Auteurs: Lisa de Kok (onderzoeker) en Marcel Spruit (lector) zijn werkzaam bij het lectoraat Cyber Security & Safety aan de Haagse Hogeschool. Lisa de Kok is te bereiken via l.c.dekok@hhs.nl, Marcel Spruit via m.e.m.spruit@hhs.nl.

Analyse volwassenheids-modellen voor informatiebeveiliging

Organisaties die belang hechten aan hun informatie moeten ervoor zorgen dat de informatiebeveiliging goed is geregeld. Als de informatiebeveiligingsprocessen niet voldoende zijn ingericht en er geen duidelijke afspraken en verantwoordelijkheden worden vastgelegd, is de kans aanwezig dat een incident (te) laat wordt gesignaleerd. Via een volwassenheidsmeting wordt inzicht verkregen op welk niveau de informatiebeveiliging is georganiseerd.

Een volwassen persoon is een volgroeid persoon. Volwassen worden gebeurt in meerdere fases en niet van de een op de andere dag wanneer iemand 18 wordt. Een organisatie kan ook in meerdere of mindere mate volwassen zijn met betrekking tot informatiebeveiliging. Hoe volwassener, des te beter de organisatie in staat is de ontwikkeling en handhaving van informatiebeveiliging in goede banen te leiden. Dit betekent echter niet, dat elke organisatie moet streven naar het hoogste niveau van volwassenheid. Er moet altijd een gedegen afweging te worden gemaakt welk niveau passend is bij de wensen van de organisatie.

Naarmate een organisatie volwassener wordt in de informatiebeveiliging, betekent dit dat de informatiebeveiliging op een meer integrale manier is georganiseerd (8). Praktisch betekent een hogere mate van volwassenheid een hogere mate van institutionalisering van het desbetreffende proces via beleid, standaarden en organisatorische structuren (12). Bij een minder volwassen organisatie wordt meer ad hoc of minder doordacht ingespeeld op de problematiek.

Wat is een volwassenheidsmodel?

Om te weten in hoeverre een organisatie volwassen is, zijn volwassenheidsmodellen ontwikkeld. Een model is een vereenvoudigde weergave aan de hand waarvan een meting kan worden uitgevoerd. Een volwassenheidsmodel is een set van kenmerken, indicatoren of patronen die gekoppeld zijn aan volwassenheidsniveaus in een bepaald domein of discipline (2). Daarmee geven volwassenheidsmodellen een indicatie van de capaciteiten van een organisatie. In elk van de gebruikelijke vijf volwassenheidsniveaus ligt vast welke kenmerken erbij horen. Deze niveaus, van initieel (1) naar geoptimaliseerd (5), vullen elkaar cumulatief aan (14).

Volwassenheidsmodellen zijn wijdverspreid in het domein van computerwetenschappen en informatiesystemen, maar ook in andere domeinen zoals biologie, sociologie en psychologie (7). De huidige volwassenheidsmodellen binnen de IT-sector zijn veelal gebaseerd op het Capability Maturity Model (CMM). Deze werd ontwikkeld door het Software Engineering Institute in het midden van de jaren ’80 (12). Bij dit model wordt gekeken naar procesvolwassenheid bij software engineering. Dit betekent dat volwassenheid zich uit in de mate waarin een (software engineering) proces effectief, gedefinieerd, beheerd, gemeten en gecontroleerd is (12).

Een meting aan de hand van een volwassenheidsmodel kan voor beschrijvende of voorschrijvende doeleinden worden gebruikt. Een volwassenheidsmeting heeft een beschrijvend doel als het wordt toegepast voor een beoordeling van de huidige capaciteiten van de organisatie op het desbetreffende domein (14). Met deze omschrijving kan een vergelijking worden gemaakt met een eerdere meting, een ander organisatieonderdeel of een vergelijkbare organisatie. Aanvullend kan het een voorschrijvend doel dienen, als richtlijnen worden gegeven met concrete maatregelen om een ander niveau van volwassenheid te bereiken (14).

Soorten volwassenheidsmodellen

Er worden verschillende soorten volwassenheidsmodellen onderscheiden in de literatuur, zoals capability modellen, progress modellen en hybride volwassenheidsmodellen. De kenmerken van deze verschillende modellen worden hieronder omschreven.

