



Risicobeheersing begint met inzicht

Waarom geen organisatie zonder **IT-jaarverslag** kan

Grote organisaties hebben een groeiende verantwoordelijkheid om transparant te rapporteren over hun IT-beleid en de realisatie daarvan. Een IT-jaarverslag, liefst goedgekeurd door de IT-auditor, is daarvoor een goede oplossing, adviseert Rob Fijneman.

ONDANKS DE CRUCIALE ROL VAN IT IN MODERNE ORGANISATIES, WORDT TECHNOLOGIE NOG TE VAAK ALS EEN ONDERSTEUNENDE FUNCTIE BESCHOUWD. Bestuursleden en toezichthouders delegeren IT-gerelateerde beslissingen doorgaans aan de CIO en zijn of haar team, terwijl de impact van digitalisering op de lan-

viteit van onze digitale transformatie? Het IT-jaarverslag kan hierbij een cruciale rol spelen. Bestuurders kunnen zich verantwoorden over hun IT-beslissingen en het toezicht daarop.

IT-governance en compliance nu

De afgelopen jaren heeft regelgeving rondom IT-veiligheid en compliance een vlucht genomen. Zowel op Europees als nationaal niveau worden steeds strengere eisen gesteld aan hoe organisaties omgaan met IT-risico's. Denk hierbij aan:

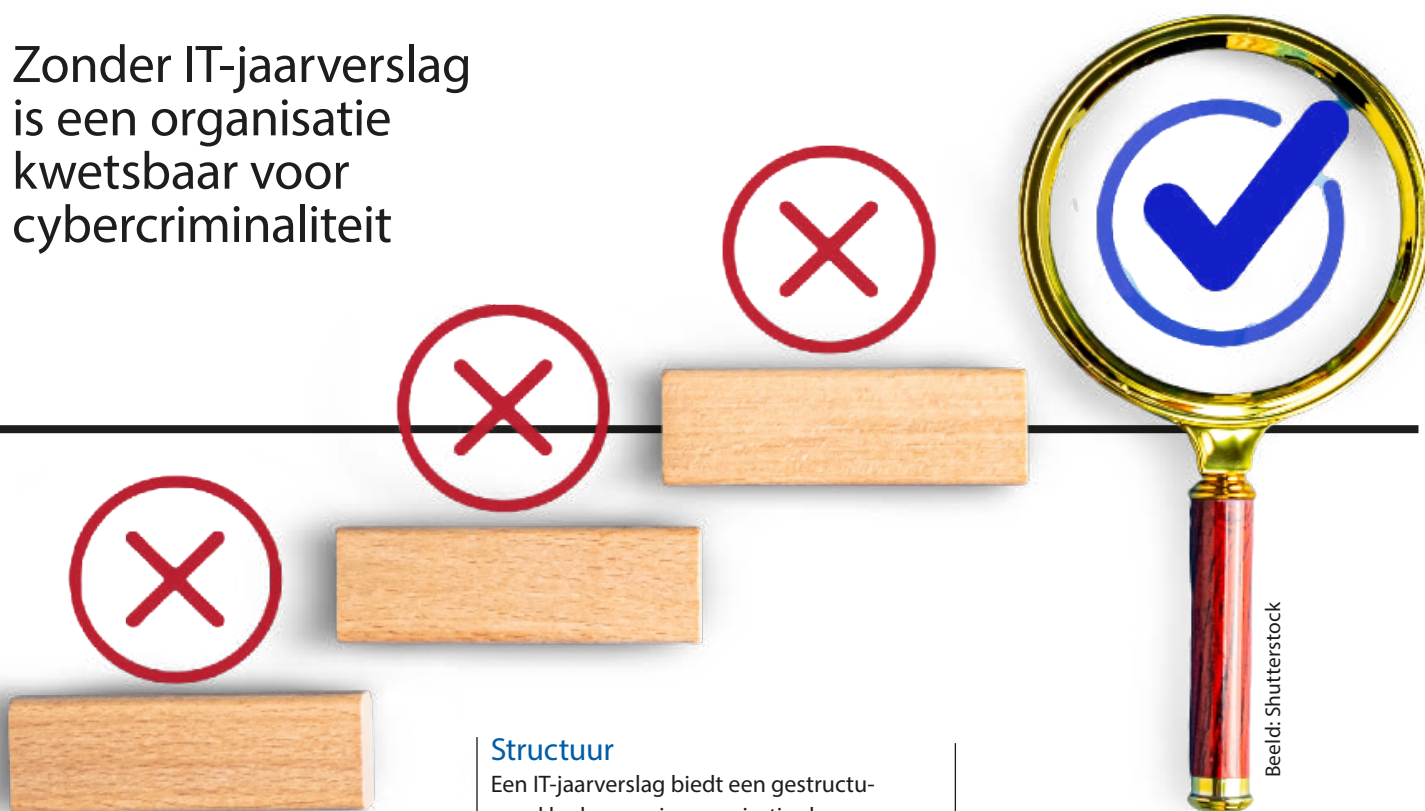
- DORA (Digital Operational Resilience Act): gericht op de weerbaarheid van financiële instellingen tegen cyberdreigingen.
 - NIS2 (Network and Information Security Directive): een bredere richtlijn voor cybersecurity in vitale sectoren.
 - AI Act: reguleert het gebruik van kunstmatige intelligentie om o.a. ethische risico's en bias te verminderen.
 - SEC Cybersecurity Rules: stelt eisen aan de rapportage van cyberrisico's voor beursgenoteerde bedrijven.
- De implementatie en naleving van

