IT-Verslag

10 mei 2023

Agenda

- Kennismaking en achtergrond CZ
- Pilot en Aanpak
- Resultaten
  - IT verslag
  - Auditrapportage
- Lessons Learned

- 14.30 Peter Slager neemt deel via teams

Kennismaking

Tom Verharen RE MHA

Quality Assurance manager
CZ

Jurgen Pertijs RE RO

Manager Interne Auditdienst
CZ

Achtergrond CZ en IAD

- CZ groep. Ooit begonnen als kleine verzekeraar. Nu zijn we met 4,1 miljoen verzekerden één van de grootste zorgverzekeraars zónder winstoogmerk.

- Missie: goede, betaalbare en toegankelijke zorg voor iedereen.

- Eigen Interne Auditdienst (IAD) met 24 medewerkers

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

- Multidisciplinaire IAD met onder andere:
  - 7 RA's (en 2 in opleiding)
  - 4 RE's (en 2 in opleiding)
  - 1 RO (en 1 in opleiding)
  - 1 datascientist

Aanleiding

C. Druk op IV-portefeuille (strategisch risico)

Druk op de Informatievoorziening (IV)-organisatie is inherent aan de verdergaande en snelle digitaliseringsslag die bij financiële dienstverleners als CZ groep plaatsvindt. Onze huidige IV-portefeuille bevat complexe projecten die soms vertraging oplopen en/of meer capaciteit vergen dan eerder ingeschat. Ook kennen de projecten regelmatig een onderlinge (al dan niet volgordelijke) afhankelijkheid van elkaar waardoor extra risico's kunnen ontstaan.

D. Toenemend belang ketenbeheersing (operationeel risico)

Voor het efficiënt uitvoeren van de bedrijfsactiviteiten besteedt CZ groep werkzaamheden uit. Dat gebeurt ook voor delen die kritiek of belangrijk zijn, zoals cloud-diensten. Derde partijen waaraan wordt uitbesteed, besteden op hun beurt ook een deel van hun bedrijfsactiviteiten verder uit. Vanuit het perspectief van CZ groep is dat onderuitbesteding: de keten bestaat uit meerdere schakels. CZ groep blijft daarbij verantwoordelijk voor de hele keten. In de loop van de tijd zijn ketens langer geworden waardoor inzicht en beheersing naar de aard complexer wordt. Daarbij nemen de eisen toe die aan de ketens worden gesteld, bijvoorbeeld ten aanzien van privacy, sanctieliisten en duurzaamheid. Door deze ontwikkelingen nemen de risico's toe.

E. Toename cybercriminaliteit (operationeel risico)

Mogelijk gemaakt door de toenemende digitalisering van processen, neemt cybercriminaliteit enorm toe. De werkwijze van criminelen is steeds geavanceerder en de organisatie erachter professioneler. Deze ontwikkeling brengt voor CZ groep operationele en strategische risico's met zich mee die vragen m een hoge, continue alertheid van al onze medewerkers ('security awareness') en een constante doorontwikkeling van onze informatiebeveiliging. Beveiligingstesten laten zien dat de technische beveiliging op orde is.

Informatiebeveiliging

Onze kernprocessen zijn in hoge mate geautomatiseerd en verlopen via een aantal centraal beheerde ICT systemen. Ook veel van de ondersteunende bedrijfsprocessen zijn sterk afhankelijk van informatie- en communicatietechnologie (ICT). Dit vereist een ICT-omgeving met waarborgen voor een optimale beschikbaarheid, betrouwbaarheid, integriteit en continuïteit van de opslag en verwerking van onze data. Door de snelle ontwikkelingen op het gebied van cybercriminaliteit is er veel aandacht voor informatiebeveiliging. ICT-systemen dienen aan de hoogste eisen te voldoen. Daarom worden die systemen regelmatig beproefd op hun weerbaarheid

Vooruitblik

De strategie van CZ is en blijft stabiel. In 2023 en verder bouwen wij voort op de fundamenten die we de afgelopen jaren met CZ 2025 hebben gelegd. In het zorgveld zullen we in lijn met het Integraal Zorgakkoord (IZA) en met focus op het vergroten en behouden van de toegang tot zorg met name investeren in de regionale aanpak en in impactvolle transformaties. Binnen onze eigen organisatie richten we ons op verdere digitalisering van onze processen, modernisering van ons IT-landschap en de doorontwikkeling van onze service. Ten aanzien van onze mensen blijven we investeren in persoonlijke ontwikkeling en in de ontwikkeling van teams. In de actualisatie van onze strategie – die gepland is in 2023 – zal dit verder zijn beslag krijgen. Onveranderd zullen wij ons ook de komende jaren in blijven zetten voor toegankelijke, betaalbare en goede zorg.

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Informatiebeveiliging

DeNederlandscheBank
EUROSYSTEEM

NZa

AUTORITEIT PERSOONSGEGEVENS

AFM

Raad van Commissarissen	Structurele vergaderingen met RvB en Ledenraad, overleg met directieleden, OR en externe accountant, themabijeenkomsten en netwerkevenementen	O.m. solvabiliteit, reputatiemanagement, risicomanagement, compliance, auditresultaten, jaarcijfers, vermogensbeheer, strategie, samenstelling RvB/RvC, zorginhoudelijke onderwerpen, stand van zaken informatiebeveiliging en premiebeleid, bedrijfsplannen, beloningsbeleid, commercieel seizoen, coronapandemie, digitalisatie, (zorg)innovatie, (ICT)security

Pilot

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.
- Inzage op de IT beheersing, groei en ambities.
- Inzage 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 en verklaring

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, pilot (v0.9, IT Governance Reporting Initiative)
- Verslag met verwijzing naar evidence

Opbouw NOREA IT Governance Reporting Initiative (june 2022)

GRI 1

ITGRI1 Foundation. This standard introduces the purpose and system of the ITGRI standards and explains key concepts of IT governance reporting

GRI 2

ITGRI2 General disclosures: This standard describes the disclosures on an organizational level, in order to give insight in the profile and scale of organization and to provide context for the readers of the report

GRI 3

ITGRI3 Material topics: this standard provides guidance for organizations on how to determine material topics, that should be addressed in the topic disclosures

ITGR 501
CyberSecurity

ITGR 502
Business Continuity management

ITGR 503
Digital Innovation & Transformation

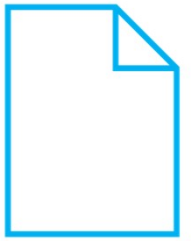
ITGR 504
Outsourcing

ITGR 505
Data Governance & Ethics

ITGR 506
Privacy

Opbouw NOREA IT Governance Reporting Initiative (june 2022)

- Organizational details
- Entities included in the organization's IT Governance reporting
- **Reporting period, frequency and contact point**
- Restatements of information
- External assurance
- Activities, value chain and other business relationships
- IT staff
- Governance structure and composition
- Role of the highest governance body in overseeing the management of IT
- Role of the highest governance body in IT-reporting
- Communication of critical concerns
- Collective IT-knowledge of the highest governance body
- Evaluation of the performance of the highest governance body
- Statement on IT strategy
- Embedding policy commitments
- Compliance with laws and regulations
- Membership associations



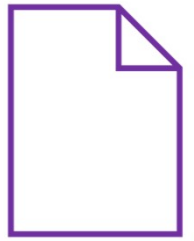
General information

Reporting period, frequency and contact point

#	GRI Disclosure
2 - 3a	specify the reporting period for, and the frequency of, its IT Governance reporting;
2 - 3b	specify the reporting period for its financial reporting and, if it does not align with the period for its IT Governance reporting, explain the reason for this
2 - 3c	report the publication date of the report or reported information
2 - 3d	specify the contact point for questions about the report or reported information

Opbouw NOREA IT Governance Reporting Initiative (june 2022)

- Process to determine material topics
- List of material topics
- Management of material topics



Material Topics

Process to determine material topics

#	GRI Disclosure
3 - 1a	describe the process it has followed to determine its material topics, including: i. how it has identified actual and potential, negative and positive impacts on the organization's goals and strategy, its environment, and people, across its activities and business relationships; ii. how it has prioritized the impacts for reporting based on their significance;
3 - 1b	specify the stakeholders and experts whose views have informed the process of determining its material topics.

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 mngt
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

Outsourcing

The structure per topic is a follows:

- Scope paragraph: depicts the IT topic within the organization;
- Disclosures: mandatory management assertions regarding the specific topic;
- Requirements: reporting elements that are mandatory to clarify the disclosure in the report;
    - Recommendations: These are cases where a particular course of action is encouraged, but not required.
    - Guidance: information to assist in the reporting process

2.3 Disclosure on governance

Requirements	The reporting organization shall report the following information: • A register of outsourcing parties and processes • Clear roles and responsibilities
Recommendations	When compiling the information specified in this disclosure, the reporting organization should report on the following topics: • Clear roles and responsibilities of IT personnel, including the management body and its committees are defined, which are documented and implemented in order to support the IT Strategic objectives. • IT and information Security key roles, such as Chief Information Officer (CIO's), Chief Operating Officer (COO) and Chief Information Security Officer (CISO) are well supported and have adequate access to the management body in order to escalate IT topics when needed. • The organization maintains a register of outsourcing parties and outsourced services. • The outsourcing policy defines roles and responsibilities, as well as competencies required to monitor and manage the risks from the IT outsourced service, including a regular risk assessment of all outsourced services.
Guidance	When describing processes, roles, and responsibilities for outsourcing the organization may describe whether: • Conflicting duties/interests and areas of responsibility are segregated to prevent unauthorized or unintentional modifications or misuse of organizations' assets. • The entity has an up-to-date register of outsourced services. Guidance on the level of detail can be found in the EBA Guidance on outsourced services section 11 article 54 and 55 [EBA/GL/2019/02, 25 February 2015 which is currently

Kennismaking

Peter Slager

Directeur IT - Data
CZ

Waarde IT-verslag

Waarde IT verslag voor de divisie IT en Data:

- 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

Lessons learned uit de pilot

Inhoudelijk
- Het is een lijvig document geworden. Naar de toekomst toe nagaan of hergebruik mogelijk is en gewerkt kan worden naar een beknoptere weergave.
- Bij volgende versie nadenken over versie voor stakeholders buiten CZ.

Proces
- Volgende periode bij de workshops ook business rollen (senior PO's en andere directieleden) betrekken. Mogelijk volgend verslag over divisies heen met een start vanuit de businesswaarde.
- Meer aandacht voor het risk managementproces.

Omgeving
- Het meewerken aan deze pilot en het bijdragen in de werkgroep van de beroepsvereniging past binnen de maatschappelijke visie van CZ.
- De IAD en ICT zien dit verslag ook als middel in de communicatie als innovatieve en aantrekkelijke werkgever.

Zorg die verder gaat