Samen aanjagen van vernieuwing

SURFaudit benchmark 2019 – rapport

Bart Bosma, SURF
surfaudit@surfnet.nl

Samenvatting

Tweejaarlijkse benchmark

Iedere twee jaar organiseert SURF de SURFaudit-benchmark, waarbij participerende instellingen een self-assessment uitvoeren tegen het Normenkader Informatiebeveiliging Hoger Onderwijs (normenkader IBHO). SURFaudit verzamelt en analyseert de resultaten, uitgedrukt in volwassenheidsniveaus (score 1 t/m 5) om een beeld te krijgen van de mate van compliance met het normenkader IBHO voor de hele sector onderwijs en onderzoek. Hiermee geeft de sector onderwijs en onderzoek invulling aan zelfregulering op dit gebied. Om tot de resultaten te komen hebben we dit jaar een nieuw toetsingskader gebruikt, dat op basis van het *NBA Volwassenheidsmodel Informatiebeveiliging v2.0*[1] is samengesteld.

Aanbevolen volwassenheidsniveaus

De Stuurgroep Informatiebeveiliging en Privacy Hoger Onderwijs heeft de huidige versie van het normenkader IBHO, inclusief de aanbevolen volwassenheidsniveaus van de maatregelen, op 30 maart 2015 besproken en goedgekeurd. De maturity werkgroep van SCIPR (voorheen SURFibo), bestaande uit security officers en auditors van verschillende instellingen, heeft de geïdentificeerde risico's afgewogen om de aanbevolen volwassenheidsniveaus te bepalen voor de maatregelen in het normenkader. Voor de meeste maatregelen heeft de werkgroep als volwassenheidsniveau 3 als aanbevolen niveau vastgesteld, sommige zijn op 4 gezet en enkele op 2, waarmee het gemiddelde van het hele toetsingskader rond volwassenheidsniveau 3 uitkomt.

Aanmeldingen en ontvangen resultaten

In 2019 waren instellingen vanaf 1 juni tot 1 december 2019 in de gelegenheid hun self-assessment uit te voeren en de resultaten in te voeren in de nieuwe benchmarktool[2].

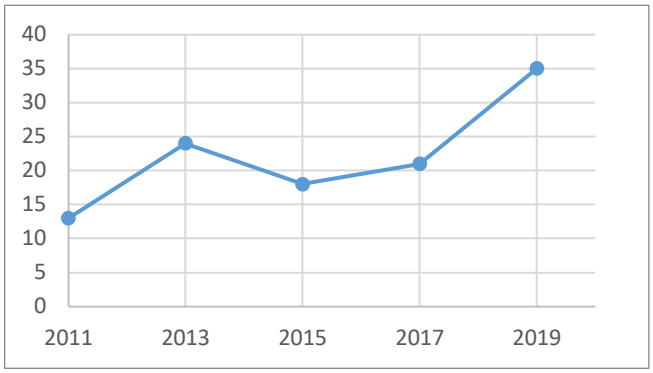
Sector	*Aangemeld*		*Resultaat ontvangen*	
	aantal	percentage van totaal	aantal	percentage van aanmeldingen
Universiteiten	12	87%	9	75%
Hogescholen	26	70%	24	92%
Overige	4	33%	2	50%
Totaal:	**42**	**67%**	**35**	**83%**

Tabel 1: Aanmeldingen en ontvangen resultaten per sector.

Van de totale doelgroep heeft bijna 67% zich inschreven voor de benchmark 2019, een stijging van ruim 15% ten opzichte van 2017[3]. Kijken we uitsluitend naar wo en hbo, dan is de stijging zo'n 10%.

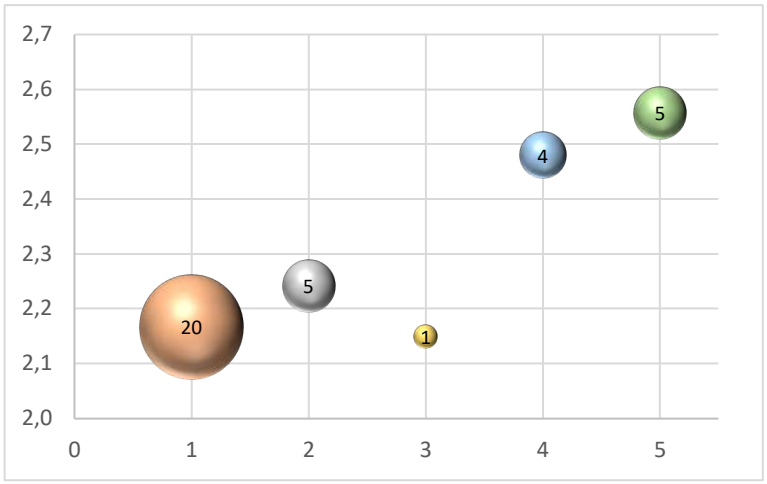
Terwijl tot 2019 de deelname rond de 19 instellingen schommelde, is in 2019 de deelname toegenomen tot 35 (zie Figuur 1), vooral door de inzet van de CSC's[4] in het hbo. Hieruit blijkt dat de "comply or explain" benadering, zoals die al enkele jaren in het mbo wordt gehanteerd, die de CSC's in het hbo voorstaan, ook bij hoger onderwijsinstellingen effect sorteert.

[1] https://www.nba.nl/intern-en-overheidsaccountants/volwassenheidsmodel-informatiebeveiliging/.
[2] Sinds 2017 beschikt SURFaudit over een benchmarktool op basis van de Smile Privacy Suite om alle benchmarkresultaten te verzamelen en te analyseren.
[3] Zorginstellingen zijn niet meegerekend in het totaal.
[4] Coördinerende SURF Contactpersoon – stroomlijnt en coördineert de communicatie tussen een instelling en SURF. De CSC wordt aangesteld door het bestuur van de instelling en is het aanspreekpunt voor SURF bij een aangesloten instelling.



Figuur 1: Trend deelname benchmarks 2011 – 2019 (aantal instellingen per benchmark jaar)

Vaker meedoen is ook zinvol, want er blijkt (in ieder geval statistisch) een positief effect te zijn op de resultaten (zie Figuur 2). Het gemiddelde van instellingen die voor het eerst meedoen is aanmerkelijk lager dan het gemiddelde van de instellingen die vanaf 2011 hebben meegedaan.



Figuur 2: Gemiddeld volwassenheidsniveau (schaal 1 – 5) gerelateerd aan aantal deelnames sinds 2011[5]

Resultaten en aanbevelingen

Het gemiddelde volwassenheidsniveau van de SURFaudit benchmark 2019 is lager uitgevallen dan die van de benchmark 2017:

Benchmark	2017	2019	Verschil 2017 - 2019
Cluster 1	2,4	2,2	-0,2
Cluster 2	2,2	2,3	0,1
Cluster 3	2,5	2,5	0,0
Cluster 4	2,6	2,4	-0,2
Cluster 5	2,5	2,2	-0,3
Cluster 6	2,0	1,9	-0,1
Gemiddelde	**2,4**	**2,3**	-0,1

Tabel 2: Gemiddeld volwassenheidsniveau 2017 en 2019

Dit is ten dele te verklaren door het gebruik van een nieuw toetsingskader dat meer nadruk legt op risicomanagement dan het vorige toetsingskader. De instellingen die eerder hebben meegedaan aan de SURFaudit benchmark scoren

[5] Gemiddeld volwassenheidsniveau op een schaal van 1 – 5. Het gemiddelde bij drie deelnames is een anomalie, omdat slechts één instelling in deze categorie valt. De grootte van iedere bol is representatief voor het aantal instellingen in die categorie.

overigens gemiddeld genomen bijna hetzelfde als in 2017. De instellingen die voor het eerst hebben meegedaan scoren significant lager. Waar dit aan ligt vereist nader onderzoek, maar een verklaring kan zijn dat ze minder ervaring hebben met het bepalen van volwassenheidsniveaus en de self-assessment conservatief hebben ingevuld. Verder zitten in deze groep een groot aantal kleine instellingen die minder mensen en middelen beschikbaar hebben voor informatiebeveiliging.

De resultaten van de SURFaudit benchmark 2019 laten zien dat de sector onderwijs en onderzoek nog het nodige kan verbeteren op het gebied van informatiebeveiliging. Vooral voor wat betreft het monitoren van het netwerk en van systemen, en het verzamelen en analyseren van log data (cluster 6). Deze categorieën scoren structureel laag in de benchmarks vanaf 2011. Het nieuwe toetsingskader benadrukt risicomanagement meer dan het oude, maar ook daar valt winst te behalen, zodat maatregelen goed afgestemd worden op het risicoprofiel van de instelling.

De trend op lange termijn laat wel zien dat instellingen die al vaker hebben meegedaan met de benchmark consequent voortgang boeken met hun weerbaarheid.

Inhoudsopgave

1 Inleiding

Dit rapport bevat de resultaten van de SURFaudit benchmark 2019. Voor de benchmark hebben 42 instellingen zich ingeschreven, waarvan er 35 de benchmark hebben uitgevoerd. Voor deze benchmark hebben we een nieuw toetsingskader gebruikt, waardoor de resultaten niet volledig vergelijkbaar zijn met de resultaten van de benchmark in 2017.

In dit hoofdstuk lees je algemene informatie over SURFaudit en de benchmark 2019. In hoofdstuk 2 gaan we in op de resultaten van de benchmark en in hoofdstuk 3 bespreken we de bevindingen, risico's en aanbevelingen. In hoofdstuk 4 sluiten we het rapport af met een bespiegeling op de resultaten.

1.1 SURFaudit

Het doel van SURFaudit is om de bij SURF aangesloten instellingen te helpen hun informatiebeveiliging onder controle brengen en te houden, door de procesmanagementcyclus te ondersteunen. SURFaudit voorziet in middelen om een instelling in staat te stellen de volwassenheid van hun informatiebeveiliging te meten. Tegelijkertijd helpt SURFaudit in kaart te brengen hoe de hele sector ervoor staat. Daarnaast vermindert SURFaudit de noodzaak voor andere (vergelijkbare) audits op het gebied van informatiebeveiliging en privacy. SURFaudit maakt gebruik van het normenkader informatiebeveiliging Hoger Onderwijs 2015 (IBHO). Dit is samengesteld door een expertgroep van aangesloten instellingen, onder meer op basis van de internationale standaard ISO/IEC 27002:2013.

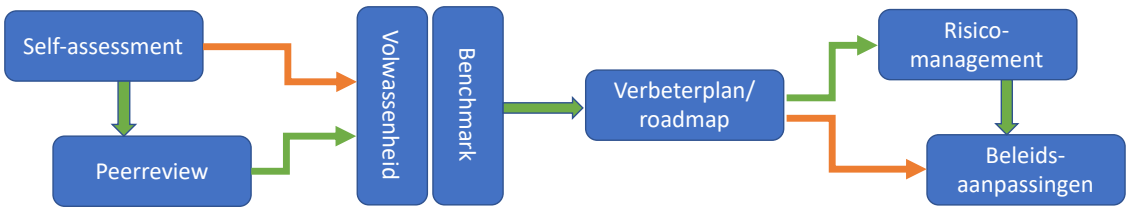
Self-assessment en peerreview

De eenvoudigste manier om een SURFaudit te doen is het uitvoeren van een self-assessment. Hiervoor is het toetsingskader informatiebeveiliging Hoger Onderwijs (toetsingskader IBHO) beschikbaar, waarin voor iedere maatregel staat beschreven welke bewijsvoering verwacht wordt per volwassenheidsniveau.

Voor de benchmark voeren deelnemende instellingen zo'n self-assessment uit. De resultaten verwerken we in een rapport waarin wordt aangegeven hoe de sector onderwijs en onderzoek ervoor staat. En we focussen op statements uit het toetsingskader die over de hele linie laag scoren (zie voor de scoringsmethodiek Figuur 7 en Tabel 4 op pagina 10). Hierbij merken we op dat de manier waarop het self-assessment wordt uitgevoerd door de verschillende instellingen niet per se hetzelfde is. De ene instelling kan vooral processen en systemen bij de centrale IT beoordelen, terwijl een andere instelling ook processen en systemen bij alle faculteiten beoordeelt. De kwaliteit van het assessment is verder afhankelijk van degene die hem invult, in hoeverre die anderen betrekt bij de beoordeling en de kwaliteit van de documentatie die als bewijsvoering wordt opgevoerd.

Om het resultaat van een assessment onafhankelijk te laten beoordelen kan een peerreview worden aangevraagd. Peerreviews worden uitgevoerd door speciaal getrainde collega's van bij SURF aangesloten onderwijsinstellingen.

Self-assessments kunnen op ieder gewenst moment worden uitgevoerd, de peerreviews worden ingepland en gecoördineerd door de Coördinerende Commissie Peer Review (CCPR) die is samengesteld uit leden van SCIPR[6].



