Uitleg volwassenheidsmodel voor informatiebeveiliging 3.0

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Intern en overheids accountants
NBA

Juni 2024

Koninklijke Nederlandse
Beroepsorganisatie
van Accountants

NBA

Nederland rekent op zijn accountants.

De leden van de Koninklijke NBA vormen een brede, pluriforme beroepsgroep van ruim 22.000 professionals werkzaam in de openbare accountantspraktijk, bij de overheid, als intern accountant en in het management van organisaties. Integriteit, objectiviteit, deskundigheid en zorgvuldigheid, geheimhouding en professioneel gedrag zijn essentiële waarden voor iedere accountant. De Koninklijke NBA helpt accountants hun cruciale rol in de maatschappij te vervullen, nu en in de toekomst.

Dit document bevat bladwijzers, hyperlinks en navigatiebutton.

 Adobe Acrobat bladwijzers - toetsencombinatie ‘Ctrl-b’

Tekst is een intern document- of externe hyperlink

Naar inhoudsopgave

Vorige pagina

Volgende pagina

Colofon

Deze uitgave is in 2024 herzien op initiatief van de Ledengroep Intern en Overheidsaccountants (LIO) van de Nederlandse Beroepsorganisatie van Accountants (NBA-LIO), met medewerking van NOREA, de beroepsorganisatie van IT-Auditors.

Samenstelling werkgroep Herziening Volwassenheidsmodel Informatiebeveiliging:

Hielkje van Staa-Oldenhuis, Peter Kornelisse, Jurgen Pertijs, Robert Warmoeskerken
Abdul Altawekji, Ludo Cuijpers, Henk Links, Johan Scheffe, Koos Vos

Inhoudsopgave

Toepassing van het volwassenheidsmodel

Zoals eerder beschreven geeft het model op conceptueel niveau inzicht in welke informatiebeveiligingsmaatregelen per volwassenheidsniveau redelijkerwijs verwacht mogen worden. Het geeft hiermee een handreiking om het volwassenheidsniveau te meten, te bepalen en te verbeteren. Maar natuurlijk blijven de genoemde beheersmaatregelen altijd een enigszins subjectief karakter hebben. Het volwassenheidsmodel is richtinggevend en daarmee een goed instrument om de dialoog aan te gaan met het verantwoordelijk management of andere stakeholders.

Ten behoeve van een succesvolle toepassing van het volwassenheidsmodel dient een aantal (rand)voorwaarden in ogenschouw te worden genomen:

- Het vaststellen van het gewenste volwassenheidsniveau wordt in belangrijke mate bepaald door de aard van de business c.q. processen, soort gegevens van de organisatie, de beschikbare applicaties en infrastructuur alsmede externe factoren c.q. dreigingen. Deze zaken alsmede de specifieke risico's en risicobereidheid van de organisatie zijn bepalend hoe hoog de lat voor de organisatie moeten liggen.
- Doordat vele organisaties delen van hun informatievoorziening en/of –verwerking hebben uitbesteed en/of afhankelijk zijn van derde partijen, dient er expliciet aandacht te worden besteed aan de afhankelijkheden van en samenwerking met business partners in de keten. Dit vergt ook een goede afstemming van de verschillende volwassenheidsniveaus binnen de keten (supply chain).
- Bedenk dat per organisatie de van toepassing zijnde wet regelgeving verschillend zijn. Het model wijst op de compliance met verplichte wet & regelgeving (b.v. AVG, GDPR), echter deze zijn niet specifiek uitgewerkt en kunnen op onderdelen bepalend zijn voor de hoogte van het gewenste volwassenheidsniveau.
- Het model voorziet ook in de grafische presentaties van de uitkomsten. Dit verbetert de leesbaarheid van uitkomsten voor stakeholders, zoals raad van bestuur en toezichthouders. Echter de toegevoegde waarde zit hem vooral in de periodieke dialoog met deze stakeholders over uitkomsten, het bespreken van impact en risico's en de opvolging van mitigerende activiteiten.

Tenslotte verwijzen we nog naar laatste hoofdstuk waar nog enkele "Tips en Tricks" ten behoeve van een succesvolle toepassing van het model zijn beschreven.

Uitleg van het volwassenheidsmodel

Het volwassenheidsmodel bestaat uit 71 statements verdeeld over 15 domeinen. Dit wordt nader toegelicht in de hiernavolgende paragrafen.

Zoals eerder aangegeven is het volwassenheidsmodel niet opgesteld met de intentie om een nieuw normenkader te introduceren. Gebruikmakend van bestaande normen c.q. referentiekaders, zijnde ISO27001, NIST(en onderliggende kaders zoals CobIT 6.0), is een consistente verzameling van statements samengesteld waar per statement vijf volwassenheidsniveaus zijn beschreven. De individuele statements wegen in dit model allen even zwaar.

Per statement kan op basis van de beschrijving van het volwassenheidsniveau alsmede de verwijzing naar één of meerdere beheersmaatregelen (“good practices”) een inschatting van het betreffende volwassenheidsniveau worden gemaakt. Hierbij dient in alle gevallen de organisatiespecifieke context (inclusief externe factoren) bepalend te zijn voor verdere explicitering van de gewenste beheersmaatregelen en de waardering van de geïmplementeerde beheersmaatregelen.

Een statement, behorend bij één van de 15 domeinen, bevat een unieke code, een titel, een risicobeschrijving, een doelstelling en 5 volwassenheidsniveaus met beheersmaatregelen.

Als voorbeeld het statement “Onafhankelijke Toetsing”

1

(GO) Governance	
1.5 (GO.05)	**Onafhankelijke Toetsing**
Risico	Naleving van wet- en regelgeving en prestaties worden niet beoordeeld en bevestigd door een onafhankelijke partij, waardoor onbekende en ongeadresseerde afwijkingen in naleving en/of prestaties kunnen optreden.
Doel	Onafhankelijke toetsing (intern of extern) wordt gedaan om te bepalen in hoeverre de informatievoorziening (inclusief IT) voldoet aan relevante wet- en regelgeving; het beleid van de organisatie, de normen en procedures van de organisatie; algemeen aanvaarde werkwijzen; en effectieve en efficiënte prestaties van IT.

2 3 4 5

6

Volwassenheidsniveau 1	(a) Er vindt geen onafhankelijke toetsing plaats.
Volwassenheidsniveau 2	(a) De interne auditfunctie is gedefinieerd en bestaat o.a. uit toetsing op naleving van relevante wet- en regelgeving, IT- of informatiebeleid, standaarden en procedures binnen de organisatie.
Volwassenheidsniveau 3	(a) Onafhankelijke toetsing (intern of extern) wordt gedaan ten aanzien van het voldoen van de informatievoorziening (incl. IT) aan relevante wet- en regelgeving, beleid, standaarden, procedures binnen de organisatie en algemeen aanvaarde werkwijzen. (b) De toetsingsactiviteiten zijn beschreven in een auditplan dat is goedgekeurd door het (senior) management en een auditcommissie. (c) De resultaten van deze toetsingsactiviteiten worden gerapporteerd aan het (senior) management en de auditcommissie.
Volwassenheidsniveau 4	(a) De performance van de onafhankelijke toetsing wordt periodiek geëvalueerd door de auditcommissie. (b) Het ontwerp van de onafhankelijke toetsingsfunctie wordt periodiek geëvalueerd door een externe partij.
Volwassenheidsniveau 5	(a) Onafhankelijke toetsing (intern of extern) omvat ook de effectiviteit en de efficiëntie van de informatieverwerking (incl. IT).

