Het NOREA Reporting Initiative

Op gestandaardiseerde wijze rapporteren over de organisatie en beheersing van IT

Alex van der Harst
is lid van de NRI-werkgroep van NOREA en is partner bij KPMG Advisory N.V.

Ronald van Langen
is lid van de NRI-werkgroep van NOREA, is senior manager bij KPMG Department of Professional Practice en is voorzitter van de Vaktechnische Commissie van NOREA.

Mariska de Kort
is senior manager bij KPMG Advisory N.V.

Tom Verharen
is lid van de NRI-werkgroep van NOREA en is junior manager Interne Auditdienst bij CZ.

Jurgen Pertijs
is senior manager Interne Auditdienst bij CZ.

In dit artikel schetsen wij de contouren van het NOREA Reporting Initiative (NRI) ([NORE24]). Dit initiatief is ontstaan vanwege de behoefte op een gestandaardiseerde wijze verslag uit te brengen en verantwoording te kunnen afleggen over de beheersing van IT. In maart 2023 heeft een publieke consultatie plaatsgevonden op het zogenoemde 'IT-verslag' en op dit moment worden de reacties verwerkt ([NORE23b]). We beschrijven de aanleiding voor dit initiatief en welke evolutie het geheel de afgelopen twee jaar heeft doorgemaakt. Uiteraard gaan wij ook in op de inhoud van de verslaggevingsstandaard. Naast het 'IT-verslag' wordt ook nagedacht over een 'IT-verklaring'. Ook hierop zullen wij nader ingaan.

Het opstellen van een verslaggevingsstandaard is één ding, maar het gebruik ervan is uiteraard iets wat in de praktijk moet blijken. Daarom schetsen wij ook de ervaringen die CZ heeft opgedaan tijdens een van de pilots waarin de verslaggevingsstandaard is toegepast.

AANLEIDING

Het behoeft inmiddels geen betoog meer dat IT van groot belang is in nagenoeg alle organisaties. Financiële administraties worden gevoed met gebruikmaking van IT, en voor veel organisaties speelt IT ook een cruciale rol in de operationele activiteiten. Hierbij kan het gaan om administratieve aspecten in de operatie zoals de import en distributie van bijvoorbeeld auto's, maar ook om de aansturing van productielijnen. Daarnaast speelt IT in de publieke taken natuurlijk ook een cruciale rol. Denk hierbij aan de aansturing van onze waterkering of aan de coördinatie bij de hulpdiensten.

Wanneer IT een rol speelt in de operatie, is zij voor een organisatie vaak een middel om strategische doelen te bereiken en is zij voor een deel bepalend voor de waardebepaling van een organisatie. In een situatie waarin het voortbestaan van een organisatie staat of valt met IT terwijl de IT-systemen slecht onderhouden zijn en qua kennis afhankelijk zijn van één of enkele persoon, zal de waardering van een organisatie lager uitvallen dan wanneer er sprake zou zijn van een kwalitatief hoogstaande IT-organisatie die snel kan inspelen op veranderende omstandigheden.

Wat opvalt is dat er voor organisaties veel specifieke verantwoordingsverplichtingen gelden op het gebied van IT, maar dat er nog een gebrek is aan een integrale verantwoording. Hier ontstaat een knelpunt: er bestaat een diversiteit aan rapportagevormen met verschillen in diepgang/reikwijdte, wat leidt tot redundantie, extra lasten, onvergelijkbaarheid en dubbelzinnigheid richting belanghebbenden.

Specifieke verplichtingen zijn er op het gebied van DigiD, ENSIA en bijvoorbeeld NEN 7510. Ook hebben toezichthouders zoals DNB en AFM specifieke verantwoordingsverplichtingen ingesteld. Internationaal gezien heeft de SEC recent een cybersecurityverantwoordingsplicht aangekondigd. Dit is de eerste verplichting waarbij een openbare verantwoording wordt verwacht. Daarnaast is een specifiek deel van de IT-beheersing (namelijk de IT-risico's die betrekking hebben op het financiële verantwoordingsproces en de beheersing van die risico's) ook een vast onderdeel van de accountantscontrole.

BW2 titel 9 artikel 393 lid 4 is een belangrijke wettekst als we spreken over IT binnen de jaarrekeningcontrole:

De accountant brengt omtrent zijn onderzoek verslag uit aan de raad van commissarissen en aan het bestuur. Hij maakt daarbij ten minste melding van zijn bevindingen met betrekking tot de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking.

Accountants controleren de jaarrekening van oudsher 'gegevensgericht', waarbij met detailcontroles en gegevensgerichte cijferanalyses wordt gecontroleerd of dit leidt tot het getrouwe beeld dat de jaarrekening dient te geven. Gedurende deze controle zal de accountant ook inzicht verwerven op het gebied van IT.

Steeds vaker zien we dat accountants een 'systeemgerichte' aanpak kiezen voor de jaarrekeningcontrole en daarbij gebruikmaken van de interne beheersingsmaatregelen die zijn ingericht rondom IT-systemen. Dit leidt doorgaans tot een combinatie van een systeem- en een gegevensgerichte controleaanpak. De accountant zal in het verslag aan de commissarissen en het bestuur mogelijk in beperkte mate rapporteren over de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking. De focus ligt alleen op die systemen die relevant zijn voor de financiële verantwoording en voor zover deze in scope zijn voor de jaarrekeningcontrole. Kortom, de informatie over de 'kwaliteit' (als die al gedefinieerd kan worden) van de geautomatiseerde gegevensverwerking als geheel wordt beperkt opgehaald in het kader van de jaarrekeningcontrole. En dat terwijl het om diverse redenen relevant kan zijn om deze beoordeling wel in een breder kader uit te voeren.