Een capability model kijkt naar de mogelijkheid in hoeverre een organisatie in staat is om specifieke taken uit te voeren in een bepaald domein of discipline (2). Aan de hand van een capability model is een organisatie in staat op verschillende onderdelen van bijvoorbeeld informatiebeveiliging zijn huidige capaciteiten (capabilities) zichtbaar te maken. De gemeten niveaus geven een indicatie van de organisatievolwassenheid; wordt iets ad hoc uitgevoerd of systematisch en kwantitatief gemonitord. Een progress model meet volwassenheid aan de voortgang (progress) van een bepaald kenmerk in een model (2). In tegenstelling tot een capability model meer dan alleen de aanwezigheid van bepaalde kenmerken, maar ook de organisatorische vaardigheid om dat kenmerk uit te voeren en het institutionaliseren ervan. Een hybride model is een combinatie van een progress en een capability model.

De vraag is in hoeverre deze soorten modellen in de praktijk daadwerkelijk te onderscheiden zijn. Uiteindelijk gaat het allemaal om een maat van de volwassenheid, ofwel in de aanwezigheid van kenmerken (progress model) dan wel in welke mate de activiteiten zijn geïnstitutionaliseerd (capability model). Belangrijker is om te weten wat een volwassenheidsmodel een goed volwassenheidsmodel maakt in de informatiebeveiliging. In dit artikel wordt daarom geen onderscheid gemaakt tussen verschillende soorten modellen, maar wel bekeken of de benodigde elementen aanwezig zijn in het volwassenheidsmodel. Daarvoor is het nodig om te weten welke elementen in een volwassenheidsmodel zouden moeten zitten en aan de hand van welke criteria volwassenheidsmodellen kunnen worden geëvalueerd.

Eerdere reviewstudies hebben in totaal negentien volwassenheidsmodellen voor informatiebeveiliging naast elkaar gelegd en met elkaar vergeleken (1, 6, 8, 9, 10, 13, 15). Er zijn een paar beperkingen aan deze eerdere studies. Zo wordt bij deze onderzoeken slechts een deel van de relevante modellen meegenomen (15), wordt geen consistente en inzichtelijke review gegeven van de modellen (6, 10, 13), is de documentatie van de modellen niet vrijelijk beschikbaar waardoor geen beoordeling kan worden gemaakt (4, 6, 9), zijn criteria aan de hand waarvan de volwassenheidsmodellen worden geëvalueerd niet duidelijk beschreven (8, 9), worden modellen meegenomen die in feite geen volwassenheidsmodellen zijn (1, 8, 10), of waarin slechts een onderdeel van informatiebeveiliging wordt gemeten (1, 3, 6, 8, 9, 10, 15). In Tabel 1 is het overzicht gegeven van de informatiebeveiligingsvolwassenheidsmodellen die niet zijn meegenomen in de nadere analyse vanwege een van bovenstaande beperkingen. Vier modellen worden wel meegenomen, namelijk NBA-LIO, C2M2, ISM3 en het 3-Pijlermodel (5, 11, 18, 20). De toegevoegde waarde van dit artikel is de combinatie van het opstellen van de elementen van een volwassenheidsmodel, het opstellen van criteria waaraan de volwassenheidsmodellen kunnen worden geëvalueerd en een overzicht van volwassenheidsmodellen waarin informatiebeveiliging met al zijn elementen wordt meegenomen. De criteria die zijn opgesteld, kunnen als checklist gebruikt worden om uiteindelijk een volwassenheidsmodel te kiezen. De vraag die hier centraal staat is: welk informatiebeveiligingsvolwassenheidsmodel is pragmatisch voor een meting in een organisatie? Daarom wordt ingegaan op welke verschillende volwassenheidsmodellen voor informatiebeveiliging er zijn en welke elementen deze bevatten. Verder worden criteria opgesteld aan de hand waarvan de volwassenheidsmodellen kunnen worden geëvalueerd.

Elementen volwassenheidsmodel

Ondanks hun verscheidenheid hebben volwassenheidsmodellen in principe eenzelfde structurele basis waar ze uit bestaan. De elementen staan hieronder benoemd. Eerdere studies waarin volwassenheidsmodellen met elkaar worden vergeleken grijpen meestal niet terug op deze structurele basis (1, 6, 9, 13). Omdat er niet wordt uitgegaan van deze structurele basis, worden modellen in de evaluatie meegenomen die eigenlijk geen volwassenheidsmodellen zijn. Caralli et al (2) hebben een overzicht gemaakt van de elementen van een volwassenheidsmodel. Dit overzicht komt overeen met een van de eerste volwassenheidsmodellen (CMM) (12).

