Commissie Beroepsreglementering

Webinar Assurance

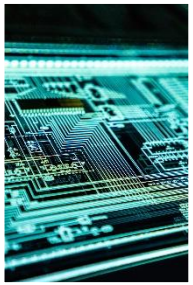
29 oktober 2020

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Agenda

- Doel en aanleiding Webinar
- Deel 1: Regelgeving en rapportering
  - 3000A/D en 3402
  - Formulering mededelingen 3000A/D en 3402
  - OKB
- Deel 2: SOC 2 en 3 (en privacy)
- Deel 3: Praktijkervaringen Assurance
  - Doelstellingen en maatregelen
  - Sub-serviceorganisaties
  - Type oordelen

Doel en aanleiding van dit Webinar



De ontwikkelingen op het gebied van Assurance.

Bevindingen kwaliteitstoetsen (door CKO).

Voorbereiding op een verplichte kennistoets.

Inhoud webinar & e-learning

Kennis mbt Richtlijnen & Handreikingen actualiseren:

- Richtlijn 3000 Assurance-opdrachten (Attest- en Directe opdrachten)
- Richtlijn 3402 Assurance-rapporten interne beheersing service-organisatie
- Richtlijn 4401 Specifieke werkzaamheden met betrekking tot informatietechnologie
- Handreiking voor SOC2 en SOC3 op basis van ISAE3000/Richtlijn 3000A
- Handreiking Opdrachtgerichte Kwaliteitsbeoordeling (OKB)

Bij de e-learning staat de regelgeving die is opgenomen in de kennistoets centraal. Deze wordt toegelicht waarbij specifieke aspecten in detail aan de orde komen. Ook worden praktijkvoorbeelden en dilemma's aan de orde gesteld.

Voor wie is de kennistoets Assurance verplicht?

Alle in 2020 PE-plichtige IT auditors die daadwerkelijk betrokken zijn bij de voorbereiding of uitvoering van assurance-opdrachten:

- Richtlijn 3000A/D;
- SOC2/3;
- Richtlijn 3402;
- Aan assurance verwante opdrachten gebaseerd op Richtlijn 4401.

PE punten:

- 1-2 PE punten voor deze kick-off (afhankelijk van de duur);
- 2 PE punten voor de e-learning & kennistoets.

FAQ op de NOREA website

Deel 1 Regelgeving en rapportering

René Ewals - ACS

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Richtlijnen 3000A en 3000D

- Richtlijnen per 1 januari 2017 ingevoerd.
- Samenwerking NOREA en NBA.
- De 3000D is een Nederlandse invulling.
- Voorkeur voor Attest indien keuze.

Verschillen tussen Richtlijnen 3000 en 3402

Onderwerp	ISAE 3402	ISAE 3000 A & D
Mededeling Auditor	Gestandaardiseerd Redelijke zekerheid	'Vormvrij' (verplichte elementen) Redelijke of beperkte zekerheid
Vermelding Management	Verplicht	Verplicht (A) Niet verplicht (D)
Reikwijdte	Gerelateerd aan externe verslaggeving	Niet financiële cijfers
Publiek	Beperkt tot service en user organisations	Niet vooraf gedefinieerd
Normenstelsel	Individueel	Individueel
Testwerkzaamheden	Opnemen in rapport	Optioneel
Conclusie testwerkzaamheden	Opnemen in rapport	Optioneel

Verschillen tussen Attest en Direct Reporting

Onderwerp	Attest	Direct reporting
Doelstelling	De mate van vertrouwen van de beoogde gebruikers over de informatie over het onderzoeksobject vergroten.	De mate van vertrouwen van de beoogde gebruikers over de uitkomst van de meting of evaluatie van een onderliggend onderzoeksobject ten opzichte van de criteria vergroten.
Informatie over onderzoeksobject	Openbaar vermelding of bewering van de verantwoordelijke partij over de meting of evaluatie van het onderliggende onderzoeksobject	Geen vermelding of bewering van de verantwoordelijke partij aan de externe partij
Evalueerder	Andere partij dan de onderzoeker (accountant of IT Auditor).	De onderzoeker (accountant of IT Auditor).