7

COBIT 5	ISO 27001:2013 27002:2013	ISO 27001:2022 27002:2022	BIO 2019	NIST Cybersecurity Framework
MEA02.05, MEA02.06, MEA02.07, MEA02.08	A.5.1.2 A.12.4.1 A.18.2.1, A.18.2.2, A.18.2.3	A5.1, A5.35, A5.36	5.1.2, 5.1.2.1 12.4.1, 12.4.1.1, 12.4.1.2, 12.4.1.3, 12.4.1.4, 12.4.1.5 18.2.1, 18.2.1.1, 18.2.1.2 18.2.2, 18.2.2.1 18.2.3, 18.2.3.1	DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5

1 Domein met domeincode, waar het betreffende statement is ondergebracht

Binnen het model zijn 15 domeinen onderscheiden, hieronder weergegevens met een beschrijving van hun generieke doelstelling:

1 (GO) Governance
Geeft richting en ondersteuning aan informatiebeveiliging c.q. cyber security in lijn met bedrijfsdoelstellingen, risicobereidheid en van toepassing zijnde wet- en regelgeving en vergewist zich van de effectieve naleving ervan.

2 (OR) Organisatie
Informatiebeveiliging (inclusief cyber security) is op het hoogst mogelijk organisatieniveau geadresseerd en het beheer van informatiebeveiliging is in lijn met de bedrijfsdoelstellingen en van toepassing zijnde risico's en compliance eisen.

3 (RM) Risk Management
Draagt zorg voor het op gestructureerde wijze identificeren en beheersen van informatiebeveiligings- en cyber securityrisico's zodanig dat de risico's in lijn zijn met de risicobereidheid en het risicoraamwerk van de organisatie.

4 (HR) Personeelsmanagement
Draagt er zorg voor dat alle medewerkers, inhuurkrachten en derde partijen zich bewust zijn van informatiebeveiligings- en cyber securityrisico's en voldoende geschoold zijn om in lijn met het beveiligingsbeleid hun werkzaamheden te kunnen verrichten.

5 (CO) Configuration Management
Draagt zorg voor de vastlegging en ontsluiting van gegevens over de IT-middelen, IT-koppelingen en IT-diensten.

6 (IM) Incident/Problem Management
Draagt zorg voor het afhandelen van verstoringen in de IT-dienstverlening en voor het tijdig herstellen van de afgesproken dienstenniveaus. Probleembeheer draagt zorg voor het wegnemen of voorkomen van structurele fouten in de IT-dienstverlening.

7 (CH) Change Management
Draagt zorg voor het beheerst doorvoeren van wijzigingen in IT-middelen, IT-koppelingen en IT-diensten (o.a. applicaties).

8 (SD) Systeemontwikkeling
Draagt zorg voor het ontwikkelen van geautomatiseerde oplossingen in lijn met ontwerpspecificaties, ontwikkel- en documentatiestandaarden en kwaliteits- en acceptatiecriteria (inclusief wet- en regelgeving).

9 (DM) Data Management
Draagt zorg voor het onderhouden van de volledigheid, juistheid, beschikbaarheid en bescherming van gegevens.

10 (ID) Identity & Access Management
Draagt zorg voor het beheren van de logische toegang tot informatie, informatiediensten (o.a. applicaties) en externe koppelingen.

11 (SM) Security Management
Draagt zorg voor het in kaart brengen en adresseren van de risico's van beschikbaarheid, integriteit en vertrouwelijkheid die van toepassing zijn op de informatievoorziening.

12 (PH) Fysieke beveiliging
Draagt zorg voor het toegangsbeheer tot ruimtes en de bescherming van personen en objecten tegen incidenten die een fysieke schade aan personen of objecten tot gevolg kunnen hebben.

13 (OP) IT-operatie
Draagt zorg voor het operationeel houden van de IT-diensten.

14 (BC) Bedrijfscontinuïteitsmanagement
Draagt zorg voor het herstellen en voorzetten van de bedrijfsvoering na het optreden van een calamiteit in overeenstemming met de hiervoor afgesproken dienstenniveaus.

15 (SC) Ketenbeheer
Draagt zorg voor het bewaken van de levering van de afgesproken dienstverlening door (interne en externe) leveranciers.

Per domein zijn twee of meer statements gedefinieerd die hun bijdrage leveren aan het bewerkstelligen van de generieke doelstelling van het domein.

2 Hoofdstuknummer en ID

Het hoofdstuknummer verwijst naar het domeinnummer en het volgnummer van het statement: 1.5 betekent dus domein 1 en statement 5 (van de 71 statements)
Elk statement heeft een unieke identificatie (ID) en bestaat uit een twee-letterig prefix gevolgd door een volgnummer. De twee-letterige prefixen verwijzen naar het domein waar het bij hoort en het volgnummer van het statement binnen het domein: GO.05 betekent dus het 5e statement van het domein Governance.
NB bij updates van het model wordt gestreefd de originele ID's te behouden.

3 Titel

De korte c.q. summiere beschrijving van het statement. De beschrijving geeft in enkele steekwoorden de kern en essentie van het statement aan.

4 Risico

De beschrijving van het (inherente) risico in het geval het betreffende statement niet of in onvoldoende mate effectief is. De risicobeschrijving is generiek van aard en indicatief.

5 Doel

De beschrijving wat het statement op het oog heeft en bijdraagt aan de informatiebeveiliging.

6 Volwassenheidsniveaus

Om een handreiking te geven bij de consistente toetsing van het statement zijn vijf volwassenheidsniveaus gedefinieerd en nader uitgewerkt. Op basis van beschrijvingen (van redelijkerwijs te verwachten beheersmaatregelen) kan worden bepaald welk volwassenheidsniveau voor het betreffende statement van toepassing is. Daarnaast helpt de indicatieve beschrijving van de (redelijkerwijs) te realiseren beheersmaatregelen ook om richting te geven aan het implementatie- c.q. verbetertraject, welke bijvoorbeeld in de vorm van een aanbeveling in een rapport kan worden opgenomen.

Per statement zijn de vijf indicaties van volwassenheidsniveaus op basis van een aantal criteria nader uitgewerkt. Er wordt opgemerkt dat in tegenstelling tot andere volwassenheidsmodellen niveau 0 ("non existent") niet is uitgewerkt. Niveau 0 maakt onderdeel uit van niveau 1 ("initial"). De volgende vijf niveaus als mede de volgende bijbehorende leidende criteria zijn hierbij onderkend:

Niveau	Naam	Omschrijving	Criteria
1	Initieel	Beheersmaatregelen zijn niet of gedeeltelijk gedefinieerd en/of worden op inconsistente wijze uitgevoerd. Grote afhankelijkheid van individuen.	• Geen of beperkte controls geïmplementeerd. • Niet of ad-hoc uitgevoerd. • Niet /deels gedocumenteerd. • Wijze van uitvoering afhankelijk van individu.
2	Herhaalbaar	Beheersmaatregelen zijn aanwezig en worden op consistente en gestructureerde, maar op informele wijze uitgevoerd.	• Control is geïmplementeerd. • Uitvoering is consistent en standaard. • Informeel en grotendeels gedocumenteerd.
3	Gedefinieerd	Beheersmaatregelen zijn gedocumenteerd en worden op gestructureerde en geformaliseerde wijze uitgevoerd. De uitvoering is aantoonbaar en wordt getoetst.	• Control gedefinieerd o.b.v. risico assessment. • Gedocumenteerd en geformaliseerd. • Verantwoordelijkheden en taken eenduidig toegewezen. • Opzet, bestaan en effectieve werking aantoonbaar. • Rapportage van uitvoering van beheersmaatregel aan management. • Effectieve werking van controls wordt periodiek getoetst, gebaseerd op het risicoprofiel van de organisatie. • De toetsing toont aan dat de control effectief is.
4	Beheerst en meetbaar	De effectiviteit van de beheersmaatregelen wordt periodiek geëvalueerd.	• Periodieke (control) evaluatie en opvolging vindt plaats. • Evaluatie is gedocumenteerd en geformaliseerd. • Frequentie waarop wordt geëvalueerd is gebaseerd op het risicoprofiel van de onderneming en is minimaal jaarlijks. • Rapportage van de evaluatie aan management.
5	Continu verbeteren	De beheersmaatregelen zijn verankerd in het integrale risicomanagement raamwerk, waarbij continu gezocht wordt naar verbetering.	• Continu evalueren van de beheersmaatregelen om de effectiviteit te verbeteren. Gebruik makend van resultaten uit Self-assessment, gap en root cause analyses. • De getroffen beheersmaatregelen worden gebenchmarkt en zijn ‘Best Practice’ in vergelijking met andere organisaties. • Real time monitoring. • Inzet automated tooling.