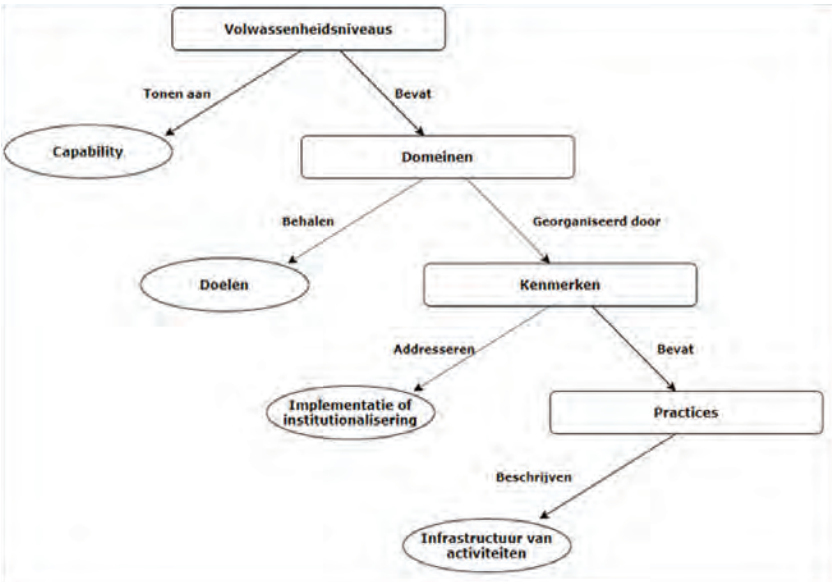
		Exclusie-criteria	Referentie
1.	CITI-ISEM	- Geen volledige documentatie beschikbaar - Omvat een te beperkt deel van informatiebeveiliging (security awareness)	[6, 8]
2.	ISM2	- Geen volledige documentatie beschikbaar	[6, 8, 9]
3.	GISMM	- Geen volledige documentatie beschikbaar	[8]
4.	Praktisch VM	- Geen volledige documentatie beschikbaar	[4]
5.	ISFM IBM	- Onvolledig uitgewerkt in beschikbare documentatie	[6, 8]
6.	ISMS (Im)-Maturity Model	- Onvoldoende uitgewerkt - Niet makkelijk en praktisch uit te voeren	[6]
7.	ISMS	- Geen volwassenheidsmodel maar een managementsysteem	[8, 10]
8.	COBIT 5	- Geen volwassenheidsmodel maar een management framework	[1]
9.	SSE CMM	- Omvat een te beperkt deel van informatiebeveiliging (security engineering)	[1, 8, 9, 15]
10.	CSF NIST	- Omvat een te beperkt deel van informatiebeveiliging (cybersecurity risk management)	[6, 8, 10, 13]
11.	CIP Privacy-model	- Omvat een te klein deel van informatiebeveiliging (privacy)	[3]
12.	CERT RMM	- Omvat niet specifiek informatiebeveiliging (operational resilience)	[8, 10, 13]
13.	NICE CSMM	- Omvat een te beperkt deel van informatiebeveiliging (workforce management)	[8, 10, 15]
14.	COBIT Process Assessment Model	- Omvat een te beperkt deel van informatiebeveiliging (IT-processen)	[1,9]
15.	CCSMM	- Omvat een te beperkt deel van informatiebeveiliging (community cyber security)	[8, 15]

Tabel 1 - Overzicht niet-geselecteerde informatiebeveiligingsvolwassenheidsmodellen.

De structurele basis bestaat uit de volgende elementen:

Niveaus:
Geven de schaal aan van de volwassenheid van (proces)capaciteit. De niveaus gaan van initieel (1) naar geoptimaliseerd (5). De niveaus zijn cumulatief, dit betekent dat de eigenschappen van de vorige niveaus behouden blijven bij een volgend niveau en er nieuwe eigenschappen aan toegevoegd worden. Van elk niveau dient een gedegen beschrijving te zijn. Elk niveau bevat een set van doelen dat een belangrijke eigenschap van het proces bevat. Elk volwassenheidsniveau bestaat uit sleutelprocesdomeinen, welke bestaan uit gemeenschappelijke kenmerken waaruit belangrijke werkwijzen worden gespecificeerd (12).

