International Digital Reporting Standards (IDRS)

Meer veiligheid tegen lagere lasten

The Institute of Internal Auditors Netherlands

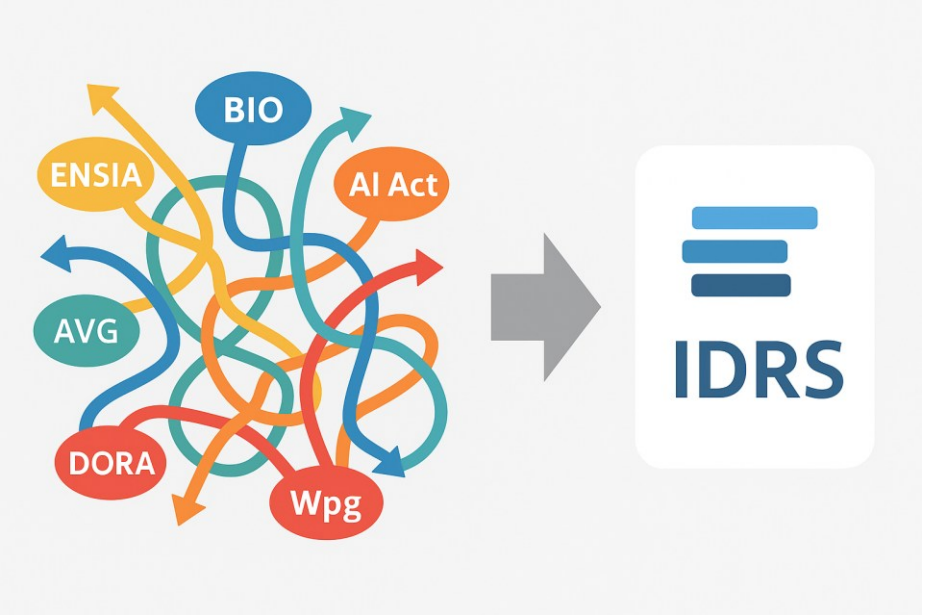
Jurgen Pertijs & Marc Welters

4 Juni 2026

IIA CONGRES 2026 PRIDE & PREJUDICE
4 & 5 JUNI AFAS THEATER LEUSDEN

Inhoud

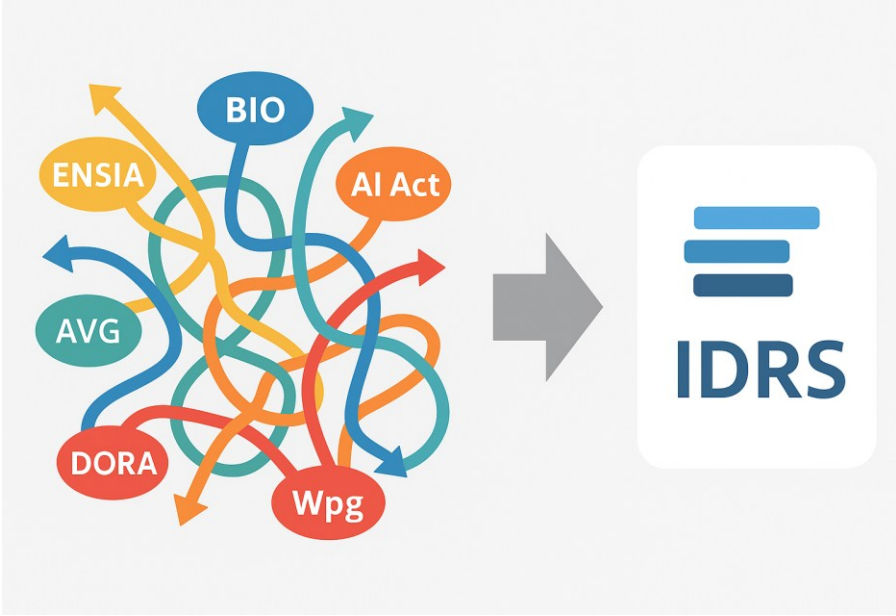
- Waarom IDRS
- IDRS – Kenmerken
- Waar staan we nu?
- Regieraad IDRS Platform
- IDRS in Publiciteit
- IDRS bij CZ



IDRS PLATFORM

Waarom IDRS

- Snelle digitalisering in Nederland verhoogt het digitale risico, terwijl de verantwoordingsstructuur gefragmenteerd blijft
- Digitale verantwoording is verdeeld over meerdere wet- en regelgevingen en frameworks (zoals NIS2, DORA, AI Act), wat consistente implementatie bemoeilijkt
- De markt heeft behoefte aan een praktische en samenhangende aanpak
- IDRS biedt één geïntegreerd framework dat digitale verantwoording bundelt in één gestructureerd model
- IDRS is in de praktijk getest (CZ Zorgverzekeraar – 2022; Arcadis – 2024; Gemeente Oss – 2024/2025) en beoordeeld door alle PPD's van de zes OOB-kantoren, waarbij feedback is verwerkt in de definitieve standaard



IDRS – kenmerken (1/2)

- Gebaseerd op COSO en in lijn met de GRI-rapportagestructuur
- Omvat alle zes kerngebieden van digitalisering IT governance, cybersecurity, privacy & data, AI & innovation, outsourcing, and continuity
- Gebaseerd op internationaal erkende standaarden per domein
- Richt zich op businessgerichte IT-governance en beheersing, met compliance als secundair resultaat

IDRS – kenmerken (2/2)

De IDRS (International Digital Reporting Standards) kan door organisaties worden toegepast om een rapportage over IT-governance op te stellen. Doel is het bieden van transparantie aan interne en externe stakeholders, bestuurders en toezichthouders over de digitale weerbaarheid van een organisatie. De voordelen van een dergelijke rapportage zijn:

- Vermindering van dubbel werk: IDRS reduceert de hoeveelheid werk en administratieve lasten door een geïntegreerde aanpak te bieden, wat leidt tot minder overlap
- Geschikt voor bestuurders en toezichthouders: IDRS is opgesteld in heldere, begrijpelijke taal en daardoor toegankelijk voor zowel IT- als non-IT-bestuurders
- Vertrouwen en innovatie: IDRS vergroot het vertrouwen in organisaties door inzicht en beheersing van IT-governance, waardoor verantwoord kan worden gegroeid en geïnnoveerd en data en continuïteit beschermd blijven
- Transparantie en verantwoording: IDRS biedt transparantie over digitale basis hygiëne, privacy, ethiek, weerbaarheid, continuïteit en verantwoorde uitbesteding
- Integrale rapportage: IDRS fungeert als een overkoepelende rapportage over IT-governance en vervangt gefragmenteerde compliance-rapportages, waarmee de governance-kloof wordt overbrugd
- Onafhankelijke standaard: IDRS is een onafhankelijke standaard die wordt ondersteund door twaalf organisaties, waarvan een deel al met IDRS werkt
- Volledige IT-scope: IDRS biedt een complete IT-scope in één document en geeft direct inzicht in de basisvereisten voor IT-governance, evenals in risicomanagement en compliance, wat organisaties weerbaar en soeverein maakt

Regieraad IDRS platform

Auditdienst Rijk

ARCADIS

CZ

DeNederlandscheBank
EUROSYSTEEM

ECP
Platform voor de InformatieSamenleving

Instituut van Internal Auditors
Nederland

Ministerie van Economische Zaken

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken

TIAS
SCHOOL FOR BUSINESS AND SOCIETY

VU VRIJE UNIVERSITEIT AMSTERDAM

IDRS - Publiciteit

Overzicht

Kunstmestbedrijf Yara benadeelde fiscus in Nederland

Poetin zegt te willen praten over vredesakkoord

'Daling van prijzen zeecontainers zal zich stabiliseren'

Markt junkbonds herstelt zich weer na Trump-shock

-6%

Bouman & Dijkman

De krapte blijft

CYBERSECURITY

Nieuw 'cyberjaarverslag' vo[illegible]or IT-beveiliging bedrijven

Nieuwe standaard zorgt voor één document voor digitale beveiliging

Voorheen moesten bedrijven vaak tientallen rapporten maken

CZ en Arcadis hebben de nieuwe IDRS-standaard getest en verfijnd

'Als je alleen naar cybersecurity kijkt, dan mis je een belangrijk deel van je beveiligingsbeeld'

AEX +0,09% 775,84 | MIDKAP -1,03% 1.086,82 | EUROSTOXX 50 +0,44% 4.206,33 | S&P 500 +0,25% 4.447,70 | €/$ NEW YORK +0,1792% 1,1742 | RENTE NL 10JR +0,009 -0,332%

fd. het financieele dagblad

Donderdag 12 augustus 2021 • Nummer 188 • 28 pagina's

'Al het geene tot het financieele eenige betrekking heeft' – sinds 1796

New York

Andrew Cuomo dacht dat hij niet te verwoesten was

PAGINA 14

Afghanistan

'Kaboel valt mogelijk binnen 90 dagen in handen taliban'

PAGINA 9

Overzicht

CYBERSECURITY

Nieuwe IT-check kan voorwaarde worden voor krediet aan bedrijf

Investeerders en banken willen weten of onderneming weerbaar is tegen hackers

Stijn van Gils en Jan Fred van Wijnen

Amsterdam

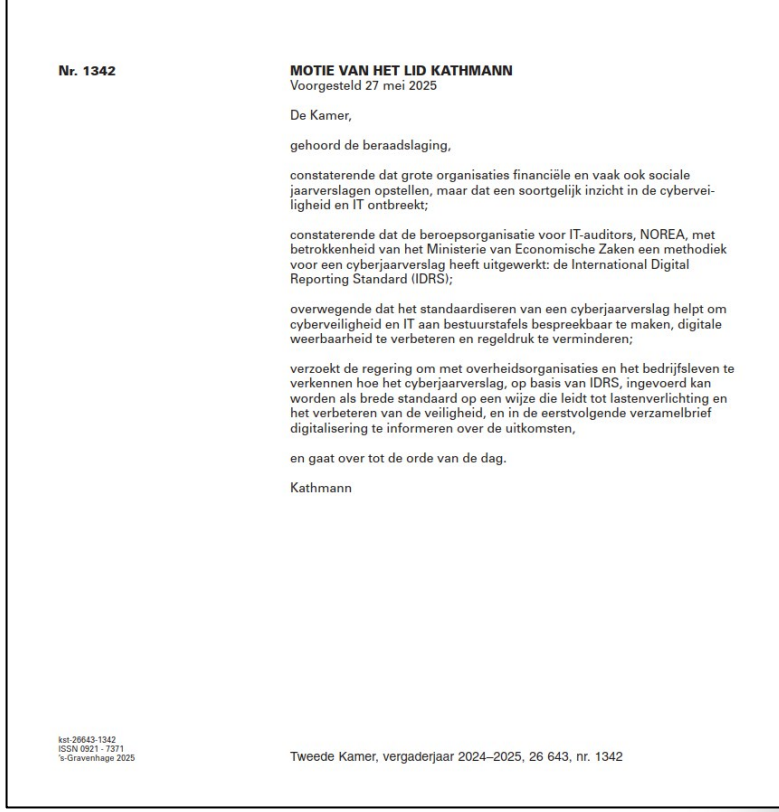
[redacted]

zijn', aldus een woordvoerder. Ook vragen ze om een geheimhoudingsplicht voor con-

Werkgeversvereniging AWVN pleit voor een algemene verruiming van de werkkostenregeling

BUITENLAND

'Aanzienlijke vooruitgang' gesprekken China en VS



Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 1342

MOTIE VAN HET LID KATHMANN

Voorgesteld 27 mei 2025

De Kamer,

gehoord de beraadslaging,

constaterende dat grote organisaties financiële en vaak ook sociale jaarverslagen opstellen, maar dat een soortgelijk inzicht in de cybervei-ligheid en IT ontbreekt;

constaterende dat de beroepsorganisatie voor IT-auditors, NOREA, met betrokkenheid van het Ministerie van Economische Zaken een methodiek voor een cyberjaarverslag heeft uitgewerkt: de International Digital Reporting Standard (IDRS);

overwegende dat het standaardiseren van een cyberjaarverslag helpt om cyberveiligheid en IT aan bestuurstafels bespreekbaar te maken, digitale weerbaarheid te verbeteren en regeldruk te verminderen;

verzoekt de regering om met overheidsorganisaties en het bedrijfsleven te verkennen hoe het cyberjaarverslag, op basis van IDRS, ingevoerd kan worden als brede standaard op een wijze die leidt tot lastenverlichting en het verbeteren van de veiligheid, en in de eerstvolgende verzamelbrief digitalisering te informeren over de uitkomsten,

en gaat over tot de orde van de dag.

Kathmann

kst-26643-1342
ISSN 0921 - 7371
's-Gravenhage 2025

Tweede Kamer, vergaderjaar 2024–2025, 26 643, nr. 1342

Instituut van Internal Auditors Nederland

IIA CONGRES 2026 PRIDE & PREJUDICE

4 & 5 JUNI AFAS THEATER LEUSDEN

Disclosures, requirements en guidance

Disclosures

Assertions /
Statements by management
of the organization

Requirements

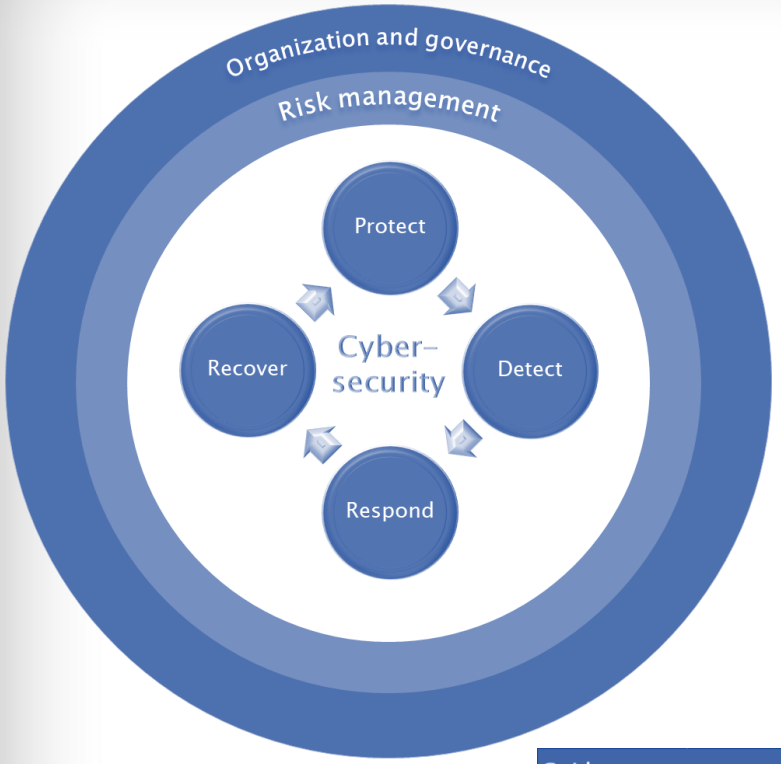
Shall = Requirement

Guidance

Should = Expectation/ Recommendation

Could = Possibility / capability

May = Permission



Disclosures IT topic cybersecurity	
CYBER-1	Developed and implemented safeguards to ensure sufficient delivery of products and services that limit or contain the impact of a potential cybersecurity event.
CYBER-2	Identified occurrence of cybersecurity events in a timely fashion.
CYBER-3	Appropriate actions regarding detected cybersecurity events to sufficiently contain the impact of these events.
CYBER-4	Maintained and tested plans for resilience and to restore any capabilities or services that were impaired due to cybersecurity events.

Requirements	
IT Topic Cybersecurity	
CYBER-1-1	The reporting organization shall report the status of, and the activities for, protection safeguards that limit cyber risks.
CYBER-2-1	The reporting organization shall report the activities for detecting cyber risk events timely.
CYBER-3-1	The reporting organization shall report the activities with regards to the response on cyber risk incidents.
CYBER-4-1	The reporting organization shall report the activities to recover from cyber risk incidents and the impact on: • business partners; • economy; • environment and /or ; • people, including impacts on their human rights.

Guidance	
Example: Topic Cybersecurity	
CYBER-1-1e	The reporting organization should report on the patch management process. The organization could report about: • identification of patch sensitive software and assets; • routine patching; • emergency patching; • emergency mitigation; • unpatchable assets (if any); • patch management security impact and controls; • impact for maintenance plans.

IDRS bij

The Institute of
Internal Auditors
Netherlands

IIA CONGRES
2026 PRIDE & PREJUDICE
4 & 5 JUNI AFAS THEATER LEUSDEN

Achtergrond

CZ Groep met 4,0 miljoen verzekerden één van de grootste zorgverzekeraars zónder winstoogmerk.
“Zorg die verder gaat” : Verzekerden nu én in de toekomst toegang bieden tot goede en betaalbare zorg

Eigen Interne Auditdienst (IAD) met 25 auditors

Samenwerking met externe accountant op basis van reviewmodel voor de jaarrekening van de CZ groep.

Multidisciplinaire IAD met onder andere:
10 RA’s (en 3 in opleiding)
4 RE’s (en 3 in opleiding)
1 RO (en 1 in opleiding)

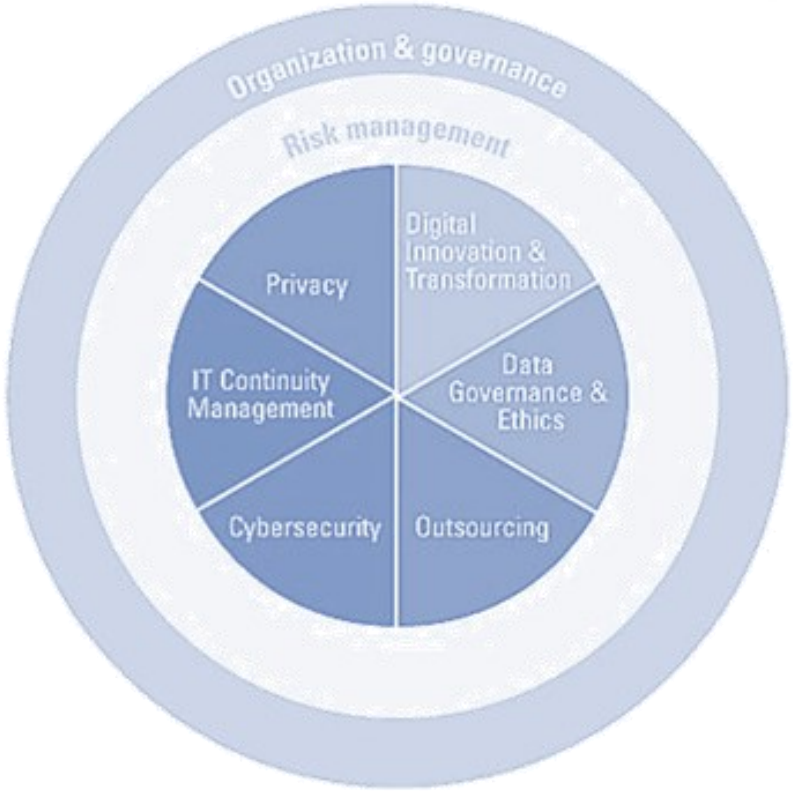
Pilot IT verslag CZ

Ons doel bij de start van de pilot:

- Een integraal inzicht over het IT landschap heen.
- Een gestructureerde wijze van het uitbrengen van een verslag.
- Inzicht in de IT beheersing, groei en ambities.
- Inzicht over de afgelopen 1,5 jaar en vooruit kijken naar de komende 1,5 jaar.
- Overlap met het divisieplan, auditrapportages, self-assessments, Q rapportages, enz..
- Intern verslag

Aanpak

- Formeel proces van een audit doorlopen
- Opdrachtgever RvB, uitvoering vanuit IT en Interne Auditdienst (IAD)
- IT verantwoordelijk voor IT verslag
- IAD verantwoordelijk voor auditrapportage
- Sessie georganiseerd vanuit IAD met verantwoordelijken per topic
- Excel opgesteld op basis van disclosures
- Verslag met verwijzing naar evidence



IT Verslag topics en relatie met COSO

Workshops

- Per Topic een workshop
- Overkoepelend overleg met Management Team ICT, business controller ICT en CIO
- In overleg met CIO deelnemers per topic vastgesteld
- Workshops voorbereid door de IAD
- Vragen geformuleerd op basis van IT verslag
- Workshops van 2 uur per onderwerp
- Direct aantoonbaarheid van antwoorden meegenomen

Workshops met verantwoordelijken per topic

Digital Innovation and transformation Manager Innovatie & Programma management Manager Data	Data Governance & Ethics Manager Data, Manager Compliance	Outsourcing Manager concerninkoop, leveranciersmanagers, manager infrastructuur
Cybersecurity CISO, Adviseurs informatiebeveiliging, Manager infrastructuur (SOC)	IT Business Continuity Management Manager Business Continuity, Manager IT Business Continuity, Manager infrastructuur	Privacy Privacy officer, compliance officer, functionaris gegevensbescherming, adviseurs informatiebeveiliging

Het resultaat – IT verslag 2021 - 2022 - 2023

Inhoudsopgave

1. Voorwoord van Directeur ICT, IPM & DATA 4
1.1. Aanleiding 4
1.2. Waarde IT-verslag 4

2. Management samenvatting 6
2.1. Kanteling van IT-gericht naar Business-gestuurd 6
2.2. Lifecyclemanagement en legacy 6
2.3. CZ als IT-werkgever 7
2.4. Uitbesteden 7
2.5. Topics framework NOREA 7
2.5.1. Digital Innovation & Transformation 8
2.5.2. Data Governance & Ethics 8
2.5.3. Outsourcing 8
2.5.4. Cybersecurity 9
2.5.5. IT Business Continuity Management 9
2.5.6. Privacy 10

3. Digitalisering 11
3.1. Digitalisering en de CZ Strategie 11
3.2. Digitaliseringsontwikkelingen 12
3.2.1. Externe digitaliseringsontwikkelingen 12
3.2.2. Interne digitaliseringsontwikkelingen 14
3.3. Duurzame inzetbaarheid medewerkers 15

4. Organisatie ICT, IPM & Data 17
4.1. Business aan het stuur met businessteams 17
4.2. BizzTech 18
4.3. ICT en IPM 19
4.4. Data 20
4.5. Doelstellingen digitalisering & CZ Strategie 2025 21

IT-verslag 2021 2022 2023

CZ groep

5. Risicomanagement 24
5.1. Risicomanagementsysteem 24
5.2. Risicohouding 26

6. Topics IT-verslag 28
6.1. Digital Innovation and transformation 28
6.2. Data Governance & Ethics 31
6.3. Outsourcing 33
6.4. Cybersecurity 36
6.5. IT Business Continuity Management 39
6.6. Privacy 41

7. Bijlage 44
7.1. Profiel CZ groep 44
7.2. Onze omgeving 45
7.3. Externe ontwikkelingen 46
7.4. Strategie CZ 2025 48
7.5. Hoe CZ waarde toevoegt 50
7.6. Organisatie 51
7.6.1. Governancestructuur CZ Groep 51
7.6.2. Organisatiestructuur 53
7.6.3. Materiële thema's CZ groep 54
7.7. ITGRI's 58
7.7.1. ITGRI 2: General Disclosures 58
7.7.2. ITGRI 3: Material Topics 68
7.7.3. 501 IT reporting standard – Cybersecurity 70
7.7.4. 502 IT reporting standard – IT Business Continuity Management 71
7.7.5. 503 IT reporting standard – Digital Innovation & Transformation 72
7.7.6. 504 IT reporting standard – Outsourcing 73
7.7.7. 505 IT reporting standard – Data Governance & Ethics 73
7.7.8. 506 IT reporting standard – Privacy 74

Waarde IT-verslag

Waarde IT verslag voor de divisie Data en IT:

- Geeft integraliteit van belangrijke aspecten binnen IT weer
- Zorgt voor inzage in beheersing, groei en ambitie

Veel van de informatie bestond al geïsoleerd, we hebben dit samengebracht in het IT verslag

Toekomst – meer naar een integraal (IT) verslag en minder naar geïsoleerde audits en assessment

Auditrapportage

(Nog) geen assurance, wel een waardevol auditrapport

- Rapport van feitelijke bevindingen
- Constateringen uit het IT verslag bevestigd en aangevuld met observaties uit eigen waarneming / eerdere audits
- Ingedeeld naar
  - Organization & Governance
  - Risk Management
  - Digital Innovation and transformation
  - Data Governance & Ethics
  - Outsourcing
  - Cyber security
  - IT Business Continuity Management
  - Privacy

Feedback RvB / RvC

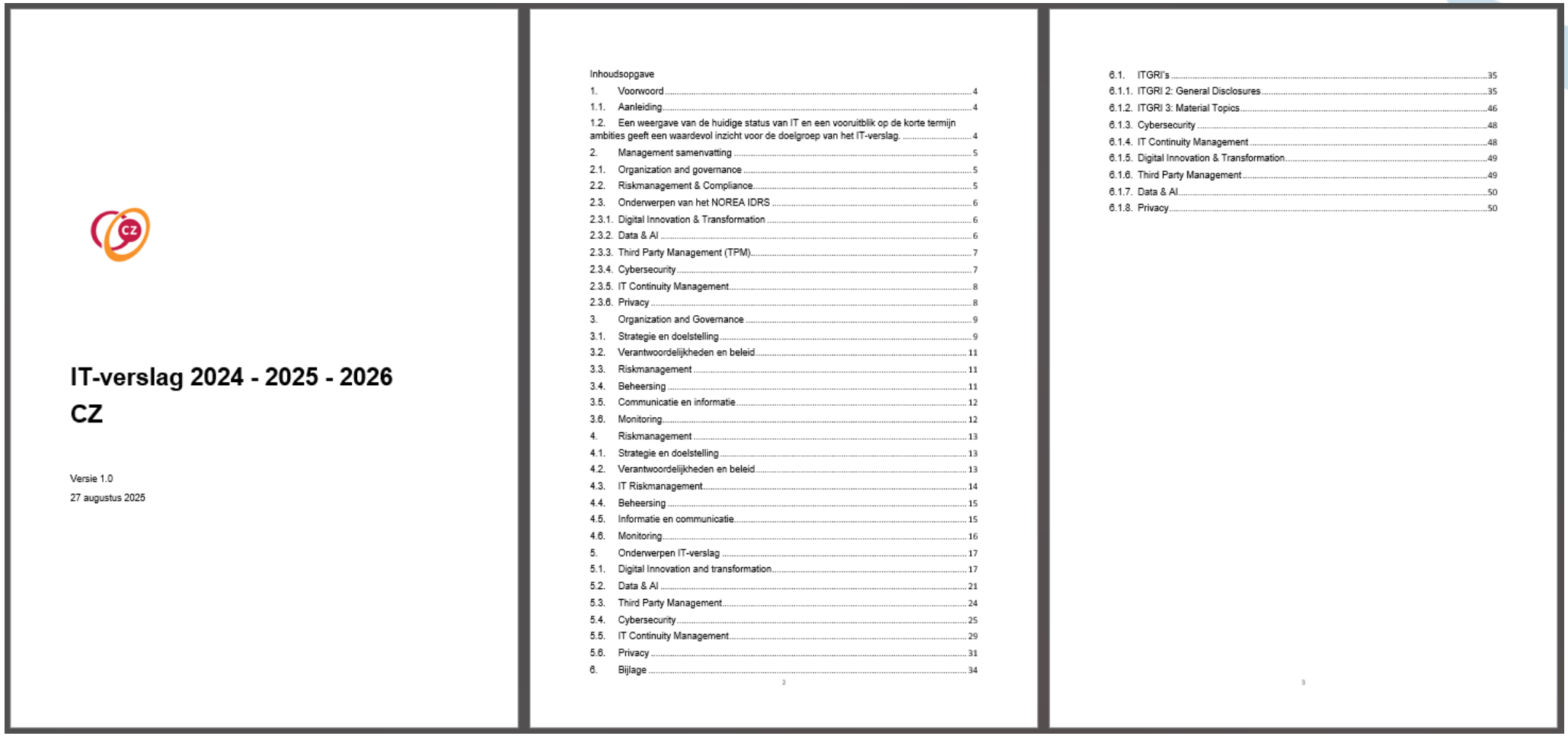
Feedback RvB CZ

- Verslag geeft een integraal beeld over risico's, status en plannen van de beheersing
- Uitgebreid verslag, volledig zelfstandig leesbaar
- Verslag delen onder directie en managementlagen CZ
- Aparte PE-sessie met RvC om IT verslag en auditrapport door te nemen

Feedback RvC

- Samenhang IT verslag en auditrapportage geeft RvC gelegenheid betere vragen te stellen
- Meer inzicht in voortgang IT strategie
- Vaak wordt IT als een technisch thema gezien, maar door de combinatie van onderwerpen komen ook de commissarissen van wie dit niet hun expertise is in hun kracht en wordt de bredere dialoog gevoerd

2025 2e IT verslag



IT-verslag 2024 - 2025 - 2026

CZ

Versie 1.0

27 augustus 2025

Inhoudsopgave

1. Voorwoord ... 4
1.1. Aanleiding ... 4
1.2. Een weergave van de huidige status van IT en een vooruitblik op de korte termijn ambities geeft een waardevol inzicht voor de doelgroep van het IT-verslag. ... 4
2. Management samenvatting ... 5
2.1. Organization and governance ... 5
2.2. Riskmanagement & Compliance ... 5
2.3. Onderwerpen van het NOREA IDRS ... 6
2.3.1. Digital Innovation & Transformation ... 6
2.3.2. Data & AI ... 6
2.3.3. Third Party Management (TPM) ... 7
2.3.4. Cybersecurity ... 7
2.3.5. IT Continuity Management ... 8
2.3.6. Privacy ... 8
3. Organization and Governance ... 9
3.1. Strategie en doelstelling ... 9
3.2. Verantwoordelijkheden en beleid ... 11
3.3. Riskmanagement ... 11
3.4. Beheersing ... 11
3.5. Communicatie en informatie ... 12
3.6. Monitoring ... 12
4. Riskmanagement ... 13
4.1. Strategie en doelstelling ... 13
4.2. Verantwoordelijkheden en beleid ... 13
4.3. IT Riskmanagement ... 14
4.4. Beheersing ... 15
4.5. Informatie en communicatie ... 15
4.6. Monitoring ... 16
5. Onderwerpen IT-verslag ... 17
5.1. Digital Innovation and transformation ... 17
5.2. Data & AI ... 21
5.3. Third Party Management ... 24
5.4. Cybersecurity ... 25
5.5. IT Continuity Management ... 29
5.6. Privacy ... 31
6. Bijlage ... 34
6.1. ITGRI's ... 35
6.1.1. ITGRI 2: General Disclosures ... 35
6.1.2. ITGRI 3: Material Topics ... 46
6.1.3. Cybersecurity ... 48
6.1.4. IT Continuity Management ... 48
6.1.5. Digital Innovation & Transformation ... 49
6.1.6. Third Party Management ... 49
6.1.7. Data & AI ... 50
6.1.8. Privacy ... 50

2025 vergeleken met 2022

- Zelfde aanpak met workshops
- Risk management nadrukkelijker betrokken

- Context anders dan in 2022
- Uitkomst: light versie.
- Volgende keer meer kwantitatief met terugblik en vooruitblik

- Kijken uit naar DORA addendum

Vragen?

Dank!

Wil je meer weten?