7 Referenties

Iedere organisatie heeft veelal een keuze gemaakt welk model en/of “good practice” zij gebruikt voor informatiebeveiliging en/of risicomanagement. Het volwassenheidsmodel is zodanig opgesteld dat op basis van “good practices” de relevante controledoelstellingen en de bijbehorende volwassenheidsniveaus voor informatiebeveiliging zijn gedefinieerd. Deze zijn zoveel mogelijk conceptueel beschreven en waar mogelijk losgekoppeld van specifiek in te richten en uit te voeren beheersmaatregelen. De meer specifieke en meer gedetailleerde implementatie richtlijnen zijn derhalve terug te vinden in de betreffende “good practice” (standaard, raamwerk of baseline) die de organisatie gebruikt.

Hiertoe zijn de verwijzingen naar de volgende “good practices” opgenomen:

- COBIT 5.0 - ISACA framework for control objectives for IT, 2012
- ISO/IEC 27001:2013 - Code of practice for information security controls (oktober 2013)
- ISO/IEC 27001:2022 - Code of practice for information security controls (oktober 2022)
- BIO- Baseline Informatiebeveiliging Overheid (tactisch, januari 2019)
- NIST – Framework for Improving Critical Infrastructure Cybersecurity (versie 2.0, april 2024)

NB De prefix “A” in de ISO-referenties verwijst naar de bijlage van ISO/IEC 27001, zijnde de control objectives en controls (uit ISO/IEC 27002).

Het Excel-werkdocument

Op de website van de NBA is in Excel een werkdocument beschikbaar.
Zo is de tekst van het model ook te verwerken in eigen documentatie en rapportages.
Het biedt ook mogelijheden om het model te importeren in een ISMS of GRC tool.

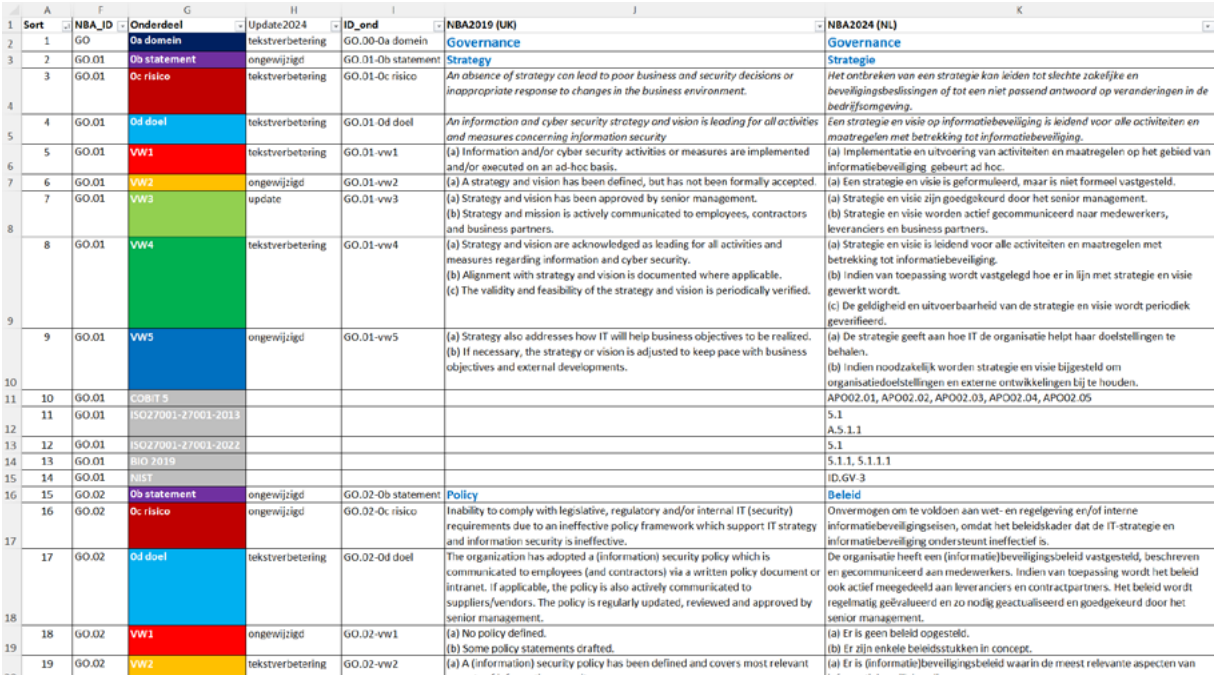
Het Excel-bestand heeft vier tabbladen:

- Tabblad Basistabel: hierin worden alle onderdelen van het Statement onder elkaar weergegeven.
- Tabblad Export: Tabel met de actuele statements weergegevens in een rij per statement (gegenereerd uit de gegevens van het Tabblad Basistabel)
- Tabblad Invul: Opgemaakte versie van het tabblad samenvoegen (gegenereerd uit de gegevens van het Tabblad Basistabel), met de mogelijkheid om de volwassenheidniveaus in te vullen.
- Tabblad Rapportage: een voorbeeld van hoe de ingevulde gegevens in een grafiek kunnen worden weergegeven.

Tabblad Basistabel

In de basistabel staan alle onderdelen van een statement onder elkaar. Op deze manier is bijvoorbeeld de Engelse versie uit 2019 (kolom J) goed te vergelijken de vernieuwde versie (kolom K).
Kolom H geeft weer wat er ten opzichte van eerdere versies is aangepast. Dat kan een tekstverbetering zijn, een update, een nieuw of verwijderd statement of een ongewijzigd onderdeel.
Hier is op te filteren. Door filtering is het ook mogelijk op specifieke domeinen, statements, volwassenheidsniveaus en referenties te selecteren.

NB Let bij het sorteren op dat je altijd terugkeert naar een oplopende sortering op kolom A: sorteren heeft namelijk invloed op de rest van de spreadsheet.



