast. Een week later meldt de partner van de IT-auditor dat een forse donatie is ontvangen van de assurance client op rekening van de goede doelenorganisatie. Welke actie acht u het best passend:

A) De aanmoediging (het F1 evenement) was niet exclusief gericht op de IT auditor en de donatie gaat de IT auditor niet aan. Geen actie, er is geen probleem;
B) U ziet een bedreiging (intimidatie) en neemt contact op met de goede doelenorganisatie en uw client en verzoekt de donatie te registreren (logboek) en te publiceren;
C) U onderkent een bedreiging en stort de waarde van het F1 evenement op rekening van de cliënt, waarmee de bedreiging van intimidatie is gemitigeerd;
D) U registreert de uitnodiging in het logboek van uw organisatie, evenals de retournering van de waarde van de uitnodiging.
E) U beëindigt de zakelijke relatie met de cliënt.

Deel 3 Sectie 400 – Netwerkonderdelen

Dennis Houtekamer - EY

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

SECTIE 400

NETWERKONDERDELEN

SECTIE 400: NETWERKONDERDELEN

Objectiviteit

Integriteit

- Definitie Netwerkonderdeel:

  Een IT–auditeenheid of andere entiteit die behoort tot een netwerk

- 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 gescheiden en te onderscheiden zijn van de ondernemingen en entiteiten.

- Een netwerkonderdeel moet onafhankelijk zijn van de assurance–cliënten van de andere kantoren binnen het netwerk zoals vereist in deze Code.

SECTIE 400: NETWERKONDERDELEN (2)

Objectiviteit

Integriteit

- Wanneer een firma geassocieerd is met een grotere structuur van andere firma's en entiteiten, moet zij:
  - Professionele oordeelsvorming uitoefenen om te bepalen of een netwerk wordt gecreëerd door een dergelijke grotere structuur;
  - 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
  - Dit oordeel consequent toepassen in de gehele grotere structuur.

SECTIE 400: NETWERKONDERDELEN (3)

Objectiviteit

Integriteit

- 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;

b) De onderdelen binnen de structuur gemeenschappelijk eigendom, zeggenschap of beheer hebben;

c) De onderdelen binnen de structuur een gemeenschappelijk beleid en procedures voor kwaliteitscontrole delen;

d) De onderdelen binnen de structuur een gemeenschappelijke bedrijfsstrategie delen;

e) De onderdelen binnen de structuur gezamenlijk een gemeenschappelijke merknaam gebruiken;

f) De onderdelen binnen de structuur een aanzienlijk deel van de professionele middelen delen.

Casus

- **Vraag: Als de IT-auditeenheid meerdere eindverantwoordelijk IT-auditors heeft kun je dan stellen dat je onafhankelijke teams kan samenstellen voor andersoortige opdrachten bij die cliënt?**

- **Antwoord indicatie:** dat ligt eraan. Alle leden van een assurance-team moeten onafhankelijk zijn en bedreigingen van de onafhankelijkheid moeten conform sectie 120 worden geïdentificeerd en zodanig worden verminderd dat deze acceptabel zijn. Verder is toepassingsmateriaal opgenomen in sectie 950.
- Let wel: er kunnen ook nog andere elementen zijn, die relevant zijn.

Casus (2)

- **Uitbreiding. Als je als IT-auditeenheid een periodieke (recurring) Richtlijn 3000 opdracht doet bij een organisatie (bijvoorbeeld DigiD Assessment), mag je dan geen ander advieswerk (op andere gebieden) bij die organisatie doen omdat je als IT-auditeenheid onafhankelijk moet zijn (bijvoorbeeld IT strategieopdracht), of moet je onafhankelijkheid ten aanzien van object van onderzoek vaststellen?**

- **Antwoord indicatie:**
- 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.

Casus (3)

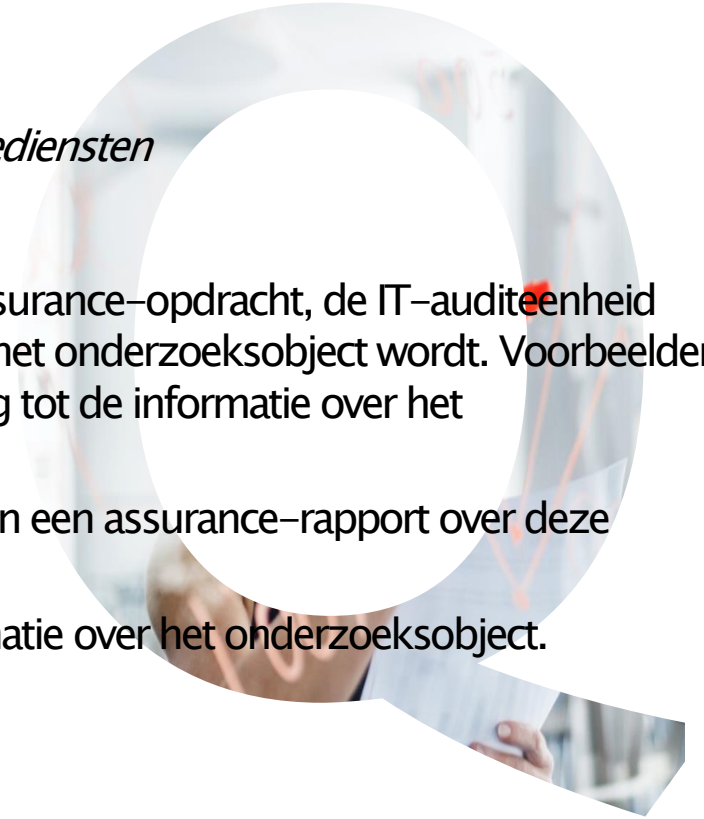
- 950.4 T1 *Beoordeling van bedreigingen*

- 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:
    - in hoeverre de uitkomst van de verleende dienst materiële of aanmerkelijke invloed heeft op het onderliggende onderzoeksobject 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 betrekking heeft;
    - de mate van expertise van het management en de werknemers van de verantwoordelijke partij ten aanzien van de soort verleende diensten.

