

## **Code of Ethics**

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 Code of Ethics is gebaseerd op de Code of Ethics van de International Federation of Accountants (IFAC) en geldt met ingang van 14 juli 2006.

*Gedragscode geldend voor iedere IT-auditor*

Hoofdstukindeling:

A-100 Inleiding en fundamentele beginselen

A-110 Integriteit

A-120 Objectiviteit

A-130 Deskundigheid en zorgvuldigheid

A-140 Geheimhouding

A-150 Professioneel gedrag

### **Hoofdstuk A-100 Inleiding en fundamentele beginselen**

#### Artikel A-100.1

De IT-auditor aanvaardt te allen tijde de verantwoordelijkheid op te treden in het algemeen belang en behartigt diens gevolge niet uitsluitend de belangen van een individuele opdrachtgever. Daartoe neemt de IT-auditor bij zijn optreden deze Code in acht en handelt in overeenstemming daarmee.

#### Artikel A-100.2

De IT-auditor maakt van het in deze Code beschreven conceptueel raamwerk gebruik bij het signaleren van een bedreiging. Hij evalueert een bedreiging naar aard en belang. Indien blijkt dat een bedreiging van niet te verwaarlozen betekenis is, treft de IT-auditor waarborgen die de bedreiging wegnemen of terugbrengen tot een aanvaardbaar niveau, zodat de naleving van de fundamentele beginselen geen geweld wordt aangedaan. De IT-auditor legt de bedreiging van niet te verwaarlozen betekenis, de naar aanleiding daarvan getroffen waarborgen en zijn conclusie vast.

#### Artikel A-100.3

Deze Code bevat de fundamentele beginselen van de beroepsethiek voor de IT-auditor, alsmede het conceptueel raamwerk voor de toepassing van deze fundamentele beginselen. Het conceptueel raamwerk geeft richting aan de toepassing van deze fundamentele beginselen.

Het NOREA-bestuur kan nadere regels uitvaardigen over de toepassing van het conceptueel raamwerk in specifieke situaties opdat waarborgen worden opgenomen die in aanmerking komen om een bedreiging weg te nemen of terug te brengen tot een aanvaardbaar niveau. Ook kunnen voorbeelden worden opgenomen van situaties waarin geen waarborgen beschikbaar zijn en van activiteiten of relaties die moeten worden vermeden.

Deze Code is van toepassing op iedere in het RE- register ingeschreven IT-auditor

## *Fundamentele beginselen*

### Artikel A-100.4

De IT-auditor neemt de volgende fundamentele beginselen in acht:

#### a) Integriteit

De IT-auditor treedt in zijn beroepsmatige en zakelijke betrekkingen eerlijk en oprecht op.

#### b) Objectiviteit

De IT-auditor accepteert niet dat zijn professioneel of zakelijk oordeel wordt aangetast door een vooroordeel, belangentegenstelling of ongepaste beïnvloeding door een derde.

#### c) Deskundigheid en zorgvuldigheid

De IT-auditor houdt zijn deskundigheid en vaardigheid op het niveau dat is vereist om aan een opdrachtgever professionele diensten te kunnen verlenen in overeenstemming met actuele ontwikkelingen in de praktijk, wetgeving en vaktechniek. De IT-auditor handelt bij het verlenen van professionele diensten zorgvuldig en in overeenstemming met de van toepassing zijnde vaktechnische en overige beroepsvoorschriften.

#### d) Geheimhouding

De IT-auditor eerbiedigt het vertrouwelijke karakter van informatie die hij in het kader van zijn beroepsmatig en zakelijk handelen heeft verkregen. Hij maakt deze informatie zonder specifieke machtiging daartoe niet aan een derde bekend, tenzij wettelijk of beroepshalve een recht of plicht daartoe bestaat. Het is de IT-auditor niet toegestaan vertrouwelijke informatie die hij bij zijn beroepsmatig of zakelijk handelen heeft verkregen, te gebruiken om zichzelf of een derde te bevoordelen.