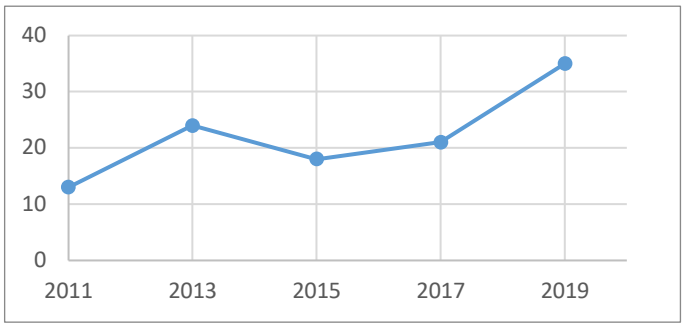
Figuur 3: Van self-assessment tot beleidsaanpassing (groen is de voorkeursroute)

Na afloop van een assessment, die al dan niet gevalideerd is in een peerreview, kan de instelling een verbeterplan opstellen om beheersmaatregelen met een laag volwassenheidsniveau te verbeteren en eventuele aanpassingen na een risicobeoordeling in het beleid op te nemen (zie *Figuur 3*).

[6] SCIPR: SURF Community voor Informatiebeveiliging en Privacy, de opvolger van SURFibo.

1.2 Benchmark 2019

De benchmark 2019 liep van 1 mei tot 1 december 2019. Het doel was een deelname van 50 instellingen (80% van de doelgroep), waarvan 40 onderwijsinstellingen. Hoewel de deelname beduidend hoger was dan in 2017, vooral omdat veel meer hbo-instellingen hebben meegedaan (zie Figuur 4), is het doel niet gehaald. Het aantal inschrijvingen was 42 en uiteindelijk hebben 35 instellingen de self-assessment ingevuld en hun resultaten ingeleverd.

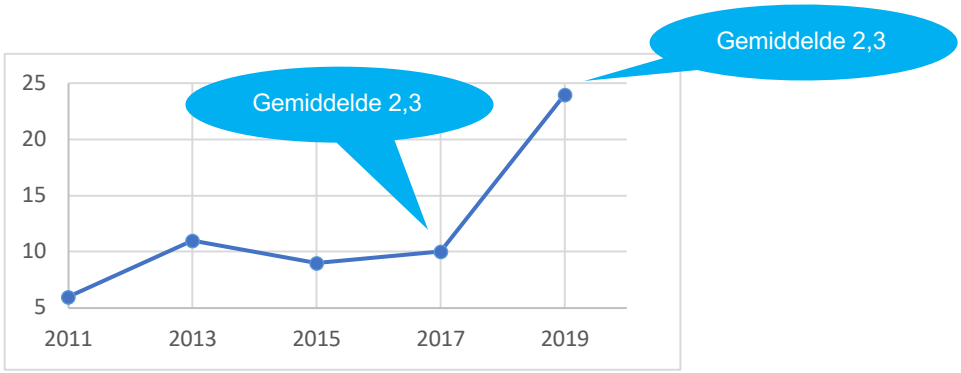


Figuur 4: Trend deelname benchmarks 2011 – 2019 (aantal instellingen per benchmark jaar)

Geschiedenis van de benchmark

In 2008 was het niveau van informatiebeveiliging bij een aantal instellingen in het hoger onderwijs al eens gemeten. In 2009 en 2010 zijn nog verschillende metingen uitgevoerd en is voor het eerst een referentiekader gebruikt om aan te geven waar een instelling zou moeten staan. Op bestuurlijk niveau is in 2010 besloten om de daaropvolgende 4 jaar op een procesmatige manier de volwassenheid van informatiebeveiliging binnen het hoger onderwijs te meten.

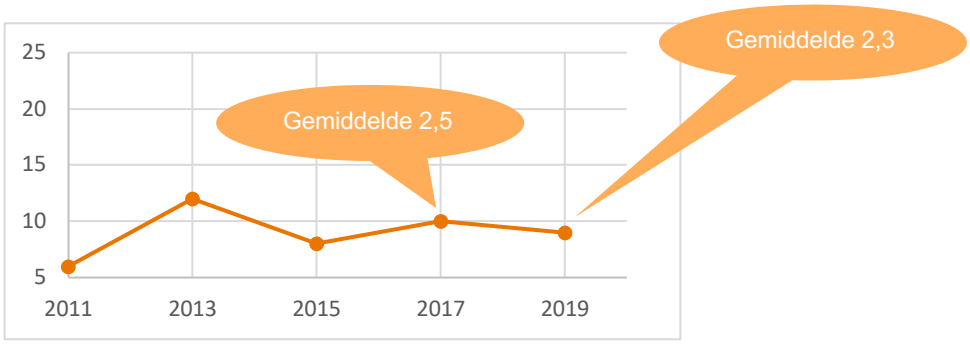
Eind 2011 heeft vervolgens de eerste ronde van de SURFaudit-benchmark plaatsgevonden. Aan deze auditronde hebben dertien instellingen deelgenomen. De tweede benchmark was in 2013; daaraan hebben 25 instellingen deelgenomen: twaalf universiteiten, elf hogescholen, een onderzoeksinstelling en een overige ho-instelling. Aan de benchmark 2015 hebben 18 instellingen deelgenomen: acht universiteiten, negen hogescholen en een onderzoeksinstelling, in 2017 hebben tien universiteiten, tien hogescholen en een onderzoeksinstelling meegedaan. De deelname per sector tot en met 2019 vind je hieronder in Figuur 5 en Figuur 6.



Figuur 5: Deelname hogescholen sinds 2011 en gemiddeld volwassenheidsniveau 2017 - 2019

Het aantal deelnemende hbo-instellingen is meer dan verdubbeld sinds 2017. Daarbij is vermeldenswaard dat een groot aantal relatief kleine hbo-instellingen[7] heeft meegedaan.

[7] Instellingen aangesloten bij Radiant Lerarenopleidingen (https://www.radiantlerarenopleidingen.nl)



Figuur 6: Deelname universiteiten sinds 2011 en gemiddeld volwassenheidsniveau 2017 - 2019

Het aantal universiteiten dat heeft meegedaan is iets teruggelopen in vergelijking met 2017.

De SURFaudit benchmark wordt sinds 2011 eens in de twee jaar uitgevoerd. Instellingen kunnen de resultaten van de SURFaudit-benchmark gebruiken voor:

- het aanjagen van interne verbeteringen;
- het vaststellen van de weerbaarheid ten aanzien van cybersecuritydreigingen;
- het verantwoorden van ingevoerde maatregelen en processen;
- het signaleren van sterke en zwakke punten in de sector onderwijs en onderzoek.

Normenkader Informatiebeveiliging Hoger Onderwijs 2015

Voor de benchmark 2019 is net als voorheen gebruik gemaakt van het Normenkader Informatiebeveiliging Hoger Onderwijs 2015 (IBHO). Dit is een gezamenlijk normenkader dat door zowel interne als externe stakeholders gedragen wordt en dat zelfregulering promoot in plaats van aanscherping van opgelegde eisen en extern toezicht. Het normenkader is een levend document dat periodiek wordt bijgewerkt aan de hand van het Cyberdreigingsbeeld – onderwijs en onderzoek, nieuwe versies van de ISO/IEC 27002 standaard en andere toepasselijke standaarden, nieuwe wet- en regelgeving en de laatste inzichten op het gebied van informatiebeveiliging en privacybescherming.

Voor de 2015-versie van het normenkader heeft de SCIPR maturity werkgroep de bestaande beheersmaatregelen geëvalueerd aan de hand van de ISO/IEC 27002:2013 standaard (de voorgaande versie van het normenkader was nog gebaseerd op ISO/IEC 27002 versie uit 2007). Er zijn enkele beheersmaatregelen toegevoegd, de clusterindeling is beter gebalanceerd, het toetsingskader is uitgebreid en voor iedere maatregel is het aanbevolen volwassenheidsniveau vastgesteld ("de baseline"). De clusterindeling zoals die al bestond in 2013 is, met de genoemde optimalisaties, gehandhaafd in 2015, zodat de vergelijking tussen de benchmarks valide blijft.

Clusters in Normenkader Informatiebeveiliging Hoger Onderwijs 2015

In het Normenkader Informatiebeveiliging Hoger Onderwijs worden de volgende zes clusters onderscheiden, gerelateerd aan de ISO 27002 standaard (zie Tabel 3).

		Clusters normenkader IBHO 2015						
		1	2	3	4	5	6	
Hoofdstukken ISO-27002	**ISO-27002**	**Beleid en Organisatie**	**Personeel, Studenten en gasten**	**Ruimten en Apparatuur**	**Continuïteit**	**Vertrouwelijkheid en Integriteit**	**Controle en Logging**	**Niet gebruikt**
5. Informatiebeveiligingsbeleid	**2**	2						
6. Organiseren van informatiebeveiliging	**7**	4		0				3
7. Veilig personeel	**6**		3					3
8. Beheer van bedrijfsmiddelen	**10**	2		1				7
9. Toegangsbeveiliging	**14**		1			9	1	3
10. Cryptografie	**2**	1				1		
11. Fysieke beveiliging en beveiliging van de omgeving	**15**	1	1	12				1
12. Beveiliging van de bedrijfsvoering	**14**			1	7	1	2	3
13. Communicatiebeveiliging	**7**	2	1			4		
14. Acquisitie, ontwikkeling en onderhoud van informatiesystemen	**13**	1			1	1	3	7
15. Leveranciersrelaties	**5**	2			1		1	1
16. Beheer van informatiebeveiligingsincidenten	**7**	2	1		2		1	1
17. Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	**4**				2			2
18. Naleving	**8**	2					2	4
Totaal aantal maatregelen, inclusief gesplitste maatregelen	**85**	**21**	**7**	**15**	**15**	**17**	**10**	

Tabel 3: Clusters in het normenkader IBHO

Toetsingskader 2019

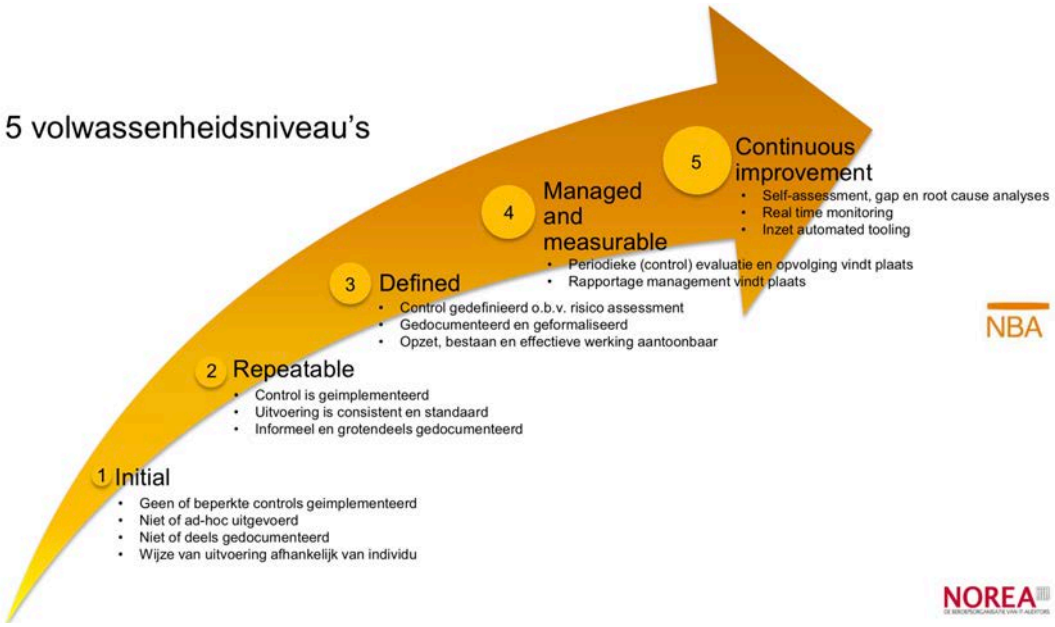
Voor de SURFaudit benchmark 2019 is een nieuw toetsingskader ontwikkeld dat beter aansluit bij de praktijk van informatiebeveiliging.

De Koninklijke Nederlandse Beroepsorganisatie van Accountants (NBA) heeft medio 2016 een volwassenheidsmodel gepubliceerd dat tot doel heeft "de interne auditafdelingen alsmede de directies van organisaties een leidraad en handvaten te geven waarmee zij doelgericht en op pragmatische wijze hun organisaties kunnen ondersteunen bij het meten, bepalen en verbeteren van het volwassenheidsniveau van informatiebeveiliging." Begin 2019 is hiervan een update gepubliceerd in samenwerking met NOREA die is gebruikt bij het samenstellen van het nieuwe toetsingskader[8].

Het model gaat uit van de risico's die relevant zijn voor de organisatie en geeft de maatregelen om die risico's te mitigeren per volwassenheidsniveau. Vervolgens worden de maatregelen gerelateerd aan verschillende normenkaders, waaronder de ISO/IEC 27002:2013 standaard, die uiteindelijk de basis vormt voor het Normenkader IBHO 2015.