Sort	NBA_ID	Onderdeel	Update2024	ID_ord	NBA2019 (UK)	NBA2024 (NL)
1	GO	0a domein	tekstverbetering	GO.00-0a domein	Governance	Governance
2	GO.01	0b statement	ongewijzigd	GO.01-0b statement	Strategy	Strategie
3	GO.01	0c risico	tekstverbetering	GO.01-0c risico	*An absence of strategy can lead to poor business and security decisions or inappropriate response to changes in the business environment.*	*Het ontbreken van een strategie kan leiden tot slechte zakelijke en beveiligingsbeslissingen of tot een niet passend antwoord op veranderingen in de bedrijfsomgeving.*
4	GO.01	0d doel	tekstverbetering	GO.01-0d doel	*An information and cyber security strategy and vision is leading for all activities and measures concerning information security*	*Een strategie en visie op informatiebeveiliging is leidend voor alle activiteiten en maatregelen met betrekking tot informatiebeveiliging.*
5	GO.01	VW1	tekstverbetering	GO.01-vw1	(a) Information and/or cyber security activities or measures are implemented and/or executed on an ad-hoc basis.	(a) Implementatie en uitvoering van activiteiten en maatregelen op het gebied van informatiebeveiliging gebeurt ad hoc.
6	GO.01	VW2	ongewijzigd	GO.01-vw2	(a) A strategy and vision has been defined, but has not been formally accepted.	(a) Een strategie en visie is geformuleerd, maar is niet formeel vastgesteld.
7	GO.01	VW3	update	GO.01-vw3	(a) Strategy and vision has been aporoved by senior management. (b) Strategy and mission is actively communicated to employees, contractors and business partners.	(a) Strategie en visie zijn goedgekeurd door het senior management. (b) Strategie en visie worden actief gecommuniceerd naar medewerkers, leveranciers en business partners.
8	GO.01	VW4	tekstverbetering	GO.01-vw4	(a) Strategy and vision are acknowledged as leading for all activities and measures regarding information and cyber security. (b) Alignment with strategy and vision is documented where applicable. (c) The validity and feasibility of the strategy and vision is periodically verified.	(a) Strategie en visie is leidend voor alle activiteiten en maatregelen met betrekking tot informatiebeveiliging. (b) Indien van toepassing wordt vastgelegd hoe er in lijn met strategie en visie gewerkt wordt. (c) De geldigheid en uitvoerbaarheid van de strategie en visie wordt periodiek geverifieerd.
9	GO.01	VW5	ongewijzigd	GO.01-vw5	(a) Strategy also addresses how IT will help business objectives to be realized. (b) If necessary, the strategy or vision is adjusted to keep pace with business objectives and external developments.	(a) De strategie geeft aan hoe IT de organisatie helpt haar doelstellingen te behalen. (b) Indien noodzakelijk worden strategie en visie bijgesteld om organisatiedoelstellingen en externe ontwikkelingen bij te houden.
10	GO.01	COBIT 5				APO02.01, APO02.02, APO02.03, APO02.04, APO02.05
11	GO.01	ISO27001-27001-2013				5.1 A.5.1.1
12	GO.01	ISO27001-27001-2022				5.1
13	GO.01	BIO 2019				5.1.1, 5.1.1.1
14	GO.01	NIST				ID.GV-3
15	GO.02	0b statement	ongewijzigd	GO.02-0b statement	Policy	Beleid
16	GO.02	0c risico	ongewijzigd	GO.02-0c risico	Inability to comply with legislative, regulatory and/or internal IT (security) requirements due to an ineffective policy framework which support IT strategy and information security is ineffective.	Onvermogen om te voldoen aan wet- en regelgeving en/of interne informatiebeveiligingseisen, omdat het beleidskader dat de IT-strategie en informatiebeveiliging ondersteunt ineffectief is.
17	GO.02	0d doel	tekstverbetering	GO.02-0d doel	The organization has adopted a (information) security policy which is communicated to employees (and contractors) via a written policy document or intranet. If applicable, the policy is also actively communicated to suppliers/vendors. The policy is regularly updated, reviewed and approved by senior management.	De organisatie heeft een (informatie)beveiligingsbeleid vastgesteld, beschreven en gecommuniceerd aan medewerkers. Indien van toepassing wordt het beleid ook actief meegedeeld aan leveranciers en contractpartners. Het beleid wordt regelmatig geëvalueerd en zo nodig geactualiseerd en goedgekeurd door het senior management.
18	GO.02	VW1	ongewijzigd	GO.02-vw1	(a) No policy defined. (b) Some policy statements drafted.	(a) Er is geen beleid oogesteld. (b) Er zijn enkele beleidsstukken in concept.
19	GO.02	VW2	tekstverbetering	GO.02-vw2	(a) A (information) security policy has been defined and covers most relevant	(a) Er is (informatie)beveiligingsbeleid waarin de meest relevante aspecten van

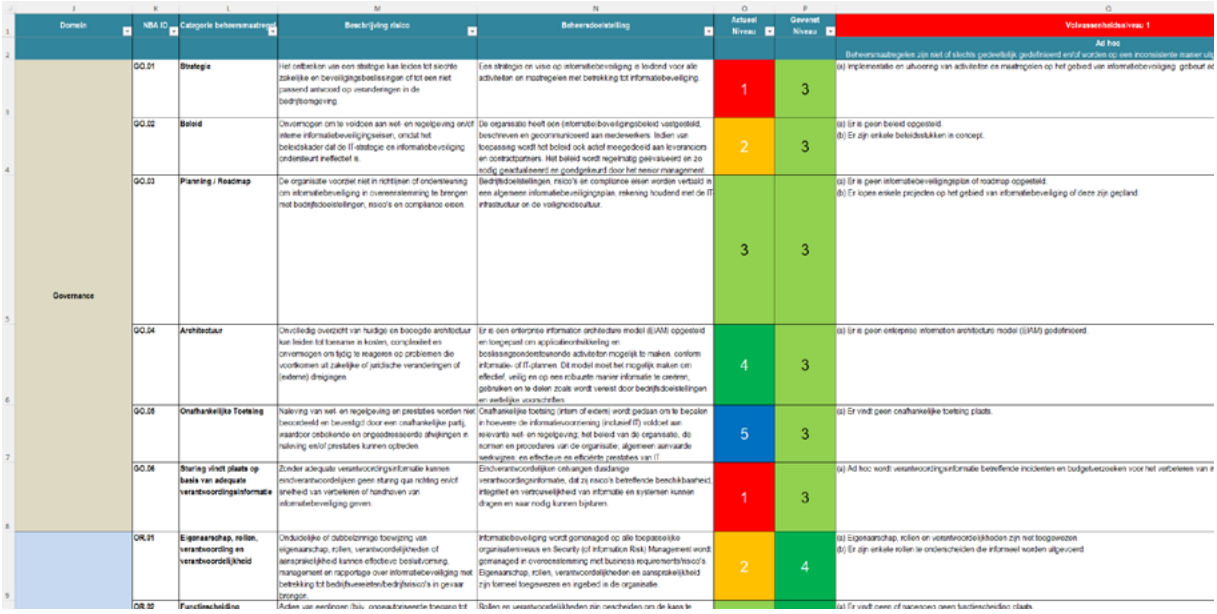
Tabblad Export

In Tabblad Export worden vanuit de Basistabel de gegevens van de actuele statements weergegeven in een rij per statement. Dit met als doel om een tabblad te maken waar het volwassenheidsniveau per statement in te vullen is en om een grafiekweergave mogelijk te maken.
Dit tabblad is ook geschikt om de gegevens te exporteren en in een andere tool te verwerken.

