Resultaten SURFaudit-benchmark 2017

Utrecht, 16 juli 2018
Versienummer: 1.0

Colofon

Resultaten SURFaudit-benchmark 2017

SURF
Postbus 19035
NL-3501 DA Utrecht
T + 31 88 78 73 000

info@surf.nl
www.surf.nl

Auteur
Bart Bosma - SURFnet

juli 2018

SURF is de ICT-samenwerkingsorganisatie van het Nederlandse hoger onderwijs en onderzoek.
Deze publicatie is digitaal beschikbaar via de website van SURF: www.surf.nl/publicaties

Samenvatting

Tweejaarlijkse benchmark op basis van normenkader IHBO

Iedere twee jaar organiseert SURF de SURFaudit-benchmark, waarbij participerende instellingen een self-assessment uitvoeren tegen het Normenkader Informatiebeveiliging Hoger Onderwijs (normenkader IBHO). De resultaten, uitgedrukt in volwassenheidsniveaus (CMM-score 1 t/m 5) worden verzameld en geanalyseerd om een beeld te krijgen van de mate van compliance met het normenkader IBHO voor de hele sector. Hiermee wordt invulling gegeven aan zelfregulering op dit gebied door hbo en WO.

Aanbevolen volwassenheidsniveaus

De huidige versie van het normenkader IBHO, inclusief de voorgestelde streefscores voor de volwassenheidsniveaus van de maatregelen en het bijbehorende toetsingskader, is op 30 maart 2015 besproken en goedgekeurd door de Stuurgroep Informatiebeveiliging en Privacy Hoger Onderwijs. In de *maturitywerkgroep* van SURFibo (nu SCIPR), die bestaat uit security officers en auditors van verschillende instellingen, zijn geïdentificeerde risico's afgewogen om de aanbevolen volwassenheidsniveaus te bepalen voor de maatregelen in het normenkader. Voor de meeste maatregelen heeft de werkgroep als baseline (streefscore) CMM-niveau **3** vastgesteld (gemiddelde voor alle clusters van het normenkader IBHO = **2,93**).

Aanmeldingen en ontvangen resultaten

In 2017 waren instellingen vanaf 1 juni in de gelegenheid hun self-assessment uit te voeren en de resultaten door te geven. Het was de bedoeling dat deelnemers uiterlijk 1 december hun resultaten zouden inleveren, maar net als bij voorgaande benchmarkrondes zijn de laatste resultaten pas in de loop van februari 2018 binnengekomen.

	Aangemeld		*Resultaat ontvangen*	
Sector	aantal	percen-	aantal	percen-
Universiteiten	13	93%	10	71%
Hogescholen	14	42%	10	30%
Onderzoeksinstellingen	3	9%	1	3%
Zorginstellingen	3	15%	0	0%
Totaal:	**33**	**33%**	**21**	**21%**

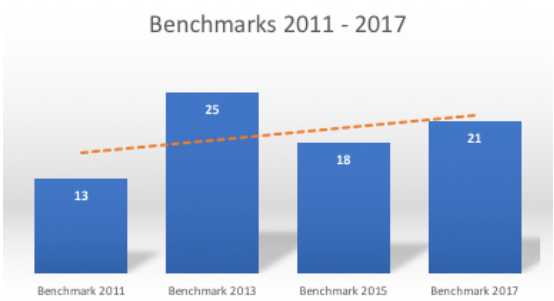
Tabel 1: Aanmeldingen en ontvangen resultaten per sector.

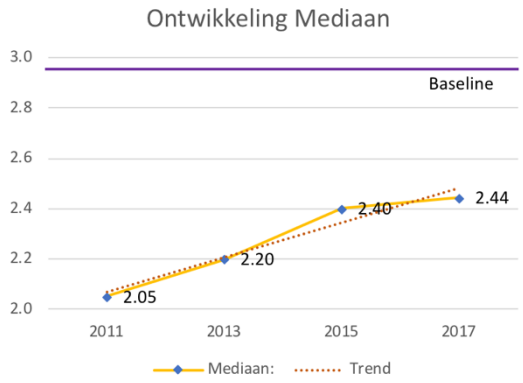
Het aantal aanmeldingen was ongeveer **1/3** van de hele doelgroep (**2/3** van alleen WO + hbo).

Het aantal ontvangen resultaten was ongeveer **2/3** van het aantal aanmeldingen (minder dan **20%** van de totale doelgroep, minder dan **45%** van alleen WO + hbo).

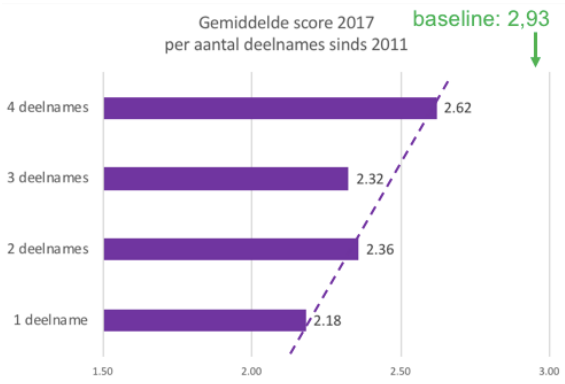
Trend

De deelname schommelt rond **19** deelnemers per benchmark, waarbij de toename van de score stagneert:





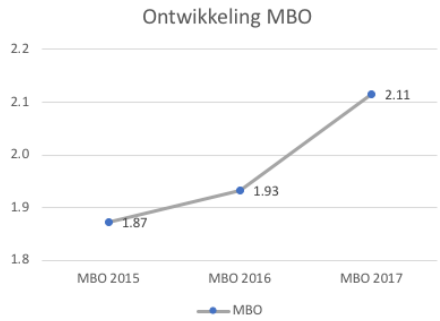
Vaker meedoen blijkt (in ieder geval statistisch) een positief effect te hebben op de resultaten:



Kanttekeningen:

- enkele security officers hebben aangegeven dat, naarmate ze vaker meedoen, ze juist strenger worden. Dit verklaart ten dele de lagere score van sommige maatregelen bij een aantal instellingen
- de scope van de self-assessment heeft invloed op de score. Bijvoorbeeld, wanneer bij de self-assessment de scope instellingsbreed is, wordt de score anders dan wanneer alleen een faculteit of een bepaald proces wordt bekeken.