[8] https://www.nba.nl/intern-en-overheidsaccountants/volwassenheidsmodel-informatiebeveiliging/?utm_medium=email&utm_campaign=NBA+Nieuws+8+februari&utm_source=Nieuwsbrief

In het model worden vijf volwassenheidsniveaus gebruikt (zie Figuur 7).



Figuur 7: Volwassenheidsniveaus uit het NBA Volwassenheidsmodel Informatiebeveiliging

Wij hebben de volwassenheidsniveaus als volgt vertaald voor gebruik in de SURFaudit benchmark:

Niveau	Omschrijving	Toelichting
1	Maatregelen zijn ad hoc	Beheersmaatregelen zijn niet of slechts gedeeltelijk vastgesteld en/of worden op een inconsistente manier uitgevoerd en zijn sterk afhankelijk van individuen.
2	Maatregelen bestaan en worden op consistente wijze uitgevoerd	Beheersmaatregelen bestaan en worden op een gestructureerde en consistente, maar informele manier uitgevoerd.
3	Maatregelen zijn gedocumenteerd en de uitvoering is aantoonbaar	Beheersmaatregelen zijn gedocumenteerd en worden op een gestructureerde en formele manier uitgevoerd. Uitvoering van de maatregelen is aantoonbaar, getest en effectief.
4	Er is een verbetercyclus aanwezig en gedocumenteerd	De effectiviteit van beheersmaatregelen wordt periodiek beoordeeld en indien nodig verbeterd. Deze beoordeling is
5	Er is een bedrijfsbrede aanpak van risico's	Een bedrijfsbreed risico- en beheersprogramma voorziet in continue en effectieve beheersing en aanpak van risico's.

Tabel 4: Volwassenheidsniveaus voor het toetsingskader informatiebeveiliging HO

Voor de meeste beheersmaatregelen geldt als aanbeveling volwassenheidsniveau 3, voor een aantal is dat niveau 4 en enkele kunnen op niveau 2 worden ingericht. Volwassenheidsniveau 4 betekent dat de betreffende maatregel regelmatig wordt geëvalueerd en bijgesteld, ofwel dat de Plan-Do-Check-Act cyclus is geïmplementeerd. Bijvoorbeeld, het hebben van een adequaat en goedgekeurd beveiligingsbeleid betekent dat het volwassenheidsniveau 3 is, met jaarlijkse evaluatie en bijstelling wordt dat niveau 4.

- De baseline is in 2015 door de stuurgroep IBP (nu commissie IB) gesteld op ca. 3 gemiddeld (in het oude toetsingskader 2,93 gemiddeld, in het nieuwe gemiddeld 3,06 – door herschikking van enkele statements waardoor afronding naar boven heeft plaatsgevonden). We noemen dit de *baseline*, het aanbevolen niveau.
- Een laag volwassenheidsniveau betekent niet per definitie een slechte score; voor de meeste statements in het normenkader is de baseline 3, voor sommige 2, voor enkele 4. Dit is bepaald op basis van een risico-afweging voor de sector.
- Op basis van een eigen risicoafweging en gebruikmakend van het *Cyberdreigingsbeeld – sector onderwijs en onderzoek* bepaalt iedere instelling zelf wat haar streefniveau is.

2 Resultaten

In dit hoofdstuk beschrijven we de uitkomsten van de benchmark voor alle deelnemers, kijken we naar de trend sinds 2011 en maken we een vergelijking met de resultaten uit 2017.

Voor de benchmark 2019 zijn we overgestapt op een nieuw toetsingskader dat is gebaseerd op het *NBA Volwassenheidsmodel Informatiebeveiliging*. In het SURFaudit toetsingskader zijn statements uit het NBA-model gegroepeerd in dezelfde clusters als in het Normenkader IBHO 2015. Een SCIPR-werkgroep waarin van Rob van Nie (VU), en later Brian Ridenberg en Anita Polderdijk-Rijntjes (beiden Hogeschool Windesheim) het voortouw hebben genomen, heeft de indeling vastgesteld. In vergelijking met het vorige toetsingskader zijn de aantallen statements per cluster iets verschillend en is het totaal aantal statements teruggebracht tot 62:

#	Cluster	Aantal statements in vorig toetsingskader	Aantal statements in huidig toetsingskader
1	Beleid en organisatie	21	12
2	Personeel, gasten, studenten	7	5
3	Ruimtes en apparatuur	15	4
4	Continuïteit	15	23
5	Toegangsbeveiliging en integriteit	17	12
6	Controle en logging	10	6
	Totaal	**85**	**62**

Tabel 5: Clusterindeling toetsingskader 2017 en 2019

De clusters van het huidige, aangepaste toetsingskader blijven op grote lijnen vergelijkbaar met die van het oude toetsingskader, maar zijn er wel accentverschillen die de score beïnvloeden. In het hele toetsingskader is meer aandacht voor risicomanagement wat in het vorige toetsingskader ontbrak.

2.1 Overzicht van de resultaten

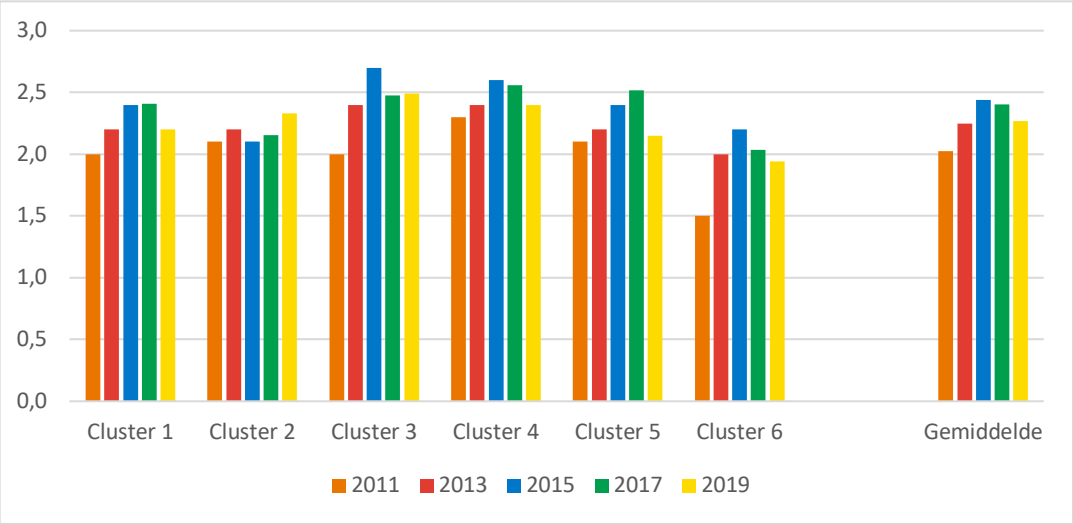
In Tabel 6 staan de scores van de benchmarks die tot nog toe gehouden zijn. In vergelijking met de SURFaudit-benchmark uit 2017 zijn de scores voor de meeste clusters gedaald, alleen cluster 2 is iets hoger uitgekomen en cluster 3 is nagenoeg hetzelfde gebleven.

Benchmark	2011	2013	2015	2017	2019*	verschil 2017 - 2019
Cluster 1	2,0	2,2	2,4	2,4	2,2	-0,2
Cluster 2	2,1	2,2	2,1	2,2	2,3	0,1
Cluster 3	2,0	2,4	2,7	2,5	2,5	0,0
Cluster 4	2,3	2,4	2,6	2,6	2,4	-0,2
Cluster 5	2,1	2,2	2,4	2,5	2,2	-0,3
Cluster 6	1,5	2,0	2,2	2,0	1,9	-0,1
Gemiddelde	**2,0**	**2,2**	**2,4**	**2,4**	**2,3**	**-0,1**

Tabel 6: High-level resultaten en trend (gemiddelde per cluster) *** Nieuw toetsingskader**

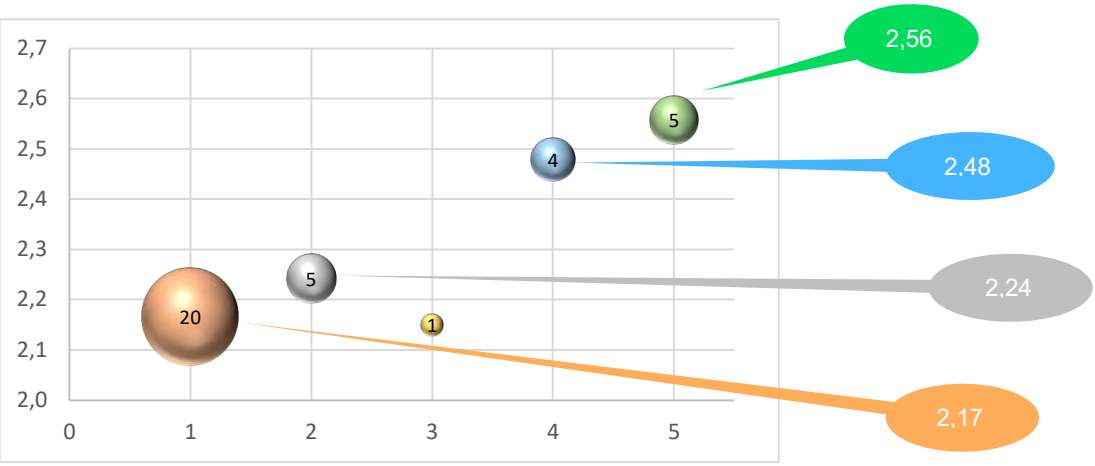
De rood gemarkeerde volwassenheidsniveaus zijn de gemiddelden die lager zijn uitgevallen dan in de voorgaande benchmarkronde, de groen gemarkeerde volwassenheidsniveaus zijn hoger dan in de voorgaande benchmarkronde.

Terwijl de benchmark in 2013 voor ieder cluster een verbetering liet zien ten opzichte van de vorige benchmark (2011) en de benchmark in 2015 in zijn totaliteit vooruitgang liet zien ten opzichte van de voorgaande benchmark (2013), stagneert die ontwikkeling vanaf de benchmark in 2017 (zie Tabel 6 en Figuur 8) .



Figuur 8: Ontwikkeling volwassenheidsniveaus per cluster

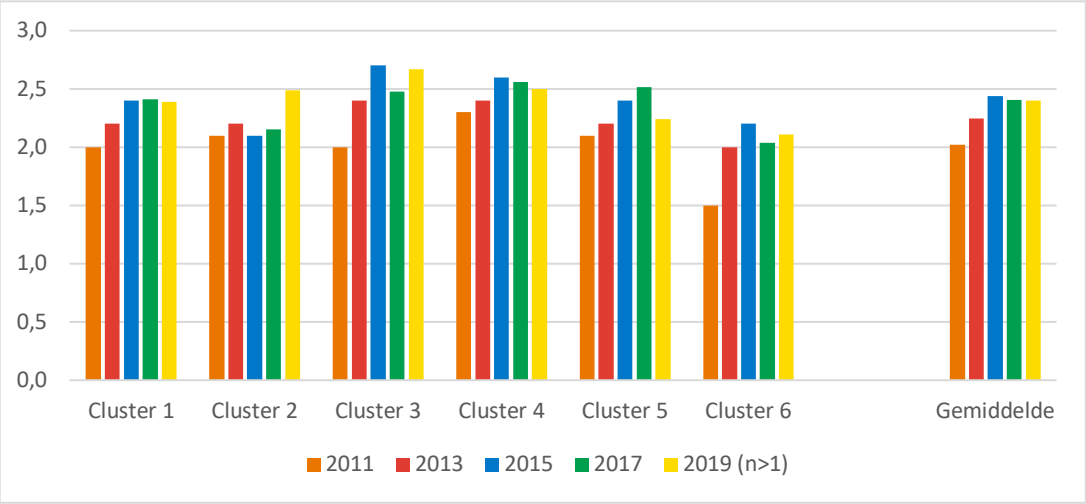
Het is echter wel zo dat instellingen die vaker meedoen, gemiddeld ook een hoger volwassenheidsniveau hebben (zie Figuur 9):



Figuur 9: Gemiddeld volwassenheidsniveau gerelateerd aan aantal deelnames sinds 2011[9]

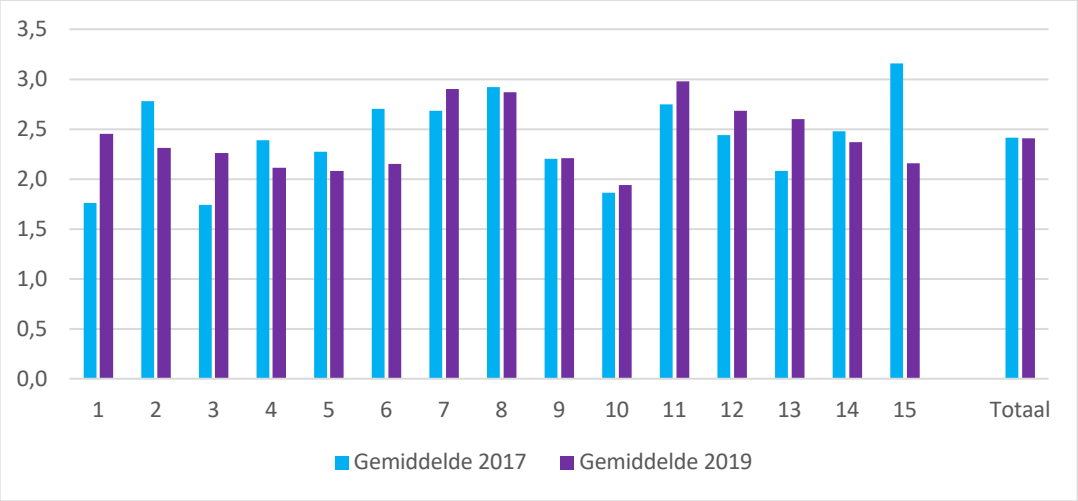
In de grafiek hieronder (Figuur 10) zie je de ontwikkeling van het gemiddelde volwassenheidsniveau per cluster voor alle instellingen die **twee of meer** keer hebben meegedaan. Voor die instellingen geldt dat de uitkomst gemiddeld vrijwel gelijk is aan die in 2017, waarbij cluster 2 en cluster 3 iets beter en de overige clusters een iets lager volwassenheidsniveau hebben dan in 2017.