Domein	StatementNr	NBA ID	Titel	Risico	Doel	VW1
Governance	1.1	GO.01	Strategie	Het ontbreken van een strategie kan leiden tot slechte zakelijke en b	Een strategie en visie op informatiebeveiliging is leidend voor alle ac	(a) Implementatie en uitvoering van activiteite
Governance	1.2	GO.02	Beleid	Onvermogen om te voldoen aan wet- en regelgeving en/of interne i	De organisatie heeft een (informatie)beveiligingsbeleid vastgesteld,	(a) Er is geen beleid oogesteld. (b) Er zijn enkel
Governance	1.3	GO.03	Planning / Roadmap	De organisatie voorziet niet in richtlijnen of ondersteuning om infon	Bedrijfsdoelstellingen, risico's en compliance eisen worden vertaald	(a) Er is geen informatiebeveiligingsplan of roa
Governance	1.4	GO.04	Architectuur	Onvolledig overzicht van huidige en beoogde architectuur kan leider	Er is een enterprise information architecture model (EIAM) opgestel	(a) Er is geen enterprise information architectu
Governance	1.5	GO.05	Onafhankelijke Toetsing	Naleving van wet- en regelgeving en prestaties worden niet beoorde	Onafhankelijke toetsing (intern of extern) wordt gedaan om te bepa	(a) Er vindt geen onafhankelijke toetsing plaats
Governance	1.6	GO.06	Sturing vindt plaats op basis van adequate verantwoordingsinformatie	Zonder adequate verantwoordingsinformatie kunnen eindverantwo	Eindverantwoordelijken ontvangen dusdanige verantwoordingsinfo	(a) Ad hoc wordt verantwoordingsinformatie
Organisatie	2.7	OR.01	Eigenaarschap, rollen, verantwoording en verantwoordelijkheid	Onduidelijke of dubbelzinnige toewijzing van eigenaarschap, rollen,	Informatiebeveiliging wordt gemanaged op alle toepassselijke organi	(a) Eigenaarschap, rollen en verantwoordelijkh
Organisatie	2.8	OR.02	Functiescheiding	Acties van eenlingen (bijv. ongeautoriseerde toegang tot gegevens)	Rollen en verantwoordelijkheden zijn gescheiden om de kans te verl	(a) Er vindt geen of nagenoeg geen functiesche
Organisatie	2.9	OR.03	Mandaat en bevoegdheden	Noodzakelijke besluiten en acties van beveiligingsfunctionarissen ku	Bevoegdheden zijn vastgesteld zodat operationele activiteiten door	(a) Er zijn geen afspraken omtrent bevoegdhe
Risk Management	3.10	RM.01	Kader voor Information Risk Management	Het kader voor Information Risk en Control Management is niet in lij	Er is een kader voor Information Risk Management opgesteld en afg	(a) Informatierisico's zijn niet of worden ad he
Risk Management	3.11	RM.02	Risicobeoordeling	Inherente en restrisico's worden niet (tijdig) geïdentificeerd en beoo	Risicobeoordelingen worden uitgevoerd om actuele risicoprofielen e	(a) Risicoanalyses worden zelden gedaan en ri
Risk Management	3.12	RM.03	Plan voor behandeling en beperking van risico's (incl. risicoacceptatie)	Risicobeperkende maatregelen worden niet goldentificeerd en gelmj	Beheersactiviteiten worden op alle niveaus geprioriteerd en gepland	(a) Er is geen plan voor het aanpakken of mitig
Personeelsmanagement	4.13	HR.01	Werving	Als het wervingsproces ontoereikend is, loopt de organisatie het risi	Rekruteringsprocessen voor personeel worden onderhouden in ove	(a) Activiteiten of maatregelen voor het werve
Personeelsmanagement	4.14	HR.07	Indiensttreding	Als de procedures en richtlijnen bij indiensttreding onduidelijk zijn o	Bij indiensttreding worden nieuwe medewerkers adequaat geïnforn	(a) Activiteiten of maatregelen voor het indien
Personeelsmanagement	4.15	HR.02	Certificering, training en scholing	Gebrek aan professionele training van (IT-)personeel kan leiden tot (	Opleiding, training en/of ervaring worden regelmatig getoetst om te	(a) Training en educatie worden ad hoc gelmpl
Personeelsmanagement	4.16	HR.03	Afhankelijkheid van individuen	Afhankelijkheid van sleutelfiguren brengt risico's met zich mee als d	Er is een opvolgingsplanning en back-upplan voor vitale medewerke	(a) Opvolgings- en back-upplannen zijn niet ge
Personeelsmanagement	4.17	HR.04	Verandering of beëindiging van functie	Gebruikersdogang wordt niet tijdig uitgeschakeld nadat medewerke	Wanneer er functiewijzigingen plaatsvinden, met name beëindiging	(a) Wanneer er functiewijzigingen of ontslagen
Personeelsmanagement	4.18	HR.05	Kennisdeling	Het ontbreken van procedures en werkinstructies voor het mogelijk	Overdracht van kennis en vaardigheden is geregeld, zodat eindgebr	(a) Overdracht van kennis is niet geïmplement
Personeelsmanagement	4.19	HR.06	Veiligheidsbewustzijn	Mensen die zich onvoldoende bewust zijn van informatiebeveiliging	Er is een Security Awareness Programma om gebruikers bewust te r	(a) Er zijn geen security-awareness activiteiten
Configuration Management	5.20	CO.01	Identificatie en onderhoud van configuratie-items	Verstoringen in de bedrijfsvoering als gevolg van ongeautoriseerde	Er zijn configuratieprocedures vastgesteld om het beheer en loggen	(a) Er is geen configuratieprocedure. (b) Werk
Configuration Management	5.21	CO.02	Configuratiedatabase en baseline	Zonder snelle detectie en correctie van onjuiste configuraties die de	Een supporttool en een centrale opslag zijn ingericht voor alle releva	(a) Basistaken op het gebied van Configuration
Incident/Problem Management	6.22	IM.01	Incident Management	Incidenten zijn niet correct geclassificeerd en worden onjuist behan	Een formeel Incident Management proces wordt gecommuniceerd	(a) Er is geen beleid voor Incident Managemen
Incident/Problem Management	6.23	IM.02	Incident escalatie	Incidenten worden niet tijdig geïdentificeerd, opgelost, beoordeeld,	Er worden procedures voor Incident Management (of voor de servic	(a) Er is geen beleid om incidenten die niet opg
Incident/Problem Management	6.24	IM.03	Incidentrespons op informatiebeveiligingsincidenten	Het ontbreken van een effectieve en tijdige reactie of follow-up van	De organisatie beschikt over mogelijkheden voor incident response	(a) Er zijn geen plannen/procedures om een ge
Incident/Problem Management	6.25	IM.04	Problem Management	Incidenten worden niet correct geclassificeerd en verkeerd afgehan	Een formeel Problem Management proces is gedefinieerd en gelmpl	(a) Er is geen beleid voor Problem Managemer
Change Management	7.26	CH.01	Normen en procedures voor aanpassingen	Het ontbreken van een formeel IT Change Management proces, dat	Procedures voor formeel Change Management zijn opgezet om alle	(a) Er is geen beleid of procedure voor Change
Change Management	7.27	CH.02	Impact assessment, prioriteren en autoriseren	Een verkeerde impact assessment, prioritering of autorisatie kan tot	Alle wijzigingsverzoeken worden op een gestructureerde manier be	(a) Er is geen procedure voor assessment, prio
Change Management	7.28	CH.03	Noodaanpassingen	Kritieke verstoring van bedrijfsprocessen kan niet tijdig worden opg	Wijzigingen tijdens een noodsituatie die onmiddellijke implementatie	(a) Er is geen procedure voor Change Manage
Change Management	7.29	CH.04	Testomgeving	Het ontbreken van een veilige, gecontroleerde en representatieve to	Er is een beveiligde testomgeving gedefinieerd en ingericht, die repr	(a) Er is geen structureel beveiligde testomgevi
Change Management	7.30	CH.05	Testen van aanpassingen	Ontoereikend of onvolledig testen kan leiden tot verstoring van de b	Voorafgaand aan migratie naar de operationele omgeving worden v	(a) Er is geen beleid voor het testen van wijzigi
Change Management	7.31	CH.06	Promotie naar productie	Als gevolg van onveilige overdracht van wijzigingen naar de product	Na testen wordt het gewijzigde systeem opgecontroleerde wijze en	(a) Er is geen beleid voor de overdracht van ge
Systeemontwikkeling	8.32	SD.01	Methodiek voor veilige softwareontwikkeling en -implementatie	Software- en/of systeemontwikkeling zijn niet ontworpen en geïmpl	Er is een gestructureerde aanpak (levenscyclus voor veilige software	(a) Er is geen gestructureerde aanpak. (b) Syst
Systeemontwikkeling	8.33	SD.02	Toegang tot de productieomgeving door ontwikkelaars	Ontwikkelaars met toegang tot de productieomgeving brengen de w	Medewerkers (ontwikkelaars) die betrokken zijn bij de ontwikkeling	(a) Er is geen beleid voor toegangsrestricties to
Systeemontwikkeling	8.34	SD.03	Data conversie en/of migratie	Afwijkingen tijdens dataconversie/ migratie worden niet (tijdig) ged	Het management heeft adequate beheersmaatregelen geïmplement	(a) Er zijn geen beheersmaatregelen gedefinie
Data Management	9.35	DM.01	Data (en systeem) eigenaarschap	Onduidelijk of dubbelzinnig eigenaarschap kan de effectieve besluit	Het bedrijf beschikt over procedures en hulpmiddelen, waarmee het	(a) Er is geen formeel beleid voor data-eigenaa
Data Management	9.36	DM.02	Classificatie	Beslissingen over het classificeren van informatie en (informatie)sys	Stel een classificatieschema op dat in de hele organisatie van toepas	(a) Er is geen classificatieschema. (b) De organ
Data Management	9.37	DM.03	Beveiligingseisen voor datamanagement	Ontoereikende (informatie)beveiligingseisen voor datamanagement	Beleid en procedures zijn vastgesteld en geïmplementeerd om (info	(a) Er is geen beleid voor veilig datamanagemer
Data Management	9.38	DM.04	Inrichting van opslag en retentie	Het ontbreken van procedures betreffende gegevensopslag, bewaar	Er zijn procedures gedefinieerd en geïmplementeerd voor het effect	(a) Er zijn geen procedures voor dataopslag. (b
Data Management	9.39	DM.05	Uitwisseling van (gevoelige) gegevens	Ongeautoriseerde toegang tot bronnen (gegevens) verbonden met	Informatiebeveiligingsbeleid en procedures zijn vastgesteld en geïm	(a) Er is geen beleid of richtlijn voor de uitwiss
Data Management	9.40	DM.06	Verwijdering van data	Het niet-grondig verwijderen van informatie kan leiden tot niet-naler	Er zijn informatiebeveiligingsprocedures vastgesteld en geïmplemen	(a) Data wordt ad hoc verwijderd. (b) Er zijn ge
Identity & Access Management	10.41	ID.01	Toegangsrechten	Onjuiste toegangsregels en/of toegangsgroepen kunnen ervoor zorg	De organisatie heeft toegangsgroepen (of rollen) gedefinieerd op ba	(a) Er is geen beleid voor informatietoegang. (I
Identity & Access Management	10.42	ID.02	Administratie van toegangsrechten	Ongeautoriseerde toegang tot gegevens, applicaties, besturingssyst	Toegangsrechten voor werknemers worden toegewezen in overeen	(a) Er is geen beleid voor gebruikersaccounts e