Domeinen:
Onderdelen van het gehele onderwerp, in dit geval informatiebeveiliging, in logische categorieën en/of praktijken verdeeld.



Figuur 1 - Visualisatie van de structuur van een volwassenheidsmodel (12).

Doelen:
Elk volwassenheidsniveau bevat een aantal procesdoelen. Deze vatten de belangrijke good practices samen en worden gebruikt om te bepalen of een organisatie effectief de domeinen heeft geïmplementeerd.

Kenmerken:
Ook wel attributen, karakterkenmerken, indicatoren, praktijken of processen genoemd. De kenmerken geven een indicatie in hoeverre de implementatie en institutionalisering van een domein effectief, herhaalbaar en blijvend is. Daarnaast is voor de uitvoering van de methode nodig:

Scoringsmethode
Zodat op een uniforme manier de meting wordt uitgevoerd.

Stappenplan ter verbetering
Op basis van de uitkomst van de scoringsmethode, concrete acties om het volwassenheidsniveau te verhogen.

Criteria volwassenheidsmodel

De criteria op basis waarvan de volwassenheidsmodellen worden geëvalueerd, staan hieronder beschreven en onderstreept. Aan de hand van gestelde criteria kunnen de volwassenheidsmodellen tegen een maatstaf worden aangelegd.
Uitgangspunt is dat een volwassenheidsmodel pragmatisch is. Wat zijn criteria voor een pragmatisch volwassenheidsmodel? Synoniemen van pragmatisch zijn: praktisch, toepasbaar, doelmatig en waardevol. Een pragmatisch volwassenheidsmodel is geschikt om gebruikt te worden door een bepaalde doelgroep. De doelgroep voor deze volwassenheidsmodellen zijn medewerkers die de meting niet op dagelijkse basis uitvoeren, maar wel gedegen kennis hebben over informatiebeveiliging en hier een beoordeling van kunnen maken.
Primair is het belangrijk dat een model de hiervoor genoemde structurele elementen bevat van een volwassenheidsmodel om zich ook zo te noemen. Een volwassenheidsmodel is bruikbaar indien het ingezet kan worden in verschillende omgevingen. Het is daarom belangrijk dat een volwassenheidsmodel algemeen van aard is en niet alleen gebruikt kan worden binnen een bepaalde organisatie of industrie. Daarvoor dient het model flexibel te zijn, zodat het aangepast kan worden aan de wensen en eisen van de organisatie waar de meting wordt uitgevoerd.
Verder is de gebruiksvriendelijkheid van belang. Een evenwicht moet worden gevonden tussen het hebben van te veel maatregelen, eigenschappen en vragen, versus te weinig eigenschappen om te komen tot een consistente en juiste beoordeling." (2). Gebruiksvriendelijkheid is essentieel; in een eerder verschenen evaluatie-template van volwassenheidsmodellen door experts krijgt het een prominente status (16). Gebruiksvriendelijkheid is onderverdeeld in de volgende kenmerken: begrijpelijkheid, gebruiksgemak en uitvoerbaarheid (16). Onder uitvoerbaarheid valt ook de hoeveelheid tijd en moeite die het kost om een meting uit te voeren. Het is niet wenselijk dat dit langer dan enkele dagen duurt of alleen door een hiervoor opgeleide specialist kan worden uitgevoerd. Onder gebruiksgemak valt ook de

toegankelijkheid van gedetailleerde documentatie (13).
Belangrijk bij een meting is dat deze valide en betrouwbaar is. De validiteit van een meting geeft aan in hoeverre het meetinstrument meet wat het zou moeten meten. Een indicatie hiervoor is hoe het begrip informatiebeveiliging in een volwassenheidsmodel wordt beschreven en gemeten. Omdat een (capability) volwassenheidsmodel de capaciteiten van een organisatie meet om informatiebeveiliging uit te voeren, ligt de nadruk op de goede manier organiseren van de informatiebeveiliging. Een startpunt daarin is het opstellen van informatiebeveiligingsbeleid. Beleid heeft een preventieve, signalerende en correctieve functie (17). Inhoudelijke input voor het beleid kan gehaald worden uit een norm, zoals bijvoorbeeld de ISO 27001. Beleid alleen is niet voldoende, controle of het beleid wordt nageleefd door systematische monitoring (17) en het toekennen van verantwoordelijkheid van informatiebeveiliging aan medewerkers is ook onderdeel van het organiseren van informatiebeveiliging (19). Verder is erkenning van het model door andere academici en/of vakgenoten van belang voor de validiteit. Tot slot is een betrouwbare meting vrij van willekeurige meetfouten. Om een betrouwbare meting te bewerkstelligen is een heldere diagnostische methode nodig.
Uit de voorgaande tekst zijn de volgende criteria af te leiden voor een pragmatisch volwassenheidsmodel:

- Bevat de benodigde elementen van een volwassenheidsmodel;
- Is flexibel;
- Is gebruiksvriendelijk (begrijpelijkheid, gebruiksgemak en uitvoerbaarheid, toegang tot gedetailleerde documentatie);
- Is valide: goede organisatie van informatiebeveiliging, informatiebeveiligingsbeleid, naleving, koppeling norm, verantwoordelijkheid, erkenning model door academici/practici;
- Is betrouwbaar (diagnostische methode).

Vier volwassenheidsmodellen

Hieronder worden de vier overgebleven volwassenheidsmodellen, NBA-LIO, C2M2, ISM3 en het 3-Pijlermodel, geëvalueerd. In een voorafgaande deskresearch die door ons is uitgevoerd zijn negentien volwassenheidsmodellen voor informatiebeveiliging naar boven gekomen. De andere vijftien zijn niet meegenomen in de analyse omdat deze niet voldoen aan de meest basale criteria, genoemd in tabel 1. De analyse is gedaan op basis van de beschikbare documentatie, tools, reviews en literatuur en aan de hand van de gestelde criteria. Ieder van de vier modellen wordt omschreven en de belangrijkste voor- en nadelen worden genoemd. De resultaten zijn samengevat in tabel 2.

	Validiteit									
	Elementen	Flexibel	Gebruiksvriendelijk	Koppeling norm	Beleid	Naleving	Verantwoordelijkheid	Erkenning	Betrouwbaarheid	Totaal
NBA-LIO	++	±	++	++	±	+	±	+	+	9
C2M2	++	±	+	+	±	+	±	+	+	7
ISM3	-	++	--	±	+	++	++	±	±	4
3PijlersIB	+	±	+	±	±	++	++	±	++	8
Meting	-- (-2) / - (-1) / ± (0) / + (1) / + + (2)									Schaal: (-18 / + 18)

Tabel 2 - Analyse volwassenheidsmodellen a.d.h.v. gestelde criteria.

NBA-LIO

De Nederlandse Beroepsorganisatie van Accountants (NBA-LIO) heeft een volwassenheidsmodel van vijf niveaus voor informatiebeveiliging gemaakt (11). In deze versie is de samenhang verwerkt met de Inherente Cyber Risicoanalyse (ICR) en het Cyber Security Assessment (CSA) van de NOREA (beroepsorganisatie van IT-Auditors). Het model vindt aansluiting met andere raamwerken en standaarden zoals het NIST-raamwerk, COBIT, ISO27002 en de Baseline Informatiebeveiliging Overheid (BIO).
Het model van NBA-LIO is gebruiksvriendelijk. In de Excel-matrix staat op een volledige en korte manier omschreven wat kenmerkend is op elk van de 15 aandachtsgebieden en deelgebieden voor dat volwassenheidsniveau. Door de matrix in te vullen kan het volwassenheidsniveau worden bepaald. Beleid heeft een plek in het gebied governance onder 'policy'. Dit heeft maar een beperkt gewicht ten opzichte van het geheel. In het tweede domein 'organisatie', wordt gefocust op het belang van verantwoordelijkheid. Naleving wordt geborgd in het domein human resources, het domein incident/problem management en Business Continuity Management. Het aangereikte volwassenheidsmodel biedt expliciete richtlijnen om organisatiebreed, organisatieoverstijgend en/of sectorbreed volwassenheidsniveaus van informatiebeveiliging vast te stellen en een handreiking om de meting uit te voeren.
Het model is nog niet erkend of beschreven in de academische wereld. Door de samenwerking met NOREA, de beroepsvereniging voor IT-auditors, kan gezegd worden dat de erkenning rond vakgenoten wel aanwezig is. De diagnostische methode is duidelijk en eenduidig, wat een positieve uitwerking heeft voor de betrouwbaarheid.