Casus (4)

- 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 informatie 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 bedreigingen als gevolg van zelftoetsing kunnen ontstaan zijn:
  - het ontwikkelen en opstellen van mogelijke informatie en het vervolgens verstrekken van een assurance-rapport over deze informatie;
  - het uitvoeren van een waardering met betrekking tot of die deel uitmaakt van de informatie over het onderzoeksobject.



CASUS – INTERCONNECTED WORLD

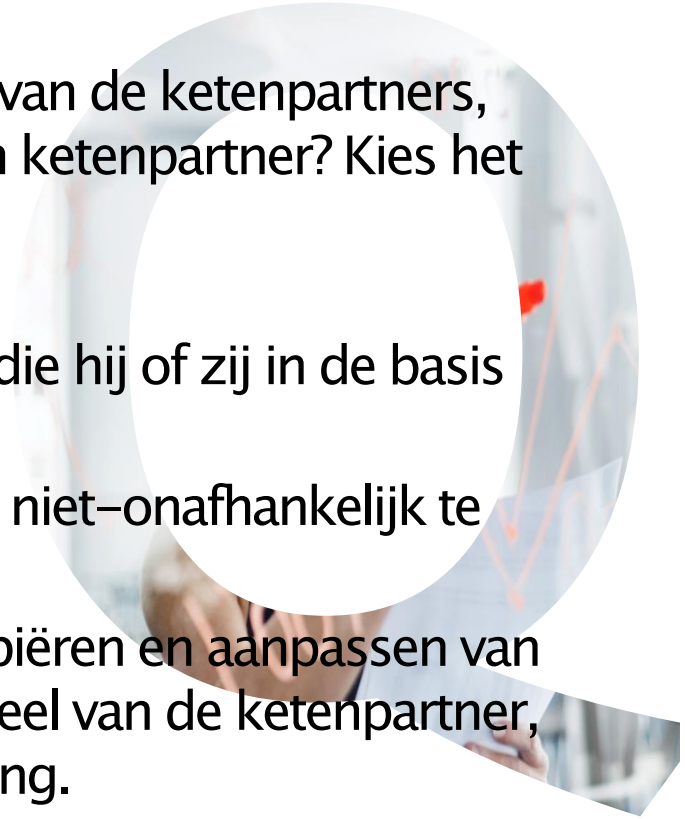
Enkele tientallen onafhankelijke en zelfstandige ketenpartners, ieder zelf met uitgebreide ICT, werken samen met een koepelorganisatie. Deze koepelorganisatie bevat juristen en lobbyisten, voor contact met de wetgever in Den Haag. Op een bepaald moment komt er een groot gemeenschappelijk additioneel ICT-systeem, dat namens de ketenpartners wordt beheerd door de koepelorganisatie. Vanuit privacy-oogpunt (AVG) komt er een convenant, waarin de koepelorganisatie en de ketenpartners vastleggen dat sprake is van een gemeenschappelijke verwerkingsverantwoordelijkheid voor dat specifieke ICT-systeem.

Een IT-auditor (RE) wordt door de koepelorganisatie ingehuurd om daar het ISMS in te richten en te helpen bij het schrijven van de ISMS-documentatie. Daarbij wordt afgesproken dat individuele ketenpartners documenten over het ISMS van de koepelorganisatie mogen kopiëren en die documenten zelf mogen omzetten naar hun eigen situatie.

Vraag: Mag deze IT-auditor assurance-werkzaamheden verrichten bij een van de ketenpartners, met name gericht op het geven van assurance over het eigen ISMS van een ketenpartner?

CASUS (2)

Vraag: Kan deze IT–auditor assurance–werkzaamheden verrichten bij een van de ketenpartners, met name gericht op het geven van assurance over het eigen ISMS van een ketenpartner? Kies het beste antwoord:



a) Nee, de IT–auditor kan bij de ketenpartner documenten tegenkomen die hij of zij in de basis zelf heeft geschreven voor de koepelorganisatie (risico zelftoetsing).
b) Nee, ondanks eventuele waarborgen heeft de IT–auditor de schijn van niet–onafhankelijk te zijn tegen; derhalve kan hij de opdracht niet accepteren.
c) Jawel, de ketenpartner is zelf verantwoordelijk voor het selecteren, kopiëren en aanpassen van documenten van de koepelorganisatie. Dit gebeurt door eigen personeel van de ketenpartner, zonder betrokkenheid van de IT–auditor. Er is geen dus geen bedreiging.
d) Jawel, met eventuele extra waarborgen, zoals expliciete vastlegging van verantwoordelijkheden rondom documentatie ISMS is er geen bedreiging.

Vragen?

Dank voor uw aandacht!