NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

International Digital Reporting Standards (IDRS)

Beheersing van IT verdient complete reset

Van versnipperde compliance naar holistisch kader

In een hyperdigitale wereld draait alles om betrouwbare en stabiele IT-systemen. Zonder maatschappelijk vertrouwen daarin zou de maatschappij niet langer functioneren. Organisaties kunnen werken aan dat vertrouwen door op de juiste manier inzichten te geven over hun digitale systemen. Om dat effectief te doen is een radicaal ander concept nodig voor rapportages. NOREA werkt aan de broodnodige ommekeer van de huidige praktijk.

Nieuwe problemen vragen om nieuwe oplossingen

- Organisaties werken steeds meer in ecosystemen en zijn zeer afhankelijk van partners voor betrouwbare digitale toepassingen.
- In zo'n sterk verknoopte digitale wereld zijn er andere oplossingen nodig om de technologie te beheersen.
- Alleen met een ecosysteembenadering kunnen we het maatschappelijk vertrouwen in technologie behouden.
- Dat is een totaal andere benadering dan de huidige praktijk waarin de individuele organisatie centraal staat.
- De International Digital Reporting Standards biedt de bouwstenen voor die oplossing.

1 Introductie

Software 'is eating the world' en dat proces versnelt de komende jaren met de opkomst van AI. Digitale technologie verknoopt organisaties steeds meer tot hechte ecosystemen waarbij de grenzen tussen organisaties vervagen en onderlinge afhankelijkheden toenemen. Dat gaat niet zonder risico's en met een flinke stapel wetgeving willen beleidsmakers grip daarop krijgen.

Een van de effecten: versnippering in de aanpak ervan. Deze versnippering is niet alleen inefficiënt (hogere regeldruk) maar dreigt ook het doel van de wetgeving naar de achtergrond te drukken. Dat doel is immers cyberweerbaarheid door het goed functioneren van organisatie-overstijgende ketens en het ecosysteem – met betrouwbare en solide digitale processen – en *niet* de compliance van afzonderlijke organisaties.

Precies daarom is er een ommezwaai nodig in (het denken over) IT-beheersing. De uitdaging: op een eenduidige en holistische manier inzicht bieden in de kwaliteit en betrouwbaarheid van IT, zodat zowel toezichthouders als direct betrokken stakeholders waardevolle inzichten krijgen. Zodat er een

einde komt aan de versnippering (en daarmee de hoge regeldruk). En zodat dit thema prominent op de bestuurstafel komt.

Dat is waar de International Digital Reporting Standards (IDRS) over gaat. Een jaarlijks verslag over IT zorgt dat (1) de maatschappij kan blijven rekenen op betrouwbare systemen (2) organisaties veel efficiënter (*zero repetition*) kunnen voldoen aan wetten en regels voor beheersing van IT en (3) onderbezette toezichthouders meer lucht krijgen omdat de uitvoering van hun toezichtstaken effectiever wordt.

2 Waarom een reset nodig is

In de zomer van 2024 moesten vliegvelden, hotels en tal van andere organisaties hun operaties stilzetten omdat medewerkers de *blue screen of death* op hun computerschermen te zien kregen. Al snel bleek dat het probleem werd veroorzaakt door de producten van beveiligingsbedrijf Crowdstrike. Veel van de getroffen organisaties waren verrast dat problemen in de keten van toeleveranciers hun organisatie zo hard raakten. De prettige bijvangst van deze ingrijpende gebeurtenissen: *resilience* – de weerbaarheid tegen verstoringen van systemen – werd meer dan ooit een belangrijk thema op menig bestuurstafel. Eens te meer werd duidelijk dat digitale technologie niet alleen cruciaal is in alles wat we doen – “software is eating the world”, zo sprak Venture Capitalist Marc Andreessen jaren geleden al – maar ook dat we leven in een wereld waar organisaties in grote mate afhankelijk zijn van door digitale technologie gestuurde systemen. Met andere woorden: “software is also connecting the world”.

Een andere beweging is de omslag in het denken over IT: van automatisering naar digitalisering. Waar IT in de afgelopen decennia vooral leidde tot procesverbeteringen en meer efficiency, bepalen IT en data nu steeds meer het verdienmodel.

Dat creëert nieuwe uitdagingen, zoals een enorme toename van complexiteit en bijbehorende risico’s op uitval of inbreuken op de bescherming van gegevens. Een bijkomend effect is dat het verzamelen van data door ontwikkelingen als Cloud en low code nu overal in de organisatie plaatsvinden. Dat maakt het lastiger om er grip op te houden.