#### e) Professioneel gedrag

De IT-auditor houdt zich aan de voor hem relevante wet- en regelgeving en onthoudt zich van handelen dat het auditberoep in diskrediet brengt. Bij samenloop van functies dient een zodanige zorgvuldigheid in acht genomen te worden dat de relatie tussen het optreden c.q. het uiting geven als Register EDP-auditor en de andere functie ondubbelzinnig bepaald is.

Deze fundamentele beginselen zijn gedetailleerd besproken in de artikelen A-110 tot en met artikel A-150.

## **Conceptueel raamwerk**

### Artikel A-100.5

De IT-auditor handelt in overeenstemming met het conceptueel raamwerk bij iedere door hem gesignaleerde bedreiging die niet van te verwaarlozen betekenis is en bij de naar aanleiding daarvan getroffen waarborgen die deze bedreiging wegnemen of terugbrengen tot een aanvaardbaar niveau.

De omstandigheid waaronder de IT-auditor zijn werkzaamheden verricht kan leiden tot een bedreiging. Het is niet mogelijk iedere situatie te beschrijven waarin een bedreiging ontstaat en aan te geven welke waarborgen daartegen kunnen worden getroffen. Bovendien kunnen de aard van de opdrachten en van de uit te voeren werkzaamheden verschillen. Als gevolg daarvan kunnen ook verschillende en meerdere bedreigingen optreden waardoor het treffen van verschillende en meerdere waarborgen noodzakelijk is. Een conceptueel raamwerk dat van de IT-auditor vraagt iedere bedreiging te signaleren, te evalueren en aan de orde te stellen, in plaats van de eis te voldoen aan een aantal min of meer arbitraire specifieke regels, is in het algemeen belang. Deze Code biedt een raamwerk ter ondersteuning van de IT-auditor bij het signaleren en evalueren van iedere bedreiging en bij het in reactie daarop treffen van de juiste waarborgen.

#### Artikel A-100.6

De IT-auditor evalueert omstandigheden of relaties waarmee hij bekend is of in redelijkheid bekend behoort te zijn, die de naleving van de fundamentele beginselen in gevaar kan brengen.

#### Artikel A-100.7

De IT-auditor betreft bij het beoordelen van de aard, het belang en de ernst van een bedreiging zowel kwalitatieve als kwantitatieve factoren. Indien De IT-auditor niet in staat is adequate waarborgen te treffen weigert of beëindigt hij een opdracht tot het verlenen van een professionele dienst of beëindigt hij de opdrachtrelatie met de cliënt, dan wel zijn relatie met de organisatie waarbij of ten behoeve waarvan hij werkzaam is.

#### Artikel A-100.8

De IT-auditor kan onopzettelijk een bepaling uit deze Code schenden. Indien dit het geval is, dan is het mogelijk, afhankelijk van de aard en de betekenis ervan, geen sprake van schending van de basisbeginselen mits de gevolgen onmiddellijk na ontdekking van de schending worden geëvalueerd, voorzover mogelijk gecorrigeerd en eventuele waarborgen worden getroffen.

#### Artikel A-100.9

De IT-auditor beperkt zich bij het toepassen van het conceptueel raamwerk niet tot de in deze Code opgenomen voorbeelden.

### **Bedreigingen en waarborgen**

#### Artikel A-100.10

Het scala aan bedreigingen is groot. Een bedreiging valt doorgaans in één of meerdere van de volgende categorieën:

- a. bedreiging als gevolg van eigenbelang: Dit is de bedreiging die ontstaat uit een financieel of ander belang van de IT-auditor dan wel van een gezins- of naast familielid van hem;
- b. bedreiging als gevolg van zelftoetsing: Dit is de bedreiging die ontstaat indien de IT-auditor zijn eigen werkzaamheden of het resultaat daarvan beoordeelt;
- c. bedreiging als gevolg van belangenbehartiging: Dit is de bedreiging die ontstaat indien de IT-auditor op een zodanige wijze een standpunt verdedigt dat objectiviteit in het gedrag komt;
- d. bedreiging als gevolg van vertrouwdsheid: Dit is de bedreiging die ontstaat indien er een nauwe band bestaat tussen de IT-auditor en zijn opdrachtgever of indien de IT-auditor te veel sympathie koestert voor de belangen van een ander;
- e. bedreiging als gevolg van intimidatie: Dit is de bedreiging die ontstaat indien de IT-auditor door feitelijke of vermeende dreigementen wordt afgehouden van objectief handelen.