Aan organisaties worden steeds hogere eisen gesteld als het gaat om IT-risicobeheersing

getermijnstrategie en risicobeheersing cruciaal is voor de organisatie als geheel. Bestuurders moeten zichzelf kritische vragen stellen:

- Hebben we redelijke zekerheid dat onze IT-strategie in lijn is met de bedrijfsdoelstellingen?
- Is ons digitale risicomanagement robuust genoeg om compliance en veiligheid te waarborgen?
- Hoe meten en evalueren we de effecti-

Zonder IT-jaarverslag is een organisatie kwetsbaar voor cybercriminaliteit



Beeld: Shutterstock

deze regels vraagt om een gestructureerde aanpak. IT-auditing speelt een sleutelrol door organisaties te helpen inzicht te krijgen in waar ze staan op het gebied van compliance en hoe ze hun digitale weerbaarheid kunnen verbeteren.

Daarnaast is de rol van IT-auditors de afgelopen jaren steeds breder geworden. IT-auditors kijken niet alleen naar de naleving van regelgeving, maar beoordelen ook de effectiviteit en efficiëntie van digitale processen. Dit is een belangrijke verschuiving, omdat organisaties niet alleen compliant willen zijn, maar ook waarde willen halen uit hun digitale investeringen. Dit betekent dat IT-auditors steeds vaker betrokken worden bij strategische besluitvorming, waarbij ze adviseren over de integratie van IT in de bredere bedrijfsstrategie.

Structuur

Een IT-jaarverslag biedt een gestructureerd kader waarin organisaties hun IT-beleid, risicobeheersing en compliance kunnen documenteren. De voordelen hiervan zijn:

1. **Transparantie en verantwoording**
Stakeholders, waaronder toezichthouders en aandeelhouders, krijgen beter inzicht in IT-gerelateerde risico's en de maatregelen die worden genomen om deze te beheersen.
2. **Versterking van digitale weerbaarheid**
Een gestructureerd verslag dwingt organisaties om hun cybersecurity en compliance-strategie grondig te analyseren en te verbeteren.
3. **Verbeterde governance en risicobeheersing**
Door IT expliciet op de agenda te zetten, wordt de betrokkenheid van bestuurders en toezichthouders vergroot.
4. **Consistente rapportage en vergelijkbaarheid**
Een gestandaardiseerd IT-jaarverslag maakt het makkelijker om pres-

taties en risico's over meerdere jaren te vergelijken en te benchmarken met andere organisaties.