De constatering van de lacune tussen het cruciale belang van IT in brede zin enerzijds en de beperkte informatievoorziening over IT aan toezichthoudende organen zoals een RvC/RvT (en mogelijk andere belanghebbenden) anderzijds, heeft geleid tot het NOREA Reporting Initiative (NRI). Het doel van het NRI is om op een gestandaardiseerde manier inzicht te geven in de wijze waarop een organisatie de IT heeft georganiseerd, op een manier die ervoor zorgt dat de IT bijdraagt aan de strategische doelen van de organisatie. Dit past in het NOREA-manifest 'Op naar een digitaal weerbare samenleving' ([NORE23a]), dat in april 2023 is aangeboden aan de staatssecretaris van Koninkrijksrelaties en Digitalisering Alexandra van Huffelen en aan Nicole Stolk, directielid van De Nederlandsche Bank. Daarin is onder andere het advies opgenomen om externe verantwoording af te leggen over de IT-beheersing binnen een organisatie. Daarmee wordt een impuls gegeven aan de verantwoordelijkheid rondom de beheersing van IT.

Om uniformiteit te waarborgen is ervoor gekozen een verslaggevingsstandaard te ontwikkelen. NOREA heeft hiertoe het initiatief genomen en een eerste opzet vervaardigd en ontvangen feedback hierin verwerkt. Het is van belang te benoemen dat deze verslaggevingsstandaard nog in ontwikkeling is en deze vooralsnog geen formele status heeft. Daarnaast wordt onderkend dat de verantwoordelijkheid voor en het beheer van een dergelijke verslaggevingsstandaard niet bij de beroepsgroep van IT-auditors behoort te liggen, maar bij een organisa-

tie die hiervoor meer geëigend is. Dat is in deze fase nog niet verder geconcretiseerd. Deze verslaggevingsstandaard geeft handvatten en benoemt tevens de te beschrijven onderwerpen die, indien toegelicht, bijdragen aan het doel van het IT-verslag.

Het nu bestaande NRI heeft in de aanloop diverse ontwikkelingen doorgemaakt, wat logisch is als we de complexiteit in ogenschouw nemen die het gevolg is van:

- een divers landschap aan soorten organisaties (groot, klein, nationaal, internationaal, IT-driven of niet et cetera);
- reeds bestaande standaarden en normenkaders;
- de link met de jaarrekeningcontrole;
- het onderscheid publiek of privaat (publieke organisaties moeten transparanter zijn);
- de vraag of een organisatie beursgenoteerd is (beursgenoteerde organisaties moeten transparanter zijn);
- de sector waarin een organisatie opereert (externe verantwoording speelt meer in streng gereguleerde sectoren zoals banken en zorg);
- verschillende informatiebehoeften van diverse belanghebbenden. Voorbeelden hiervan zijn inzicht in verschillende aspecten van IT, mate van diepgang, focus op verantwoording over het verleden of toekomstbestendigheid et cetera.

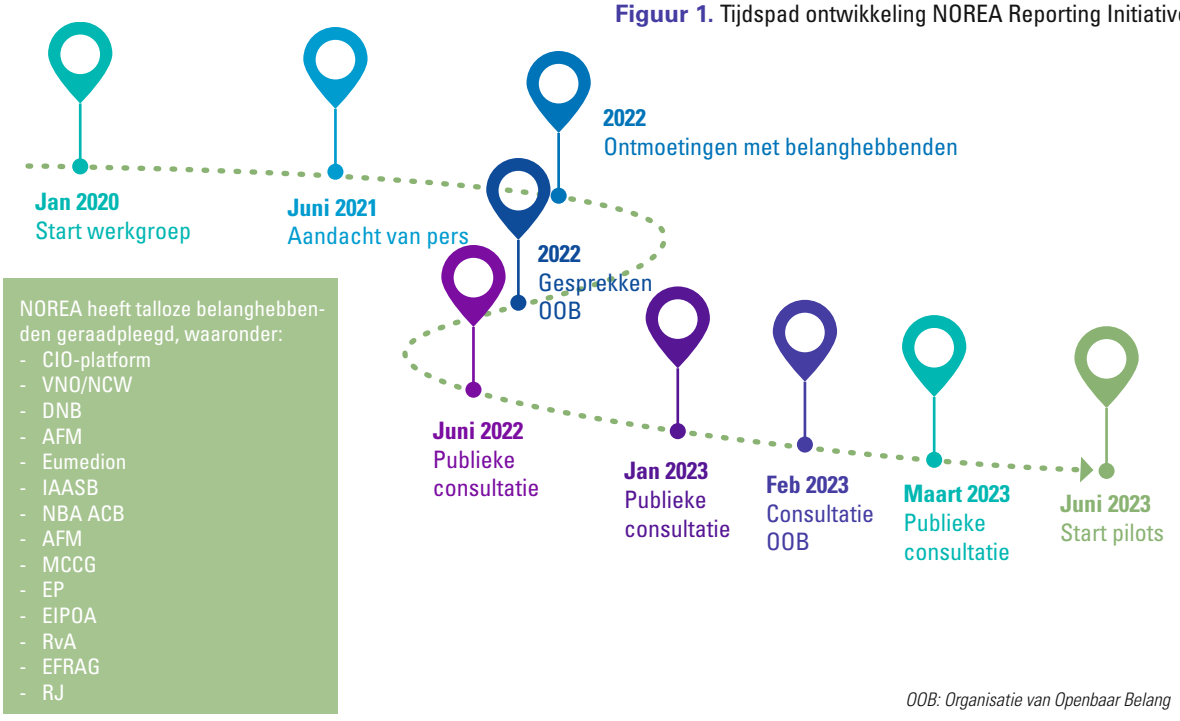
Een van de eerste vraagstukken was of de verslaggevingsstandaard een normenkader voor minimaal gewenste interne beheersingsmaatregelen en/of beheersingsdoelstellingen zou moeten omvatten. Het werd al snel duidelijk dat zo'n uniform normenkader niet is op te stellen, omdat organisaties zeer verschillend zijn. Daarnaast zijn er al verschillende normenkaders op de markt en een overlap met die normenkaders leek geen logische gedachte. Het NRI omvat dus zeker geen minimaal vereiste interne beheersingsdoelstellingen en interne beheersingsmaatregelen.