Mbo



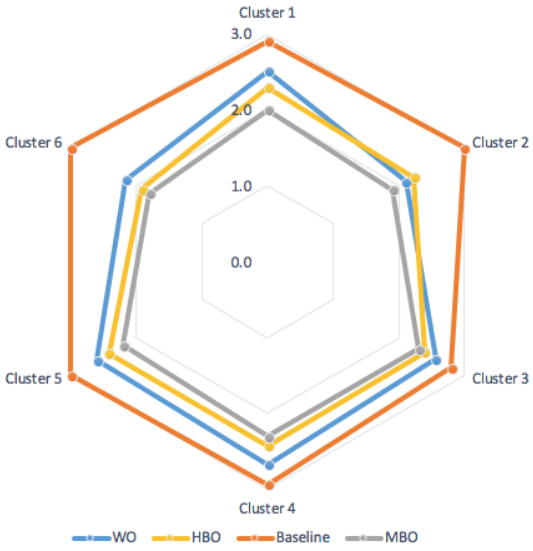
Ter vergelijking: in 2017 waren er 61 deelnemers aan de mbo-benchmark, die eens per jaar op dezelfde manier en tegen hetzelfde normenkader wordt uitgevoerd (**77%)**. Ten dele komt dit door de “comply or explain” benadering van de mbo-raad, in 2016 was de deelname nog 47% (geen “comply or explain”). Het gemiddelde resultaat (**2,11)** is wel lager dan bij de SURF-audit-benchmark, maar de stijging neemt toe in plaats van af (zie figuur links). De gemiddelde streefscore voor het mbo is **2,0**.

Resultaat

De (mediaan) score van de participanten was **2,44** – beter dan in 2015, maar lager dan de baseline.

Per cluster ziet het beeld er zo uit:

Cluster 2 (Personeel, studenten en gasten) en cluster 6 (Controle en logging) scoren duidelijk het zwakst ten opzichte van de baseline. De andere clusters zitten dichter bij de baseline.



Cyberdreigingsbeeld

Door de tegenvallende scores van maatregelen in met name cluster 2 en cluster 6 worden een aantal dreigingen met een hoog risico onvoldoende gemitigeerd:

- Manipulatie van digitaal opgeslagen data
- Identiteitsfraude
- Verkrijging en openbaarmaking van data
- Spionage

Inhoudsopgave

1. Inleiding

1.1. Doel van SURFaudit

Het primaire doel van SURFaudit is om informatiebeveiliging onder controle brengen en te houden, door de procesmanagementcyclus te ondersteunen. Daarnaast vermindert SURFaudit de noodzaak voor andere (vergelijkbare) audits op het gebied van informatiebeveiliging en privacy.

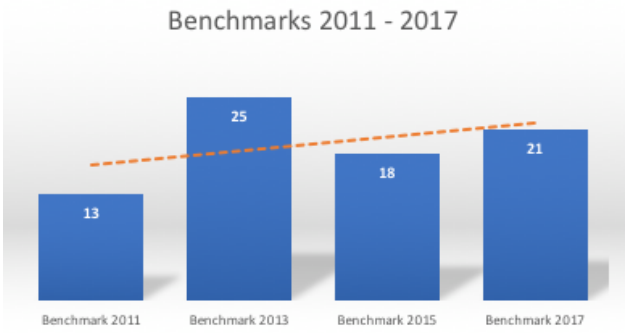
Self-assessment en peerreview

De eenvoudigste manier om een SURFaudit te doen is het uitvoeren van een self-assessment. Hiervoor is het Normenkader Informatiebeveiliging Hoger Onderwijs (normenkader IBHO) beschikbaar, met bijbehorend toetsingskader, waarin voor iedere maatregel staat beschreven welke bewijsvoering vereist is om een bepaald volwassenheidsniveau te halen. Om het resultaat van een assessment onafhankelijk te laten beoordelen kan een peerreview worden aangevraagd. De peerreview wordt uitgevoerd door speciaal getrainde collega's van bij SURF aangesloten onderwijsinstellingen.

Self-assessments kunnen op ieder gewenst moment worden uitgevoerd, de peerreviews worden via de Coördinerende Commissie Peer Review (CCPR) gepland.

1.2. Benchmark 2017

Van 1 juni tot 1 december 2017 heeft de tweejaarlijkse benchmark weer plaatsgevonden. De doelstelling was een deelname van tenminste 40 instellingen (80% van de doelgroep). Die is niet gehaald, de deelname was wel iets hoger dan in 2015, maar niet zo hoog als in 2013. Het aantal inschrijvingen was 33 en uiteindelijk hebben 21 instellingen de benchmark ingevuld. Desalniettemin is er een stijgende lijn te ontwaren. Gemiddeld schommelt de deelname per benchmark rond de 19 instellingen:



Figuur 1: ontwikkeling van de deelname aan de benchmarkrondes

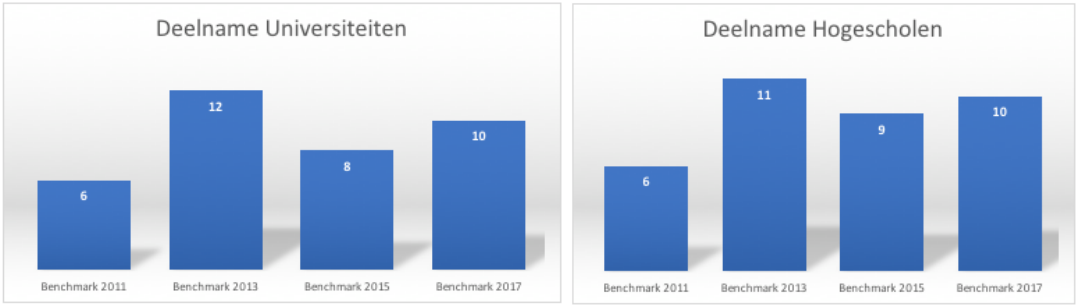
De resultaten van de SURFaudit-benchmark kunnen worden gebruikt voor:

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

1.2.1. Geschiedenis van de benchmark[1]

In 2008 was het niveau van informatiebeveiliging bij een flink 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 en in 2017 hebben tien universiteiten, tien hogescholen en een onderzoeksinstelling meegedaan (zie **Figuur 1** en **Figuur 2**).