Het NOREA IT-Reporting Initiative

De beroepsorganisatie voor IT-auditors, NOREA, heeft het IT-Reporting Initiative (NRI) ontwikkeld om organisaties te ondersteunen bij het opstellen van een IT-rapportage.

Dit initiatief is bedoeld om:

- Een uniforme structuur te bieden voor IT-rapportage.
- Transparantie te vergroten rondom IT-governance en risicomanagement.
- Organisaties te helpen bij het naleven van relevante wet- en regelgeving.

Het IT-jaarverslag, zoals voorgesteld door NOREA, richt zich op zes kerngebieden:



1. Digitale innovatie & transformatie
Organisaties moeten inspelen op technologische ontwikkelingen en nieuwe digitale oplossingen implementeren. Dit vraagt om een strategische aanpak waarbij innovatie wordt gekoppeld aan bedrijfsdoelstellingen.
2. Data governance & ethiek
De betrouwbaarheid en ethische verwerking van data staan centraal. Dit omvat beleid en maatregelen rondom datakwaliteit, eigenaarschap en compliance met regelgeving zoals GDPR.
3. Outsourcing
Veel organisaties besteden IT-diensten uit. Dit brengt specifieke risico's met zich mee op het gebied van contractbeheer, beveiliging en compliance. Het verslag beschrijft hoe organisaties deze risico's beheersen.
4. Cybersecurity
Beveiliging van IT-systemen tegen cyberdreigingen is een prioriteit. Dit omvat risicobeheer, monitoring, incidentrespons en naleving van regelgeving zoals NIS2 en DORA.
5. IT continuïteitsbeheer
Organisaties moeten voorbereid zijn

op IT-storingen en cyberaanvallen. Dit vraagt om robuuste business continuity plannen en disaster recovery strategieën.

6. Privacy

Bescherming van persoonsgegevens en naleving van privacyregelgeving zoals de AVG is essentieel. Organisaties moeten aantonen hoe ze privacy-risico's beheren en mitigeren.

Risico zonder jaarverslag

Het ontbreken van een IT-jaarverslag brengt aanzienlijke risico's met zich mee voor organisaties. Zonder een gestructureerde IT-rapportage lopen organisaties en overheden de volgende risico's:

- Gebrek aan inzicht in IT-risico's
Zonder een centraal verslag ontbreekt het overzicht op IT-gerelateerde dreigingen, waardoor organisaties kwetsbaarder worden voor cyberaanvallen en datalekken.
- Onvoldoende naleving van wet- en regelgeving
Zonder een gestructureerde aanpak kunnen organisaties moeite hebben om te voldoen aan wet- en regelgeving zoals DORA,

Uit de praktijk: lessen van CZ

Zorgverzekeraar CZ heeft als eerste organisatie in Nederland geëxperimenteerd met het opstellen van een IT-jaarverslag. De ervaring leerde dat:

- Het verslag hielp bij het verkrijgen van een holistisch beeld van de IT-status.
- De samenwerking tussen verschillende afdelingen werd verbeterd.
- Het bestuur en de raad van commissarissen beter werden geïnformeerd over IT-gerelateerde risico's en investeringen.

CZ heeft inmiddels besloten om periodiek een IT-jaarverslag uit te brengen en dit proces verder te verfijnen. Daarnaast heeft het experiment bij CZ geleid tot inzichten die NOREA heeft meegenomen in de verdere ontwikkeling van de rapportagestandaard. Tevens is NOREA gestart met het ontwikke-

len van een beoordelingsstandaard, zodat de IT-jaarverslagen ook kunnen worden voorzien van een kwaliteitsoordeel, een mededeling af te geven door een IT-auditor.

