

FAQ IT-verslag en IT-auditverklaring

##	Vraag	Antwoord
1	Wat is het 'IT-verslag'?	De scope van een jaarverslag in zijn huidige vorm is te beperkt om een adequaat oordeel te vellen over de inrichting van de IT-beheersorganisatie en de beheersing van IT in brede zin (dus niet enkel de scope van de jaarrekening). Laat staan dat daarnaast ruimte is om bijvoorbeeld als organisatie verantwoording af te leggen of deze voldoende weerbaar is tegen cyberaanvallen en qua IT voorbereid is op de nabije toekomst. Een nieuwe rapportagevorm, het IT-verslag opgesteld door het management van de organisatie, geeft hier invulling aan.
2	Voor wie is het IT-verslag bestemd?	Bedrijfsleven en de overheid digitaliseren in hoog temp. De behoefte om 'in control' te zijn en te blijven wordt groter. Niet alleen voor de eigen organisatie maar ook in de toe- en afleveringsketen. Een IT-verslag om dit uit te dragen aan bijvoorbeeld een Raad van Commissarissen, dan wel om ketenpartners en andere belanghebbenden hierover te informeren is hiertoe bij uitstek geschikt. Belanghebbenden zijn niet alleen leveranciers, maar ook banken, consumenten, ratingbureaus, toezichthouders en in brede algemene zin het maatschappelijk verkeer.
3	Waarover wordt verslag gedaan?	Naar verwachting zal het IT-verslag bestaan uit zowel generieke onderwerpen (zoals informatiebeveiliging en continuïteit) als uit onderwerpen die cruciaal zijn binnen de sector waarin de organisatie opereert. Onderwerpen hierbij zijn onder meer: — Terugblik (afgelopen jaar) en vooruitblik (lopend jaar) — IT-strategie

##	Vraag	Antwoord
		— Gebruik moderne IT — Belangrijke projecten — Risico-analyse gericht op de inzet van IT — Patching — Versiebeheer — Continuïteit — Toegangsbeveiliging — Incidentmanagement — Changemanagement — Security — Cybersecurity — Uitbesteding — Investerings in IT — Kwaliteit Projectmanagement — Kwaliteit Systeemontwikkeling — Afhankelijkheid derde partijen — Innovatief vermogen — Artificial Intelligence
4	Wat is het verschil met bestaande rapportages als SOC1/2, ISAE 3000/3402, ISO-27001; Privacy Audit Proof, etc?	Er bestaan SOC1/2-rapporten, ISAE 3000 en/of 3402-rapporten, ISO-27001 certificaten en Privacy Audit Proof-rapporten die een belangrijke rol vervullen. Dergelijke rapporten hebben of een beperkte(re) scope, zijn primair historisch gericht en geven daarmee weinig ruimte om te rapporteren over de strategie, volwassenheidsniveau, ambities en de risico's daarbij. ISO27001 heeft de focus op informatiebeveiliging en is een standaard voor een Information Security Management System. De scope en doelstellingen van de

##	Vraag	Antwoord
		IT-auditverklaring is anders, informatiebeveiliging zal daar een onderdeel van zijn. Door de combinatie van het IT-verslag en een IT-auditverklaring kan daar invulling aan worden gegeven. Daarbij worden binnen de IT-auditverklaring, die naar verwachting op een ISAE3000 richtlijn zal worden gebaseerd uitgaan van andere auditstandaarden (IFAC). De IT-auditverklaring zal ongetwijfeld teruggrijpen op al bestaande best practices en bestaande normen en standaarden als het gaat om IT-processen. In de het IT-verslag kan bijvoorbeeld worden vermeld hoe de beheersing van IT in het afgelopen jaar heeft plaatsgevonden en wat de organisatie heeft gedaan om herhaling van incidenten te voorkomen. Het IT-verslag kan ook iets zeggen over de het beoogde volwassenheidsniveau en over de mate waarin IT binnen een organisatie toekomstbestendig is. Dat is voor de verschillende stakeholders belanghebbenden immers het meest relevant.
5	Wat zijn de verslaggevingscriteria voor een IT-verslag?	Los van de onderwerpen moet er nog werk worden verricht om te komen tot een set van criteria. Waaraan moet zo'n IT-verantwoording voldoen, welke onderwerpen en met welke diepgang kan een organisatie hierover verslag doen. Bij de ontwikkeling van de verslaggevingscriteria kijken we met name hoe GRI-standaarden voor duurzaamheidsverslaggeving diverse onderwerpen behandelt (globalreporting.org).
6	Hoe kun je als IT-auditor zekerheid geven over toekomstige gebeurtenissen (cyber incidents)?	Het zal duidelijk zijn dat de IT-auditor geen glazen bol heeft om de toekomst te voorspellen. We kunnen wel toetsen of aan de (verslaggevings)criteria wordt voldaan.