Ook is in de loop van de ontwikkeling duidelijk geworden dat het niet per definitie de doelstelling is om een IT-verslag voor het algemene publieke belang op te stellen. Al snel werd tegen het begrijpelijke bezwaar aangelopen dat een organisatie geen vertrouwelijke aspecten van haar IT-organisatie naar buiten wil brengen. Dit heeft er uiteindelijk in geresulteerd dat het NRI beoogt om primair een IT-verslag op te stellen voor bijvoorbeeld het toezichthoudende orgaan, waarbij het aan het toezichthoudende orgaan wordt overgelaten om te besluiten of het IT-verslag openbaar moet worden gemaakt. Het NRI omvat dus geen enkele verplichting om een IT-verslag openbaar te maken, maar wil in eerste instantie een verslaggevingskader bieden om organisaties inzicht te verschaffen in de stand van zaken rondom IT.

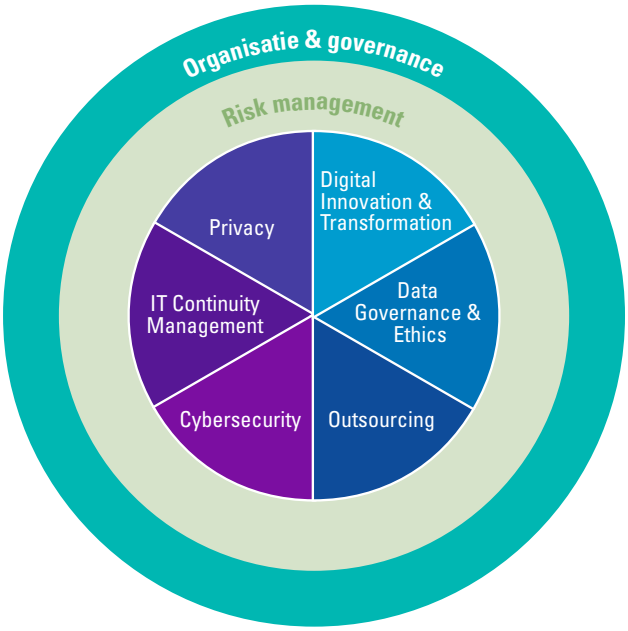
HOE ZIET EEN IT-VERSLAG CONFORM HET NRI ERUIT?

Zoals eerder beschreven is het IT-verslag geen normenkader met interne beheersingsdoelstellingen en/of -maatregelen. Dat betekent niet dat het ongestructureerd is. Er is gekozen voor een opzet en structuur in lijn met de GRI Sustainability Reporting Standards ([GRI]). Ener-

Figuur 1. Tijdspad ontwikkeling NOREA Reporting Initiative.



OOB: Organisatie van Openbaar Belang



Figuur 2. Samenhang generieke en specifieke thema's ([NORE23b]).

zijds biedt dit een modulaire opbouw, waarbij nu zes IT-thema's zijn uitgewerkt. Eventuele andere (optionele) IT-thema's kunnen later hieraan worden toegevoegd. Anderzijds geeft het NRI weer wat er per thema moet worden gerapporteerd, zonder dat hierbij een expliciet oordeel wordt gevraagd of de huidige IT-omgeving voldoet aan een bepaalde norm/vereiste zoals DORA, AVG of de Cyber Resilience Act. Ter illustratie omvat *GRI 418: Customer Privacy 2016* ([GRI16]) één rapportagevereiste zonder normstelling: 'rapporteer het totale aantal ontvangen gegronde klachten over inbreuken op de privacy van klanten, en het totale aantal geïdentificeerde lekken, diefstallen of verliezen van klantgegevens'. Aanvullend kan het Privacy Control Framework (PCF) van NOREA door entiteiten worden gebruikt om vast te stellen of de maatregelen ten aanzien van privacybescherming adequaat zijn in relatie tot bijvoorbeeld de AVG en omvat het 95 beheersingsmaatregelen. Het PCF kan leiden tot een Privacy Audit Proof-uiting.

Het IT-verslag kijkt in de breedte naar de organisatie van IT. Daarbij worden in het NRI twee hoofdsecties benoemd. De eerste sectie gaat in op meer algemene thema's rondom de organisatie van IT en de bijbehorende governance en op , alsmede risk management. De tweede sectie gaat in op specifieke thema's die per organisatie meer of minder relevant kunnen zijn.