Tabblad Invul

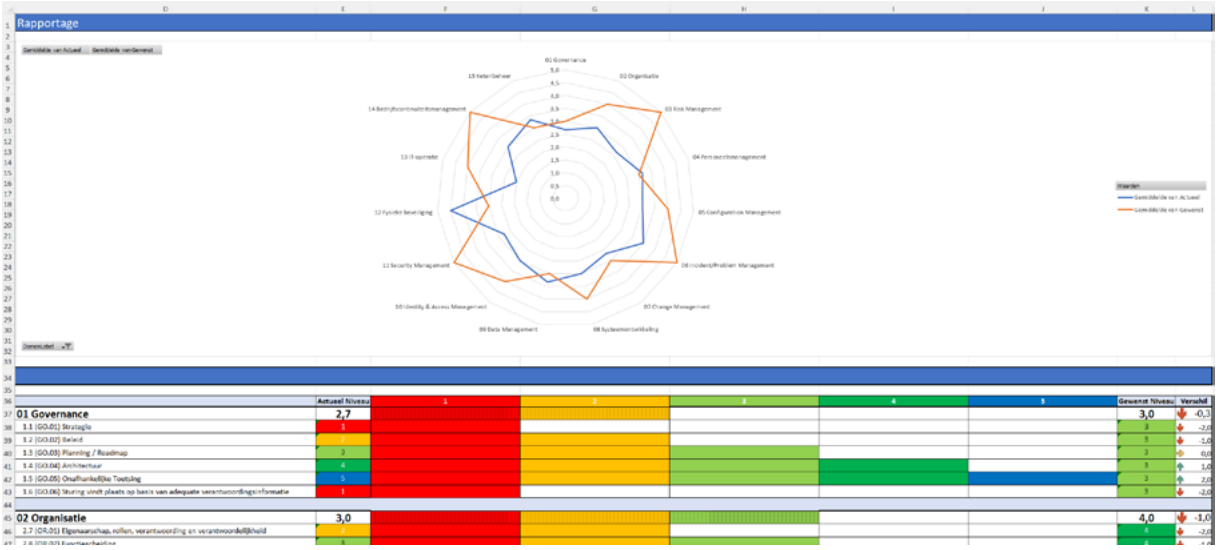
Hier is een opgemaakte versie van het complete model te vinden en hier kunnen de actuele en de gewenste volwassenheidsniveaus per statement ingevoerd worden. Dit tabblad heeft eenzelfde opmaak als de eerder uitgegeven versies van het model.



