



Overzicht veelgestelde vragen over de toepassing van de IDRS

Wat is de IDRS?

IDRS staat voor Internationale Digitaal Rapportage Standaarden. (In het Engels: International Digital Reporting Standards). Het is een rapportagestandaard ontwikkeld door NOREA waarmee organisaties jaarlijks kunnen verantwoorden hoe zij hun digitale processen en IT-risico's beheersen. Net zoals een financieel jaarverslag, biedt IDRS een gestructureerd overzicht van Digital Innovation and Transformation; Data & AI; Third Party Management; Cybersecurity; IT Continuity Management en Privacy. Het doel is om transparantie te bieden aan stakeholders, bestuurders en toezichthouders over de digitale weerbaarheid van een organisatie.

Is het gebruik van de IDRS verplicht?

Nee, het gebruik van de IDRS is (nog) niet wettelijk verplicht. Het is een standaard die organisaties vrijwillig kunnen gebruiken om hun digitale verantwoording te structureren. Wel sluit de IDRS aan bij bestaande en opkomende wetgeving zoals NIS2/Cyberbeveiligingswet, DORA en GDPR/AVG, waardoor het een waardevol hulpmiddel is om aan compliance-eisen te voldoen. De verwachting is dat het gebruik ervan in de toekomst breder wordt gestimuleerd, ook door toezichthouders.

Waarom is de IDRS ontwikkeld?

De IDRS is ontwikkeld om grip te krijgen op digitale risico's en om versnipperde IT-verantwoording te vervangen door één integraal samenhangend rapport. In een wereld waarin IT de kern vormt van vrijwel alle bedrijfsprocessen, is transparantie over digitale veiligheid en compliance cruciaal. De inzet van de IDRS helpt organisaties om stakeholders te informeren, vertrouwen te versterken en strategische keuzes te onderbouwen. Het biedt ook een raamwerk voor assurance door auditors.

Waar is de IDRS niet voor bedoeld?

De IDRS is geen normenkader voor IT-beheersing of voor compliance met regelgeving. De IDRS schrijft voor over welke beheersingsaspecten moet worden gerapporteerd, maar niet hoe die beheersing moet zijn geregeld.

Zorgt IDRS voor een betere IT-beheersing?

Ja, de IDRS biedt een holistisch raamwerk dat IT-governance, risicobeheersing en compliance integreert. Door jaarlijks te rapporteren volgens de PDCA-cyclus (Plan–Do–Check–Act), krijgen organisaties beter inzicht in hun digitale kwetsbaarheden, verbeterpunten en strategische IT-doelen. Dit leidt tot meer grip op IT-processen, betere besluitvorming en minder verrassingen bij incidenten of audits.

Zorgt de IDRS voor meer digitale veiligheid?

Absoluut. De toepassing van de IDRS dwingt organisaties structureel na te denken over cybersecurity, IT-continuïteit en privacy. Door risico's te identificeren en maatregelen te documenteren, ontstaat een cultuur van digitale verantwoordelijkheid. Het rapport maakt kwetsbaarheden zichtbaar en stimuleert verbeteracties, waardoor de digitale weerbaarheid toeneemt.

Zorgt de IDRS voor lagere kosten?

Indirect zeker. Door alle digitale verantwoording te bundelen in één rapportage, bespaart de toepassing van de IDRS tijd en middelen die anders naar losse verantwoordingen zouden gaan. Het voorkomt dubbel werk en versnelt interne en externe communicatie. Bovendien geeft het toezichthouders (waaronder RvT en RvC) betrouwbare informatie over de beheersing van IT maar ook de eventuele gaten daarin.

Zijn er kosten verbonden aan het gebruik van de IDRS?

Het gebruik van IDRS zelf is kosteloos, maar het opstellen van een rapportage vergt tijd en inzet van interne en soms externe experts. Deze kosten hangen af van de complexiteit van de organisatie, de mate van digitalisering en of er externe ondersteuning nodig is. Op termijn levert het echter besparingen op door efficiëntere compliance en risicobeheersing. Tevens leidt betere beheersing van IT tot minder uitval en betere kwaliteit van dienstverlening en producten, hetgeen ook besparingen en concurrentievoordeel met zich meebrengt.

Heb ik een auditor nodig?

Een auditor is niet verplicht om de IDRS toe te passen. IT-auditors kunnen wel helpen bij het opstellen, beoordelen en valideren van de rapportage. Dit verhoogt de betrouwbaarheid en maakt het mogelijk om assurance te geven aan stakeholders.

Helpt het toepassen van de IDRS bestuurders te voldoen aan hun zorgplicht?

