

Wie tot 3 kan tellen, kan zijn cyberweerbaarheid versnellen

Werken met volwassenheidsniveaus

Update volwassenheidsniveau 3 in
SBA-Cyberweerbaarheid DNB 2025

15 oktober 2025

Afier

it-auditors adviseurs risk managers security en privacy officers

Wie tot 3 kan tellen, kan zijn cyberweerbaarheid versnellen

Update DNB SBA-Cyberweerbaarheid 2025

De Nederlandsche Bank (hierna DNB) heeft op 14 oktober 2025 de al eerder in concept toegelichte sectorbrede analyse Cyberweerbaarheid (hierna SBA-Cyberweerbaarheid) gepubliceerd. In het kader van de door de Europese Commissie vastgestelde Digital Operational Resilience Act (hierna DORA) heeft DNB deze SBA-Cyberweerbaarheid vragenlijst geactualiseerd. DNB stelt dat zij met deze actualisatie invulling geeft aan de vereisten van DORA voor verzekeraars en pensioenfondsen die onder de reikwijdte van DORA vallen.

De SBA-Cyberweerbaarheid pensioen- en verzekeringssector behandelt achtereenvolgens de onderwerpen Governance and strategy, ICT risk management, Information security, ICT Operations management, Business continuity management en Uitbesteding. In haar toelichting geeft DNB aan dat voor verzekeraars en pensioenfondsen die niet onder de reikwijdte van DORA vallen, er voorlopig niets verandert. Zij ontvangen de sectorbrede analyse vragenlijst op basis van de DNB Good Practice Informatiebeveiliging 2023 (hierna GPIB).

Deze GPIB 2023 sluit zoveel mogelijk aan op de indeling van de GPIB 2019/2020, waarbij de 58 beheersmaatregelen op dezelfde wijze zijn genummerd. In haar toelichting heeft DNB de belangrijkste wijzigingen samengevat toegelicht.

Aanscherpingen in volwassenheidsniveaus

Toen DNB op 19 december 2023 de geactualiseerde versie van de GPIB publiceerde, was het opvallend dat DNB naast inhoudelijke wijzigingen in de beheersmaatregelen ook wijzigingen had doorgevoerd in de omschrijving van de volwassenheidsniveaus. De praktijk bij financiële instellingen die onder het toezicht op basis van het GPIB vielen was erop gericht dat de beheersmaatregelen minimaal op volwassenheidsniveau 3 dienden te functioneren en de Risk Management Cyclus op volwassenheidsniveau 4.

In de SBA-Cyberweerbaarheid die op 15 oktober 2025 gepubliceerd is, komen volwassenheidsniveau 4 en 5 te vervallen. Financiële instellingen dienen met een self-assessment vast te stellen in hoeverre de beheersing van informatiebeveiliging en cyberweerbaarheid op het vereiste niveau is. Daarom is het raadzaam om dit aspect van de geactualiseerde SBA-Cyberweerbaarheid verder te verkennen.

Voor het overzicht van de wijzigingen in de volwassenheidsniveaus richt de hiernavolgende analyse zich op volwassenheidsniveau 3. Dit is 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.

"De volwassenheidsniveaus 4 en 5 komen in de geactualiseerde vragenlijst SBA-Cyberweerbaarheid te vervallen."

In tabel 1 is volwassenheidsniveau 3 voor zowel de SBA-Cyberweerbaarheid als de GPIB 2023 als de GPIB 2019/2020 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 tabel 1 zijn de tekstuele wijzigingen tussen SBA-Cyberweerbaarheid en GPIB 2023 *cursief* weergegeven. Voor de volledigheid zijn in tabel 2 de verschillen tussen GPIB 2023 en GPIB 2019/2020 ook *cursief* weergegeven.