Figuur 2: deelname universiteiten en hogescholen

Vanaf 2015 heeft ook de mbo-sector een benchmark georganiseerd. Deze is gebaseerd op hetzelfde normenkader als de SURFaudit-benchmark en daarmee zijn beide benchmarks met elkaar vergelijkbaar. Sinds 2016 omvat de mbo-benchmark ook een privacy assessment. De mbo-benchmark wordt jaarlijks gehouden en deelname is verplicht (“comply or explain”).

[1] Bron: https://www.surf.nl/binaries/content/assets/surf/nl/kennisbank/2012/SURF02_NL_+juni_2012.pdf (opgehaald op 5 april 2016).

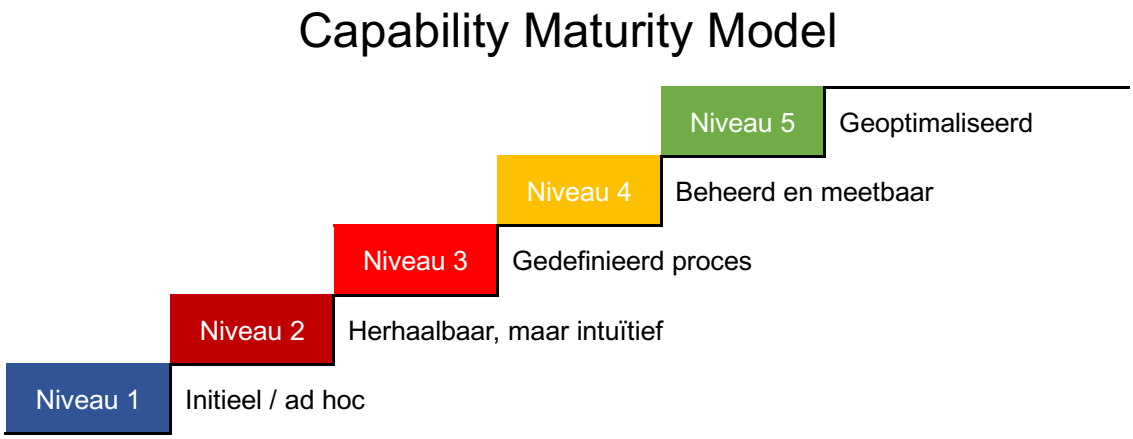
1.2.2. CMM-niveaus en baseline

De volwassenheidsniveaus voor informatiebeveiliging en bescherming van persoonsgegevens worden beschreven aan de hand van het Capability Maturity Model (CMM) zoals dat in CobiT wordt gebruikt.

Voor iedere maatregel in het normenkader wordt een CMM-niveau aanbevolen, onder andere gebaseerd op risicoanalyses uit het Cyberdreigingsbeeld. Alle CMM-niveaus samen vormen de baseline. De niveaus zijn vastgesteld door de Stuurgroep Security en Privacy aan de hand van een van de volgende regels:

- CMM-niveau 4 – de maatregel is dermate essentieel dat een regelmatige toetsing (uitvoeren van Plan-Do-Check-Act cyclus) noodzakelijk is;
- CMM-niveau 3 – de maatregel is zo basaal dat deze niet kan ontbreken of de maatregel is als essentieel geclassificeerd op basis van de analyse van het Cyberdreigingsbeeld Hoger Onderwijs;
- CMM-niveau 2 – alle overige maatregelen.

Voor de meeste beheersmaatregelen geldt dat het basisniveau 3 is, voor een aantal is dat niveau 4 en enkele kunnen op niveau 2 worden ingericht.



Figuur 3: CMM-niveaus

CMM-niveau 4 impliceert dat de betreffende maatregel regelmatig wordt geëvalueerd en bijgesteld, ofwel dat de volledige PDCA-cyclus is geïmplementeerd. Het hebben van een adequaat en goedgekeurd beveiligingsbeleid betekent dat het CMM-niveau 3, met jaarlijkse evaluatie en bijstelling wordt dit niveau 4.

Op basis van een eigen risicoafweging en het cyberdreigingsbeeld sector onderwijs en onderzoek bepaalt iedere instelling voor zichzelf wat haar streefniveau is.

1.2.3. Normenkader Informatiebeveiliging Hoger Onderwijs 2015

Voor de benchmark 2017 is net als in 2015 gebruik gemaakt van het Normenkader Informatiebeveiliging Hoger Onderwijs 2015 (“het normenkader”). 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 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[2] *maturitywerkgroep* de bestaande beheersmaatregelen geëvalueerd aan de hand van de ISO 27002:2013 standaard (de voorgaande versie van het normenkader was nog gebaseerd op ISO 27002:2007). Er zijn enkele beheersmaatregelen toegevoegd, de clusterindeling is beter gebalanceerd, het toetsingskader is uitgebreid en voor iedere maatregel is het aanbevolen CMM-niveau vastgesteld ("de baseline"). De clusterindeling zoals die al bestond in 2013 is, met de eerdergenoemde optimalisaties, gehandhaafd in 2015, zodat de vergelijking tussen de benchmarks valide blijft.