[9] De grootte van iedere bol is representatief voor het aantal instellingen in die categorie. Het gemiddelde bij drie deelnames is een anomalie, omdat slechts één instelling in deze categorie valt.



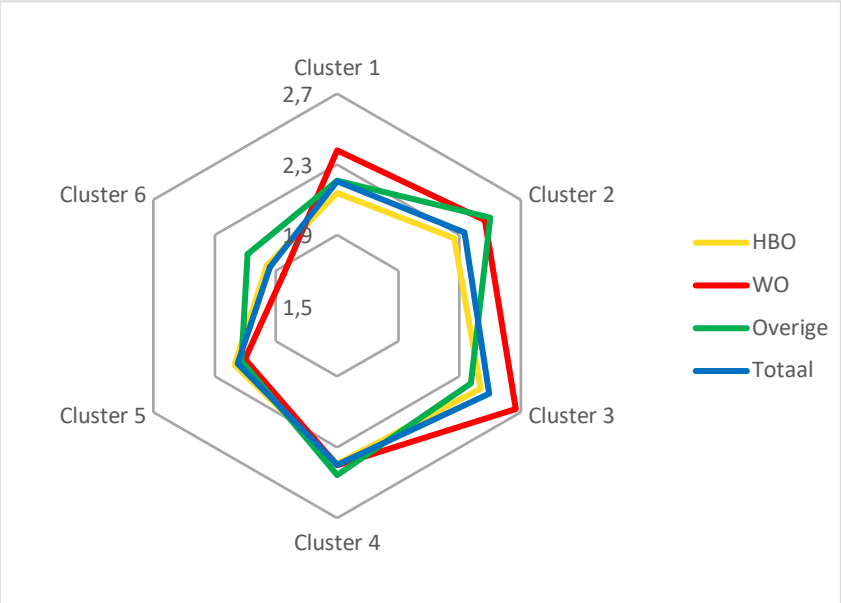
Figuur 10: Ontwikkeling volwassenheidsniveaus per cluster (meer dan een deelname in 2019)

Vergelijken we de vijftien instellingen die zowel in 2017 als in 2019 hebben meegedaan, dan zien we gemiddeld genomen weinig verandering. Zes van de 15 instellingen scoren beter dan in 2017, en zes scoren lager dan in 2017. Een scoort vrijwel hetzelfde als in 2017.



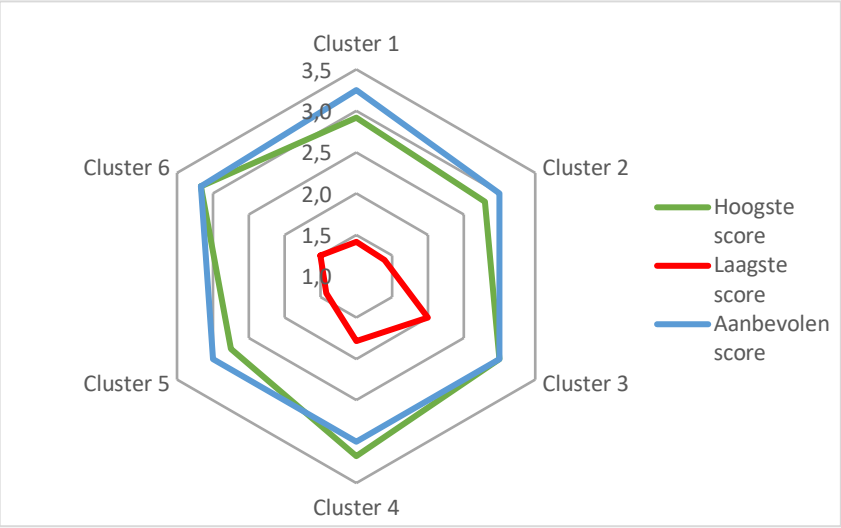
Figuur 11: Ontwikkeling volwassenheidsniveaus (deelname in 2107 en 2019)

Voor de gemiddelden van de clusters per sector valt op dat de *wo-instellingen* voor de clusters 1, 2 en 3 hoger scoren dan de andere instellingen. En dat de *overige instellingen* hoger scoren voor de clusters 2 en 6. De *hbo-instellingen* scoren voor de clusters 1, 2 en 3 iets onder het gemiddelde en voor de andere clusters ongeveer op het gemiddelde (zie Figuur 12).



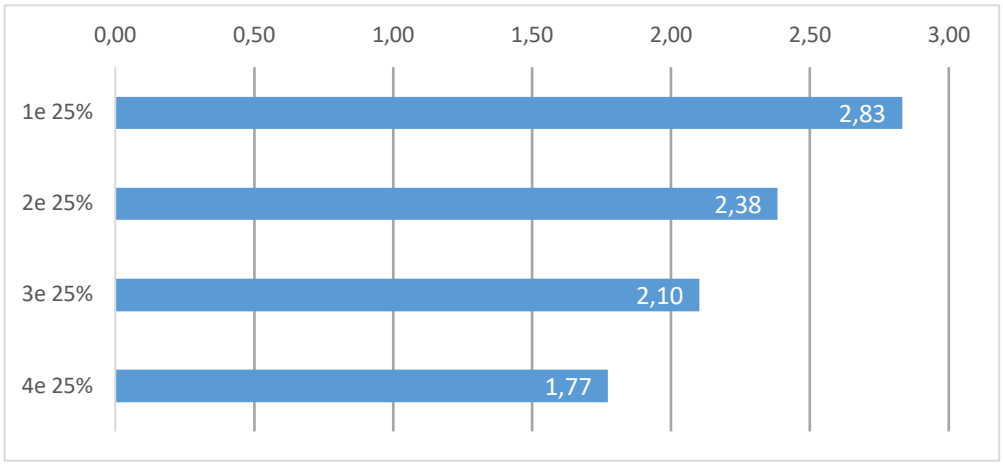
Figuur 12: Cluster-gemiddelden (schaal 1 – 5) per sector

De hoogst scorende instelling is de enige instelling die de baseline haalt (op cluster 5 na). De laagst scorende instelling heeft als hoogste gemiddelde volwassenheidsniveau 2 (cluster 3) en scoort verder minder dan 2 (zie Figuur 13).



Figuur 13: Hoogst en laagst scorende instelling vs. aanbevolen volwassenheidsniveau per cluster (schaal 1 – 5).

De top 25% van de deelnemers scoort gemiddeld bijna op het aanbevolen volwassenheidsniveau (zie Figuur 14).

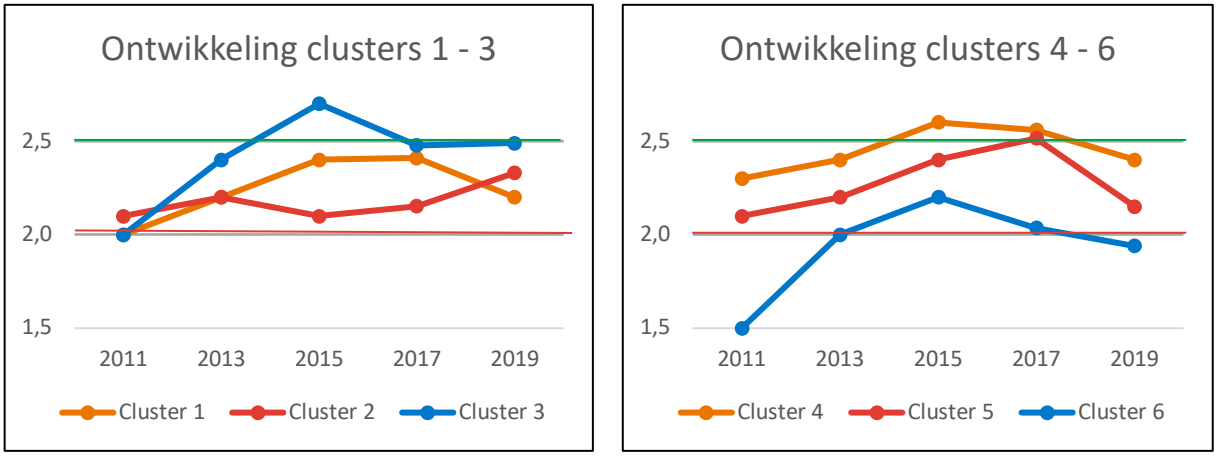


Figuur 14: Gemiddelde volwassenheidsniveau (schaal 1 – 5) van de deelnemers naar score ingedeeld in 4 groepen.

2.2 Detail-resultaten

In het vorige hoofdstuk hebben we de resultaten op hoofdlijnen weergegeven. In dit hoofdstuk gaan we dieper in op de resultaten per cluster en zullen we inzoomen op een aantal beter en minder scorende beheersmaatregelen.

In Figuur 15 is duidelijk te zien dat vanaf 2015 cluster 3, 4 en 6 een dalende lijn vertonen. Hetzelfde geldt voor cluster 1, 4, 5 en 6 vanaf 2017. In het verleden was vooral cluster 2 relatief zwak en daar is sinds 2015 veel meer aandacht voor gekomen, onder andere met het ontwikkelen van de CSY-campagne[10] door SURF voor deelnemende instellingen. Dat heeft geleid tot een stijgende lijn in het volwassenheidsniveau voor dat cluster. De hoogst scorende clusters in 2019 zijn cluster 3 en cluster 4, de laagst scorende clusters zijn cluster 1 en cluster 6.

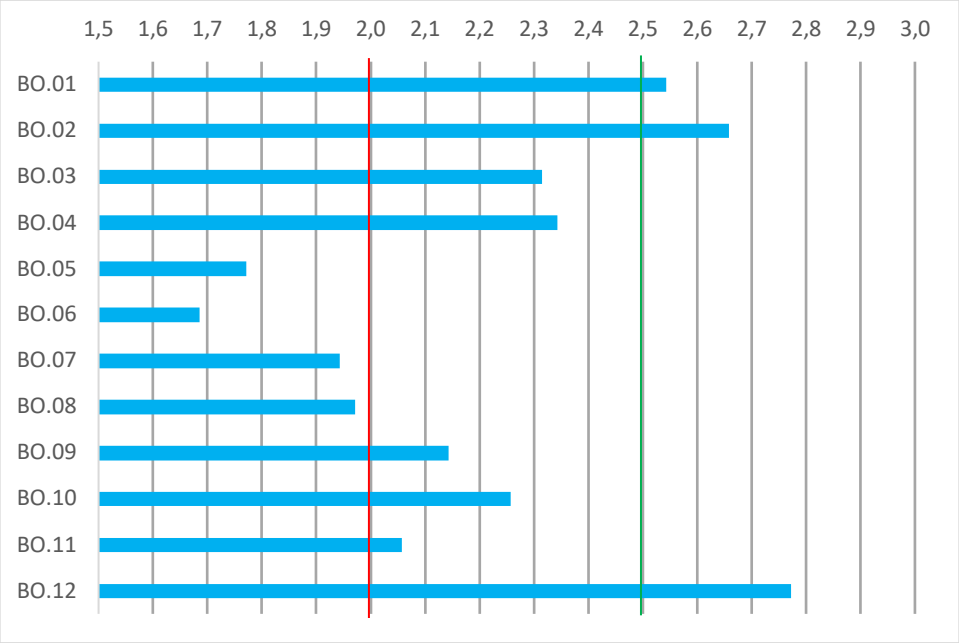


Figuur 15: Ontwikkeling individuele clusters 2011 – 2019 (schaal 1 – 5)

[10] Zie https://cybersaveyourself.nl/

2.2.1 Cluster 1 – Beleid en organisatie

Dit cluster bevat 12 statements. Het gemiddelde volwassenheidsniveau van dit cluster is 2,2.