SBA-Cyberweerbaarheid 2025		GPIB 2023	
Definitie van het volwassenheidsniveau	Criteria ter verduidelijking	Definitie van het volwassenheidsniveau	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. - De beheersmaatregel is gedefinieerd op basis van een risico assessment. - De beheersmaatregel is bepaald, schriftelijk vastgelegd en ingebed in de organisatie. - Taken en verantwoordelijkheden incl. noodzakelijke functiescheiding zijn uitgeschreven geïmplementeerd en getoetst op werking en worden geëvalueerd. - De effectieve werking is over een periode van minimaal 6 maanden risicogebaseerd getoetst, aangetoond en vastgelegd. - Over de uitvoering van de beheersmaatregel wordt aan het management gerapporteerd.	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. - De beheersmaatregel is gedefinieerd op basis van een risico assessment. - De beheersmaatregel is bepaald, schriftelijk vastgelegd en ingebed in de organisatie. - Taken en verantwoordelijkheden incl. noodzakelijke functiescheiding zijn uitgeschreven geïmplementeerd en getoetst op werking en worden geëvalueerd. - De effectieve werking is over een periode van minimaal 6 maanden risicogebaseerd getoetst, aangetoond en vastgelegd. - Over de uitvoering van de beheersmaatregel wordt aan het management gerapporteerd.

Tabel 1 Definitie volwassenheidsniveau 3 SBA-Cyberweerbaarheid vergeleken met GPIB 2023

Wat opvalt:

- De definitie van het volwassenheidsniveau zelf is niet gewijzigd;
- De criteria ter verduidelijking zijn niet gewijzigd; is 'opzet, bestaan en effectieve werking zijn aantoonbaar' als eerste genoemd;
- Volwassenheidsniveaus 4 en 5 zijn komen te vervallen volgens de toelichting.

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. <i>Daar waar nodig wordt de beheersmaatregel verbeterd.</i>	- Opzet, bestaan en effectieve werking zijn aantoonbaar. - De beheersmaatregel is gedefinieerd <i>op basis van een risico assessment.</i> <i>De beheersmaatregel is bepaald, schriftelijk vastgelegd en ingebed in de organisatie.</i> - Taken en verantwoordelijkheden <i>incl. noodzakelijke functiescheiding zijn uitgeschreven geïmplementeerd</i> en getoetst op werking en worden geëvalueerd. - De effectieve werking is over een periode van minimaal 6 maanden risicogebaseerd getoetst, aangetoond <i>en vastgelegd.</i> - 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. - Gedocumenteerd en geformaliseerd. - Verantwoordelijkheden en taken zijn eenduidig toegewezen. - Opzet, bestaan en effectieve werking zijn aantoonbaar. - Effectieve werking van controls wordt periodiek getoetst. - De toetsing vindt risicogebaseerd plaats en toont aan dat de control effectief is over een langere periode (>6 maanden). - De uitvoering van de beheersingsmaatregel wordt aan het management gerapporteerd.

Tabel 2 Definitie volwassenheidsniveau 3 GPIB 2023 vergeleken met GPIB 2019/2020

Wat opvalt:

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 aantoonbare cyberweerbaarheid

DNB handhaaft in de SBA-Cyberweerbaarheid de definitie van volwassenheidsniveau 3 uit de GPIB 2023. Aantoonbaarheid van het functioneren van beheersmaatregelen in opzet, bestaan en effectieve werking van minimaal 6 maanden blijft daarmee belangrijk voor financiële instellingen om aantoonbare risicobeheersing van cyberweerbaarheid te laten zien. Het volwassenheidsniveau 3 sluit aan bij het Advised Maturity Level 3 uit het NOREA DORA in control framework¹. Dit raamwerk is een bruikbaar hulpmiddel om invulling te geven aan het inzichtelijk maken van de effectieve werking over een periode van minimaal 6 maanden door risicogebaseerde toetsing en aantoonbare vastlegging.

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 gehandhaafd. Financiële instellingen zullen dit perspectief als net zo belangrijk herkennen als het voldoen aan toezicht vereisten. Het is ook een mooie prikkel continu te blijven streven naar deze verbeteringen. Beheersing van informatiebeveiligings- en cyberrisico's om daarmee cyberweerbaar te zijn en blijven 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 actualisatie van de SBA-Cyberweerbaarheid onze waakzaamheid en weerbaarheid versterkt wordt.

"Wie tot 3 kan tellen, kan zijn cyberweerbaarheid 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 cyberweerbaarheid versnellen' – analyse volwassenheidsniveau 3 DNB SBA-Cyberweerbaarheid, Afier, drs. F.W. Hanekamp RE, 15 oktober 2025

¹ De actuele versie van dit raamwerk is te raadplegen via <https://www.norea.nl/dora>