Ja. Bestuurders hebben een wettelijke zorgplicht om risico's te beheersen en verantwoording af te leggen (bijvoorbeeld in de Cyberbeveiligingswet en de Corporate Governance Code). De IDRS biedt een gestructureerde manier om te laten zien dat de betreffende organisatie digitale risico's serieus neemt en passende maatregelen treft. Dit versterkt hun positie richting toezichthouders, aandeelhouders en de maatschappij.

Hoe helpt de IDRS toezichthouders?

De IDRS biedt toezichthouders één helder document waarin alle relevante IT-risico's, maatregelen en compliance-informatie zijn gebundeld. Dit vergemakkelijkt toezicht, voorkomt versnipperde rapportages en verhoogt de transparantie. Het helpt toezichthouders om sneller risico's te beoordelen en gericht vragen te stellen, wat hun werk efficiënter maakt.

Kan ik de IDRS internationaal gebruiken?

Ja. IDRS is ontworpen als internationale standaard en sluit aan bij Europese regelgeving zoals NIS2/Cyberbeveiligingswet, DORA en GDPR/AVG. De IDRS is toepasbaar in verschillende sectoren en landen. Er zijn gesprekken gaande om de IDRS ook op Europees niveau te verankeren, waardoor het een waardevol tool is voor internationaal opererende organisaties.

Welke wetten dekt de IDRS af?

Er zijn meer dan 100 EU-wetten in ontwikkeling en deels al ingevoerd waar IT een onderwerp is en waarvan een aantal wetten vereist dat er verantwoording over wordt afgelegd. De toepassing van de IDRS helpt organisaties te voldoen aan een aantal IT-gerelateerde wet- en regelgeving, waaronder:

- NIS2/Cyberbeveiligingswet (netwerk- en informatiebeveiliging)
- DORA (digitale operationele veerkracht in financiële sector)
- GDPR/AVG (privacy)

Niet alle wetten geven precies aan hoe tot een verantwoording gekomen moet worden, maar door alle eisen te bundelen in één rapportage, ontstaat een overzichtelijke en samenhangende verantwoording. Momenteel wordt een organisatie, het IDRS platform, ingericht voor het onderhoud van de IDRS waaronder het verankeren van meer wetten in de IDRS.

Welke functies moet ik intern betrekken om de IDRS toe te passen?

Voor een goede IDRS-rapportage zijn meerdere afdelingen nodig, maar in elk geval de eigenaren van de volgende onderdelen:

1. Digital Innovation and Transformation
2. Data & AI
3. Third Party Management
4. Cybersecurity
5. IT Continuity Management
6. Privacy

Denk dan aan de volgende personen:

1. CIO, CTO, CITO
2. CISO
3. Compliance en Juridische Zaken
4. Risk management

5. Privacy officers
6. Data governance
7. Bestuur en interne audit

Samen zorgen zij voor een compleet beeld van digitale processen, risico's en beheersmaatregelen.

Hoeveel tijd kost het opstellen van de IDRS rapportage?

Organisaties kunnen beginnen met aantal hoofdstukken uit te werken van een rapportage op basis van de IDRS. De eerste volledige rapportage kost gemiddeld 200-300 uur, afhankelijk van de volwassenheid van IT-processen en beschikbare data. Daarna wordt het jaarlijks bijwerken eenvoudiger. Organisaties die al werken met ISO, NIST of andere frameworks kunnen sneller schakelen. Periodieke updates maken het tot een dynamisch en beheersbaar proces. Overigens zal in veel gevallen een deel van de inhoud die in het rapport wordt opgenomen al binnen de organisatie aanwezig zijn maar niet, of niet in een gestructureerd en samenhangend rapport, op de bestuurstafel terecht komen.

Wat doet het IDRS platform?

In mei 2025 is de finale versie van de IDRS opgeleverd. Het doel van het IDRS platform is om de IDRS te onderhouden langs de volgende invalshoeken:

- Nieuwe wetten kunnen aanleiding zijn tot het aanpassen van de standaard.
- Nieuwe IT-ontwikkelingen (bijvoorbeeld quantum) kunnen een aanleiding zijn tot het aanpassen van de set van standaarden.
- Opstellen van sectorstandaarden. Te denken valt aan een addendum op de IDRS voor de financiële sector (om te rapporteren over DORA), de kritische infrastructuur (om te rapporteren over NIS2) of de lokale overheid waarbij huidige verantwoordingen kunnen vervallen ten gunste van één rapportage op basis van de IDRS
- Het geven van gevraagd en ongevraagd advies.

Een groep van deskundigen zorgt vervolgens voor het aanpassen van de IDRS indien dat nodig is.

Hoe kan ik deelnemen aan het IDRS platform?

Op deze [pagina](#) vindt u meer informatie over de activiteiten van het IDRS platform. Als u interesse heeft om aan te sluiten bij het IDRS platform, dan nodigen we u graag uit contact op te nemen met Lianne van Helten via idsplatform@ecp.nl.