Verschillen tussen Attest en Direct Reporting

Onderwerp	Attest	Direct reporting
Van toepassing zijnde criteria	Andere partij dan de onderzoeker besluit over de van toepassing zijnde criteria bij het opstellen van de informatie voer het onderzoeksobject. De onderzoeker bepaalt of de van toepassing zijnde criteria geschikt zijn in de omstandigheden van de opdracht.	De onderzoeker besluit veelal over de van toepassing zijnde criteria en zoekt overeenstemming met de verantwoordelijke partij dat de criteria geschikt zijn.
Niet voldoen aan de criteria	**Afwijking** van de informatie over het onderzoeksobject.	**Verschil** van het onderliggende onderzoeksobject met de van toepassing zijnde criteria.
Rapportage	• Het assurance-rapport bevat een conclusie welke betrekking kan hebben op het onderzoeksobject en de van toepassing zijnde criteria. • De informatie over het onderzoeksobject en de van toepassing zijnde criteria; of • Een overzicht dat door de geschikte partij is gemaakt.	Het assurance-rapport bevat een conclusie of het onderzoeksobject, in alle materieel van belang zijnde opzichten, overeenkomt met de van toepassing zijnde criteria.

Wanneer 3402 of 3000?

- De reikwijdte is bepalend.
- Een Richtlijn 3402 betekent dat de reikwijdte ***alle*** onderdelen bevat die (waarschijnlijk) relevant zijn in het kader van de jaarrekeningcontrole.
- Distributie van 3402–rapportage naar de cliënten en accountants van deze cliënten. Geen publicatie op Internet.

- Bij een 3000–rapport afspraken maken over:
  - Reikwijdte;
  - Distributie.

Nieuwe structuur mededelingen 3000 en 3402

- Waarom nieuwe structuur? Vanwege streven naar betere communicatie met ontvangers assurance-rapporten.
- Een assurance-rapport nieuwe stijl bestaat uit 10 onderdelen.
  - Titel
  - Aanhef
  - Ons Oordeel (met beperking)
  - De basis voor ons oordeel (met beperking)
  - Aangelegenheden met betrekking tot de reikwijdte van ons onderzoek
  - Beperkingen van een beschrijving en aan interne beheersingsmaatregelen bij een serviceorganisatie
  - Beperkingen in gebruik en verspreidingskring
  - Verantwoordelijkheden van het bestuur van de serviceorganisatie
  - Verantwoordelijkheden van de IT-auditor
  - Ondertekening
- De volgorde wordt mede ingegeven door het relatieve belang voor de lezer van het oordeel.
- De templates worden binnenkort gepubliceerd op de NOREA site.

Overwegingen rondom uitvoering OKB

- Door NOREA is een Handreiking OKB opgesteld (per 1 januari 2020). Hierin zijn suggesties voor het uitvoeren van een OKB opgenomen (in welke gevallen) alsmede een voorbeeld checklist die kan worden gebruikt (hoe).
- Bijvoorbeeld: een OKB wordt uitgevoerd als sprake is van een opdracht waarbij een externe deskundige is ingeschakeld en het rapport een brede verspreidingskring heeft.
- Een OKB omvat bijvoorbeeld:
  - Bespreking met de eindverantwoordelijke IT-auditor;
  - Een onderzoek van het dossier en het rapport (voornamelijk gericht op juistheid);
  - Onderzoeken geselecteerde dossierstukken die betrekking hebben op belangrijke standpunten van het opdrachtteam, alsmede de eindoordelen en adviezen.
- De OKB moet zijn afgerond voordat het concept-rapport wordt afgegeven.

Checklist OKB

Belangrijke aspecten van de OKB–checklist:

- Beoordeel de deskundigheid van het opdrachtteam;
- Beoordeel de klant– en opdrachtacceptatie, waaronder (indien van toepassing) of de IT–auditorganisatie en het opdrachtteam onafhankelijk zijn ten opzichte van het onderzoeksobject én de verantwoordelijke voor het onderzoeksobject.
- Beoordeel of de verantwoordelijkheid van de IT–auditorganisatie ten opzichte van de opdrachtgever duidelijk is afgebakend in de opdrachtbevestiging. Stel vast dat de inhoud van de opdrachtbevestiging minimaal overeenkomt met:
  a) Het doel van de opdracht.
  b) De verantwoordelijkheden van de IT–auditorganisatie.
  c) De verantwoordelijkheden van de opdrachtgever.
  d) De reikwijdte van de opdracht.
  e) De wijze van rapportering en andere vormen van communicatie over de resultaten van de opdracht, voor zover van toepassing.
  f) De waarborg voor de vrije toegang tot alle personen, informatiesystemen, vastleggingen, documentatie en andere informatie die in het kader van de opdracht wordt gevraagd.
  g) De wijze waarop het honorarium wordt vastgesteld en afspraken inzake het declareren, voor zover van toepassing.
  h) De afspraken over de planning.
  i) Een verzoek aan de opdrachtgever de acceptatie van de opdrachtvoorwaarden te bevestigen door het terugsturen van een getekend exemplaar van de opdrachtbevestiging.

Checklist OKB

- Andere relevante aspecten:
  - Werkprogramma past bij de opdracht;
  - Werkprogramma is uitgevoerd;
  - Rapport past bij opdrachtbrief;
  - Review is uitgevoerd op de uitgevoerde werkzaamheden;
  - Beoordeel de werkzaamheden van het opdrachtteam met betrekking tot de belangrijke risico's die tijdens de planning en het uitvoeren van de opdracht zijn gesignaleerd.
  - Beoordeel of geselecteerde dossierstukken passen bij de werkzaamheden/werkprogramma en bij de bevindingen/conclusies/adviezen.
  - Opmerkingen van de OKB-er moeten worden afgewerkt en akkoord zijn voordat concept-rapport wordt verstuurd.
  - De conclusie van de OKB-er.

Deel 2 SOC 2 en 3 reporting

Jeroen Francot - BDO

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

SOC rapporten

Guide van de AICPA (American Institute of Certified Public Accountants):

- SOC 1 (equivalent van de ISAE3402)
- SOC 2 (gericht op (IT) serviceorganisaties)
- SOC 3 (verkorte variant van SOC 2 gericht op een breed publiek)

SOC 2 versus ISAE3402

In de Nederlandse praktijk wordt nog vaak gebruik gemaakt van de bekende Standaard– of Richtlijn 3402 rapportages, ook wanneer er geen directe link is met financiële transactieverwerking.

SOC 2: Specifiek voor (IT) serviceorganisaties, met vaste beheersingsdoelstellingen (criteria) om eenzelfde basis te gebruiken.

SOC 2 - Toepassingsgebied

SOC 2 – gericht op IT serviceorganisaties

Gebaseerd op de Trust Services Criteria, onderverdeeld in vijf categorieën (categories):

- Security (verplicht);
- Availability;
- Processing Integrity;
- Confidentiality;
- Privacy.

Per categorie zijn een vast aantal beheersingsdoelstellingen (criteria) gedefinieerd. Het is echter niet verplicht alle criteria in de scope van de rapportage te betrekken, zo lang in de systeembeschrijving onderbouwd wordt welke criteria buiten de scope geplaatst zijn en daarbij een onderbouwing te geven.

SOC 2 - Systeembeschrijving

Description criteria: vereisten die worden gesteld aan de systeembeschrijving (system description)

- De systeembeschrijving is in overeenstemming met de description criteria wanneer:
  - Deze het systeem dat de serviceorganisatie heeft geïmplementeerd beschrijft;
  - Deze informatie bevat voor elk description criterion dat relevant is voor de verleende diensten;
  - Deze niet (on)bewust informatie weglaat die relevant zou kunnen zijn voor gebruikers.

- Tegelijkertijd wordt er ruimte gegeven om details in de systeembeschrijving weg te laten zodat een ‘hostile party’ te veel te weten zou kunnen komen over bijvoorbeeld security maatregelen

SOC 2 - Rapportage

- In Nederland is het niet mogelijk om te rapporteren op basis van AT–C205, dit is voorbehouden aan CPA's.

- Daarom wordt de SOC 2 rapportage in Nederland uitgebracht als een 3000 Attest–variant, gebaseerd op de Trust Services Criteria.

SOC 2 Logo

- In de USA is het mogelijk om een logo te verkrijgen. Dit is in Nederland niet zonder meer mogelijk, hiervoor is afstemming met de AICPA noodzakelijk.