Verantwoordelijkheid zit in het domein workforce management en in de richtlijnen bij de managementdoelen

Doordat automatisch grafieken worden gegenereerd, worden vergelijkingen tussen bedrijfsonderdelen of 'industry peers' eenvoudig gemaakt. Het model heeft een overzichtelijke matrix met gewichten en eisen. Of de meting wordt uitgevoerd op basis van een automatische matrixrapportage of door interviews, komt niet duidelijk naar voren.

C2M2

Het beschrijvende Cybersecurity Capability Maturity Model (C2M2) is ontwikkeld door 'the United States Department of Energy' (20). Dit model hanteert vier niveaus in plaats van de gebruikelijke vijf, genoemd Maturity Indicator Levels (MILs). Hierdoor is minder spreiding en moeten meer activiteiten uitgevoerd worden om een volgend niveau te halen. Binnen het model zijn tien domeinen die zich onderscheiden in verschillende soorten processen van de organisatie. Elk domein heeft een logische groepering van cybersecuritypraktijken (15). De inhoud van het model komt voort uit standaarden van NIST en ISO.

De gebruiksvriendelijkheid van C2M2 is vrij goed. De Excel vult makkelijk in, maar het aanvullende document van meer dan tachtig bladzijdes is niet erg prettig. Met betrekking tot de validiteit laat de focus op beleid te wensen over. In elk domein staan een of enkele punten voor het streven naar documentatie en/of beleid. Hierin is echter geen duidelijke lijn en bovendien is documentatie niet hetzelfde als beleid. Verantwoordelijkheid zit in het domein workforce management en in de richtlijnen bij de managementdoelen voor ieder domein. Deze richtlijnen zijn slechts 10 van de in totaal meer dan 300 richtlijnen, waardoor uiteindelijk weinig gewicht hangt aan het zorgen voor verantwoordelijkheid met betrekking tot informatiebeveiliging. Naleving is ook een van de managementdoelen. Daarnaast wordt op verschillende domeinen gecheckt op logging en monitoring, waardoor de naleving van de cybersecurity wordt gecontroleerd.

Erkenning van dit model kan gevonden worden in de wetenschappelijke kringen; veel artikelen namen C2M2 mee en het is een geregistreerd trademark van de Carnegie Mellon University. Een evaluatie met de C2M2 is uit te voeren met een zelfevaluatie toolkit in één dag. De omschrijvingen zijn abstract waardoor het model breed toepasbaar is voor organisaties van verschillende groottes en contexten. Er zijn geen 'good practices' aan gekoppeld en bij het invullen van het format wordt niet gerefereerd aan welk(e) (deel van) de norm dit is gekoppeld. Of de meting wordt uitgevoerd door interviews of dat medewerkers het zelf invullen, komt niet naar voren in de handleiding.

ISM3

Information Security Management Maturity Model, ISM3, is een informatiebeveiliging volwassenheidsstandaardgepubliceerd door de Open Group (standaardisatieorganisatie), voor het laatst herzien in 2017 (5). Volwassenheid uit zich in de uitvoering van de belangrijkste processen die gekoppeld zijn aan de doelen van een organisatie. In plaats van te kijken naar maatregelen, ligt de focus op processen die in bepaalde mate voor elke organisatie van toepassing zijn. Beveiligingsdoelen zijn gekoppeld aan de doelen van de organisatie. ISM3 is toepasselijk voor allerlei soorten organisaties en gekoppeld aan verschillende standaarden, waaronder ISO 27001.

Het procesmodel van ISM3 wordt als uitgangspunt genomen en bestaat uit vier punten: good practices en strategisch, tactisch en operationeel management. Als basis wordt het belang van goede documentatie genoemd in de algemene good practices; hier valt beleid ook onder. Naleving wordt geborgd middels operationeel management door rapportages, controles, testen, monitoring en het omgaan met incidenten.