1.2.4. 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:

		Clusters IBHO						
		1	2	3	4	5	6	
Chapters ISO-27002	**ISO-27002**	**Beleid en organisatie**	**Personeel, studenten en gasten**	**Ruimten en apparatuur**	**Continuïteit**	**Vertrouwelijkheid en integriteit**	**Controle en logging**	**Niet gebuikt**
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
Totaalaantal maatregelen, inclusief gesplitste maatregelen:	**85**	21	7	15	15	17	10	

Tabel 2: Clusters in het normenkader IBHO

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

2. Resultaten

2.1. High-level resultaten

In de tabel hieronder zijn de CMM-scores van de benchmarks die tot nog toe gehouden zijn te vinden:

Cluster		HO 2011	HO 2013	HO 2015	HO 2017	Mbo 2015	Mbo 2017
	Totaal	**2.0**	**2.2**	**2.4**	**2.4**	**1.9**	**2.1**
1	Beleid en organisatie	2.0	2.2	**2.4**	2.4	1.7	2.0
2	Personeel, gasten, studenten	2.1	2.2	**2.1**	**2.2**	1.7	1.9
3	Ruimtes en apparatuur	2.0	2.4	**2.7**	**2.5**	2.1	2.3
4	Continuïteit	2.3	2.4	**2.6**	2.6	2.0	2.3
5	Toegangsbeveiliging en integriteit	2.1	2.2	**2.4**	2.5	2.0	2.3
6	Controle en logging	1.5	2.0	**2.2**	**2.0**	1.6	1.8

Tabel 3: high-level resultaten en trend (gemiddelde per cluster)

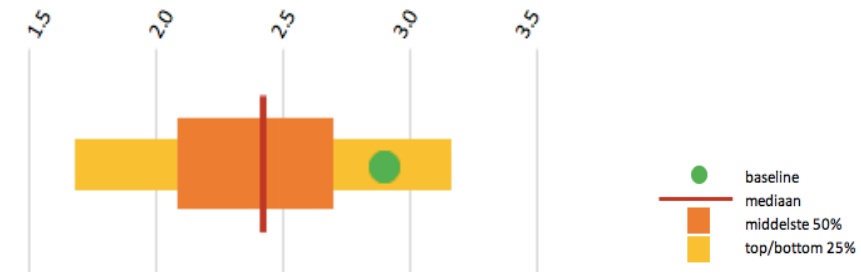
De **rood gemarkeerde** scores zijn de gemiddelde scores van clusters die lager zijn uitgevallen dan in de voorgaande benchmarkronde, de **groen gemarkeerde** scores zijn gestegen ten opzichte van de voorgaande benchmarkronde. De **mbo-scores** zijn ter vergelijking toegevoegd.

2.1.1. Ten opzichte van 2015 weinig vooruitgang

In vergelijking met de SURFaudit-benchmark uit 2015 is er voor de meeste clusters weinig veranderd, en dus wordt ook, net als in 2015, de baseline voor geen enkel cluster gehaald:

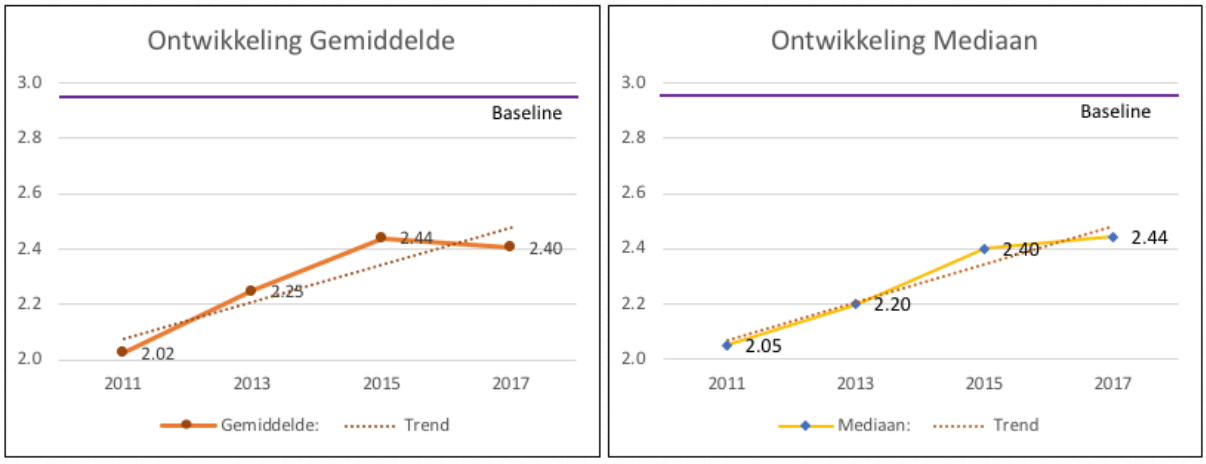
Benchmark	2011	2013	2015	2017	verschil 2015 - 2017	Baseline
Cluster 1	2,00	2,20	2,40	2,41	0,0	2,90
Cluster 2	2,10	2,20	2,10	2,15	0,1	3,00
Cluster 3	2,00	2,40	2,70	2,48	-0,2	2,80
Cluster 4	2,30	2,40	2,60	2,56	0,0	2,93
Cluster 5	2,10	2,20	2,40	2,51	0,1	3,00
Cluster 6	1,50	2,00	2,20	2,04	-0,2	3,00
Cluster 1-6						
Gemiddelde:	2,02	2,25	2,44	2,40	-0,04	2,93
Mediaan:	2,05	2,20	2,40	2,44	0,04	2,97

Tabel 4: resultaten benchmarkrondes en baseline



Figuur 4: Score verdeling benchmark 2017 (gemiddelde van alle instellingen)

In **Figuur 5** is te zien dat er een stijgende lijn in de uitkomsten (mediaan[3]) van de benchmarkrondes zit, maar dat het iets afvlakt. De baseline blijft in zicht, maar om die te behalen dienen nog stappen gemaakt te worden. Wel is het gemiddelde iets gedaald.