#### Artikel A-100.11

Waarborgen die een bedreiging wegnemen of tot een aanvaardbaar niveau terugbrengen zijn globaal in twee categorieën te verdelen:

- a) waarborgen tot stand gebracht door de wetgever, de NOREA of andere regelgevers; en
- b) waarborgen in de werkomgeving.

#### Artikel A-100.12

De waarborgen tot stand gebracht door de wetgever, de NOREA of andere regelgevers omvatten onder meer:

- a. regelgeving ten aanzien van Corporate- en/of IT-Governance;
- b. eisen voor inschrijving in het RE-register ter zake van, opleiding, ervaring en goed gedrag;
- c. eisen ten aanzien van de permanente educatie;
- d. vaktechnische en overige beroepsvoorschriften;
- e. stelsel van kwaliteitsbeheersing;
- f. externe beoordeling van de door de IT-auditor uitgevoerde assurance en daaraan verwante opdrachten;
- g. klacht- en tuchtrecht.

#### Artikel A100.13

P.M.

#### Artikel A-100.14

Bepaalde waarborgen kunnen de kans vergroten dat onethisch gedrag wordt voorkomen of wordt ontdekt. Dergelijke waarborgen die kunnen zijn getroffen door de wetgever, de NOREA, andere regelgevers of de huishouding waaraan de IT-auditor is verbonden of waarbij hij werkzaam is, omvatten onder meer een effectieve en in ruime kring bekend gemaakte procedure, uitgevoerd door de werkgever, de NOREA of een regelgever, die het mogelijk maakt dat collega's, werkgevers of andere personen onprofessioneel of onethisch gedrag kunnen melden.

#### Artikel A-100.15

In zijn professionele oordeelsvorming neemt de IT-auditor in aanmerking hetgeen een redelijk en goed geïnformeerde derde die over alle relevante informatie beschikt, waaronder de aard en het belang van de bedreiging en de getroffen waarborgen, als aanvaardbaar zal aanmerken.

De aard en het belang van de te treffen waarborgen zijn afhankelijk van de specifieke omstandigheden.

### **Oplossen van beroepsethische conflicten**

#### Artikel A-100.16

Bij het beoordelen van het al dan niet naleven van de fundamentele beginselen is het mogelijk dat van de IT-auditor wordt verlangd dat hij een oplossing vindt voor een conflict over de toepassing van de fundamentele beginselen.

#### Artikel A-100.17

Indien de IT-auditor formeel dan wel informeel het initiatief neemt een conflict over de toepassing van de fundamentele beginselen op te lossen neemt hij de volgende aspecten, hetzij afzonderlijk, dan wel in hun onderlinge samenhang, in aanmerking:

- a. de relevante feiten;
- b. de relevante beroepsethische aspecten;
- c. de fundamentele beginselen die van toepassing zijn op het conflict;
- d. de geldende interne procedures; en
- e. de mogelijke alternatieve handelwijzen.

Nadat de IT-auditor deze aspecten in aanmerking heeft genomen, kiest hij een adequate handelwijze overeenkomend met de in het geding zijnde fundamentele beginselen. Daarbij weegt de IT-auditor de gevolgen van de alternatieve handelwijzen tegen elkaar af.

Indien voor het conflict geen oplossing wordt gevonden vraagt de IT-auditor advies aan de daartoe aangewezen personen van de auditororganisatie waarbij hij werkzaam is of waaraan hij is verbonden of van de organisatie waarbij of ten behoeve waarvan hij werkzaam is.

#### Artikel A-100.18

Als de kwestie bestaat uit een conflict met of binnen een organisatie overweegt de IT-auditor daarnaast om degenen die zijn belast met het bestuur van of met het toezicht op die organisatie te raadplegen.

Hierbij kan gedacht worden aan de directie, Raad van Commissarissen of de audit commissie.