Figuur 16: Gemiddeld volwassenheidsniveau (schaal 1 – 5) per maatregel in cluster 1

In dit cluster scoren 4 van de twaalf maatregelen lager dan volwassenheidsniveau 2,0:

ID	Categorie	Risicobeschrijving	Beheersdoelstelling
BO.05	Informatie risico-management framework	Het informatierisico- en beheersingskader is niet in lijn met het organisatiebrede model voor risicobeheer, resulterend in verkeerde interpretaties van risico's en/of het niet voldoen aan bedrijfs- en IT-doelstellingen.	Er is een raamwerk voor informatierisicobeheer opgesteld en afgestemd op de doelstellingen van de organisatie en het (bedrijfs) risicobeheerraamwerk.
BO.06	Risicobeoordeling	Inherente en restrisico's worden niet (tijdig) geïdentificeerd en beoordeeld. Kans en impact zijn niet vastgesteld, waardoor actieplannen, beperkende maatregelen of risico-initiatieven niet worden ingevoerd.	Risicobeoordelingen worden uitgevoerd om actuele risicoprofielen met betrekking tot bedrijfsdoelstellingen te bepalen. De waarschijnlijkheid en impact van alle geïdentificeerde risico's worden regelmatig beoordeeld, met behulp van kwalitatieve en kwantitatieve methoden. De waarschijnlijkheid en impact van inherente en rest-risico's worden bepaald per categorie, op portefeuillebasis.
BO.07	Plan voor behandeling en beperking van risico's (inclusief risicoacceptatie)	Risico beperkende maatregelen worden niet geïdentificeerd en geïmplementeerd. Vereiste acties worden niet gecommuniceerd en uitgevoerd, wat leidt tot mogelijke manifestatie van risico's. Hoge kosten/lage baten gerelateerd aan matige of lage risico's. Het niet prioriteren van risico's kan leiden tot hogere kosten, lagere uitkeringen of reputatieschade.	Beheersactiviteiten worden op alle niveaus geprioriteerd en gepland om de benodigde mitigerende maatregelen te implementeren, inclusief het bepalen van kosten en baten en de verantwoordelijkheid voor de uitvoering. Goedkeuring wordt verkregen voor aanbevolen acties en acceptatie van rest risico's en er wordt voor gezorgd dat uitgevoerde acties onder verantwoordelijkheid van betrokken proceseigenaar(s) vallen. De uitvoering van plannen wordt bewaakt en eventuele

ID	Categorie	Risicobeschrijving	Beheersdoelstelling
			afwijkingen worden gerapporteerd aan het senior management.
BO.08	Methodologie voor veilige softwareontwikkeling en -implementatie	Software- en/of systeemontwikkeling zijn niet ontworpen en geïmplementeerd volgens overeengekomen functionele, technische en beveiligingseisen, goedkeuringsnormen en de informatiearchitectuur, waardoor niet aan de business requirements wordt voldaan.	Er is een gestructureerde aanpak (levenscyclus voor veilige softwareontwikkeling) voor interne ontwikkeling en aanschaf van software geïmplementeerd, die ervoor zorgt dat potentiële risico's voor bedrijfsvoering adequaat worden beoordeeld en beperkt, en dat aspecten van vertrouwelijkheid, integriteit en beschikbaarheid worden meegenomen. Voor elke nieuwe ontwikkeling of acquisitie is goedkeuring vereist door het juiste niveau van bedrijfs- en IT-management.

Tabel 7: Laag scorende statements in cluster

Statements BO.05, BO.06 en BO.07 hebben betrekking op risicomanagement. Kennelijk ontbreekt beleid om risico's in kaart te brengen en mitigerende maatregelen op basis van de geïdentificeerde risico's in te voeren.

Bij statement BO.05 geldt dit voor 94% van de respondenten, bij BO.06 voor 89% en bij BO.07 voor 86% van de respondenten.

Statement BO.08 heeft betrekking op het (zelf) ontwikkelen van software maar ook op de aanschaf van software. Hiervoor is in veel gevallen (80% van de respondenten) nog geen gestructureerde aanpak ontwikkeld.

Drie van de twaalf statements scoren hoger dan volwassenheidsniveau 2,5:

ID	Categorie	Risicobeschrijving	Beheersdoelstelling
BO.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 informatie- en cyber security is leidend voor alle activiteiten en maatregelen met betrekking tot informatiebeveiliging.
BO.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 en 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.
BO.12	Service-level overeenkomst	Overeengekomen serviceniveaus voldoen niet aan bedrijfsdoelstellingen of wettelijke eisen.	IT-services die aan de organisatie worden geleverd, worden gedefinieerd in het contract en bijhorende SLA. Er zijn maatregelen genomen om ervoor te zorgen dat diensten voldoen aan de huidige en toekomstige behoeften van de organisatie.

Tabel 8: Hoger scorende statements in cluster 1

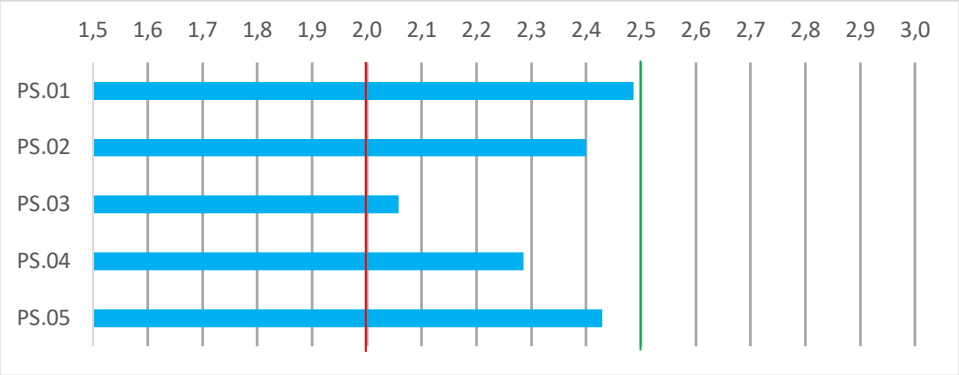
Voor deze statements geldt dat ruim de helft van de respondenten een volwassenheidsniveau hoger dan 2,5 heeft (respectievelijk 54%, 63% en 57%).

Conclusie

Doordat de statements die betrekking hebben op governance meer uitgaan van een risicobenadering dan in het vorige toetsingskader het geval was, valt de score ten opzichte van voorgaande jaren voor dit cluster lager uit. Desalniettemin valt op het vlak van risicomanagement en, in mindere mate, controle op service-levels, wel winst te behalen.

2.2.2 Cluster 2 – Personeel, studenten en gasten

Dit cluster bevat 5 statements. Het gemiddelde volwassenheidsniveau van dit cluster is 2,3.



Figuur 17: Gemiddeld volwassenheidsniveau per maatregel in cluster 2

In dit cluster scoort geen van de respondenten onder volwassenheidsniveau 2,0. De maatregel met het laagste volwassenheidsniveau in dit cluster is PS.03:

ID	Categorie	Risicobeschrijving	Beheersdoelstelling
PS.03	Verandering of beëindiging van functie	Gebruikerstoegang wordt niet tijdig uitgeschakeld nadat medewerkers het team hebben verlaten of om een andere reden geen toegang meer mogen hebben. Door gebrekkige kennisoverdracht wordt de continuïteit van de functie bedreigd.	Wanneer er functiewijzigingen plaatsvinden, met name beëindiging van het dienstverband, wordt direct effectief actie ondernomen. Kennisoverdracht wordt geregeld, verantwoordelijkheden worden opnieuw toegewezen en toegangsrechten worden verwijderd, zodat risico's worden geminimaliseerd en de continuïteit van de functie wordt gewaarborgd.

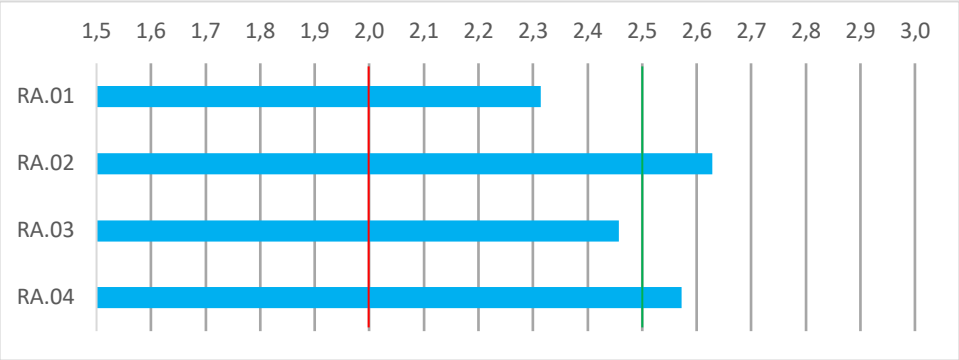
Tabel 9: Laagst scorende maatregel in cluster 2

Conclusie

Hoewel in het algemeen de maatregelen in dit cluster goed scoren, blijft de implementatie van de benodigde wijzigingen bij functieverandering achter. Hier is nog verbetering te behalen.

2.2.3 Cluster 3 – Ruimten en apparatuur

Dit cluster bevat 4 statements. Het gemiddelde volwassenheidsniveau van dit cluster is 2,5.



Figuur 18: Gemiddeld volwassenheidsniveau per maatregel in cluster 3

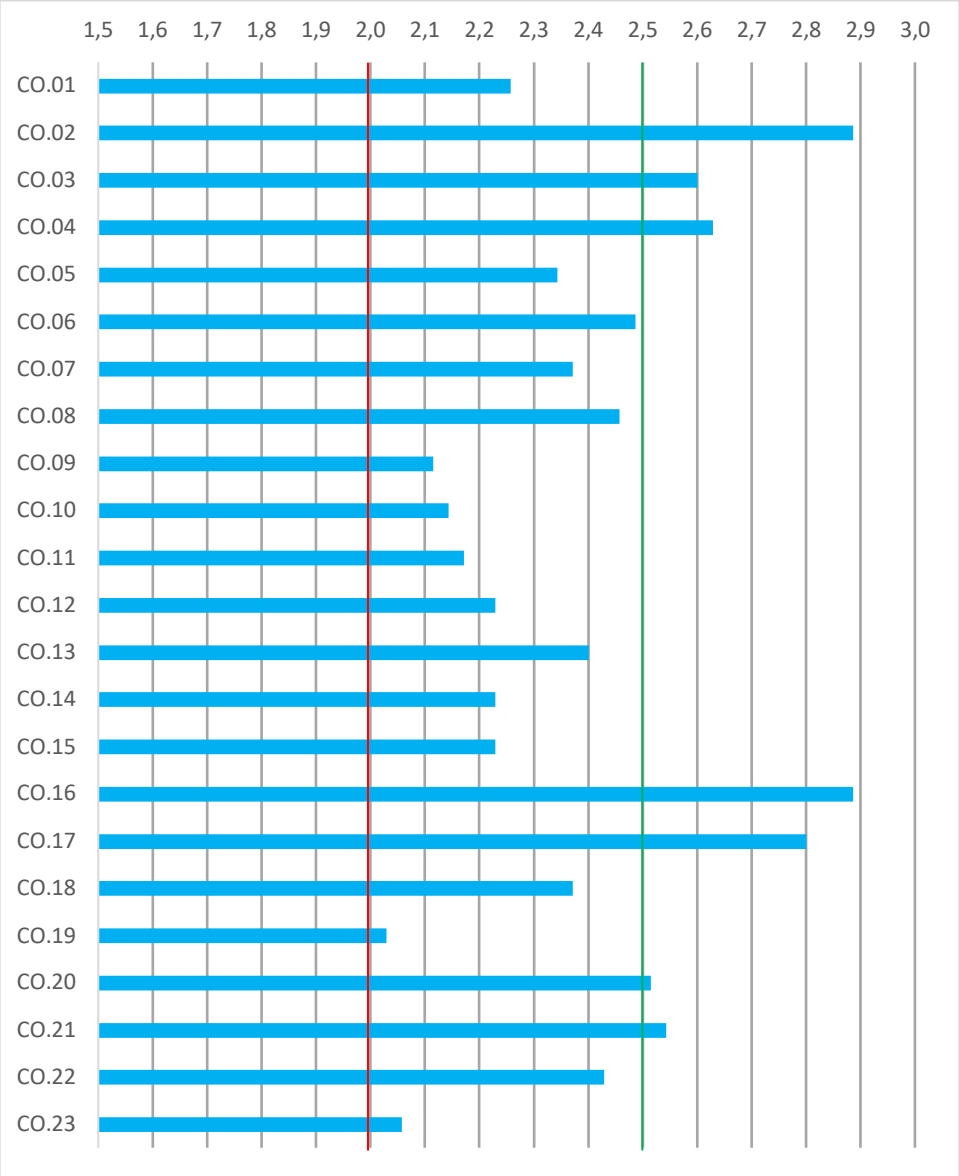
Alle maatregelen scoren ruimschoots boven volwassenheidsniveau 2,0.