Trust Services Criteria 2017

- Aanpassingen aan de security categorie op basis van COSO 2013
  - Hierdoor meer gericht op governance en interne beheersing
  - Criteria zijn nu mede gebaseerd op COSO Principles, bijvoorbeeld:

    COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

Trust Services Criteria 2017

- Toevoeging van points of focus
  - Points of focus geven richting aan de invulling van criteria, maar zijn niet verplicht.

2017 Trust Services Criteria (TSC)		
TSC Ref.	***Criteria***	***Points of Focus***
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	
		Establishes Oversight Responsibilities—The board of directors identifies and accepts its oversight responsibilities in relation to established requirements and expectations.
		Applies Relevant Expertise— The board of directors defines, maintains, and periodically evaluates the skills and expertise needed among its members to enable them to ask probing questions of senior management and take commensurate action.
		Operates Independently— The board of directors has sufficient members who are independent from management and objective in evaluations and decision making.
		Supplements Board Expertise —The board of directors supplements its expertise relevant to security, availability, processing integrity, confidentiality, and privacy, as needed, through the use of a subcommittee or consultants.

De privacy categorie

- Voorheen niet opgenomen, omdat criteria zeer gebaseerd waren op Amerikaanse wet– en regelgeving.
- Nu met de AVG wel mogelijk, mapping met het Privacy Control Framework.
- Voldoen aan de privacy categorie betekent echter niet dat de organisatie AVG–compliant is.

Verantwoordelijke versus verwerker:

- Criteria buiten scope plaatsen
- Onderbouwing van criteria buiten scope

SOC 3

- Verkorte variant van het SOC 2 rapport, bedoeld voor een ongelimiteerde verspreidingskring
  - Management statement
  - Assurance rapport
  - Verkorte systeembeschrijving
  - Geen beheersingsmaatregelen, testwerkzaamheden en testresultaten

SOC 3

- Onderliggende werkzaamheden zijn gelijk aan een SOC 2 rapport
- Het is uitsluitend mogelijk om een SOC 3 rapport uit te brengen met een goedkeurend oordeel

Deel 3: Praktijkervaringen Assurance

Dennis Houtekamer - EY

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Praktijkervaringen Assurance opdrachten

- Nieuwe standaarden/ mogelijkheden
- Beheersingsdoelstellingen
- Beheersingsmaatregelen
- Sub-serviceorganisaties en leveranciersmanagement
- Type oordelen
- Q & A

Nieuwe standaarden/ mogelijkheden

AICPA Attestation Vision

Beheersingsdoelstellingen

- Polling question:
  Als ik naar mijn eigen files kijk besteed ik voldoende aandacht aan de risicoanalyse?

1) Ja
2) Nee

Beheersingsdoelstellingen (2)

Formulering van Beheersingsdoelstellingen

- Specifiek
- Meetbaar
- Haalbaar en auditable
- Relevant en realistisch

Beheersingsmaatregelen

Management identificeert / update beheersingsmaatregelen die bijdragen aan het behalen van de beheersingsdoelstellingen, of voldoen aan de criteria.

1) Beoordeling van beheersingsmaatregelen

2) Omvat de formulering van de maatregelen onderstaande elementen:

- **Wat** is de inhoudelijke activiteit van de beheersingsmaatregel?
- **Wie** voert de maatregel uit?
- **Hoe** wordt de maatregel uitgevoerd?
- **Wanneer** wordt de maatregel uitgevoerd (met welke frequentie)?

Beheersingsmaatregelen (3)

Typical Risk	New IT application programs or changes to the production IT application programs (including reports and interfaces) are not appropriate for the business or the IT environment.	
Common ITGC	Changes are approved by management prior to the move to production based on vendor-supplied release notes.	
Control objective (WHY)	Controls provide reasonable assurance that no unapproved vendor-supplied changes do not disrupt the operation of the production environment.	
Test attributes	**Description**	**Guideline procedures**
A. WHAT	What evidence supports the performance of the control	Obtain a complete list of changes, select a sample of changes from the list and determine per inspection of evidence that the vendor-supplied release notes were reviewed and changes are approved.
B. WHEN	When is the control performed	Determine per inspection of evidence that the vendor-supplied release notes were reviewed and changes were approved prior to moving the change to production.
C. WHO	Who performs the control	Determine per inspection of evidence that approval is given by an appropriate member of business management other than the requestor.
D. HOW	How precise and sensitive is the control	Determine per inspection of evidence that appropriate actions are taken during the review of the vendor-supplied release notes.