Daarbij maakt de organisatie op zes IT-thema's een inventarisatie op het gebied van de huidige status van IT-beheersing enerzijds en de ambitie van de organisatie op het desbetreffende thema anderzijds. De rapportagestandaard besteedt specifiek aandacht aan elementen die cruciaal zijn voor een organisatie en die impact kunnen hebben op haar belanghebbenden, waaronder klanten, leveranciers, werknemers en andere werknemers, toezichthouders, investeerders en de samenleving. De standaard benoemt momenteel zes thema's:

- Digital Innovation & Transformation;
- Data Governance & Ethics;
- Outsourcing;
- Cybersecurity;
- IT Continuity Management;
- Privacy.

De verslaggevingsstandaard biedt handvatten door per thema de scope te duiden en door specifieke rapporteringsvereisten te beschrijven met bijbehorende specificaties ter onderbouwing. De verslaggevingsstandaard biedt lezers structuur en uniformiteit in de vorm van een gemeenschappelijk kader voor verslaglegging op het gebied van IT. Het verslag faciliteert daarmee het op een uniforme wijze schetsen van een beeld van verschillende organisaties.

OP WELK NIVEAU WORDT ER GERAPPORTEERD?

Het IT-verslag wordt opgesteld door de organisatie en is nadrukkelijk geen audit- of assurancerapport dat, zoals bekend, wordt opgesteld door een onafhankelijke externe auditor. De organisatie beschrijft op één moment in de tijd de huidige stand van zaken in de organisatie, waarbij in de beschrijving anderhalf jaar terug wordt gekeken en ook anderhalf jaar vooruit. Hierdoor worden gemaakte keuzes en ambities toegelicht in het verslag.

Het verslag beschrijft, zoals eerder gezegd, niet de opzet, het bestaan en de werking[1] van beheersingsmaatregelen, maar is gericht op het bieden van inzicht in de organisatie van IT aan relevante belanghebbenden. Er bestaat een nadrukkelijk onderscheid tussen het IT-verslag en normenkaders zoals NIST of ISO 27001 en tussen het IT-verslag en assurancerapportagestandaarden zoals SOC1, 2 en 3 en NOREA Richtlijn 3000. Daarnaast zullen vertrouwelijke detailgegevens over bijvoorbeeld cyberincidenten ook geen plaats krijgen in het verslag.

1 De opzet van een beheersingsmaatregel heeft betrekking op het ontwerp van de maatregel en de vraag in welke mate deze een onderkend risico afdekt. Het bestaan heeft betrekking op het op enig moment daadwerkelijk functioneren van de beheersingsmaatregel, terwijl de werking betrekking heeft op het daadwerkelijk functioneren van de beheersingsmaatregel over een langere (vaak gespecificeerde) periode.

Outsourcing

Om een beeld te schetsen van de uitwerking volgens het NRI beschrijven wij hieronder het thema 'Outsourcing'.

Het managen van outsourcing wordt volgens de standaard in zijn algemeenheid geadresseerd in hoofdstuk 1 van het verslag 'Management van IT' waarin zowel de organisatie van outsourcing als het risicomanagement op hoofdlijnen wordt beschreven als een resultaat van disclosure 'MGT-1.1: IT organization and governance'.

Daarnaast zijn er nog twee specifieke disclosures die betrekking hebben op het managen van outsourcing:

MGT-OUTS-1.1 - The reporting organization shall report how it manages outsourcing using requirements and the context and scope of the outsourcing in addition to 'Management of IT topics'.

MGT-OUTS-1.2 - The reporting organization shall describe how it manages risks related to its outsourcing of processes and services in addition to 'Management of IT topics'.

Een organisatie die heeft vastgesteld dat het uitbesteden van processen en diensten materieel is, is conform de standaard verplicht te rapporteren hoe hiermee wordt omgegaan. Organisaties beschrijven de impact van outsourcing op de eigen organisatie en ook op de keten van vraag en aanbod waarin de organisatie zich bevindt. Een organisatie beschrijft de inrichting van outsourcing langs drie relevante disclosures zoals beschreven in de standaard:

- *OUTS-1 Outsourcing is governed and managed and the value and other overall objectives of outsourcing are monitored and evaluated.*
- *OUTS-2 Candidate providers for outsourcing of processes and services are selected, evaluated (to determine preferred candidate) and services are contracted, implemented and (eventually) terminated based on identified requirements.*
- *OUTS-3 The delivery of services is managed based on identified requirements, including the connections (interfaces and handovers) with the rest of the organization, and service management.*

Om een uniforme verslaglegging te kunnen garanderen zijn de volgende vereisten verankerd in het NRI:

- *OUTS-1.1 The organization shall report how it conducts ongoing oversight over its outsourcing portfolio, including the ongoing evaluation of the overall outsourcing performance against objectives.*
- *OUTS-2.1 The reporting organization shall report on its processes, policies and procedures for the initiation, implementation and termination of outsourcing.*
- *OUTS-3.1 The reporting organization shall report on its policies and procedures on the ongoing monitoring of the performance of outsourced processes and services. This includes responding to occurrences (e.g. incidents) and other service management aspects.*

Vervolgens biedt het NRI per disclosure een nadere guidance om te komen tot een goede beschrijving. Ter illustratie hieronder een voorbeeld van guidance in relatie tot de tweede disclosure:

OUTS-2.1e The organization could describe how it handles the following topics:

- *the (re-)transfer of assets and data;*
- *documentation and archiving of the results of the termination efforts;*
- *fulfilment of contractual, compliance and regulatory obligations.*

DE ORGANISATIE BESCHRIJFT ZELF HAAR IT-ORGANISATIE EN IT-BEHEERSING

Het NRI heeft, zoals vermeld, tot doel om op een gestandaardiseerde uniforme manier inzicht te geven in de wijze waarop een organisatie de IT heeft georganiseerd en hoe IT bijdraagt aan de strategische doelen van de organisatie. Het management van de organisatie is het aangewezen orgaan om verslag te doen op basis van het NRI. Uiteraard kan de organisatie hiervoor ook gebruikmaken van externe partijen, maar het uitgangspunt is dat de organisatie zelf verantwoordelijk is voor het opstellen van het IT-verslag.

Het is hierbij relevant om terug te pakken op de eerdere stelling dat het NRI geen normenkader is. Het NRI schrijft bijvoorbeeld niet voor dat een organisatie aan NIST of ISO 27001/2 moet voldoen. Wel vraagt het NRI om te beschrijven of, en zo ja, aan welke informatiebeveiligingsstandaard de organisatie voldoet of wil gaan voldoen. Als er specifieke verantwoordingsverplichtingen gelden op het gebied van IT (bijvoorbeeld DORA, BIO of NEN 7510), dan zal dat vermeld worden. Tegelijkertijd geldt dat als de organisatie geen formele informatiebeveiligingsstandaard hanteert en dit als zodanig rapporteert, dit passend is in de geest van het IT-verslag.

ZEKERHEID GEVEN OVER HET IT-VERSLAG

Naar analogie van de jaarrekening, waarbij de organisatie de jaarrekening opstelt (conform een bepaalde verslaggevingsstandaard) en waarbij de accountant de jaarrekening controleert (conform auditstandaarden), bestaat uiteraard wel de mogelijkheid om het IT-verslag te laten onderzoeken door de interne auditor of externe accountant/IT-auditor. Hierbij is het mogelijk om een assuranceverklaring af te geven bij het IT-verslag, oftewel een IT-verklaring. Een IT-verklaring is een assurancerapport op basis van NOREA Richtlijn 3000A en omvat een oordeel of de inhoud van het IT-verslag een getrouw beeld geeft van de werkelijkheid om daarmee aanvullende zekerheid te verschaffen voor derde gebruikers. Dat NOREA nu initieel de verslaggevingscriteria zelf heeft vervaardigd behoeft in beginsel geen probleem te zijn om die te gebruiken voor een assuranceopdracht, mits de IT-auditor overeenstemming zoekt met de verantwoordelijke partij dat de criteria geschikt zijn.

Een IT-verslag kan worden opgenomen in het jaarverslag van de organisatie. Dit is dan complementair aan andere aspecten, zoals beschrijvingen van diverse ontwikkelingen binnen of rondom de organisatie. Ook hier kan de analogie met CSRD/ESG/sustainability reporting worden gemaakt en kan de organisatie ervoor kiezen het IT-verslag op te nemen in het jaarverslag.

Desondanks zitten daar wel enkele haken en ogen aan. In eerste instantie moet worden bepaald wat de rol is van de controlerend accountant met betrekking tot de beweringen in het IT-verslag (wordt er een afzonderlijk oordeel over opgesteld of is het te beschouwen als 'andere informatie'?). Een ander aspect dat hierbij speelt en dat wellicht wat weerbarstiger is, is de mogelijke tegenstrijdigheid tussen de beschrijving van IT-onvolkomenheden in het IT-verslag enerzijds en een goedkeurende verklaring anderzijds. Er zullen situaties zijn waarin vragen kunnen worden gesteld over hoe bepaalde beweringen in het IT-verslag zich verhouden tot een goedkeurende verklaring bij de jaarrekening. Daar waar de controlerend accountant ogenschijnlijke tegenstrijdigheden uitstekend kan rechtvaardigen, zal dit voor een lezer mogelijk niet altijd duidelijk zijn.

Het NRI beoogt niet om het IT-verslag een onderdeel te laten zijn van het jaarverslag. Wij denken dat het daarvoor op dit moment nog te vroeg is en dat er eerst bredere ervaring moet worden opgedaan met het IT-verslag zodat dit soort overwegingen kunnen worden geëvalueerd.

PILOT BIJ CZ: EEN IT-VERSLAG OPSTELLEN

Het afgelopen jaar heeft CZ ervaring opgedaan met het opstellen van een IT-verslag. CZ is onderdeel van de NRI-werkgroep van NOREA en vanuit deze rol heeft CZ een interne pilot uitgevoerd. De resultaten van de pilot zijn gedeeld met de werkgroep van NOREA. CZ was de eerste organisatie in Nederland die in pilotvorm aan de slag is gegaan met het schetsen van een integraal beeld van de thema's Digital Innovation and Transformation, Data Governance & Ethics, Outsourcing, Cybersecurity, IT Continuity Management & Privacy en het opstellen van een gerelateerd auditrapport.

Vanuit de Internal Auditdienst (IAD) van CZ waren Tom Verharen (senior auditor IAD) en Jurgen Pertijs (IT-auditmanager IAD) ieder op een eigen manier betrokken bij het opstellen van het IT-verslag en auditrapport.