Deze ontwikkelingen zijn de beleidsmakers en wetgevers niet ontgaan. Zij weten dat de weerbaarheid van organisaties in het geding is, en daarmee de weerbaarheid van de gehele samenleving. Dat heeft op nationaal en Europees niveau geleid tot wetgeving die weerbaarheid moet vergroten, en ook andere aspecten regelt, zoals risico’s van digitalisering, privacy en ethische toepassing.

De uitdaging is nu om te komen tot een (veel) effectievere implementatie. We signaleren daarbij de volgende uitdagingen:

- Er is het risico van *form over substance*. Wetgeving heeft een duidelijk doel en het motto bij implementatie zou moeten zijn 'niet omdat het moet maar omdat het ertoe doet'. Toch staat bij implementaties vaak de formele compliance voorop en zo raken de inhoudelijke doelstellingen van de wet uit het zicht.
- Er ligt veel focus op (de compliance van) individuele organisaties. De vraag is echter niet of een enkele organisatie aan de wet voldoet, de vraag is of een organisatie voldoende in control is en daarmee bijdraagt aan een stabiel en weerbaar ecosysteem in de digitale samenleving.
- Voor vergelijkbare onderwerpen bestaan verschillende regels en regimes en dat leidt tot een stapeling van regeldruk. Deze zal de komende jaren verder groeien: er staan meer dan 100 initiatieven op de agenda in EU-verband. De Europese commissie herkent dit risico en zet in op harmonisatie. Organisaties kunnen er zelf ook wat aan doen door het bundelen van wetgeving in hun implementatie (*zero repetition*). Ze slagen daar maar ten dele in en ook in de praktijk van audits en certificering is – tot verdriet van veel bestuurders – sprake van te veel repeterende en overlappende activiteiten.
- Toezichthouders staan voor praktische uitdagingen. Ze krijgen met de komst van een golf aan wetgeving steeds meer taken en zoeken naar manieren om dit uitdijend takenpakket aan te kunnen.
- De veelgehoorde roep om 'duidelijke regels' kan gemakkelijk ontaarden in gedetailleerde lagere regelgeving, met een zogenaamd 'rules-based' in plaats van 'principle-based' karakter. Dat beperkt de ruimte voor organisaties om maatregelen op maat te nemen die passen bij de typologie en specifieke context van een organisatie. Zo kan er een mismatch ontstaan tussen enerzijds wat er vanuit management optiek nodig is voor goede beheersing en anderzijds wat de wetgeving beoogt.
- Tot slot is er sprake van een door de CSR (CyberSecurityRaad) benoemde 'bestuurlijke kloof'. Die dient zich aan als het managen van digitale technologie, cybersecurity, weerbaarheid en gerelateerde onderwerpen volledig 'weg' wordt gedelegeerd naar IT- of securitymanagers en -afdelingen. Bestuurders hebben dan weinig zicht op hoe digitale technologie effectief en beheerst wordt ingezet. Een belangrijke oorzaak is het ontbreken van bruikbare, heldere en voor bestuurders begrijpelijke communicatie van IT naar bestuur, en van bestuur naar interne toezichthouders.

3 Hoe het anders kan: een jaarlijkse verantwoording

Ons idee is in de kern heel simpel. Organisaties geven nu elk jaar inzicht in hun financiële performance (en de maatschappelijke impact) in een jaarverslag. Op soortgelijke wijze kunnen ze ook een verslag over hun IT uitbrengen.

De International Digital Reporting Standards (IDRS) maakt dit werkelijkheid. Ontwikkeld door NOREA, de beroepsorganisatie van IT-auditors in Nederland, biedt IDRS een gestandaardiseerde aanpak voor rapportage over IT-beheersing. Stakeholders krijgen zo helder inzicht in hoe zij kritieke IT-thema's aanpakken, zoals cybersecurity, data governance en IT-continuïteit. Geïnspireerd door de methodiek van de GRI Sustainability Reporting Standards stelt het organisaties in staat om IT-rapportage naadloos te integreren bestaande rapportages.

Kenmerken van IDRS zijn:

- **Keuze voor materiële onderwerpen:** IDRS omvat alle 6 centrale IT-thema's, waarbij organisaties zelf op basis van hun specifieke situatie kunnen bepalen welke de voor hen relevante thema's zijn. Dat is een praktijk die ook gehanteerd wordt voor CSRD-rapportages, waar zogeheten dubbele materialiteit het uitgangspunt is.
- **Gestandaardiseerde rapportage:** IDRS is een gedeeld raamwerk dat consistente en zinvolle rapportages over belangrijke IT-onderwerpen mogelijk maakt. Elk thema bevat verplichte openbaarmakingen, rapportagevereisten en richtlijnen voor consistente en uitgebreide rapportages. Juist vanwege de hiervoor geschetste uitdaging om naar het ecosysteem als geheel te kijken is het belangrijk dat partijen dezelfde taal spreken, niet alleen inhoudelijk maar ook voor de wijze van toetsing. Dan is het voor alle stakeholders beter te begrijpen.
- **Gericht op continue verbetering:** IDRS vereist een systematische aanpak om verbeterpunten in het IT-management van organisaties te identificeren en aan te pakken.
- **Een efficiënte aanpak:** IDRS omvat een framework dat eisen vanuit wetgeving integreert en daarmee een einde maakt aan de bestaande versnippering van compliance- en auditwerk.
- **Focus op governance en risicomanagement:** De nadruk ligt op de cruciale rol van organisatie, governance en risicomanagement binnen effectief IT-beheer.
- **Afstemming op best practices:** De richtlijnen zijn gebaseerd op erkende standaarden en best practices, wat benchmarking en continue verbetering vergemakkelijkt.
- **Audit-ready:** IDRS biedt handvatten voor onafhankelijke assurance over gerapporteerde informatie, wat het vertrouwen van stakeholders verder versterkt.
- **Gericht op niet-IT-experts**. De rapportages zijn bedoeld om niet-IT'ers inzicht te geven in de kwaliteit van control, in een voor hen leesbare en begrijpelijke vorm

De voordelen van het toepassen van IDRS zijn evident. Het verslag speelt niet alleen in op de moderne eisen aan transparantie vanuit de maatschappij maar stimuleert ook bewustzijn binnen organisaties – en bij partners in het ecosysteem – over de verantwoordelijkheden. Het legt de verantwoordelijkheid voor deze onderwerpen waar deze hoort, bij de hoogste leiding (chefsache).

Essentieel is, dat een IDRS IT-verslag geen ‘afvinkexercitie’ is, maar een grondige inventarisatie. Het heeft substantie en geeft inzicht in alle relevante IT-gerelateerde thema’s voor de organisatie. Het biedt daarmee breed inzicht in de digitale fitheid van de organisatie met ook inzicht in de innovatieve kracht en invulling van de ethische toepassingen.

4 Een onvermijdelijke toekomst waarin IT-beheersing nog belangrijker wordt

De toekomst voorspellen is onmogelijk. Maar het is onvermijdelijk dat het beheersen van digitale technologie steeds belangrijker wordt nu digitalisering in hoog tempo verder gaat. Het is waarschijnlijk dat er de komende jaren sprake zal zijn van een toename van dreigingen voor weerbaarheid en continuïteit. De potentiële impact van die verstoringen kan zeer groot zijn voor organisaties die zich onvoldoende voorbereiden.

Precies daarom is het essentieel als organisaties jaarlijks inzicht krijgen in hoe ze dat doen, om zich daarmee ook scherp te kunnen houden. Net zoals het financiële jaarverslag de geaccepteerde norm is zal een jaarlijks IT-verslag *business as usual* worden. Het is welbeschouwd onbegrijpelijk dat zo’n verslag er nog niet is, aangezien digitale technologie de bloedsomloop van de moderne samenleving vormt. Er staat veel op het spel: het gaat over het dagelijks functioneren van de maatschappij. Het belang van dit verslag zal dan ook belangrijker worden dan het financiële jaarverslag, ook al omdat IT-beheersing randvoorwaardelijk is voor financiële beheersing.

Een aantoonbaar beheerste IT wordt een factor waarmee ondernemingen het verschil kunnen maken in de markt, bij aandeelhouders en in de maatschappij.

Over NOREA

NOREA is de beroepsorganisatie van IT-auditors in Nederland en beheert het register van gekwalificeerde IT –auditors (RE’s). De organisatie heeft ruim 1.600 leden en 300 aspirant-leden (d.w.z. IT-auditors in opleiding). Het register geeft aan opdrachtgevers en derden de mogelijkheid om vast te stellen of iemand op grond van zijn of haar opleiding en ervaring heeft voldaan aan de eisen die door de beroepsorganisatie worden gesteld.

NOREA is geaccrediteerd door de NBA (Nederlandse Beroepsorganisatie van Accountants) waardoor RE’s op gelijke voet met registeraccountants opereren. NOREA houdt toezicht op de kwaliteit van de beroepsuitoefening van de RE’s.

In onze gedigitaliseerde wereld kennen IT-auditors drie aandachtsgebieden, te weten:

1. Waarborgen van de continuïteit van IT om reputatieschade en verlies van omzet te voorkomen.
2. Beheersen van (Cyber)risico’s om betrouwbare gegevensverwerking te waarborgen.
3. Beveiligen van het ‘goud’ (de data) en waarborgen dat deze data betrouwbaar blijft.