Samenvatting consultatieversie NOREA Reporting Initiative (NRI)

31 maart 2023

De voortschrijdende digitalisering van de samenleving vraagt om nieuwe verantwoording over IT-beheersing

Onze maatschappij wordt in snel tempo steeds digitaler en nagenoeg alle organisaties zijn hierdoor volledig afhankelijk van hun IT. Het management van organisaties geeft aan dat ze meer consistent inzicht wil hebben in, en verantwoording wil afleggen over, de inzet van IT en de strategische doelen die daarmee gerealiseerd (kunnen) worden.

NOREA, de beroepsorganisatie van IT-auditors, heeft het initiatief genomen om een verslaggevingsstandaard te ontwikkelen waarmee organisaties zich kunnen verantwoorden over hun IT-beheersing. Deze standaard (het NOREA-rapportage-initiatief, kortweg NRI) biedt een handvat voor het management om zich in een IT-beheerverslag te verantwoorden en belanghebbenden te informeren over de IT *Governance, Risk and Compliance* en essentiële IT-onderwerpen zoals Digital Innovation and Transformation, Data Governance & Ethics, Outsourcing, Cybersecurity, IT Continuity Management en Privacy. Een rapportage over het beheer van IT is nog niet (wettelijk) verplicht. Met deze verslaggevingsstandaard is er nu een solide basis voor organisaties van verschillende omvang om op een consistente manier te rapporteren over hun IT.

Momenteel is er al veel (Europese) wet- en regelgeving(of onderhanden), op deelaspecten van de hierboven genoemde IT-onderwerpen. Deze vragen om verantwoordingen door het management van organisaties, maar bieden daar geen raamwerk voor. Rapporteren volgens de NRI verslaggevingsstandaard kan een belangrijke bijdrage leveren aan het benodigde inzicht in IT voor belanghebbenden.

Het verslag over het beheer van IT behoort daarbij te kijken naar de huidige situatie en naar ontwikkelingen in de nabije toekomst, en toe te lichten hoe de organisatie daarop wil inspelen. De gehanteerde principes, benoemde rapportage-eisen en toegelichte aanbevelingen in deze standaard zijn geïnspireerd op algemeen, en internationaal, aanvaarde standaarden en *best practices* voor elk van de onderwerpen. Deze standaarden en best practices zijn tot stand gekomen met de inbreng van industrie, overheden, deskundigen en andere belanghebbenden en worden vaak ook in de bedrijfsvoering als referentiekader gebruikt.

Deze verslaggevingsstandaard zal worden aangevuld met een audithandreiking, waarmee onafhankelijke IT-auditors de getrouwe weergave van de feitelijke situatie kunnen bevestigen d.m.v. een assurance-rapport. Het oordeel van de onafhankelijke IT-auditor vergroot het vertrouwen van de beoogde gebruikers van het rapport en moedigt de

opstellende organisatie aan om voortdurend aandacht te besteden aan adequaat beheer van IT, teneinde de veiligheid en continuïteit van de organisatie te waarborgen.

Vereisten per onderwerp

De standaard schrijft voor dat de volgende IT onderwerpen (IT topics), indien voor de organisatie en/of belanghebbenden van materieel belang, en bijbehorende punten in de rapportage worden opgenomen.

Over de hele IT organisatie en het beheersen van de relevante IT topics beschrijft de organisatie:

a. Organisatie en governance
   - De besturing van IT, volgens het beleid van de organisatie, waaronder de context van IT (intern en extern), de organisatiestructuur, de belangrijkste IT investeringen (zoals gebruikte kernsystemen en/of geïmplementeerde platformen) en de monitoring van IT op strategisch niveau;
   - De huidige en toekomstig gewenste/benodigde IT capaciteiten van de organisatie;
   - Of de IT voldoet aan geldende wet- en regelgeving, en zo nee hoe dat wordt opgelost. Inclusief de communicatie met eventuele toezichthouders.

b. IT Risk management
   - De rol en plaats van IT binnen het risk management van de organisatie, het belang ervan, de geïdentificeerde kritieke IT systemen en het gehanteerde risk management raamwerk;
   - De continue monitoring en bijsturing van het IT risk management om in de pas te blijven met de veranderende omgeving (intern en extern);
   - De periodieke evaluatie van de effectiviteit van het risk management raamwerk.

Per IT topic kunnen de voor dat IT topic specifieke punten op gebied van 'organisatie & governance' en risk management worden beschreven en verder worden verwezen naar hetgeen al is verantwoordt over de IT organisatie als geheel.

<u>Per relevante IT topic beschrijft de organisatie:</u>

1. Digital Innovation and Transformation;
   - De (strategische) visie op (digitale) innovatie en hoe deze innovaties plaats vinden;
   - De inzet van (IT) architectuur;
   - De veranderorganisatie (projecten, programma's en/of andere soorten van wijzigingen zoals agile methodes) en hoe (IT-)wijzingen worden doorgevoerd.

2. Data Governance & Ethics;
   - De aansluiting van de data strategie met het data management;

- Het (bevorderen van het) bewustzijn van de risico's, aandachtspunten en mogelijkheden van data governance en data ethiek;
- De beheersing van algoritmes en andere data gedreven (beslis-)systemen;
- Het data classificatie beleid en de procedures en maatregelen die per classificatie zijn voorgeschreven.

3. Outsourcing;
   - De besturing van de outsourcing portefeuille, waaronder monitoren van de prestaties versus (strategische) doelstellingen en bijsturen waar nodig;
   - Het beleid en procedures voor initiëren, implementeren en (op termijn) beëindigen van outsourcing van processen;
   - Het beleid en de procedures voor continu monitoren van de prestaties en uitkomsten van outsourcing van processen, waaronder het reageren op en afhandelen van incidenten en andere service management elementen.

4. Cybersecurity;
   - De activiteiten ter bescherming tegen cyber risico's;
   - De activiteiten voor het tijdig detecteren van (mogelijke) cyber incidenten;
   - De activiteiten voor het reageren op (mogelijke) cyber incidenten;
   - Het herstel van cyber incidenten, waaronder de impact op derde partijen, de externe omgeving (economie als geheel) en mensen in het bijzonder.

5. IT Continuity Management;
   - De status van de getroffen maatregelen voor het voorkomen van (IT-)verstoringen en het beperken van de nadelige effecten ervan;
   - De activiteiten voor het tijdig detecteren van (mogelijke) verstoringen;
   - De activiteiten voor het reageren op (mogelijke) verstoringen;
   - Herstel van verstoringen, waaronder die met impact op derde partijen, de externe omgeving (economie als geheel) en mensen in het bijzonder.

6. Privacy.
   - De activiteiten voor het bevorderen van het bewustzijn binnen de organisatie van het belang van en de regels voor privacy;
   - De getroffen beheersingsmaatregelen op gebied van privacy binnen de processen waar persoonsgegevens worden verwerkt;
   - De classificering van gegevens om te bepalen welke maatregelen nodig zijn voor de naleving van de privacyregels.

In de beschrijvingen wordt per IT topic steeds aandacht geschonken aan de management cyclus (Plan-Do-Check-Act) die door de organisatie is ingericht.