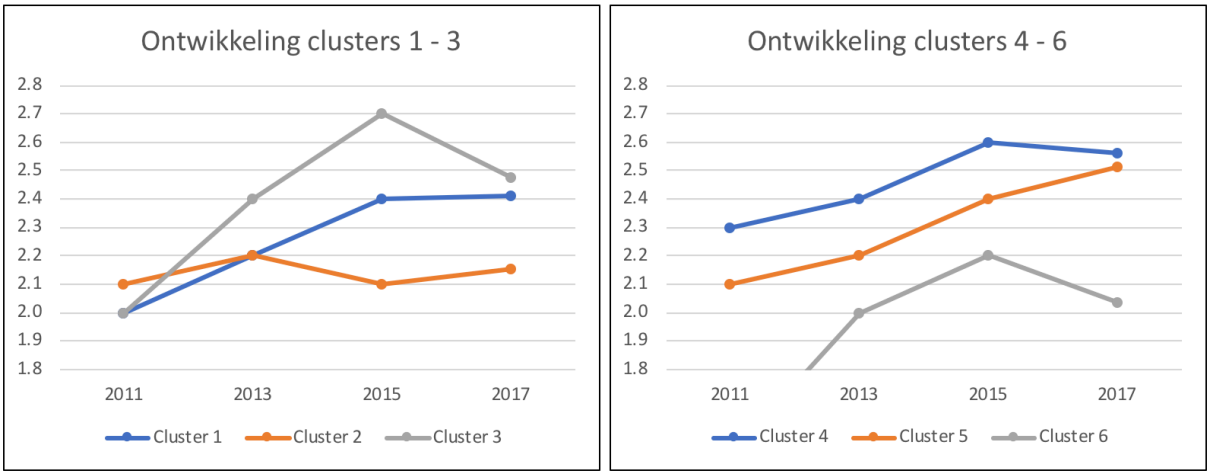


Figuur 5: ontwikkeling van gemiddelde en mediaan uitkomsten

Terwijl de benchmark 2013 voor ieder cluster een verbetering liet zien ten opzichte van de vorige benchmark (2011) en de benchmark 2015 in zijn totaliteit vooruitgang liet zien ten opzichte van de vorige benchmark (2013), stagneert die ontwikkeling bij de benchmark 2017. Ten dele wordt dit veroorzaakt door een paar instellingen die heel laag scoren. Van instellingen die vaker hebben meegedaan heeft een aantal security officers aangegeven dat ze na een aantal deelnames steeds strenger oordelen, waardoor hun scores gedaald zijn.

[3] De mediaan is de middelste score van een serie, zie bijlage voor meer detail.

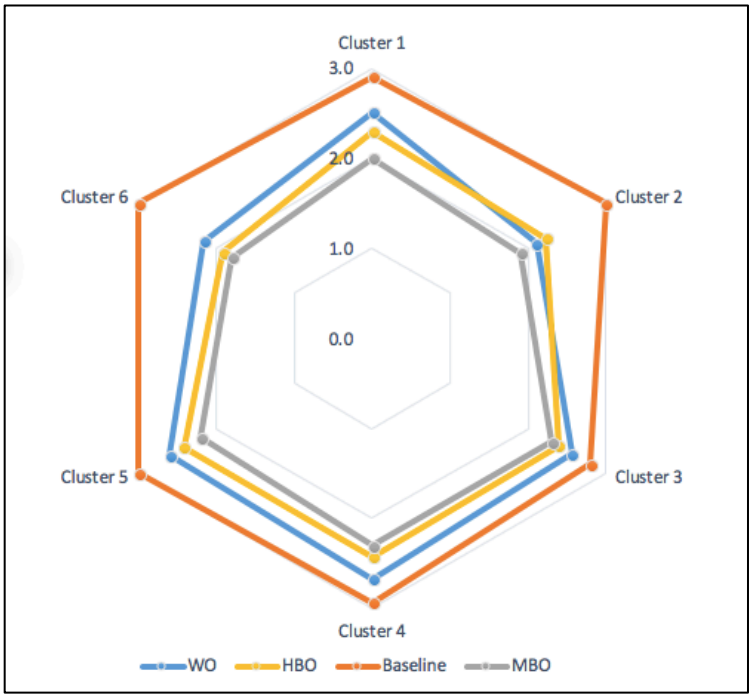
In **Figuur 6** is duidelijk te zien hoe cluster 3 en cluster 6 beduidend lager scoren dan in 2015, en ook dat cluster 4 iets is gedaald:



Figuur 6: ontwikkeling clustergemiddeldes

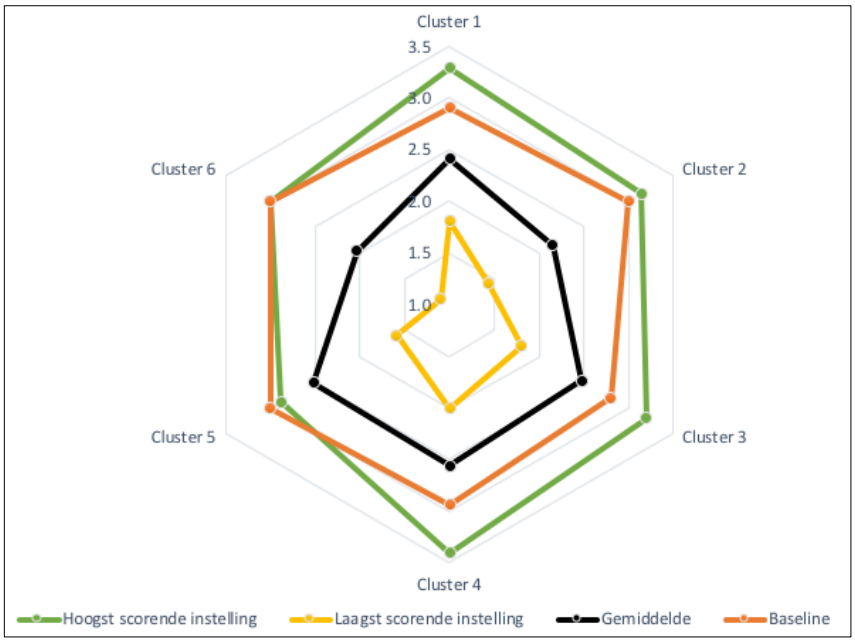
Positief is dat de score van cluster 2, die bij de vorige benchmarkronde was gedaald, weer vooruit is gegaan (hoewel nog niet tot het niveau van 2013).