Domein	NBA ID	Categorie beheersmaatregel	Beschrijving risico	Beheersdoelstelling	Actueel Niveau	Gewenst Niveau	Volwassenheidsniveau 1
							Ad hoc
							Beheersmaatregelen zijn niet of slechts gedeeltelijk gedefinieerd en/of worden op een inconsistente manier uit
Governance	GO.01	Strategie	Het ontbreken van een strategie kan leiden tot slechte zakelijke en beveiligingsbeslissingen of tot een niet passend antwoord op veranderingen in de bedrijfsomgeving.	Een strategie en visie op informatiebeveiliging is leidend voor alle activiteiten en maatregelen met betrekking tot informatiebeveiliging.	1	3	(a) Implementatie en uitvoering van activiteiten en maatregelen op het gebied van informatiebeveiliging gebeurt ad
	GO.02	Beleid	Onvermogen om te voldoen aan wet- en regelgeving en/of interne informatiebeveiligingseisen, omdat het beleidskader dat de IT-strategie en informatiebeveiliging ondersteunt ineffectief is.	De organisatie heeft een (informatie)beveiligingsbeleid vastgesteld, beschreven en gecommuniceerd aan medewerkers. Indien van toepassing wordt het beleid ook actief meegedeeld aan leveranciers en contractpartners. Het beleid wordt regelmatig geëvalueerd en zo nodig geactualiseerd en goedgekeurd door het senior management.	2	3	(a) Er is geen beleid opgesteld. (b) Er zijn enkele beleidsstukken in concept.
	GO.03	Planning / Roadmap	De organisatie voorziet niet in richtlijnen of ondersteuning om informatiebeveiliging in overeenstemming te brengen met bedrijfsdoelstellingen, risico's en compliance eisen.	Bedrijfsdoelstellingen, risico's en compliance eisen worden verbsld in een algemeen informatiebeveiligingsplan, rekening houdend met de IT infrastructuur en de veiligheidscultuur.	3	3	(a) Er is geen informatiebeveiligingsplan of roadmap opgesteld. (b) Er lopen enkele projecten op het gebied van informatiebeveiliging of deze zijn gepland.
	GO.04	Architectuur	Onvolledig overzicht van huidige en beoogde architectuur kan leiden tot foutieve is kosten, complexiteit en onvermogen om tijdig te reageren op problemen die voortkomen uit zakelijke of juridische veranderingen of (externe) dreigingen.	Er is een enterprise information architecture model (EIAM) opgesteld en toegepast om applicatieontwikkeling en beslissingsondersteunende activiteiten mogelijk te maken, conform informatie- of IT-plannen. Dit model moet het mogelijk maken om effectief, veilig en op een robuuste manier informatie te creëren, gebruiken en te delen zoals wordt vereist door bedrijfsdoelstellingen en wettelijke voorschriften.	4	3	(a) Er is geen enterprise information architecture model (EIAM) gedefinieerd.
	GO.05	Onafhankelijke Toetsing	Naleving van wet- en regelgeving en prestaties worden niet beoordeeld en beveiligd door een onafhankelijke partij, waardoor onbekende en ongoddeesseerde afwijkingen in naleving en/of prestaties kunnen optreden.	Onafhankelijke toetsing (intern of extern) wordt gedaan om te bepalen in hoeverre de informatievoorziening (inclusief IT) voldoet aan relevante wet- en regelgeving, het beleid van de organisatie, de normen en procedures van de organisatie, algemeen aanvaarde werkwijzen, en effectieve en efficiënte prestaties van IT.	5	3	(a) Er vindt geen onafhankelijke toetsing plaats.
	GO.06	Sturing vindt plaats op basis van adequate verantwoordingsinformatie	Zonder adequate verantwoordingsinformatie kunnen eindverantwoordelijken geen sturing qua richting en/of snelheid van verbeteren of handhaven van informatiebeveiliging geven.	Eindverantwoordelijken ontvangen duidelijke verantwoordingsinformatie, dat zij risico's betreffende beschikbaarheid, integriteit en vertrouwelijkheid van informatie en systemen kunnen dragen en waar nodig kunnen bijsturen.	1	3	(a) Ad hoc wordt verantwoordingsinformatie betreffende incidenten en budgetverzoeken voor het verbeteren van i
	OR.01	Eigenaarschap, rollen, verantwoording en verantwoordelijkheid	Onduidelijke of dubbelzinnige toewijzing van eigenaarschap, rollen, verantwoordelijkheden of aansprakelijkheid kunnen effectieve besluitvorming, management en rapportage over informatiebeveiliging met betrekking tot bedrijfsvaseidetsuitbedrijfsrisico's in gevaar brengen.	Informatiebeveiliging wordt gemanaged op alle toepasselijke organisatieniveaus en Security (of Information Risk) Management wordt gemanaged in overeenstemming met business requirements/risico's. Eigenaarschap, rollen, verantwoordelijkheden en aansprakelijkheid zijn helmeel toegewezen en ingebed in de organisatie.	2	4	(a) Eigenaarschap, rollen en verantwoordelijkheden zijn niet toegewezen. (b) Er zijn enkele rollen te onderscheiden die informeel worden uitgevoerd.
	OR.02	Functiescheidiing	Acties van medewerkers (bijv. ongeautoriseerde toegang tot	Rollen en verantwoordelijkheden zijn gescheiden om de kans te			(a) Er vindt geen of nagenoeg geen functiescheiding plaats.

Tabblad Rapportage

In dit tabblad is een voorbeeld te zien hoe er gerapporteerd kan worden. De actuele score is hier afgezet tegen de gewenste score. Er zijn nog tal van mogelijkheden te bedenken om hierover te rapporteren en in grafieken weer te geven. Daarom is dit werkdocument beschikbaar gesteld om er mee aan de slag te gaan.



Rapportage

	Actueel Niveau	1	2	3	4	5	Gewenst Niveau	Verschil
01 Governance	2,7						3,0	-0,3
1.1 [GO.01] Strategie	1						3	-2,0
1.2 [GO.02] Beleid	2						3	-1,0
1.3 [GO.03] Planning / Roadmap	3						3	0,0
1.4 [GO.04] Architectuur	4						3	1,0
1.5 [GO.05] Onafhankelijke Toetsing	5						3	2,0
1.6 [GO.06] Sturing vindt plaats op basis van adequate verantwoordingsinformatie	1						3	-2,0
02 Organisatie	3,0						4,0	-1,0
2.7 [OR.01] Eigenaarschap, rollen, verantwoording en verantwoordelijkheid	2						4	-2,0

Gewenst volwassenheidsniveau

Op basis van het ingeschatte risico is een bepaald volwassenheidsniveau vereist dat het inherente risico waaraan de organisatie wordt blootgesteld afdoende mitigeert c.q. binnen de risicobereidheid (risk appetite) van de organisatie terugbrengt. In de vorige versie van het model werd dit Required maturity level based on inherent risk estimation genoemd.

De volgende volwassenheidsniveaus zijn van toepassing:

Score	Inherente risico-inschatting	Vereist volwassenheidsniveau
NVT	Niet van toepassing	Niet van toepassing
1	Nihil	Laag
2	Beperkt Ruim binnen risicobereidheid	Beperkt
3	Gemiddeld Net binnen of net buiten risicobereidheid	Gemiddeld
4	Aanzienlijk Buiten risicobereidheid	Meer dan gemiddeld
5	Hoog Ruim buiten risicobereidheid	Hoog

Tips & Tricks

- Het voorliggende model betreft een handreiking, die richtinggevend is voor een bepaalde aanpak en eventuele prioritering. De interne en externe context van een organisatie alsmede de bijbehorende bedreigingen, kwetsbaarheden en risico's zijn te allen tijde leidend voor het implementeren en uitvoeren van de beheersmaatregelen. Denk bijvoorbeeld aan het feit dat elke organisatie een onderdeel uitmaakt van een (waarde)keten en dat bij risicomitigatie en -acceptatie ook altijd een kosten-baten afweging plaatsvindt. Beiden zaken zijn voor elke organisatie specifiek c.q. anders.

- Het verdient aanbeveling om de risico indicatie organisatiespecifiek te maken door er herkenbare kengetallen en/of criteria aan te koppelen. Denk aan financiële impact (kosten / verliezen in euro's), operationele impact (kosten herstelwerk, aantal uren productieverstoring, organisatorisch omvang van verstoring) en reputationele impact (in regionaal of landelijke pers, intrekking van licentie).

- Betrek de auditor in de vorm van facilitator of laat ze een (plausibiliteits-)toets op de scores en bijbehorende documentatie (evidence) uitvoeren. Een onafhankelijke (plausibiliteits-)toets heeft zeker meerwaarde als de scores en bijbehorende documentatie richting externe stakeholders of een toezichthouder moeten worden gepresenteerd en/of verdedigd.

- Informatiebeveiliging is integraal onderdeel van de bedrijfsvoering en het verantwoordelijk management is eigenaar van de betreffende risico's. Organiseer daarom een "challenge" sessie, waarbij de verantwoordelijke directie wordt uitgedaagd met betrekking tot de geïmplementeerde en uitgevoerde maatregelen en bijbehorende restrisico's in relatie tot het toegekende volwassenheidsniveau. Op basis van de opgeleverde documentatie c.q. onderbouwing dient de verantwoordelijke directie zich te vergewissen dat deze passend is voor het toegekende volwassenheidsniveau.

- In geval dat de volwassenheidsscores worden gebruikt voor externe verantwoording verdient het aanbeveling om het verantwoordelijke directielid af te laten tekenen voor de volwassenheidsniveaus (en bijbehorende documentatie) behorende bij de aandachtsgebieden waar hij/zij verantwoordelijk voor is.