#### Artikel A-100.19

Het is in het belang van de IT-auditor de meest belangrijke aspecten van het conflict, de details van de gevoerde besprekingen en de daaromtrent genomen besluiten te documenteren.

#### Artikel A-100.20

Indien de IT-auditor een ernstig conflict niet kan oplossen, verdient het aanbeveling dat hij, zonder de vertrouwelijkheid geweld aan te doen, advies vraagt aan de NOREA (Raad voor Beroepsethiek) of aan een juridische adviseur.

Indien de IT-auditor bijvoorbeeld wordt geconfronteerd met een fraude waarvan bekendmaking kan leiden tot een bedreiging voor de naleving van de geheimhoudingsplicht, overweegt hij of het noodzakelijk is juridisch advies in te winnen om te bepalen of hij al dan niet verplicht is de fraude bij de daarvoor aangewezen instanties te melden.

#### Artikel A-100.21

Indien, nadat alle denkbare oplossingen in de beoordeling zijn betrokken, het niet mogelijk blijkt het beroepsethische conflict op te lossen, maakt de IT-auditor, indien mogelijk, een einde aan zijn betrokkenheid bij de aangelegenheid die heeft geleid tot het conflict.

Dit kan betekenen dat de IT-auditor, gezien de omstandigheden, moet besluiten zich uit het opdrachtteam terug te trekken, zijn medewerking aan een deelopdracht te beëindigen, zijn functie bij de opdracht neer te leggen of zijn relatie met de auditororganisatie of de organisatie waarbij of ten behoeve waarvan hij werkzaam is te verbreken of ontslag te nemen.

### Hoofdstuk A-110 **Integriteit**

#### Artikel A-110-1

De IT-auditor treedt in zijn beroepsmatige en zakelijke betrekkingen eerlijk en oprecht op, doet eerlijk zaken en doet de waarheid geen geweld aan.

#### Artikel A-110.2

De IT-auditor vermijdt dat hij in verband wordt gebracht met informatie die naar zijn oordeel een bewering bevat die:

- a. materieel onjuist of misleidend is;
- b. op ongefundeerde gronden is gedaan;
- c. niet volledig is of een verkeerde indruk wekt als gevolg waarvan de bewering als misleidend kan worden ervaren.

#### Artikel A-110.3

De IT-auditor handelt niet in strijd met het bepaalde in artikel A-110.2 indien hij aan bedoelde informatie een mededeling toevoegt waarin hij zijn bezwaren tegen deze informatie tot uitdrukking brengt.

## Hoofdstuk A-120 **Objectiviteit**

### Artikel A-120.1

De IT-auditor accepteert niet dat zijn professioneel of zakelijk oordeel wordt aangetast door een vooroordeel, belangentegenstelling of ongepaste beïnvloeding door een derde.

### Artikel A-120.2

De IT-auditor vermijdt iedere situatie die zijn professionele oordeelsvorming op een ongepaste wijze beïnvloedt.

De IT-auditor kan in een situatie komen te verkeren waarin zijn objectiviteit in het gedrang komt. Het is onmogelijk al deze situaties te beschrijven.

## Hoofdstuk A-130 **Deskundigheid en zorgvuldigheid**

### Artikel A-130.1

De IT-auditor houdt zijn deskundigheid en vaardigheid op het niveau dat is vereist om aan een opdrachtgever professionele diensten te kunnen verlenen in overeenstemming met actuele ontwikkelingen in de praktijk, wetgeving en vaktechniek. De IT-auditor handelt bij het verlenen van professionele diensten zorgvuldig en in overeenstemming met de van toepassing zijnde vaktechnische en overige beroepsvoorschriften.

### Artikel A-130.2

Deskundige dienstverlening vereist van de IT-auditor een deugdelijke oordeelsvorming bij de toepassing zijn van professionele kennis en vaardigheid.

Professionele deskundigheid kan worden verdeeld in twee verschillende fasen:

- a. het verwerven van professionele deskundigheid; en
- b. het in stand houden van professionele deskundigheid.

### Artikel A-130.3

Voor het in stand houden van de professionele deskundigheid van de IT-auditor is kennis van en inzicht in de relevante vaktechnische en beroepsmatige ontwikkelingen vereist, alsmede van ontwikkelingen in het bedrijfsleven.