Conclusie

Van oudsher is dit het best scorende cluster. Ook in deze benchmark is dat het geval. En na een terugval bij de benchmark in 2017 ten opzichte van de benchmark in 2015, scoort dit cluster in 2019 weer hoger dan in 2017.

2.2.4 Cluster 4 – Continuïteit

Dit cluster bevat 23 statements. Het gemiddelde volwassenheidsniveau van dit cluster is 2,4.



Figuur 19: Gemiddeld volwassenheidsniveau per maatregel in cluster 4

Alle maatregelen scoren een volwassenheidsniveau van meer dan 2,0. De minder scorende maatregelen zijn CO.19 en CO.23:

ID	Categorie	Risicobeschrijving	Beheersdoelstelling
CO.19	Bedrijfscontinuïteits-planning	Het ontbreken van aan risico gerelateerd inzicht in potentiële impact op de bedrijfsvoering en in de eisen betreffende herstelvermogen, alternatieve verwerking en herstel van alle kritieke IT-services. Dit zou uiteindelijk kunnen leiden tot een grote verstoring van de belangrijkste bedrijfsfuncties.	Business- en IT-continuïteitsplannen worden ontwikkeld op basis van het raamwerk en zijn ontworpen om de impact van een grote verstoring op de belangrijkste bedrijfsfuncties en -processen te verminderen. De plannen zijn gebaseerd op risicogericht inzicht in potentiële bedrijfsimpact en houden rekening met vereisten betreffende veerkracht, alternatieve verwerkings- en

ID	Categorie	Risicobeschrijving	Beheersdoelstelling
			herstelmogelijkheden in alle kritieke IT-services. De plannen omvatten ook gebruiksrichtlijnen, rollen en verantwoordelijkheden, procedures, communicatieprocessen en de testmethode.
CO.23	Risicobeheer van leveranciers	Geen op risico gebaseerd toezicht die non-disclosure agreements (NDA's), aanbetalingsovereenkomsten, blijvende levensvatbaarheid van de leverancier, naleving van beveiligingseisen, alternatieve leveranciers, conventionele vergoedingen en bonussen in overweging nemen. Gebrek aan juridisch toezicht waardoor contracten niet worden opgesteld in overeenstemming met de organisatie-eisen of wet- en regelgeving.	Risico's met betrekking tot het vermogen van leveranciers om effectieve dienstverlening op een veilige en efficiënte manier voort te zetten worden voortdurend geïdentificeerd en beperkt. Contracten voldoen aan universele zakelijke standaarden in overeenstemming met wet- en regelgeving. Risicobeheer neemt aspecten als niet-openbaarmakingsovereenkomsten (NDA's), escrow-contracten, voortdurende levensvatbaarheid van de leverancier, conformiteit met beveiligingseisen, alternatieve leveranciers, boetes en beloningen, enz. in overweging.

Tabel 10: Laag scorende maatregelen in cluster 4

Beide maatregelen zijn afhankelijk van het in kaart brengen van risico's. Aangezien in cluster 1 de risicoaanpak al laag scoorde is het niet verwonderlijk dat dit hier ook het geval is.

Zeven van de 23 statements in dit cluster scoren hoger dan 2,5:

ID	Categorie	Risicobeschrijving	Beheersdoelstelling
CO.02	Incident management	Incidenten zijn niet correct geclassificeerd en worden onjuist behandeld in het incidentbeheerproces, wat uiteindelijk leidt tot verminderde prestaties en kwaliteit van de informatievoorziening.	Een formeel incidentbeheerproces wordt gecommuniceerd en geïmplementeerd. Er zijn procedures ingesteld om ervoor te zorgen dat alle incidenten en storingen worden geregistreerd, geanalyseerd, gecategoriseerd en geprioriteerd naar impact. Alle incidenten worden bijgehouden en periodiek beoordeeld om ervoor te zorgen dat ze tijdig worden verholpen.
CO.03	Incident escalatie	Incidenten worden niet tijdig geïdentificeerd, opgelost, beoordeeld, geëscaleerd en geanalyseerd, wat uiteindelijk leidt tot verminderde prestaties en kwaliteit van de informatievoorziening.	Er worden procedures voor incidentbeheer (of voor de servicedesk) vastgesteld, zodat wanneer incidenten niet binnen de afgesproken termijn kunnen worden opgelost, serviceniveaus adequaat worden geëscaleerd en, indien nodig, wordt voorzien in een tijdelijke oplossing. Eigenaarschap van incidenten en levenscyclusmonitoring blijven de verantwoordelijkheid van de servicedesk voor gebruikersincidenten, ongeacht welke IT-groep aan de oplossing werkt.
CO.04	Incidentrespons op (cyber) beveiligingsincidenten	Het ontbreken van een effectieve en tijdige reactie of follow-up van (cyber) beveiligingsincidenten.	De organisatie beschikt over mogelijkheden voor incidentrespons om (cyber-) beveiligingsincidenten snel te detecteren, te isoleren en de impact te beperken en om diensten op een betrouwbare manier te herstellen en weer in de lucht te brengen.

ID	Categorie	Risicobeschrijving	Beheersdoelstelling
CO.16	Beheersing van malware-aanvallen	Als er onvoldoende maatregelen zijn getroffen tegen kwaadaardige software en voor het installeren van actuele beveiligingspatches kan ten gevolge van ongeautoriseerde wijzigingen door niet-geautoriseerde gebruikers afbreuk worden gedaan en schade worden toegebracht aan de integriteit van informatiesystemen (en gegevens). Dit kan uiteindelijk leiden tot diefstal, verminking en ongepast of ongeautoriseerd gebruik van informatie.	Preventie-, detectie- en correctiemaatregelen zijn aanwezig (met name actuele beveiligingspatches en virusscanning) in de hele organisatie om informatiesystemen en technologie te beschermen tegen malware (bijv. virussen, wormen, spyware, spam).
CO.17	Procedures voor back-up en herstel	Verlies van gegevens in geval van een systeemstoring of integriteitskwestie als gevolg van onnauwkeurige, onvolledige, niet tijdige back-up van kritieke gegevens en monitoring daarvan.	De organisatie heeft een strategie geïmplementeerd voor het maken van back-ups van relevante data en programma's. Back-up en herstelprocedures zijn formeel gedefinieerd en geïmplementeerd voor alle daarvoor aangewezen systemen. Het back-up schema en de retentie periode zijn in lijn met de door de organisatie geaccepteerde risico's voor dataverlies gebaseerd op de gevoeligheid van het systeem en de kosten voor handmatig herstel. Herstelprocedures worden periodiek getest en gedocumenteerd.
CO.20	Offsite back-upopslag	Kritieke media worden niet off-site opgeslagen, waardoor back-upgegevens niet beschikbaar zijn in geval van een calamiteit in het datacenter. Back-ups van kritieke media worden niet periodiek getest, met als mogelijk gevolg dat gegevens niet kunnen worden hersteld omdat ze niet compatibel zijn met de huidige software en hardware systemen en -configuratie.	Alle kritieke back-upmedia, documentatie en andere IT-resources die nodig zijn in het kader van IT-herstel- en bedrijfscontinuïteitsplannen worden offsite opgeslagen. De inhoud van back-upopslag wordt bepaald in samenspraak met de eigenaren van bedrijfsprocessen en IT-personeel. Het beheer op de externe opslagfaciliteit werkt op basis van het beleid voor dataclassificatie en de gebruikelijk manier van mediaopslag van de organisatie. IT-beheer zorgt ervoor dat offsite-arrangementen periodiek, ten minste jaarlijks, worden beoordeeld op inhoud, bescherming tegen omgevingsfactoren en beveiliging. De compatibiliteit van hardware en software voor het herstellen van gearchiveerde gegevens is gewaarborgd en gearchiveerde gegevens worden periodiek getest en ververst.
CO.21	Gegevensreplicatie	Afwezigheid van of verkeerd geconfigureerde datareplicatie kan betekenen dat kritische financiële en/of operationele gegevens niet (tijdig) beschikbaar zijn in geval van een incident.	Gegevensreplicatie is opgezet tussen de productiefaciliteit van de organisatie en de disaster-recoveryfaciliteit, zodat kritieke financiële en operationele gegevens op korte termijn beschikbaar zijn. Replicatiestatus wordt bewaakt als onderdeel van het bewakingsproces voor systeemtaken.

Tabel 11: Hoog scorende maatregelen in cluster 4

Bij CO.02 en CO.16 scoort meer dan 70% van de respondenten hoger dan 2,5, bij CO.17 is dat 66% en bij de overige maatregelen in dit cluster zit het percentage instellingen dat hoger scoort dan volwassenheidsniveau 2,5 rond de 50%.

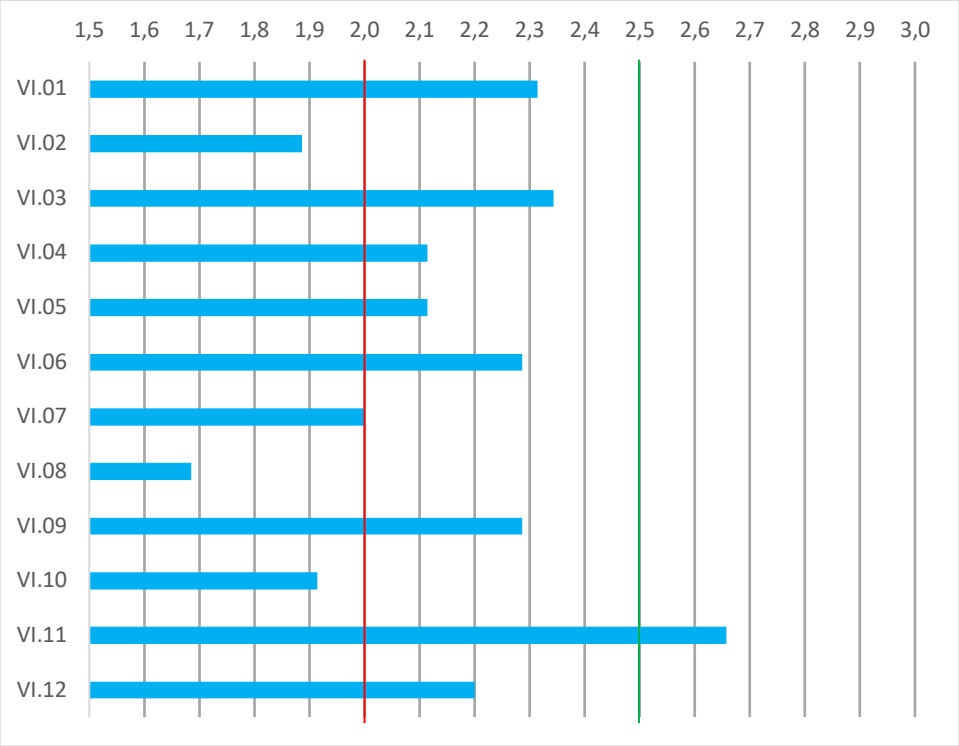
Conclusie

Volgens deze uitkomst is incident management bij de meeste instellingen goed geregeld en zijn malware-preventie en back-up bij meer dan de helft van de instellingen ook goed geregeld.

In het licht van recente incidenten is het wel verstandig deze uitkomsten goed te valideren, met name procedures rond en inrichting van malware-preventie en off-site back-up!

2.2.5 Cluster 5 – Vertrouwelijkheid en integriteit

Dit cluster bevat 12 statements. Het gemiddelde volwassenheidsniveau van dit cluster is 2,2.



Figuur 20: Gemiddeld volwassenheidsniveau per maatregel in cluster 5

Van de twaalf statements in dit cluster scoren er drie ruimschoots lager dan volwassenheidsniveau 2,0:

ID	Categorie	Risicobeschrijving	Beheersdoelstelling
VI.02	Toegang tot de productieomgeving door ontwikkelaars	Ontwikkelaars met toegang tot de productieomgeving brengen de scheiding van taken in gevaar, wat uiteindelijk zou kunnen leiden tot ongeoorloofde toegang tot of wijzigingen in programma's en gegevens.	Medewerkers (ontwikkelaars) die betrokken zijn bij de ontwikkeling en implementatie van wijzigingen in in-scope-applicaties en ondersteunende besturingssystemen en databases, hebben geen schrijftoegang tot de productieomgeving. Medewerkers (ontwikkelaars) die verantwoordelijk zijn voor het vrijgeven van de broncode voor productie hebben geen schrijftoegang tot de test- of ontwikkelomgeving.
VI.08	Noodtoegang (envelopprocedure/breek-het-glasprocedure)	Het ontbreken van een adequate procedure voor noodtoegang kan leiden tot ongeoorloofde toegang tot programma's en gegevens of tot verstoring van IT-services.	Er is een noodprocedure vastgesteld om in geval van nood toegang tot accounts met super-user rechten te beheren, die door de organisatie wordt gevolgd.