Verantwoordelijkheid is overal in verweven omdat het als onderdeel wordt gezien van procesmanagement.
ISM3 heeft niet het standaard format van volwassenheidsmodellen; het bestaat niet uit domeinen maar heeft wel volwassenheidsniveaus. Meetwijzen zijn zelf te kiezen en gekoppeld aan de doelen van de organisatie. Grootste nadeel is dat het geen self-assessment tool is die vrijelijk beschikbaar is. Desondanks is dit volwassenheidsmodel wel meegenomen in de analyse omdat uit de beschikbare documentatie naar eigen invulling en wens wel een check kan worden gedaan op de mate van volwassenheid. Een uiteindelijke beoordeling is gemaakt op basis van referenties vanuit ISM3 zelf, eerder uitgevoerde cases, en de wetenschappelijke literatuur (6, 8). Hierdoor is ook geen beoordeling te maken over de gebruiksvriendelijkheid.

3 Pijlermodel, volwassenheid informatiebeveiliging

Het volwassenheidsmodel ontwikkeld door Spruit, 3-Pijlermodel, gaat uit van drie pijlers: 1 - het uitvoeren van de goede activiteiten, 2 - het goed uitvoeren van de activiteiten en 3 - het goed beleggen van de uitvoering en aansturing (18). De norm ISO 27001 is als uitgangspunt genomen voor de eerste pijler. Een omschrijving van elk van deze pijlers is gekoppeld aan vijf volwassenheidsniveaus. De meting wordt uitgevoerd met een vragen-format voor semigestructureerd interviews.
Onder de eerste pijler wordt beleid als slechts een van de acht belangrijke onderdelen gezien, wat duidt op een beperkte nadruk op beleid. De tweede pijler checkt de kwaliteit van de werkwijze. De focus in dit model ligt op de uitvoering en naleving; de meeste interviewvragen worden gesteld over testen, risicoanalyses, monitoring en rapporteren van incidenten. Bij de derde pijler ligt het accent op verantwoordelijkheid en dit uit zich ook in een veelvoud aan vragen in het interviewformat met betrekking tot verantwoordelijkheid.
Het onderscheidend kenmerk van dit model is dat de meting wordt uitgevoerd door middel van semigestructureerde interviews en dat de vragen hiervoor al zijn uitgeschreven. Het uiteindelijke volwassenheidsniveau kan worden vastgesteld aan de hand van een analyseschema. Het voordeel en gelijk het nadeel van deze methode is dat het vrijheid geeft aan de interpretatie van de afnemer van de meting. Daarnaast is slechts één eerdere meting uitgevoerd onder 23 waterschappen en is er nog niet (wetenschappelijk) over gepubliceerd, waardoor de erkenning beperkt is. Verder is het model alleen beschikbaar in het Nederlands.

Welke volwassenheidsmeting is de beste?

In dit artikel zijn de vier meest relevante informatiebeveiligingsvolwassenheidsmodellen omschreven en geanalyseerd aan de hand van gestelde criteria, zodat elke organisatie kan bepalen welk volwassenheidsmodel het meest relevant is. Drie van de vier geselecteerde volwassenheidsmodellen hadden een vergelijkbare score, waar het model van NBA-LIO uiteindelijk de hoogste score had.
Samengevat hebben de modellen de volgende sterke en

minder sterke punten. **NBA-LIO** springt er positief uit op het gebied van de aanwezigheid van de elementen van een volwassenheidsmodel, gebruiksvriendelijk, koppeling met de verschillende normen. Minder sterk ontwikkeld is de flexibiliteit, de nadruk op het belang van beleid en verantwoordelijkheid. **C2M2** scoort over zijn geheel voldoende maar niet uitzonderlijk en heeft een goede structurele basis die alle elementen van een volwassenheidsmodel bevat. **ISM3** is flexibel en benadrukt het belang van de naleving en verantwoordelijkheid. De gebruiksvriendelijkheid laat echter te wensen over doordat de documentatie niet in zijn geheel beschikbaar is. Het **3-Pijlermodel** legt de nadruk op uitvoering, naleving en verantwoordelijkheid en heeft een betrouwbaar meetinstrument, over zijn geheel scoort het ook voldoende maar niet uitzonderlijk positief of negatief.
De korte omschrijvingen in dit stuk zijn waarschijnlijk te beperkt voor een uiteindelijke keuze, maar geeft een mooie opstap voor een gesprek over welk model in een organisatie toepasselijk is. Als in de toekomst een volwassenheidsmeting op de planning staat, kan deze analyse als input dienen.

Referenties

(1) Almuhammadi, S., & Alsaleh, M. (2017). Information Security Maturity Model for Nist Cyber Security Framework. Computer Science & Information Technology (CS&IT), 7(3), 51-62.