Permanente educatie stelt de IT-auditor in staat in de omgeving waarin hij beroepsmatig werkzaam is in continuïteit deskundig op te treden.

### Artikel A-130.4

Zorgvuldigheid omvat de verantwoordelijkheid van de IT-auditor op te treden in overeenstemming met de eisen die gelden voor de uitvoering van een opdracht, te weten, toewijding, voldoende diepgang en tijdigheid.

### Artikel A-130.5

De IT-auditor treft maatregelen die ervoor zorgen dat degenen die onder zijn verantwoordelijkheid werken de juiste opleiding hebben en onder adequaat toezicht staan.

### Artikel A-130.6

De IT-auditor maakt indien daartoe aanleiding bestaat zijn opdrachtgevers of andere gebruikers van zijn professionele diensten attent op de inherente beperkingen die zijn verbonden aan zijn diensten. Aldus voorkomt hij dat een door hem gegeven oordeel wordt geïnterpreteerd als een feitelijke bewering.

#### Artikel A-130.7

Het bestuur kan nadere voorschriften geven aangaande het bepaalde in artikel A-130.1 t/m A-130.6 ten aanzien van permanente educatie, audit- en overige standaarden.

### Hoofdstuk A-140 **Geheimhouding**

#### Artikel A-140.1

De IT-auditor onthoudt zich van:

- a. het buiten de auditpraktijk waarbij hij werkzaam is of waaraan hij is verbonden of buiten de organisatie waarbij of ten behoeve waarvan hij werkzaam is, bekend maken van vertrouwelijke informatie, die hij in het kader van zijn beroepsmatig en zakelijk optreden heeft verkregen, tenzij hij is gemachtigd tot bekendmaking over te gaan of wettelijk dan wel beroepshalve daartoe een recht of plicht bestaat; en
- b. het gebruikmaken van vertrouwelijke informatie die hij in het kader van zijn beroepsmatig en zakelijk handelen heeft verkregen om zichzelf of een derde te bevoordelen.

#### Artikel A-140.2

De IT-auditor houdt zich in zijn sociale omgang ook aan zijn geheimhoudingsplicht. De IT-auditor is erop bedacht dat bij een langdurige omgang met een zakenrelatie, een gezinslid of een naast familielid de mogelijkheid bestaat onopzettelijk te handelen in strijd met zijn geheimhoudingsplicht.

#### Artikel A-140.3

De IT-auditor neemt zijn geheimhoudingsplicht ook in acht ter zake van informatie die hem ter beschikking is gesteld door een potentiële opdrachtgever.

#### Artikel A-140.4

De IT-auditor overweegt de noodzaak de geheimhoudingsplicht in acht te nemen binnen de auditororganisatie waaraan hij is verbonden of waarbij hij werkzaam is of binnen de organisatie waarbij of ten behoeve waarvan hij werkzaam is.

#### Artikel A-140.5

De IT-auditor treft de redelijkerwijs te nemen maatregelen om te waarborgen dat de voor hem geldende geheimhoudingsplicht tevens in acht wordt genomen door personeelsleden die hiërarchisch aan hem ondergeschikt zijn en door personen aan wie hij om advies of ondersteuning vraagt.

#### Artikel A-140.6

De IT-auditor houdt zich aan zijn geheimhoudingsplicht ook na het beëindigen van de verbintenis met een cliënt of met een organisatie waarbij of ten behoeve waarvan hij werkzaam is.

Wanneer een IT-auditor van werkgever verandert of nieuwe opdrachten verwerft, is het hem toegestaan gebruik te maken van de bij zijn eerdere werkzaamheden verkregen kennis en opgedane ervaring. De vertrouwelijke informatie die De IT-auditor tijdens deze eerdere werkzaamheden heeft verkregen mag hij niet gebruiken of bekendmaken.