Aanleiding

Een samenloop van omstandigheden heeft ertoe geleid dat CZ behoefte had aan een integraal beeld op het gebied van IT en dat het IT-verslag werd opgesteld. De CIO was destijds nieuw in zijn rol en het was vanuit zijn perspectief uitermate welkom om een beeld te krijgen van de IT-omgeving van de organisatie. Ook beschikt CZ over een IAD met RE's en een sterke relatie met de specialistische werk- en kennisgroepen van NOREA, waardoor CZ al in een vroeg stadium kennismaakte met het initiatief tot het NRI. Daarnaast bood het verslag een mogelijkheid om in samenhang zich een beeld te vormen van de IT-beheersing, groei en ambities.

Voorbereiding en aanpak

De raad van bestuur van CZ heeft opdracht gegeven een onderzoek uit te voeren en een IT-verslag op te stellen. De eigenaar en eindverantwoordelijke voor het verslag was de CIO. Hij heeft de aanpak mede bepaald om te komen tot het verslag en heeft ook een eerste indeling gemaakt van de functionarissen die erbij betrokken dienden te worden om te komen tot een IT-verslag. CZ heeft gekozen voor een projectmatige aanpak waarin met behulp van één workshop per thema informatie werd opgehaald voor het IT-verslag. De senior auditor van de IAD heeft als procesbegeleider het hele project begeleid; hij bracht vanuit zijn rol de inhoudelijke vaktechnische kennis in op het gebied van verslaglegging.

Iedere workshop nam twee uur in beslag en werd inhoudelijk voorbereid door de senior auditor vanuit de IAD. Per thema waren relevante stakeholders aanwezig bij de workshop. Denk voor het thema 'Outsourcing', zoals eerder in dit artikel uitgewerkt, bijvoorbeeld aan de manager concerninkoop, leveranciersmanagers en de manager infrastructuur. Gedurende de workshop werden alle disclosures van het NRI besproken. Daarbij werd teruggekeken en werd ook de ambitie op dat gebied besproken. De workshops werden ondersteund door het secretariaat om een goede vastlegging te waarborgen.

‘Op basis van de disclosures uit het NRI hebben we voor elk thema vragen opgesteld om een goede invulling te kunnen geven aan de workshops.’

– Tom Verharen (CZ)

‘Het uitvoeren van een audit op de totstandkoming van het IT-verslag was nieuw voor ons. De IAD van CZ heeft een rapport van feitelijke bevindingen uitgebracht.’

– Jurgen Pertijs (CZ)

Nadat de informatie was opgehaald in de workshops, heeft de CIO-afdeling per thema een samenvatting gemaakt die is afgestemd met relevante functionarissen. Deze samenvattingen tezamen hebben geleid tot het IT-verslag. Vanuit de IAD is hierbij ondersteuning verleend zodat werd gewaarborgd dat het verslag werd uitgebracht conform de NRI-standaard.

Het hele project om te komen tot een IT-verslag heeft vanuit de CIO-afdeling in totaal zo’n dertien dagen inzet gevraagd en ook de IAD heeft zich ongeveer elf dagen ingezet om te komen tot een IT-verslag. Het project kende een doorlooptijd van acht weken en heeft geleid tot een uitgebreid verslag dat vanuit meerdere perspectieven als zeer waardevol is ervaren.

Audit op het IT-verslag

Al tijdens de opzet van het project was de IT-auditmanager van de IAD voornemens om ook een audit uit te voeren op het IT-verslag om de raad van bestuur meer zekerheid te bieden over de inhoud van het verslag. Om deze audit effectief en efficiënt te laten verlopen heeft CZ ervoor gekozen de uitvoering van deze audit gedurende het project uit te voeren. Er is een auditdossier aangemaakt en gedurende de workshops heeft de IAD vragen gesteld en aanvullende documentatie opgevraagd om de betrouwbaarheid van uitspraken vast te stellen. De IAD heeft constateringen uit het IT-verslag bevestigd en aangevuld met observaties uit eigen waarneming van eerdere audits. De IAD heeft een auditrapportage over het IT-verslag uitgebracht en deze is, samen met het verslag, aangeboden aan de RvB, RvC en Audit-Risk Commissie. Het uitvoeren van de audit heeft van de IAD ongeveer zes dagen inzet gevraagd.

Het IT-verslag over 2021-2022-2023

Het IT-verslag is opgebouwd langs de eerder genoemde zes thema’s. CZ heeft al deze thema’s afgepeld en heeft daarbij, conform de verslaggevingsstandaard, anderhalf jaar terug- en ook anderhalf jaar vooruitgekeken. Alle thema’s zijn beschreven in het rapport op basis van de gestelde eisen in de standaard. Wel is het zo dat in bepaalde gevallen een keuze is gemaakt over de diepgang waarmee het thema is beschreven. In het geval van cyber security bijvoorbeeld is ervoor gekozen om bepaalde details niet op te nemen in het verslag.

Naast de zes specifieke thema’s heeft CZ ervoor gekozen om ook een aantal algemene hoofdstukken te beschrijven, omdat in de praktijk bleek dat er een aantal onderwerpen waren die werden herhaald bij ieder thema. Denk hierbij aan de strategiebeschrijving, de algemene organisatie en een beschrijving van de opzet en werking van de interne risicobeheersings- en controlesystemen van CZ.