In **Figuur 7** is te zien hoe de gemiddelde scores per cluster voor de sectoren WO (+onderzoek), hbo en mbo zich verhouden tot de baseline:



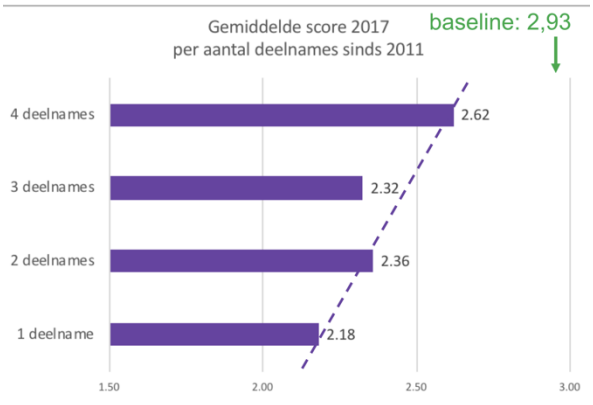
Figuur 7: gemiddeldes en baseline per cluster

En Figuur 8 geeft weer hoe de hoogst en de laagst scorende instelling ten opzichte van het gemiddelde en de baseline scoren (WO en hbo):

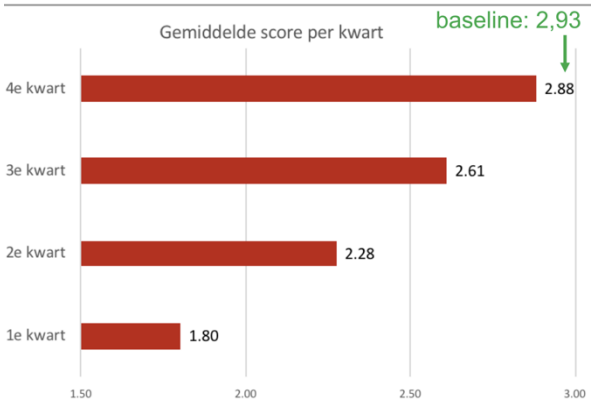


Figuur 8: hoogst en laagst scorende instelling

De hoogst scorende instelling is de enige instelling die de baseline echt haalt, de eerstvolgende zit er vlak onder. De top 25% van de deelnemers scoort gemiddeld ook in de buurt van de baseline (zie **Figuur 10**).



Figuur 9: relatie aantal deelnames en score



Figuur 10: gemiddelde score per kwart

Verder lijkt er (in ieder geval statistisch) een relatie te zijn tussen de gemiddelde score en het aantal keren dat een instelling heeft meegedaan (zie **Figuur 9**).

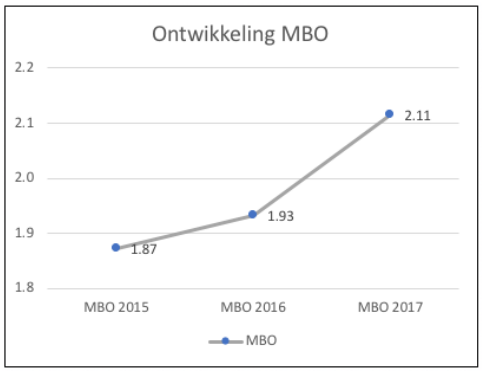
Belangrijke kanttekeningen hierbij zijn dat enkele security officers hebben aangegeven dat naarmate ze vaker meedoen ze ook strenger worden, doordat ze beter weten waarop ze moeten letten. In die optiek wordt de score daardoor weliswaar soms lager, maar gaat de kwaliteit van de beoordeling omhoog.

Ook de scope van de self-assessment heeft invloed op de score. Bijvoorbeeld, wanneer bij de self-assessment de scope instellingsbreed is, wordt de score anders dan wanneer een enkele faculteit of alleen een bepaald proces wordt bekeken.

2.1.2. Mbo-instellingen

Ook mbo-instellingen hebben een benchmark uitgevoerd in 2017 aan de hand van het *normenkader mbo*, onder auspiciën van de *regiegroep ibp in het mbo*[4].

Het *normenkader mbo* is afgeleid van het normenkader IBHO, waardoor de resultaten vergeleken kunnen worden met die van de SURFaudit-benchmarks. In dit rapport gaan we verder niet in op de specifieke resultaten van de mbo-benchmark 2017. Gedetailleerde resultaten van de mbo-benchmark zijn beschikbaar op de site van saMBO-ICT[5]. Op het moment van schrijven zijn die van 2017 nog niet officieel gepubliceerd.



Een opvallend verschil tussen de SURFaudit-benchmark en de mbo-benchmark is het aantal respondenten. Bij de SURFaudit-benchmark is dat ongeveer 44% van de doelgroep (universiteiten en hogescholen), bij het mbo is dat 77%. Daarnaast is de mbo-benchmark sinds 2016 uitgebreid met een privacy benchmark.