#### Artikel A-140.7

De IT-auditor kan in een situatie komen te verkeren waarin hij verplicht is of waarin het maatschappelijk juist is vertrouwelijke informatie bekend te maken. Voorbeelden hiervan zijn:

- (a) bekendmaking is wettelijk toegestaan en door de opdrachtgever goedgekeurd;
- (b) bekendmaking is wettelijk verplicht, bijvoorbeeld in geval van:

- (i) de oplevering van documenten of levering van bewijs in het kader van een rechtsgeding;
- (b) (ii) de melding aan de geëigende overheidsinstanties van aan het licht gekomen schendingen van de wet; en
- (c) de IT-auditor heeft een beroepsplicht, of is gerechtigd, tot bekendmaking, wanneer zulks niet bij wet verboden is:
  - (i) ter naleving van vaktechnische standaarden en ethische vereisten;
  - (ii) ter bescherming van de beroepsbelangen van een IT-auditor bij een rechtsgeding;
  - iii) teneinde medewerking te verlenen aan de kwaliteitsbeoordeling door de beroepsorganisatie; of
  - (iv) om te beantwoorden aan een verzoek om inlichtingen of een onderzoek door de beroepsorganisatie of een toezichthoudend lichaam.

#### Artikel A-140.8

Alvorens de IT-auditor besluit tot bekendmaking van vertrouwelijke informatie over te gaan betreft hij in zijn besluitvorming:

a. in hoeverre de belangen van alle partijen, inclusief een derde waarvan de belangen in het spel zijn, kunnen worden geschaad in de situatie waarin een opdrachtgever de IT-auditor toestemming geeft tot het bekendmaken van de vertrouwelijke informatie;

b. in hoeverre alle relevante informatie bij hem bekend en voor zover uitvoerbaar, onderbouwd is. Indien het betreft het bekendmaken van onbewezen gegevens, onvolledige informatie of ongefundeerde conclusies, is professionele oordeelsvorming noodzakelijk om de wijze van bekendmaking vast te stellen; en

c de wijze van communicatie die wordt verwacht en degene aan wie deze wordt gericht. In het bijzonder overtuigt de IT-auditor zich ervan dat degene met wie wordt gecommuniceerd de juiste ontvanger is.

#### Hoofdstuk A-150 **Professioneel gedrag**

##### Artikel A-150.1

De IT-auditor houdt zich aan de voor hem relevante wet- en regelgeving en onthoudt zich van handelen dat het auditberoep in diskrediet brengt. Tot dit handelen behoren die handelingen die door een redelijke en goed geïnformeerde derde die over alle relevante informatie beschikt, zullen worden opgevat als schadelijk voor de goede naam van het auditberoep.

##### Artikel A-150.2

De IT-auditor brengt bij het zichzelf of zijn werk aanprijzen het auditberoep niet in diskrediet. De IT-auditor is eerlijk en oprecht in zijn promotionele activiteiten en onthoudt zich van:

a) het wekken van overdreven verwachtingen ter zake van de diensten die hij kan verlenen, de kwaliteiten die hij bezit en de ervaring waarover hij beschikt;

b) het maken van afkeurende verwijzingen naar of niet onderbouwde vergelijkingen met het werk van een derde.



## **Definities**

- a. IT-auditor: de Register EDP-auditor (RE), ingeschreven in het register van de NOREA;
- b. NOREA, de Orde, de beroepsorganisatie: De Nederlandse Orde van Register EDP-auditors
- c. auditororganisatie: de organisatorische eenheid waarbinnen één of meer IT-auditors professionele diensten verrichten;
- d. bedreiging: het risico van het niet volledig naleven door de IT-auditor van één of meer van de fundamentele beginselen;
- e. bestuur: het bestuur van de Nederlandse Orde van Register EDP-Auditors;
- f. fundamentele beginselen: de beginselen integriteit, objectiviteit, deskundigheid en zorgvuldigheid, geheimhouding en professioneel gedrag
- g. opdracht: de tussen een opdrachtgever en auditororganisatie overeengekomen professionele dienst;
- h. opdrachtgever: een cliënt waarmee de IT auditor een zakelijke relatie heeft, dan wel de organisatie waarmee de IT auditor een dienstverband heeft;
- i. professionele dienst: de werkzaamheden van de IT-auditor waarvoor IT-auditdeskundigheid en deskundigheid op aanverwante terreinen is vereist.