Inmiddels zijn meerdere organisaties gestart met het uitwerken van een IT-jaarverslag, hierdoor wordt meer ervaring opgedaan met de gewenste diepgang van een dergelijk verslag. Als onderdeel van de master theses van de Executive Master opleiding IT auditing aan de Tias School for Business and Society werken ook enkele afstudeerders aan het beoordelen van de audit standaarden voor het IT-jaarverslag.

Hiermee worden in de loop van 2025 ervaringen verzameld om het IT-jaarverslag en de beoordeling daarvan voldoende volwassen in de markt te zetten.

NIS2 en de AI Act, wat kan leiden tot boetes en reputatieschade.

- Onduidelijke IT-verantwoordelijkheden

Als er geen verslag is waarin IT-governance expliciet wordt vastgelegd, blijven verantwoordelijkheden vaak onduidelijk, wat kan resulteren in inefficiënt beleid en ondoeltreffend risicobeheer.

- Moeilijkheden bij strategische besluitvorming
Zonder IT-rapportage missen bestuurders en toezichthouders de juiste informatie om weloverwogen beslissingen te nemen over technologische investeringen en digitale transformatie.
- Lager vertrouwen van stakeholders
Transparantie over IT-beheer en -beveiliging wordt steeds belangrijker voor klanten, aandeelhouders en toezichthouders. Een gebrek aan rapportage kan het vertrouwen van stakeholders ondermijnen.

De noodzaak voor transparantie en verantwoording op IT-gebied neemt toe, met name bij grote instellingen en de overheid. Een IT-jaarverslag biedt een waardevol instrument om inzicht te bieden in IT-governance, compliance en digitale weerbaarheid. Initiatieven zoals het NOREA IT-Reporting Initiative dragen bij aan de professionalisering van een IT-rapportage.

Organisaties die nu investeren in een gestructureerde IT-rapportage zullen niet alleen beter in staat zijn om risico's te beheersen, maar ook een voorsprong nemen in een digitale economie waarin vertrouwen en compliance steeds belangrijker worden. Daarbij is het van groot belang dat IT niet langer als een geïsoleerd domein wordt beschouwd, maar volledig wordt geïntegreerd in de bestuurskamer als een strategisch aandachtsgebied.

Beginnen

Organisaties die serieus werk willen maken van IT-transparantie kunnen direct aan de slag met de volgende

concrete stappen:

- Beoordeel de bestaande IT-governance om vast te stellen of de verantwoordelijkheden en kennis over IT en het toezicht daarop helder zijn uitgewerkt.
- Stel vast welke interne rapportages voorhanden zijn over de zes kerngebieden van het IT-reporting initiatief en of deze van voldoende kwaliteit zijn om te gebruiken in een IT-jaarverslag.
- Werk een concept IT-jaarverslag uit en bespreek dit gezamenlijk tussen het bestuur, de commissarissen en de directe IT-verantwoordelijken.
- Laat de kwaliteit van het IT-jaarverslag beoordelen door een IT-auditor om zekerheid te krijgen over de inhoud en betrouwbaarheid van de rapportage.
- Publiceer het IT-jaarverslag als aanvulling op andere externe verslagen en verzamel reacties hierop om toekomstige verbeteringen door te voeren.

In een wereld waar cyberdreigingen toenemen en regelgeving strenger wordt, is transparantie rondom IT geen luxe, maar een noodzaak. Organisaties die proactief aan de slag gaan met een IT-jaarverslag, laten zien dat ze controle hebben over hun digitale toekomst en bouwen daarmee aan vertrouwen bij zowel interne als externe stakeholders. De vraag is dan ook niet óf een IT-jaarverslag nodig is, maar hoe snel uw organisatie ermee aan de slag gaat.



Rob Fijneman
is hoogleraar IT-
auditing bij TIAS.

Reacties en bijdragen

Voor reacties en
nieuwe bijdragen van

IT-experts:

Tanja de Vrede

020-2467230

t.d.vrede@agconnect.nl