Figuur 11: resultaten mbo-benchmark (gemiddeldes)

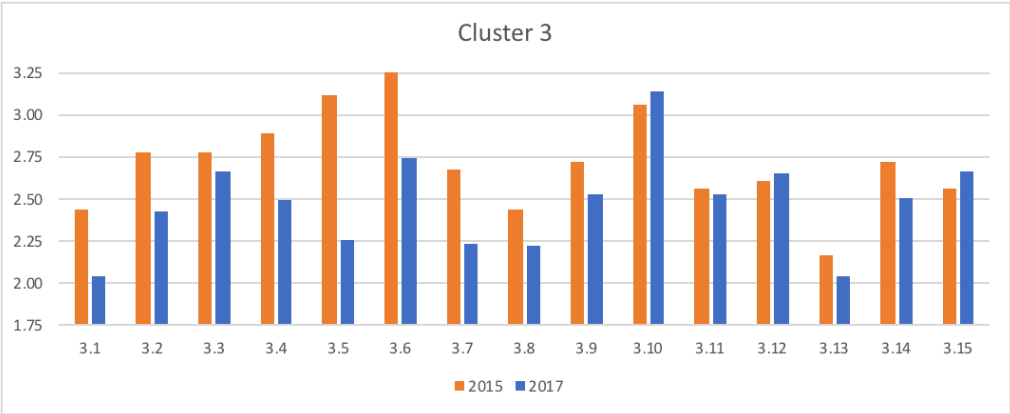
2.2. Cluster 3 en 6 nader bekeken

2.2.1. Cluster 3

Cluster 3 “Ruimtes en apparatuur” bevat 15 maatregelen die vooral betrekking hebben op de beveiliging van de fysieke omgeving. Voor het merendeel van de maatregelen is het basis CMM-niveau vastgesteld op 3.

Zoals eerder beschreven in hoofdstuk 2.1.1 zijn de resultaten van Cluster 3 sinds de benchmark 2015 aanmerkelijk gedaald (zie **Figuur 6**).

Ten opzichte van 2015 zijn de scores van twaalf van de vijftien maatregelen gedaald:



Figuur 12: scores voor cluster 3 – 2015, 2017

[4] Zie: https://www.sambo-ict.nl/2017/08/benchmark-ibp-mbo-2017/

[5] Zie: https://www.sambo-ict.nl/2017/02/benchmark-2016/

Deze vijf beheersmaatregelen zijn het meeste gedaald sinds 2015:

				CMM-niveaus				
Maatregel	**2017**	**2015**	**Wijziging**	**1**	**2**	**3**	**4**	**5**
3.5	2,25	3,11	-0,86	4	9	7	1	0
3.6	2,75	3,28	-0,53	1	6	12	2	0
3.7*	2,24	2,67	-0,43	3	10	8	0	0
3.4	2,49	2,89	-0,40	1	12	5	3	0
3.1	2,05	2,44	-0,39	6	9	5	1	0

Tabel 5: top 5 grootste dalers in cluster 3

*Noot: het basis CMM-niveau voor deze maatregel is vastgesteld op 2

De grootste daler, maatregel 3.5, heeft betrekking op de fysieke beveiliging voor kantoren, ruimten en faciliteiten. Deze maatregel scoort ook laag ten opzichte van het clustergemiddelde. Waarschijnlijk heeft fysieke beveiliging meer aandacht gekregen, waardoor kritischer is gekeken naar de bestaande maatregelen en in hoeverre ze worden toegepast.

Deze vijf beheersmaatregelen scoren het laagst in dit cluster:

				CMM-niveaus				
Maatregel	**2017**	**2015**	**Wijziging**	**1**	**2**	**3**	**4**	**5**
3.1	2,05	2,44	-0,39	6	9	5	1	0
3.13	2,05	2,17	-0,12	5	10	6	0	0
3.8*	2,22	2,44	-0,22	2	14	4	1	0
3.7*	2,24	2,67	-0,43	3	10	8	0	0
3.5	2,25	3,11	-0,86	4	9	7	1	0

Tabel 6: top 5 laagst scorende maatregelen in cluster 3

*Noot: het basis CMM-niveau voor deze maatregel is vastgesteld op 2

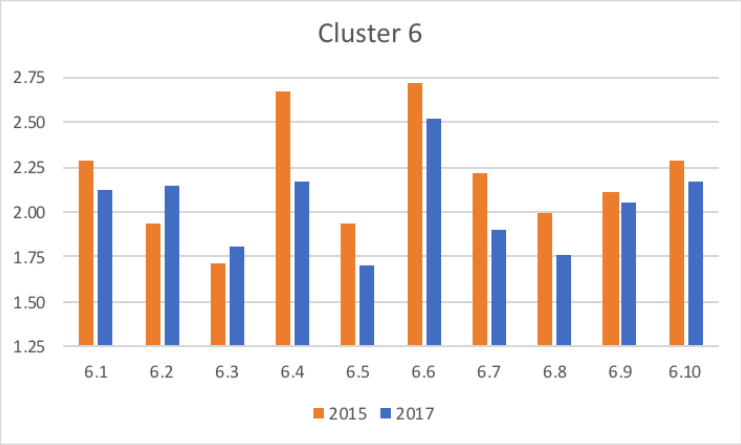
Maatregel 3.1 heeft betrekking op het beheersen van informatieveiligheidsrisico's die samenhangen met het gebruik van mobiele apparatuur. De volwassenheidsscore is gedaald ten opzichte van 2015 én scoort ook nog eens als laagste in het cluster. Ruim 70% van de instellingen scoort deze maatregel op CMM-niveau 1 of 2 (de baseline is 3). De reden daarvoor is tweeledig: er is geconstateerd dat er geen of te weinig beveiligingsmaatregelen zijn en men is zich veel meer bewust geworden van het gebruik van mobiele apparaten, waardoor kritischer is gekeken naar maatregelen op dit vlak. Wel worden bij veel instellingen middelen beschikbaar gesteld om mobiele apparaten te beveiligen, maar er is kennelijk geen sprake van een formele en gestructureerde aanpak.

Maatregel 3.13 heeft betrekking op apparatuur die buiten de organisatie wordt gebruikt. De CMM-score is iets gedaald ten opzichte van 2015. Zestien van 21 respondenten scoort deze maatregel op CMM-niveau 1 of 2, terwijl de baseline op 3 staat. De lage score voor deze maatregel hangt samen met die van maatregel 3.1, omdat apparatuur die off-premises wordt gebruikt in de regel mobiele apparatuur is.

2.2.2. Cluster 6

Cluster 6 “Logging en controle” bevat 10 maatregelen waarvan het basis CMM-niveau is vastgesteld op 3. Zoals eerder beschreven zijn ook de resultaten van Cluster 6 sinds de benchmark 2015 aanmerkelijk gedaald (zie **Figuur 6**).