##	Vraag	Antwoord
		Een accountant zal bij grote ondernemingen in de nabije toekomst beperkte mate van zekerheid verschaffen over de duurzaamheidsverslaggeving van organisaties omtrent: — het bedrijfsmodel en de strategie van de onderneming inclusief de veerkracht ten aanzien van de risico's en de kansen — de wijze waarop de strategie is uitgevoerd en de plannen van de onderneming. We zijn van mening dat op een vergelijkbare wijze ook zekerheid omtrent de verslaggeving van IT-aspecten kan worden gegeven.
7	Welke assurance-richtlijn dient de IT-auditor toe te passen	Richtlijn 3000 (herzien) 'Assurance-opdrachten door IT-auditors' is hiertoe een geschikte standaard.
8	Wat is de relatie met de jaarrekeningcontrole van de accountant en kunnen de werkzaamheden in verband met de jaarrekeningcontrole en beoordeling van het IT-verslag geïntegreerd plaatsvinden?	Een IT-verslag kan onderdeel uitmaken of een overlap hebben met het bestuursverslag dat de organisatie als onderdeel van haar jaarlijkse financiële rapportage opstelt. Bij de jaarrekeningcontrole zal de accountant inzicht verwerven in het informatiesysteem en de IT-omgeving van de entiteit die relevant is voor het opstellen van de financiële overzichten. De scope van het IT-verslag is breder dan specifiek relevant voor het opstellen van financiële rapportages. Maar het inzicht dat is verkregen bij de jaarrekeningcontrole is een belangrijke input voor de toetsing van zo'n IT-verslag. Naar analogie van de sustainabilityverklaring zijn er twee mogelijkheden: ofwel de IT-auditverklaring en IT-verslag van de organisatie staan los van de accountantsverklaring en jaarrekening en jaarverslag, ofwel beiden zijn

##	Vraag	Antwoord
		geïntegreerd. Dit laatste (integratie) zal naar verwachting niet gelijk worden toegepast.
9	Hoe verhoudt zich het IT-verslag tot het oordeel van de accountant over de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking?	De accountant geeft geen oordeel over de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking. Indien bij de controle bevindingen zijn te melden zal de accountant dit in het accountantsverslag rapporteren. Het IT-verslag is een verantwoording van de organisatie waarbij de IT-auditor aanvullende zekerheid kan verstrekken.
10	Is het alleen voor bedrijven of ook voor instellingen en overheid?	Nee, het kan voor elke soort organisatie relevant zijn. Het gaat om het belang van de IT / digitalisering voor betrokken stakeholders.
11	Is er ook een Europese connectie of is het alleen een Nederlandse aangelegenheid? Denk ook aan regelgeving vanuit Europa, ontwikkeling als NIST-2 directive.	Het is primair een Nederlands initiatief. Maar er is in die zin een connectie dat EU-regelgeving relevant is voor de IT Auditverklaring. NOREA heeft connecties gelegd met de zowel de Online Trust Coalition met EU-verbindingen als GAIA-X waarbij vraagstukken als cloud en assurance op Europees niveau worden besproken. Overigens is NOREA een IFAC-affiliated organisatie waarbij internationale auditstandaarden worden gehanteerd. Deze standaarden zullen ook voor de IT-auditverklaring worden gehanteerd. In die zin zal er internationale herkenning zijn van de IT-auditverklaring die verder gaat dan Europa.
12	Is het IT-verslag alleen bedoeld voor kredietverstrekkers. Het FD-artikel geeft die indruk?	Nee, het kan voor alle betrokken stakeholders relevant zijn, daar kunnen kredietverstrekkers bij zitten.
13	Is het IT-verslag alleen voor grote ondernemingen, beursfondsen?	Nee, kan relevant zijn voor elke organisatie daar waar er sprake is van de inzet van een digitale systemen met een relevante impact op de organisatie of haar omgeving.
14	Kent het IT-verslag ook een volwassenheidsmodel?	Deze optie wordt nadrukkelijk door de werkgroep onderzocht.

##	Vraag	Antwoord
15	Is het IT-verslag vergelijkbaar met een 'in control statement'?	Nee, het IT-verslag is een verantwoording van de organisatie over diverse onderwerpen en is niet slecht een bewering of de organisatie in control is of niet.