Gebruikerservaringen

De destijds nieuw aangestelde CIO heeft het verslag positief ontvangen, enerzijds omdat hij in vrij korte tijd een goed beeld heeft gekregen van de status van de IT binnen CZ, en anderzijds omdat hij richting de voor hem relevante stakeholders een goede nulmeting en ook een communicatiemiddel had. Een bijkomend voordeel is dat de IAD de inhoud van het verslag onafhankelijk heeft getoetst.

Voor de RvB en de RvC is het van toegevoegde waarde geweest dat zij in één rapport, dat geschreven is in duidelijke taal, een totaalbeeld op het gebied van IT konden verkrijgen. Veel van de informatie was al geïsoleerd beschikbaar, maar is nu samengebracht in het IT-verslag. Daarbij is het zo dat de gestructureerde analyse van

IT-thema's het mogelijk heeft gemaakt om patronen te herkennen binnen deze thema's. Zo is bijvoorbeeld duidelijk op te merken dat de rol van CZ als IT-werkgever belangrijk is voor CZ als men kijkt naar de toekomst.

Het IT-verslag wordt door de gebruikers ervaren als een verrijking ten opzichte van de testuitkomsten die periodiek worden gecommuniceerd op het gebied van de werking van algemene IT-beheersingsmaatregelen (GITC's). Waar de algemene IT-beheersingsmaatregelen meer operationeel van aard zijn, is dit verslag door de wijze waarop de disclosures zijn opgesteld, veel meer tactisch en strategisch van aard.

Ervaringen en lessons learned uit het project

CZ kijkt met een positieve blik terug op het project 'IT-verslag'. Het NRI is niet als benauwend keurslijf ervaren en heeft de CIO in staat gesteld zijn verhaal op een gestructureerde manier te presenteren. De CIO heeft ervoor gekozen om periodiek een verslag te blijven uitbrengen. In welke vorm dit precies zal plaatsvinden is nog niet vastgesteld. CZ is van plan om in 2024 een verkorte versie van het IT-verslag op te stellen.

Door de positieve ervaringen heeft de IAD ervoor gekozen haar auditprogramma's in de toekomst vorm te geven langs de zes thema's van het verslag.

Bij een volgend verslag zullen, naast het gehele CIO office, business stakeholders en ook de afdeling risk management nog verder worden betrokken bij de workshops. Business stakeholders zijn eigenaar van het primaire proces en daarmee ook verantwoordelijk voor de inzet van IT hierin. Risk management beheert het risicomanagementproces waarin ook brede aandacht is voor IT-gerelateerde risico's. De ervaring heeft geleerd dat ook deze actoren zodoende een belangrijke rol spelen in het opstellen van een integraal beeld van de IT-beheersing.

'Het verslag leefde echt bij de raad van commissarissen. Je merkte dat zij het integrale beeld heel erg konden waarderen.'

– Jurgen Pertijs (CZ)

De pilot bij CZ heeft NOREA nieuwe inzichten gebracht. Zo zijn de algemene hoofdstukken zoals CZ deze heeft gedefinieerd, nu een vast onderdeel geworden van de NRI-standaard.

CONCLUSIE

Het NOREA Reporting Initiative is een initiatief dat is ontstaan om verslag uit te brengen en verantwoording af te leggen over de beheersing van IT op een integrale en gestandaardiseerde manier. Het initiatief is ontwikkeld vanwege het groeiende belang van IT in bijna alle organisaties en de noodzaak om hierover intern dan wel extern verantwoording af te leggen.

Het NRI is een verslaggevingsstandaard die ook de mogelijkheid biedt tot het afgeven van aanvullende zekerheid (assurance) omtrent de getrouwheid van een dergelijk verslag door een onafhankelijke auditor ('IT-verklaring'). Het NRI is geen normenkader voor minimum interne beheersingsmaatregelen, maar vraagt organisaties wel om bijvoorbeeld te beschrijven of, en zo ja, aan welke informatiebeveiligingsstandaard zij voldoen. Het NRI heeft als doel om op een gestandaardiseerde manier inzicht te geven in de manier waarop een organisatie IT heeft georganiseerd en hoe IT bijdraagt aan de strategische doelen van de organisatie.

Wij zijn van mening dat het NRI invulling geeft aan het groeiende belang dat IT heeft in het functioneren en de toekomstbestendigheid van organisaties. De structuur die het NRI hierbij biedt, geeft handvatten om de juiste relevante thema's te benoemen op een manier die herkenbaar zal zijn voor belanghebbenden als meerdere IT-verslagen naast elkaar worden gelegd. Organisaties worden in staat gesteld periodiek conform deze standaard verslag te doen. Daarbij kunnen vanwege de standaardisatie eenvoudig vergelijkingen worden gemaakt tussen meerdere rapportageperiodes. Wij kunnen ons ook voorstellen dat deze standaard kan worden gebruikt in due-diligenceonderzoeken; de standaardisatie en herkenbaarheid zullen daarbij een groot pluspunt zijn voor investeerders. In brede zin kan de standaard ook worden gebruikt om een nulmeting uit te voeren en om op basis hiervan acties te definiëren om het gewenste ambitieniveau te bereiken. Interne auditdiensten kunnen de standaard gebruiken om bijvoorbeeld in een driejarige cyclus de genoemde onderwerpen te onderzoeken om op basis hiervan een breed gesprek met het management aan te gaan over de wijze waarop IT kan bijdragen aan de doelen van de organisatie. Door de standaardisatie en het feit dat er een goed

doordachte verslaggevingsstandaard ligt, zijn de toepassingsmogelijkheden naar onze mening legio.