(2) Caralli, R., Knight, M., & Montgomery, A. (2012). Maturity Models 101: A Primer for Applying Maturity Models to Smart Grid Security, Resilience, and Interoperability Mark Knight, CGI Group and GridWise Architecture Council (GWAC) Member.

(3) CIP. (2017). Grip op Privacy: Privacy Volwassenheidsmodel - Model voor organisaties om te groeien in de omgang met privacy. www.cip-overheid.nl/media/1141/20171102-privacy-volwassenheidsmodel-v3_0_9.pdf

(4) De Bruine, H., Lucero Garau, F., & Spruit, M.E.M. (2019, 6) Een praktisch volwassenheidsmodel voor informatiebeveiliging. iB-Magazine, 4-9 www.pvib.nl/actueel/ib-magazines/ib-magazine-2019-6/downloaden

(5) ISM3 Consortium. (2007). ISM 3 Information Security Management Maturity Model

(6) Karokola, G., Kowalski, S., & Yngström, L. (2011). Towards An Information Security Maturity Model for Secure e-Government Services : A Stakeholders View. In Proceedings of the 5th International Symposium on Human Aspects of Information Security & Assurance, Haisa (pp. 58-73).

(7) Kohlegger, M., Maier, R., & Thalmann, S. (2009). Understanding maturity models results of a structured content analysis. Proceedings of I-KNOW 2009 - 9th International Conference on Knowledge Management and Knowledge Technologies and Proceedings of I-SEMANTICS 2009 - 5th International Conference on Semantic Systems, (December 2016), 51-61

(8) Le, N.T., & Hoang, D. B. (2016). Can maturity models support cyber security? In Proceedings of the 35th IEE International Performance Computing and Communications Conference. Las Vegas.

(9) Luma, A., Abazi, B., Selimi, B., & Hamiti, M. (2018). Comparison of Maturity Model Frameworks in Information Security and Their Implementation. In International Conference on Engineering Technologies (ICENTE'18) (pp. 102–104)

(10) Miron, W., & Muita, K. (2018). Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure. In Technology Innovation Management Review (Vol. 4).

(11) NBA-LIO. (2019). Handreiking bij Volwasssenheidsmodel Informatiebeveiliging. www.nba.nl/globalassets/over-de-nba/ledengroepen/lio/lio-new/nba-lio-norea-handreiking-bij-volwassenheidsmodel-informatiebeveiliging-januari-2019.pdf

(12) Paulk, C., Curtis, B., & Chrissis, M. B. (1993). Capability Maturity Model , Version 1.1. Software Engineering Institute, 18–27. https://doi.org/10.1109/52.219617

(13) Payette, J., Anegbe, E., Caceres, E., & Muegge, S. (2015). Secure by Design: Cybersecurity Extensions to Project Management Maturity Models for Critical Infrastructure Projects. Technology Innovation Management Review, 5(6), 26-34.

(14) Poppelbuss, J., & Roglinger, M. (2011). What Makes A Useful Maturity Model? A Framework of General Design Principles for Maturity Models and Its Demonstration In Business Process Management. In European Conference on Information Systems (ECIS)

(15) Rea-Guaman, A., San Feliu, T., Calvo-Manzano, J. A., & Sanchez-Garcia, I. D. (2017). Comparative Study of Cybersecurity Capability Maturity Models. In Mas, A., Mesquida, A., O'Connor, R.V., Rout, T., Dorling, A. (eds.) SPICE 2017. CCIS, vol. 770 (pp. 100-113)

(16) Salah, D., Paige, R., & Cairns, P. (2014). An Evaluation Template for Expert Review of Maturity Models. In Product-Focused Software Process Improvement (pp. 318-321).

(17) Saleh, M.F. (2011). Information Security Models. International Journal of Computer Science and Security, 5(3), 316-337.

(18) Spruit, M. (2017). Volwassenheid Informatiebeveiliging; 3-Pijlermodel. RAAK-project Veilig Water.

(19) Thomson, K., & Von Solms, R. (2006). Towards an Information Security Competence Maturity Model. Computer Fraud & Security, (May), 11-15.

(20) US Department Homeland Security. (2014). Oil and Natural Gas Subsector Cyber Security Capability Maturity Model (ONG-C2M2) Version 1.1.