ID	Categorie	Risicobeschrijving	Beheersdoelstelling
VI.10	Beheer van cryptografische sleutels	Bescherming betreffende de vertrouwelijkheid, authenticiteit of integriteit van informatie mislukt als gevolg van ontoereikende cryptografische technieken. Dit kan uiteindelijk leiden tot diefstal, corruptie, onjuist of ongeautoriseerd gebruik van informatiemiddelen.	Er zijn beleid en procedures voor het genereren, veranderen, intrekken, vernietigen, verspreiden, certificeren, opslag, invoer, gebruik en archivering van cryptografische sleutels om sleutels te beschermen tegen aanpassing en ongeautoriseerde toegang.

Tabel 12: Laag scorende maatregelen in cluster 5

Het feit dat VI.02 laag scoort (86% van de instellingen scoort lager dan volwassenheidsniveau 2,0) komt overeen met de lage score van BO.08 in cluster 1, die al aangaf dat er bij veel instellingen geen gestructureerde aanpak van softwareontwikkeling en -aanschaf is.

De hoogst scorende maatregel is VI.11:

ID	Categorie	Risicobeschrijving	Beheersdoelstelling
VI.11	Netwerkbeveiliging	Ongeautoriseerde toegang tot systemen verbonden met een netwerk of openbaarmaking van gevoelige informatie die over het netwerk wordt verzonden. Dit kan uiteindelijk leiden tot diefstal, corruptie, onjuist of ongeautoriseerd gebruik van informatiemiddelen.	Beveiligingstechnieken en bijbehorende beheerprocedures (bijv. firewalls, beveiligingsapparatuur, netwerksegmentatie en inbraakdetectie) worden gebruikt voor het autoriseren van toegangs- en besturingsinformatiestromen van en naar netwerken. Er wordt gebruik gemaakt van "best practices" op dit gebied (bijv. NCSC, ISO/IEC, ITSec).

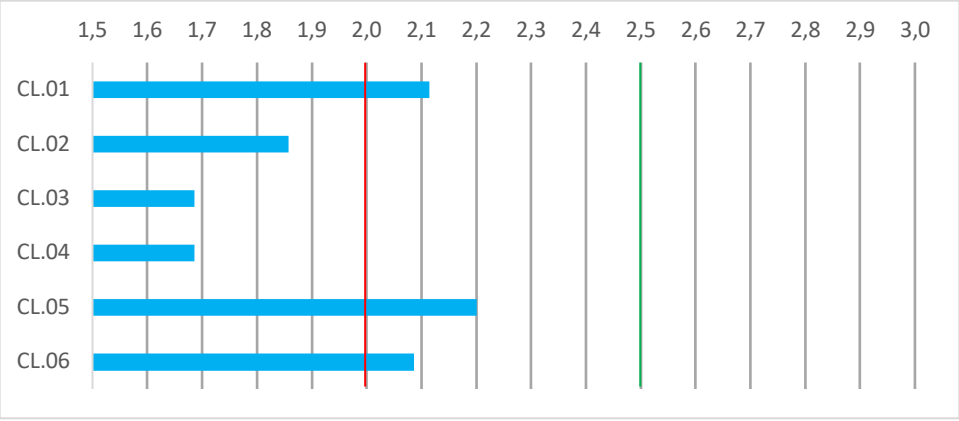
Tabel 13: Hoogst scorende maatregel in cluster 5

Conclusie

Volgens de uitkomsten in dit cluster scoort netwerkbeveiliging hoog (60% van de respondenten scoort hoger dan volwassenheidsniveau 2,5). In het licht van recente incidenten is het wel verstandig deze uitkomst goed te valideren, aangezien onvoldoende netwerksegmentering en onvolledige inbraakdetectie daar een rol hebben gespeeld.

2.2.6 Cluster 6 – Monitoring en logging

Dit cluster bevat 6 statements. Het gemiddelde volwassenheidsniveau van dit cluster is 1,9.



Figuur 21: Gemiddeld volwassenheidsniveau per maatregel in cluster 6

In dit cluster scoort maar liefst 50% van de maatregelen ruimschoots onder volwassenheidsniveau 2,0:

ID	Categorie	Risicobeschrijving	Beheersdoelstelling
CL.02	Periodieke beoordeling van toegangsrechten	Ongeautoriseerde toegang tot het besturingssysteem, gegevens en applicaties (inclusief programma's, tabellen en gerelateerde bronnen) veroorzaakt door onjuiste toegangsrechten en onvoldoende bewaking van schending daarvan. Onjuiste toekenning van toegangsrechten aan gebruikers en niet tijdig intrekken van toegangsrechten kan leiden tot problemen op het gebied van scheiding van taken of ongeoorloofde toegang tot informatie waardoor bedrijfsprocessen en applicatieprestaties negatief beïnvloed worden.	Het management beoordeelt periodiek de gebruikerstoegang die geïmplementeerd is voor de relevante applicaties (IST-situatie) om de juistheid van geïmplementeerde accounts en rollen (de toegangsrechten) te bevestigen, en valideert dat toegangsrechten passend zijn voor toegewezen taken, zoals bepaald door de toegangsregels (SOLL-situatie). Elke onjuiste toegang die tijdens het beoordelingsproces wordt opgemerkt, wordt direct ingetrokken. Deze controle houdt in dat SOLL- en IST-matrices worden vergeleken door het verantwoordelijke management.
CL.03	Logging	Niet registreren en/of het ontbreken van periodieke beoordeling van logbestanden kan ertoe leiden dat ongepaste of ongebruikelijke activiteiten niet op tijd worden opgemerkt of dat er onvoldoende vervolgacties worden uitgevoerd. Bewaartermijnen van logbestanden en toegangsrechten tot logbestanden zijn niet in overeenstemming met bedrijfseisen of wet- en regelgeving.	Eisen voor logging zijn gedefinieerd op basis van monitoring- en rapportagebehoeften en geïmplementeerd in systemen, databases en netwerkcomponenten. Logs worden periodiek beoordeeld op indicaties van ongepaste of ongebruikelijke activiteiten en er worden adequate follow-upacties gedefinieerd. Bewaartermijnen van logs en toegangsrechten zijn in lijn met de business requirements.
CL.04	Testen van, inspectie van en toezicht op beveiliging	Wanneer beveiligingsmaatregelen niet worden getest en inspectie en monitoring ontbreken, kan dit ertoe leiden dat ongebruikelijke en/of abnormale activiteiten niet tijdig worden gedetecteerd en/of aangepakt. Het niet onderhouden van de baseline voor informatiebeveiliging kan leiden tot onveilige implementatie van IT-componenten.	Implementatie van IT-beveiliging wordt proactief getest en bewaakt. IT-beveiliging moet regelmatig worden getoetst om ervoor te zorgen dat de door de organisatie goedgekeurde baseline voor informatiebeveiliging wordt gehandhaafd. Een log- en bewakingsfunctie maakt vroegtijdige preventie en/of detectie en daaropvolgende tijdige rapportage van ongebruikelijke en/of abnormale activiteiten die moeten worden aangepakt, mogelijk.

Tabel 14: Laag scorende maatregelen in cluster 6

Voor zowel CL.03 als CL.04 geldt dat meer dan 90% van de deelnemende instellingen lager scoort dan volwassenheidsniveau 2,0. Het feit dat CL.02 laag scoort (ruim 80% scoort onder de 2,0) komt overeen met de lage score van PS.03 in cluster 2.

Het hoogst scorende statement in cluster 6 is CL.05:

ID	Categorie	Risicobeschrijving	Beheersdoelstelling
CL.05	Service-level beheer	Gebrek aan beheer en monitoring van de levering van diensten waardoor afwijkingen in de prestaties van leveranciers niet op tijd worden gedetecteerd. Trends in prestatiestatistieken voor specifieke en algemene diensten worden niet geïdentificeerd en niet opgevolgd, wat kan leiden tot een afname van de algemene bedrijfsprestaties.	Business requirements en de manier waarop IT-services en serviceniveaus bedrijfsprocessen ondersteunen, worden periodiek geanalyseerd. Services en serviceniveaus worden besproken en overeengekomen met de organisatie en vergeleken met het huidige serviceportfolio om nieuwe of gewijzigde services of serviceniveau-opties te identificeren.

Tabel 15: Hoogst scorende maatregel in cluster 6

Dit komt weliswaar overeen met de score van statement BO.12 in cluster 1 dat hoog scoort, maar geeft aan dat de monitoring van service-level beheer nog tekortschiet.

Conclusie

Van oudsher scoort dit cluster laag. De gebeurtenissen in Maastricht illustreren dat dit een gemis is dat aangepakt moet worden.

3 Conclusie en aanbevelingen

In dit hoofdstuk gaan we in op de laag scorende beheersmaatregelen, geven we aan welke risico's daaraan verbonden zijn en doen we enkele aanbevelingen voor verbetering.

3.1 Bevindingen, risico's en aanbevelingen

3.1.1 Cluster 1 – Beleid en organisatie

Bevindingen

De laagst scorende beheersmaatregelen in *Cluster 1 – Beleid en organisatie* zijn BO.05 en BO.06. Beide maatregelen zitten in het NBA-domein *Risk Management*:

> BO.05 – Er is een raamwerk voor informatierisicobeheer opgesteld en afgestemd op de doelstellingen van de organisatie en het (bedrijfs) risicobeheerraamwerk.
>
> BO.06 – Risicobeoordelingen worden uitgevoerd om actuele risicoprofielen met betrekking tot bedrijfsdoelstellingen te bepalen. De waarschijnlijkheid en impact van alle geïdentificeerde risico's worden regelmatig beoordeeld, met behulp van kwalitatieve en kwantitatieve methoden. De waarschijnlijkheid en impact van inherente en rest risico's worden bepaald per categorie, op portefeuillebasis.

Ook redelijk laag scoort BO.07 dat in hetzelfde domein zit:

> BO.07 – Beheersactiviteiten worden op alle niveaus geprioriteerd en gepland om de benodigde mitigerende maatregelen te implementeren, inclusief het bepalen van kosten en baten en de verantwoordelijkheid voor de uitvoering. Goedkeuring wordt verkregen voor aanbevolen acties en acceptatie van rest risico's en er wordt voor gezorgd dat uitgevoerde acties onder verantwoordelijkheid van betrokken proceseigenaar(s) vallen. De uitvoering van plannen wordt bewaakt en eventuele afwijkingen worden gerapporteerd aan het senior management.

Risico's

Deze drie beheersmaatregelen vereisen dat er risicomanagement wordt ingericht, waarbij op regelmatige basis risicoanalyses worden uitgevoerd om te zien of de mitigerende maatregelen nog voldoen aan de bedrijfsdoelstellingen. Zonder risicomanagement bestaat de kans op maatregelen, die qua kosten niet passen bij het risicoprofiel van de instelling.

Aanbevelingen

Richt risicomanagement op structurele wijze in op volwassenheidsniveau 4, zodat er sprake is van periodieke evaluatie en bijstelling (Plan-Do-Check-Act-cyclus). En zodat de uitkomsten leiden tot het opnemen van nieuwe of aangepaste maatregelen in de begrotingscyclus.

3.1.2 Cluster 2 – Personeel, studenten en gasten

Bevindingen

De laagst scorende beheersmaatregel in *Cluster 2 – Personeel, studenten en gasten* is PS.03 in het NBA-domein *Human Resources*:

> PS.03 – Wanneer er functiewijzigingen plaatsvinden, met name beëindiging van het dienstverband, wordt direct effectief actie ondernomen. Kennisoverdracht wordt geregeld, verantwoordelijkheden worden opnieuw toegewezen en toegangsrechten worden verwijderd, zodat risico's worden geminimaliseerd en de continuïteit van de functie wordt gewaarborgd.

Risico's

Hoewel de meeste instellingen maatregelen met betrekking tot human resources goed op orde hebben is het invoeren en onderhouden van rollen en rechten en het overdragen van kennis minder goed geregeld. Medewerkers kunnen daardoor bij functieverandering te veel rechten krijgen ('stapelen van rechten') en er kan kennis verloren gaan wat de continuïteit van de functie negatief kan beïnvloeden.

Aanbevelingen

Zorg ervoor dat naast het toekennen en intrekken van rollen en rechten van medewerkers ook bij verandering van functie een review plaatsvindt van de benodigde rollen en rechten, dat kennis wordt overgedragen als een medewerker vertrekt en dat dit alles geborgd is in een proces waarbij regelmatig controle plaatsvindt op de autorisaties.