Wanneer het gaat om vereisten aan verantwoording vanuit diverse toezichthouders, is de druk op organisaties hoog. Veel organisaties moeten voldoen aan specifieke wet- en regelgeving, wat beslag legt op de beschikbare tijd van niet alleen de tweede, maar ook de eerste lijn. In dat licht zal ook ESG-regelgeving de komende tijd veel tijd vergen van organisaties. Het NRI zal naar onze mening de compliancegerelateerde werkdruk in de eerste lijn niet verder verhogen. Een IT-verslag opstellen conform het NRI kost uiteraard tijd, maar het betreft een weergave van de bestaande situatie, waarbij niet wordt voorgeschreven aan welke vereisten een organisatie moet voldoen. Uiteraard kan het opstellen van het IT-verslag ertoe leiden dat een organisatie bepaalde aspecten rondom de beheersing van IT anders c.q. beter wil aanpakken, maar dat komt dan voort uit een intern geïnitieerde behoefte aan verandering om de organisatie als geheel te verbeteren.

Wij zien derhalve het NRI als een gedegen hulpmiddel om inzicht te geven aan toezichthoudende organen en als middel voor organisaties om zichzelf te verbeteren. Wij denken dat het voor een verplichte toepassing momenteel te vroeg is. Er dient in de komende tijd meer ervaring te worden opgedaan met de standaard. Wel verwachten wij dat er vanuit toezichthoudende organen en investeerders meer vraag zal komen naar verslaglegging over de IT-omgeving, waarvoor deze standaard, zoals uiteengezet, een sterke basis is, mits deze ook wordt voorzien van een assuranceverklaring die aangeeft dat het verslag een getrouw beeld geeft van de werkelijkheid. Daarmee kan het self-assessmentkarakter worden overstegen en zal de toegevoegde waarde verder toenemen.

Literatuur

[NORE23a] Norea. (2023, maart 30). *NOREA-Manifest Op naar een digitaal weerbare samenleving.* Geraadpleegd op https://www.norea.nl/nieuws/norea-manifest-op-naar-een-digitaal-weerbare-samenleving

[NORE23b] Norea. (2023, 31 maart). *Norea Reporting Initiative v0.11.* Geraadpleegd op https://www.norea.nl/uploads/bfile/6357a197-6fd2-4904-b43e-7a85e123cb59

[NORE24] Norea. (2024). *Werkgroep Reporting Initiative.* Geraadpleegd op https://www.norea.nl/organisatie/werkgroepen/werkgroep-norea-reporting-initiative

[Fijn23] Fijneman, R. (2023, januari). *IT governance report: food for thought and next steps.* Board Leadership News KPMG.

[GRI] Global Reporting Initiative. (z.d.). *Standards.* Geraadpleegd op 23 januari 2024, van https://www.globalreporting.org/standards/

[GRI16] Global Reporting Initiative. (2016). *GRI 418: Customer Privacy 2016.* Geraadpleegd op https://www.globalreporting.org/standards/media/1033/gri-418-customer-privacy-2016.pdf

Over de auteurs

Alex van der Harst is lid van de werkgroep NRI van NOREA en is partner bij KPMG Advisory N.V. met meer dan 25 jaar ervaring op het gebied van IT-audit (RE), projectmanagement, informatiebeveiliging en IT-audit in het kader van de jaarrekeningcontrole. Hij was tot juli 2023 bestuurslid van NOREA en heeft een brede portefeuille van private en beursgenoteerde organisaties, voornamelijk projectorganisaties en klanten in de energiesector.

Ronald van Langen is lid van de werkgroep NRI van NOREA en is als senior manager werkzaam bij KPMG Department of Professional Practice (DPP). Hij houdt zich binnen DPP onder meer bezig met audit- en assurancemethodologie, IT in de audit, XBRL en ESG-assurance. Daarnaast is hij de voorzitter van de Vaktechnische Commissie van NOREA.

Mariska de Kort is senior manager bij KPMG Advisory N.V op het gebied van IT-audit. Zij heeft een achtergrond als klinisch informaticus en heeft tevens een graad in de bestuurskunde. Ze heeft ervaring met het controleren van ondernemingen op het gebied van de gezondheidszorg, life science en welzijn.

Tom Verharen is junior manager Interne Auditdienst van CZ en is lid van de werkgroep NRI van NOREA. Daarnaast is hij lid van de NOREA Kennisgroep Cybersecurity en is hij medeauteur van het NOREA Handreiking Security Operations Center Maturity Framework. Binnen CZ houdt hij zich bezig met audits op onder andere IT-governance, artificial intelligence en cybersecurity.

Jurgen Pertijs is senior manager Interne Auditdienst van CZ en vanuit die rol verantwoordelijk voor de IT- en operational audits binnen CZ. Daarnaast is hij lid van de werkgroep voor de herziening van het Maturity Model Informatiebeveiliging van NBA-LIO en NOREA.

De NRI-werkgroep binnen NOREA bestaat uit ongeveer twintig personen met een brede afvaardiging uit diverse organisaties, waaronder EY, KPMG, Deloitte, PwC, BDO, Mazars, ACS, TOPP Audit, Verdonck Klooster en Associates, ABN Amro, UWV en CZ. Een volledige lijst is opgenomen in de versie die is uitgebracht voor publieke consultatie.