- In de gevallen waar het volwassenheidsniveau achterblijft bij het gewenste niveau verdient het aanbeveling de aandachtsgebieden (area's) te prioriteren. Bedenk dat er afhankelijkheden en/of randvoorwaardelijke aandachtsgebieden zijn. Voorbeelden hiervan zijn: uitkomsten uit risicomanagement proces of dataclassificatie proces zijn bepalend en richtinggevend voor diverse andere beveiligingsmaatregelen.

- Het verdient aanbeveling te identificeren waar het nemen van onmiddellijke actie het meeste effect sorteert om managementbetrokkenheid en ondersteuning voor het gebruik van deze handreiking (en het model) te krijgen voor hun eigen gemak, comfort en/of management control.

- Evalueer jaarlijks het model en het gebruik en de toepassing ervan. Informeer NBA in het geval er zaken zijn die verbetering of aanpassing behoeven in het model of bijbehorende aanpak.

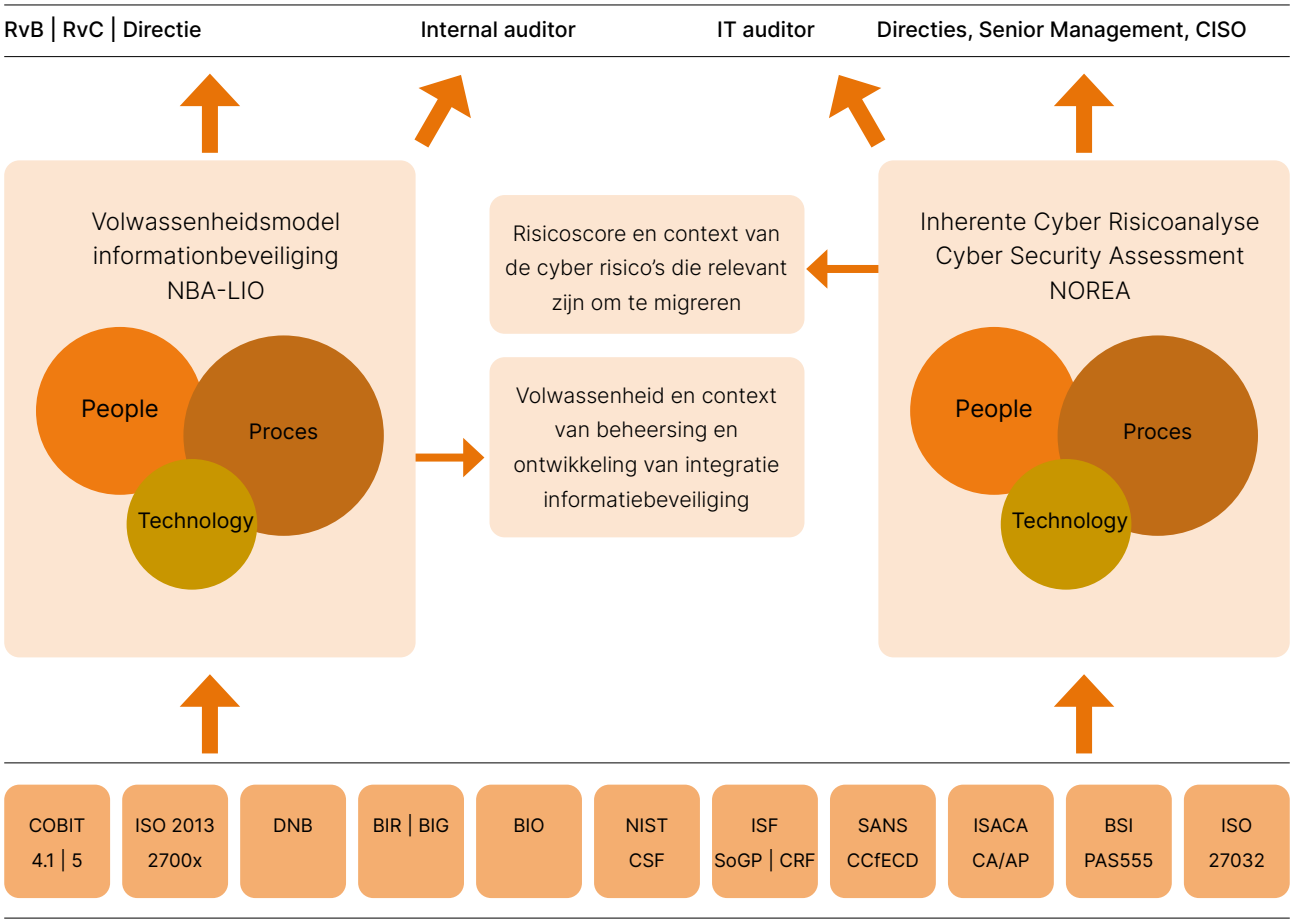
Relatie met andere NOREA handreikingen

De NBA-LIO en NOREA hebben er zorg voor gedragen dat de andere aanpalende NOREA handreikingen, in het bijzonder het Cyber Security Assessment (CSA)[1], zoveel mogelijk aansluiten op het NBA-LIO volwassenheids-model informatiebeveiliging en vice versa. Beide modellen kunnen als instrument voor het uitvoeren van een self-assessment worden gebruikt. Het volwassenheidsmodel informatiebeveiliging heeft controledoelstellingen gedefinieerd waarbij diverse controledoelstellingen relevant zijn voor cyber security. Deze controledoelstellingen zijn hoofdzakelijk geënt Proces en People en geven door middel van inschaling van beheersmaatregelen inzicht in het betreffende volwassenheidsniveau. Bij het CSA zijn alle aspecten gerelateerd aan cyber security en ligt de nadruk meer op Technology. Het CSA bestaat uit een lijst van gesloten vragen om een globaal inzicht te verkrijgen in de cyber risico's die de organisatie loopt.

Het CSA (en ICR) kan in de praktijk worden ingezet om te bepalen op welke onderdelen cyber risico's bestaan en door middel van welke standaarden de te treffen acties kunnen worden opgepakt. Hiermee biedt het een middel voor IT en informatiebeveiliging experts om een gesprek aan te gaan met IT- en algemeen management. Hiermee is het model ook bruikbaar voor de (internal) IT auditor die op het gebied van cyber security werkzaamheden verricht. Ook het ICR/CSA maakt als basis gebruik van standaarden zoals NIST, ISF en ISO.

Het complementair karakter van beide modellen kan gevonden worden in het feit dat de dialoog met de bestuurskamer dan wel senior management, IT en CISO's ondersteund kan worden door de juiste context te creëren. Technische maatregelen om te treffen vanuit de inherente cyber risicoanalyse en het cyber security assessment kunnen snel op houdbaarheid en haalbaarheid getoetst worden door het te beschouwen vanuit het volwassenheidsniveau waarop de organisatie zich bevindt. Een geavanceerd intrusion detection system kan bijvoorbeeld heel goed werken maar schiet wellicht zijn doel voorbij als randvoorwaardelijke beheersmaatregelen niet aanwezig zijn of de organisatie hier verder geen tijdige opvolging aan kan geven.

1 NOREA heeft een handreiking voor Inherente Cyber Risicoanalyse (ICR) opgesteld, die een aanvulling is op de bestaande CSA. Er is een update beschikbaar, (versie 2.2) met een gecombineerde/integrale spreadsheet op basis van nieuwe/actuele standaarden en referenties.



Figuur 1: NBA-LIO volwassenheidsmodel en NOREA CSA in verhouding

Koninklijke Nederlandse
Beroepsorganisatie
van Accountants

NBA

Mercuriusplein 3
2132 HA Hoofddorp
Postbus 242
2130 AE Hoofddorp

T 088 4960 301
E nba@nba.nl
I www.nba.nl

2024034