Handreiking volwassenheidsniveaus SBA-IB

Hieronder volgt de handreiking voor het inschatten van de volwassenheidsniveaus. Zie DNB Good Practice Informatiebeveiliging, voor verdere informatie op de elementen van Informatiebeveiliging, beheersmaatregelen en volwassenheidsniveaus.

Niveau:	Definitie van het volwassenheidsniveau	Criteria ter verduidelijking
0	**Niet bestaand** – Aan deze beheersingsmaatregel is geen aandacht besteed.	
1	**Initieel** – De beheersingsmaatregel is (gedeeltelijk) gedefinieerd maar wordt op inconsistente wijze uitgevoerd. Er is een grote afhankelijkheid van individuen bij de uitvoering van de beheersingsmaatregel.	■ Geen of beperkte beheersingsmaatregel geïmplementeerd. ■ Niet of ad-hoc uitgevoerd. ■ Niet /deels gedocumenteerd. ■ Wijze van uitvoering afhankelijk van individu (niet gestandaardiseerd)
2	**Herhaalbaar maar informeel** – De beheersingsmaatregel is aanwezig en wordt op consistente en gestructureerde, maar op informele wijze uitgevoerd.	■ De uitvoering van de beheersingsmaatregel is gebaseerd op een informele maar wel gestandaardiseerde werkwijze. Deze werkwijze is niet volledig gedocumenteerd.
3	**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.
4	**Beheerst en meetbaar** – De effectiviteit van de beheersingsmaatregel wordt periodiek geëvalueerd. Daar waar nodig wordt de beheersingsmaatregel verbeterd of vervangen door andere beheersingsmaatregel(en). De evaluatie wordt vastgelegd.	Criteria voor niveau 3 plus de volgende onderscheidende criteria: ■ Periodieke (control) evaluatie en opvolging vindt plaats. ■ Evaluatie is gedocumenteerd. ■ Taken en verantwoordelijkheden voor het evalueren zijn geformaliseerd. ■ Frequentie waarop wordt geëvalueerd is gebaseerd op het risicoprofiel van de instelling en is minimaal jaarlijks. ■ In de evaluatie worden (operationele) incidenten meegenomen. ■ De uitkomsten van de evaluatie wordt aan het management gerapporteerd.
5	**Continu verbeteren** – De beheersingsmaatregelen zijn verankerd in het integrale risicomanagement raamwerk, waarbij continu gezocht wordt naar verbetering van de effectiviteit van de maatregelen. Hierbij wordt gebruik gemaakt van externe data en benchmarking. Medewerkers zijn pro-actief betrokken bij de verbetering van de beheersingsmaatregelen	Criteria voor niveau 4 plus de volgende onderscheidende criteria: ■ Continu evalueren van de beheersingsmaatregelen om de effectiviteit van beheersmaatregelen voortdurend te verbeteren. ■ Gebruik makend van resultaten uit self-assessments, gap en root cause analyses. ■ De getroffen beheersingsmaatregelen worden gebenchmarkt op basis van externe data en zijn 'Best Practice' in vergelijking met andere organisaties.