Sub-serviceorganisaties en leveranciersmanagement

Is de derde partij een sub–serviceorganisatie (SSO) of een leverancier?

- De definitie van een SSO is ongewijzigd gebleven de vernieuwde standaard:

Een serviceorganisatie die door een andere serviceorganisatie wordt gebruikt om sommige diensten uit te voeren die aan gebruikersorganisaties worden verleend, waarvan de diensten deel uitmaken van het voor de (financiële) verslaggeving relevante informatiesysteem van die gebruikersorganisatie

- Meer focus op Third Party Risk Management

Sub-serviceorganisaties en leveranciersmanagement (2)

- Polling question:
  Datacenter is dat een SSO in een ISAE 3402–rapportage?

1) Ja
2) Nee

Sub-serviceorganisaties en leveranciersmanagement (3)

- Polling question:
  Het beveiligingsbedrijf ingehuurd door een DC is een SSO

1) Eens of
2) Oneens

Sub-serviceorganisaties en leveranciersmanagement

Subservice organizations	▪ Those vendors who execute controls necessary to achieve one or more of the objectives ▪ Monitoring controls over the subservice organization are described by the (primary) service organization
Carve-out method	▪ Controls are not included in scope ▪ Complementary subservice organization controls are described by the (primary) service organization
Inclusive method	▪ Controls are included in scope ▪ Subservice organization provides description and assertion relevant to the services executed

Toepassen van criteria op relevantie sub-serviceorganisatie

Beoordeling impact functies sub-service-organisatie	Effectiviteit van beheersingsmaatregelen bij de serviceorganisatie			
	Beheersingsmaatregel dekt de relevante beheersingsdoelstelling af.	Een combinatie van beheersingsmaatregelen dekt de relevante beheersingsdoelstelling af.	Beheersingsmaatregelen bij alleen de service-organisatie dekken de beheersingsdoelstellingen **niet** af.	Beheersingsmaatregelen bij de serviceorganisatie dekken de beheersings-doelstellingen **niet** af.
Beperkt	Niet verplicht	Niet verplicht	Verplicht	Verplicht
Gemiddeld	Niet verplicht	Verplicht	Verplicht	Verplicht
Uitgebreid	Verplicht	Verplicht	Verplicht	Verplicht

Type oordelen

Hoe om te gaan met (relevante) bevindingen?

Opinion	Conclusion
Unqualified opinion	The auditor concludes that all in-scope controls were suitably designed and/or operating effectively (when reporting on controls only) / all control objectives were achieved (when reporting on controls and related control objectives / Trust Services Criteria) and (in case of a ISAE3402 or SOC2 report) the system description fairly presented the system.
Qualified opinion	The auditor concludes that one or more controls were not suitably designed and/or not operating effectively (when reporting on controls only) / one or more control objectives were not achieved (when reporting on controls and related control objectives / Trust Services Criteria) and/or (in case of a ISAE3402 or SOC2 report) the system description did not fairly presented the system. We conclude that the possible effects on the subject matter of undetected misstatements, if any, could be material, but not pervasive.
Adverse opinion	We have obtained sufficient appropriate evidence, conclude that misstatements, individually or in the aggregate, are both material and pervasive to the subject matter.
Disclaimer of opinion	We are unable to obtain sufficient appropriate evidence on which to base the opinion, and we conclude that the possible effects on the subject matter of undetected misstatements, if any, could be both material and pervasive.

Volgende Webinar

Donderdag 5 november, 17:30 uur

Herziening Gedragscode – Code of Ethics

Bedankt

Voor meer informatie kun je contact opnemen met:

Commissie Beroepsreglementering
René Ewals, Robert Boon, Dennis Houtekamer, Jeroen Francot, Jan Matto, Jeroen Meulendijks

06 15 85 34 21
r.ewals@acs.nl

29 oktober 2020

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS