# Wie tot 3 kan tellen, kan zijn risicobeheersing versnellen

## Werken met volwassenheidsniveaus

Update volwassenheidsniveau 3 in Good Practice Informatiebeveiliging DNB 2023

19 december 2023

Afier

it-auditors adviseurs risk managers security en privacy officers

# Wie tot 3 kan tellen, kan zijn risicobeheersing versnellen

## Update DNB Good Practice Informatiebeveiliging 2023

De Nederlandsche Bank (hierna DNB) heeft op 19 december de al even verwachte update van haar Good Practice Informatiebeveiliging gepubliceerd. Mede in het kader van de door de Europese Commissie vastgestelde Digital Operational Resilience Act (hierna DORA) voor de gehele Europese financiële sector heeft DNB deze Good Practice geactualiseerd. DNB stelt dat zij met deze actualisatie uitdraagt dat informatiebeveiliging en cybersecurity permanente aandacht behoeft. Deze aandacht is nodig op strategisch en bestuurlijk niveau en richt zich op de verbetering van de effectiviteit van de beheersmaatregelen, die past bij een voortdurend veranderend dreigingsbeeld waarmee instellingen worden geconfronteerd. Dit sluit aan bij DORA, een verordening die als 'lex specialis' bestaande regelgeving vervangt en wettelijke bepalingen stelt om de cyberweerbaarheid van de financiële sector te verhogen.

De 'Good Practice Informatiebeveiliging 2023' sluit zoveel mogelijk aan op de indeling van de 'Good Practice Informatiebeveiliging 2019/2020', waarbij de 58 beheersmaatregelen op dezelfde wijze zijn genummerd. In haar toelichting heeft DNB de belangrijkste wijzingen samengevat toegelicht. Met de update Good Practice Informatiebeveiliging 2023 (hierna GPIB) nog vers van de pers is een alomvattende analyse van de verschillen in detail met de vorige versie nog niet te geven.

## Aanscherpingen in volwassenheidsniveaus

Opvallend is dat DNB naast inhoudelijke wijzigingen in de beheersmaatregelen ook wijzigingen heeft doorgevoerd in de omschrijving van de volwassenheidsniveaus. Het begrip van deze volwassenheidsniveaus is cruciaal, omdat de praktijk erop gericht is om de beheersmaatregelen minimaal op volwassenheidsniveau 3 te hebben (en de Risk Management Cyclus op niveau 4). Financiële instellingen dienen met een self-assessment vast te stellen in hoeverre de beheersing van informatiebeveiliging en cybersecurity op het vereiste niveau is. Daarom is het raadzaam om dit aspect van de update GPIB verder te verkennen.

Voor het overzicht van de wijzigingen in de volwassenheidsniveaus richt de hierna volgende analyse zich op volwassenheidsniveau 3. Dit is voor verreweg de meeste beheersmaatregelen het minimaal gewenste streefniveau. In de praktijk, en zeker niet alleen in de financiële sector, is de tendens zichtbaar dat organisaties inzicht dienen te geven in hoeverre beheersmaatregelen op volwassenheidsniveau 3 zijn ingericht.

In tabel 1 is volwassenheids-niveau 3 voor zowel de 2023 als de 2019/2020 versie van de GPIB weergegeven. Voor de overzichtelijkheid zijn wijzigingen in volwassenheidsniveau 1, 2, 4 en 5 buiten beschouwing gelaten. Voor de volledigheid, volwassenheidsniveau 0 is logischerwijs niet gewijzigd. Er kan niet minder dan niets zijn voor een beheersmaatregel op dit volwassenheidsniveau.

In de tabel zijn de tekstuele wijzigingen tussen GPIB 2023 en de vorige versie *cursief* weergegeven.

| GPIB 2023 | | GPIB 2019/2020 | |
|---|---|---|---|
| **Definitie van het volwassenheids-niveau** | **Criteria ter verduidelijking** | **Definitie van het volwassenheids-niveau** | **Criteria ter verduidelijking** |
| **Gedefinieerd** ***(opzet bestaan en werking)*** – De opzet van de beheersmaatregel is gedocumenteerd en wordt op gestructureerde en geformaliseerde wijze uitgevoerd. De vereiste effectiviteit van de beheersmaatregel is aantoonbaar en wordt getoetst. *Daar waar nodig wordt de beheersmaatregel verbeterd.* | ▪ Opzet, bestaan en effectieve werking zijn aantoonbaar.<br>▪ De beheersmaatregel is gedefinieerd *op basis van* een risico assessment.<br>▪ *De beheersmaatregel is bepaald, schriftelijk vastgelegd en ingebed in de organisatie.*<br>▪ Taken en verantwoordelijkheden *incl. noodzakelijke functiescheiding zijn uitgeschreven geïmplementeerd* en getoetst op werking en worden geëvalueerd.<br>▪ De effectieve werking is over een periode van minimaal 6 maanden risicogebaseerd getoetst, aangetoond *en vastgelegd*.<br>▪ *Over* de uitvoering van de beheersmaatregel wordt aan het management gerapporteerd. | **Gedefinieerd** – De opzet van de beheersingsmaatregel is gedocumenteerd en wordt op gestructureerde en geformaliseerde wijze uitgevoerd. De vereiste effectiviteit van de beheersingsmaatregel is aantoonbaar en wordt getoetst. | ▪ Beheersingsmaatregel is gedefinieerd o.b.v. risico assessment.<br>▪ Gedocumenteerd en geformaliseerd.<br>▪ Verantwoordelijkheden en taken zijn eenduidig toegewezen.<br>▪ Opzet, bestaan en effectieve werking zijn aantoonbaar.<br>▪ Effectieve werking van controls wordt periodiek getoetst.<br>▪ De toetsing vindt risicogebaseerd plaats en toont aan dat de control effectief is over een langere periode (>6 maanden).<br>▪ De uitvoering van de beheersingsmaatregel wordt aan het management gerapporteerd. |

*Tabel 1 Definitie volwassenheidsniveau 3 GPIB 2023 vergeleken met GPIB 2019/2020*

**De volgende verschillen vallen op:**

1. In de definitie van het volwassenheidsniveau zelf is het perspectief van daar waar nodig verbeteren van de beheersmaatregel toegevoegd;
2. In de criteria ter verduidelijking is ‘opzet, bestaan en effectieve werking zijn aantoonbaar’ als eerste genoemd;
3. In de criteria ter verduidelijking is noodzakelijke functiescheiding onder taken en verantwoordelijkheden toegevoegd;
4. In de criteria ter verduidelijking is toegevoegd dat de toetsing van de effectieve werking wordt vastgelegd.

## Toenemend belang aantoonbaarheid functioneren beheersmaatregelen

Op basis van deze verschillen is de verwachting dat aantoonbaarheid van het functioneren van beheersmaatregelen in opzet, bestaan en effectieve werking in 2024 en daarna nog belangrijker wordt voor DNB. Het expliciet toevoegen van de vastlegging van de effectieve werking benadrukt dit. Bovendien besteedt DNB in de update van de GPIB veel aandacht aan het toetsen van de beheersmaatregelen. DNB benadrukt hierbij op diverse plaatsen in de GPIB het belang van passende scheiding en onafhankelijkheid van ICT-risicobeheer functies, controlefuncties en interne auditfuncties en van assurance vanuit externe IT-auditors. Ook op dit onderwerp is de actualisatie van de GPIB goed zichtbaar, doordat DNB de relatie legt met (inter)nationale assurance standaarden en ontwikkelingen daarbinnen, waaronder NOREA richtlijn 3000, SOC2 verklaringen en de in 2023 door NOREA ontwikkelde IT-auditverklaring (NOREA Reporting Initiative).

## Verantwoorden, verbeteren én versnellen

Het is tot slot goed om te zien dat DNB in de definitie het perspectief van het verbeteren van de beheersmaatregel heeft toegevoegd. Financiële instellingen zullen dit perspectief als net zo belangrijk herkennen als het voldoen aan toezicht vereisten. Het is ook een mooie prikkel om dit perspectief toe te voegen in andere vergelijkbare volwassenheidsmodellen, zoals het Volwassenheidsmodel informatiebeveiliging van NBA-LIO en NOREA, dat inmiddels als basis in diverse sectoren waaronder het brede onderwijsveld gehanteerd wordt. Beheersing van informatiebeveiligings- en cyberrisico's is immers nooit af. Nieuwe en toenemende dreigingen blijven waakzaamheid en versterkte weerbaarheid vragen.

Het goede nieuws is dat door met elkaar in gesprek te zijn over risico's en maatregelen aan de hand van hulpmiddelen zoals deze actuele update van de GPIB onze waakzaamheid en weerbaarheid versterkt wordt.

*"Wie tot 3 kan tellen, kan zijn risicobeheersing versnellen."*

**Meer informatie?**

IT gaat verder dan alleen het kloppend hart van vitale en ondersteunende bedrijfsprocessen. IT is essentieel in het invulling geven aan de steeds hogere eisen die gesteld worden aan beveiliging, transparantie, ondernemingsbestuur en compliance (wet en regelgeving).

De IT-auditors van Afier zijn gekwalificeerd en geregistreerd en beschikken over veel expertise op informatiebeveiliging en cybersecurity, beheersing van IT en de afstemming tussen IT en bedrijfsprocessen. Met ons team van Register IT-auditors (RE), data-analisten, consultants en coaches helpen we u van implementatie tot en met certificering en van analyse tot het coachen van uw medewerkers. We bieden zekerheid op het snijvlak van geautomatiseerde informatiesystemen, bedrijfsprocessen en administraties. We ondersteunen u in het continu toetsen of uw dienstverlening in overeenstemming is met de afgesproken eisen.

Onze analyses en beoordelingen helpen u sturing op processen te verbeteren, bieden u ondersteuning bij management en bestuurlijke beslissingen en zorgen voor grip op projectplanningen. Daarnaast bieden ze u een verantwoordingsinstrumentarium dat toezichthoudende autoriteiten de benodigde zekerheden en daarmee het vertrouwen in uw organisatie geeft.

Neem gerust contact op voor meer informatie of het maken van een afspraak. We helpen u graag.

**Afier IT-auditors**
info@afier.com
tel. 0592 - 53 09 53
www.afier.com

Gebruik deze analyse gerust in gesprekken over risico's en maatregelen voor informatiebeveiliging en cybersecurity binnen je eigen organisatie. Het wordt daarbij gewaardeerd als je naar dit document verwijst conform onderstaande:
'Wie tot 3 kan tellen, kan zijn risicobeheersing versnellen' – analyse update volwassenheidsniveau 3 GPIB, Afier, drs. F.W. Hanekamp RE, 19 december 2023