3.1.3 Cluster 3 – Ruimten en apparatuur

Bevindingen

De laagst scorende beheersmaatregel in *Cluster 3 – Ruimten en apparatuur* is RA.01 in het NBA-domein *Data Management*:

> RA.01 – Er zijn (cyber)procedures vastgesteld en geïmplementeerd om ervoor te zorgen dat aan business requirements voor het beschermen van (gevoelige) gegevens en software wordt voldaan bij het verwijderen of overdragen van gegevens of hardware.

Risico's

Wanneer gevoelige informatie en software niet grondig verwijderd worden van oude media, kunnen data lekken en software licenties misbruikt worden. Hierdoor kunnen gevoelige data op straat komen te liggen wat juridische consequenties kan hebben.

Aanbevelingen

Richt procedures in voor het verwijderen van (gevoelige) data en het opschonen van hardware wanneer die afgedankt worden. Of sluit een contract af met een gecertificeerde derde partij die dit voor de instelling kan uitvoeren.

3.1.4 Cluster 4 – Continuïteit

Bevindingen

De laagst scorende beheersmaatregelen in *Cluster 4 – Continuïteit* zijn CO.19 in het NBA-domein *Business Continuity Management* en CO.23 in het NBA-domein *Supply Chain Management*:

> CO.19 – Business- en IT-continuïteitsplannen worden ontwikkeld op basis van het raamwerk en zijn ontworpen om de impact van een grote verstoring op de belangrijkste bedrijfsfuncties en -processen te verminderen. De plannen zijn gebaseerd op risicogericht inzicht in potentiële bedrijfsimpact en houden rekening met vereisten betreffende veerkracht, alternatieve verwerkings- en herstelmogelijkheden in alle kritieke IT-services. De plannen omvatten ook gebruiksrichtlijnen, rollen en verantwoordelijkheden, procedures, communicatieprocessen en de testmethode.
>
> CO.23 – Risico's met betrekking tot het vermogen van leveranciers om effectieve dienstverlening op een veilige en efficiënte manier voort te zetten worden voortdurend geïdentificeerd en beperkt. Contracten voldoen aan universele zakelijke standaarden in overeenstemming met wet- en regelgeving. Risicobeheer neemt aspecten als niet-openbaarmakingsovereenkomsten (NDA's), escrow-contracten, voortdurende levensvatbaarheid van de leverancier, conformiteit met beveiligingseisen, alternatieve leveranciers, boetes en beloningen, enz. in overweging.

Risico's

Wanneer geen inzicht bestaat in de risico's die impact hebben op de weerbaarheid van de organisatie, kunnen geen doeltreffende maatregelen worden genomen om de continuïteit van de organisatie te waarborgen. Dit geldt ook voor contractuele verplichtingen die leveranciers hebben om bijvoorbeeld de continuïteit van cloudapplicaties te

waarborgen; wanneer geen inzicht bestaat in de risico's van uitval van cloudapplicaties en de contractuele afspraken die er zijn, kan dit onvoorziene gevolgen hebben voor de continuïteit.

Aanbevelingen

Deze twee beheersmaatregelen vereisen dat er risicomanagement wordt ingericht om inzicht te hebben in de risico's en passende maatregelen kunnen worden genomen om risico's op kosteneffectieve wijze te mitigeren om zo de bedrijfscontinuïteit te waarborgen. Dit hangt samen met de aanbeveling om cluster 1 te verbeteren (zie pagina 27). Zorg er tevens voor dat contractmanagement en het beheer van Service Level Afspraken (SLA) goed is ingericht.

3.1.5 Cluster 5 – Vertrouwelijkheid en integriteit

Bevindingen

De laagst scorende beheersmaatregelen in *Cluster 5 – Vertrouwelijkheid en integriteit* zijn VI.02 in het NBA-domein *Software* Development, VI.08 in het NBA-domein *Identity and Access Management* en VI.10 in het NBA-domein *Security Management*:

> VI.02 – Medewerkers (ontwikkelaars) die betrokken zijn bij de ontwikkeling en implementatie van wijzigingen in in-scope-applicaties en ondersteunende besturingssystemen en databases, hebben geen schrijftoegang tot de productieomgeving. Medewerkers (ontwikkelaars) die verantwoordelijk zijn voor het vrijgeven van de broncode voor productie hebben geen schrijftoegang tot de test- of ontwikkelomgeving.
>
> VI.08 – Er is een noodprocedure vastgesteld om in geval van nood toegang tot accounts met super-user rechten te beheren, die door de organisatie wordt gevolgd.
>
> VI.10 – Er zijn beleid en procedures voor het genereren, veranderen, intrekken, vernietigen, verspreiden, certificeren, opslag, invoer, gebruik en archivering van cryptografische sleutels om sleutels te beschermen tegen aanpassing en ongeautoriseerde toegang.

Risico's

Wanneer er geen procedures zijn met betrekking tot softwareontwikkeling, on-premises of bij leveranciers, bestaat de kans dat productiedata gebruikt worden bij het testen en accepteren van nieuwe versies van software.

Het ontbreken van een 'break-glass' procedure in noodsituaties kan leiden tot ongewenste onderbreking van diensten of ongewenste toegang tot programmatuur die niet wordt gelogd.

Wanneer ongeschikte cryptografische middelen worden ingezet kunnen data en systemen niet adequaat beschermd worden tegen ongeoorloofde toegang, waardoor data kunnen lekken of aangepast kunnen worden.

Aanbevelingen

Wanneer de instelling software ontwikkelt, behoort er een OTAP-procedure[11] te zijn. Wanneer de instelling softwareontwikkeling uitbesteedt, behoort de leverancier een OTAP-procedure te hebben, zodat ontwikkelaars geen toegang hebben tot productiedata of -systemen.

Richt een procedure in om in geval van nood met een super-user account toegang te verkrijgen tot systemen. De procedure beschrijft onder welke omstandigheden de toegang wordt verleend en er is logging om achteraf te kunnen zien wat er is gedaan tijdens de noodsituatie.

Richt procedures in voor het toepassen van passende cryptografische middelen inclusief sleutelmanagement.

[11] Ontwikkel – Test – Acceptatie – Productie.

3.1.6 Cluster 6 – Monitoring en logging

Bevindingen

De laagst scorende beheersmaatregelen in *Cluster 6 – Controle en logging* zijn CL.02 in het NBA-domein *Identity and Access Management*, CL.03 en CL.04 in het NBA-domein *Security Management*:

> CL.02 – Het management beoordeelt periodiek de gebruikerstoegang die geïmplementeerd is voor de relevante applicaties (IST-situatie) om de juistheid van geïmplementeerde accounts en rollen (de toegangsrechten) te bevestigen, en valideert dat toegangsrechten passend zijn voor toegewezen taken, zoals bepaald door de toegangsregels (SOLL-situatie). Elke onjuiste toegang die tijdens het beoordelingsproces wordt opgemerkt, wordt direct ingetrokken. Deze controle houdt in dat SOLL- en IST-matrices worden vergeleken door het verantwoordelijke management.
>
> CL.03 – Eisen voor logging zijn gedefinieerd op basis van monitoring- en rapportagebehoeften en geïmplementeerd in systemen, databases en netwerkcomponenten. Logs worden periodiek beoordeeld op indicaties van ongepaste of ongebruikelijke activiteiten en er worden adequate follow-upacties gedefinieerd. Bewaartermijnen van logs en toegangsrechten zijn in lijn met de business requirements.
>
> CL.04 – Implementatie van IT-beveiliging wordt proactief getest en bewaakt. IT-beveiliging moet regelmatig worden getoetst om ervoor te zorgen dat de door de organisatie goedgekeurde baseline voor informatiebeveiliging wordt gehandhaafd. Een log- en bewakingsfunctie maakt vroegtijdige preventie en/of detectie en daaropvolgende tijdige rapportage van ongebruikelijke en/of abnormale activiteiten die moeten worden aangepakt mogelijk.

Risico's

Wanneer niet periodiek wordt getoetst of toegekende toegangsrechten nog in overeenstemming zijn met het beleid, of beveiligingsmaatregelen nog adequaat zijn en logbestanden niet regelmatig worden geanalyseerd, kunnen ongeautoriseerde gebruikers of programma's ongemerkt toegang krijgen tot data en systemen. Hierdoor worden vertrouwelijkheid en integriteit gecompromitteerd.

Aanbevelingen

Richt procedures in om toegangsrechten periodiek te evalueren en bij geconstateerde afwijkingen maatregelen te nemen. Zorg voor adequate logging én analyse van log data door de eerste lijn om afwijkende patronen te detecteren en, indien nodig, tegenmaatregelen te nemen. Test bestaande maatregelen en procedures regelmatig met behulp van kwetsbaarhedenscans, penetratietesten en crisisoefeningen.

Zorg ervoor dat deze procedures zijn ingebed in het beveiligingsbeleid van de organisatie.

4 Nawoord

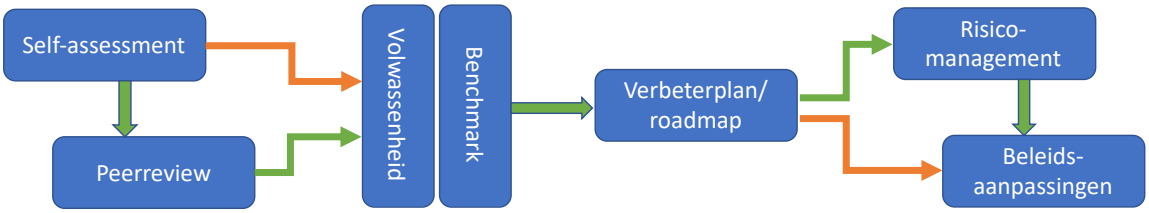
De resultaten van de SURFaudit benchmark 2019 laten zien dat de sector onderwijs en onderzoek nog het nodige werk heeft te verrichten op het gebied van informatiebeveiliging. Hoewel het gemiddelde van alle deelnemende instellingen wat lager is uitgevallen dan bij de benchmark in 2017, is dit ten dele te verklaren door het gebruik van een nieuw toetsingskader dat meer nadruk legt op risicomanagement dan het vorige toetsingskader. Verder scoren instellingen die eerder hebben meegedaan aan de SURFaudit benchmark gemiddeld genomen bijna hetzelfde als in 2017. Vaker meedoen resulteert ook in een hogere score. Instellingen die alle benchmarks hebben meegedaan scoren significant hoger dan gemiddeld, instellingen die nu voor het eerst hebben meegedaan scoren significant lager dan gemiddeld. Waar die lagere score precies door veroorzaakt wordt vereist nader onderzoek, maar een verklaring kan zijn dat ze minder ervaring hebben met het bepalen van volwassenheidsniveaus en conservatief hebben ingevuld. Bovendien zijn er onder de instellingen die nu voor het eerst meedoen een groot aantal kleine instellingen die minder mensen en middelen beschikbaar hebben voor informatiebeveiliging.

Meest zorgwekkend is de lage score op cluster 6 – monitoring en logging, dat in 2019 gemiddeld onder volwassenheidsniveau 2,0 is uitgekomen, en

ook in 2017 al laag scoorde. Hier zullen instellingen stappen moeten zetten om zowel het verzamelen van logging als de analyse daarvan op een hoger plan te brengen en daarmee hun weerbaarheid te verhogen.

Het zou goed zijn als bij de volgende SURFaudit benchmark álle instellingen in de sector onderwijs en onderzoek meedoen met de benchmark om zo de weerbaarheid van de hele sector in beeld te brengen en voor de instellingen zelf om ervaring op te doen met self-assessments. Het zou nog beter zijn als meer instellingen bovendien gebruik maken van de mogelijkheid een peerreview te laten uitvoeren, zodat de resultaten van het self-assessment gevalideerd zijn door onafhankelijke collega's en de beoordelingen over de hele linie consistenter worden.

Nu de benchmark is afgerond begint het echte werk: het is aan iedere instelling een plan van aanpak te maken om geconstateerde deficiënties te verbeteren.



Figuur 22: Van self-assessment tot beleidsaanpassingen (groen is de voorkeursroute)

Het ransomware-incident van december 2019 bij Maastricht University illustreert hoe belangrijk het is voor instellingen om goed zicht te hebben op de eigen staat van informatiebeveiliging en om de geïdentificeerde risico's structureel aan te pakken als onderdeel van risicomanagement.

Hiermee wordt de sector onderwijs en onderzoek als geheel weerbaarder. Door bij het inrichten van adequate maatregelen de samenwerking tussen instellingen te zoeken kan dit bovendien op een effectieve en efficiënte manier worden aangepakt.

Informatie over SURFaudit, self-assessments en peerreview vind je op de SURFaudit-wiki (https://edu.nl/vuku3) of neem contact op met surfaudit@surfnet.nl.

Colofon

Auteur(s):	Bart Bosma, SURF
Review:	René Ritzen – SURF
	Remco Poortinga-van Wijnen – SURF
	Martijn Bijleveld – saMBO-ICT
	Ludo Cuijpers – HAS Hogeschool
Redactie:	Yvonne Klaassen – SURF
Versie:	1.0
Datum:	6 maart 2020