Ten opzichte van 2015 zijn de scores van acht van de tien beheersmaatregelen lager geworden:



Figuur 13: scores voor cluster 6 – 2015, 2017

Deze vijf beheersmaatregelen zijn het meeste gedaald:

				CMM-niveaus				
Maatregel	**2017**	**2015**	**Wijziging**	**1**	**2**	**3**	**4**	**5**
6.4	2,17	2,67	-0,50	5	10	4	2	0
6.7	1,90	2,22	-0,32	7	9	5	0	0
6.5	1,70	1,94	-0,24	9	10	2	0	0
6.8	1,76	2,00	-0,24	8	11	1	1	0
6.6	2,52	2,72	-0,20	0	10	11	0	0

Tabel 7: top 5 grootste dalers in cluster 6

De grootste daler, maatregel 6.4, heeft betrekking op hoe wordt omgegaan met het uitbesteden van softwareontwikkeling. De maatregel vereist het overwegen van een twintigtal punten in de externe toeleveringsketen van de organisatie. Het merendeel van de respondenten scoort deze maatregel op CMM-niveau 1 of 2. Kennelijk hebben de meeste instellingen proces voor het uitbesteden van softwareontwikkeling, maar wordt dit op een as-needed basis gedaan.

En deze vijf beheersmaatregelen scoren het laagst in dit cluster:

				CMM-niveaus				
Maatregel	**2017**	**2015**	**Wijziging**	**1**	**2**	**3**	**4**	**5**
6.5	1,70	1,94	-0,24	9	10	2	0	0
6.8	1,76	2,00	-0,24	8	11	1	1	0
6.3	1,81	1,72	0,09	4	17	0	0	0
6.7	1,90	2,22	-0,32	7	9	5	0	0
6.9	2,05	2,11	-0,06	5	11	4	1	0

Tabel 8: top 5 laagst scorende maatregelen in cluster 6

Maatregel 6.5 heeft betrekking op het testen van beveiligingsfunctionaliteit tijdens het ontwikkelen van software voor zowel nieuwe als bijgewerkte systemen. De meeste instellingen scoren deze maatregel op CMM-niveau 1 of 2. Dit geeft aan dat het testen tijdens ontwikkeling ad hoc of per project gebeurt, niet is ingebed in de organisatie of niet op onafhankelijke wijze plaatsvindt.

Maatregel 6.8 gaat over het verzamelen van bewijsmateriaal. Uit diverse bijeenkomsten is gebleken dat hierover veel vragen leven bij instellingen en er weinig kennis is over adequate procedures en wat te doen als er forensisch onderzoek moet worden uitgevoerd. Het is dan ook geen wonder dat op twee na alle respondenten deze maatregel op CMM-niveau 1 of 2 scoren.

Cluster 6 als geheel scoort het laagst van alle clusters van normenkader IBHO. De baseline is 3 terwijl het cluster gemiddeld net boven CMM-niveau 2 uitkomt (2,04). Cluster 6 is altijd al het laagst scorende cluster geweest, wat aangeeft dat hier extra aandacht nodig is.

2.3. Positieve noten

De beheersmaatregelen met basis CMM-niveau 2 worden gemiddeld door meer dan 80% van de participanten gehaald en ruim 1/3 haalt zelfs een score van 3 of hoger voor die maatregelen. In het algemeen scoort bijna 10% van de respondenten hoger dan het basis CMM-niveau van een maatregel.

2.3.1. Maatregelen met basis CMM-niveau 2

Interessant is dat maatregel 1.6 die betrekking heeft op de toeleveringsketen van ICT door 2/3 van de respondenten hoger wordt gescoord dan het basis CMM-niveau en dat maatregel 1.4 door ruim 1/3 van de respondenten hoger wordt gescoord dan het basis CMM-niveau. Vooral maatregel 1.16 valt op; kennelijk is er veel aandacht voor ketenbeveiliging. De maatregel scoort gemiddeld 2,5 en de mediaan komt zelfs op 3,0 uit. De hoger scorende maatregelen uit cluster 3 (3.7 en 3.15) zijn meer voor de hand liggende maatregelen die IT-afdelingen altijd al hebben genomen.

Maatregel 1.14
Voor maatregel 1.14 uit cluster 1 *"De eisen die verband houden met informatiebeveiliging zijn opgenomen in de eisen voor nieuwe informatiesystemen en voor uitbreidingen van bestaande informatiesystemen."* scoren 8 van de 21 (38%) van de respondenten hoger.

Maatregel 1.16
Voor maatregel 1.16 uit cluster 1 *"Overeenkomsten met leveranciers bevatten eisen die betrekking hebben op de informatiebeveiligingsrisico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie."* scoren 13 van de 21 (62%) van de respondenten hoger.

Maatregel 3.7
Voor maatregel 3.7 uit cluster 3 *"Voor het werken in beveiligde gebieden zijn procedures ontwikkeld en deze worden toegepast."* scoren 8 van de 21 (38%) van de respondenten hoger.

Maatregel 3.15
Voor maatregel 3.15 (cluster 3) *"De klokken van alle relevante informatie verwerkende systemen binnen een organisatie of beveiligingsdomein worden gesynchroniseerd met één referentietijdbron."* scoren 12 van de 21 respondenten (57%) hoger.

2.3.2. Maatregelen met basis CMM-niveau 3

Hier zijn de hoger scorende maatregelen ook standaard IT-maatregelen. Iedere instelling beschermt apparatuur met een UPS (of anderszins), heeft antivirus maatregelen genomen en maakt back-ups.

Maatregel 3.10
Voor maatregel 3.10 uit cluster 3 *"Apparatuur is beschermd tegen stroomuitval en andere storingen door onderbreking van nutsvoorzieningen."* scoren 6 van de 21 (29%) van de respondenten hoger.

Maatregel 4.3
Voor maatregel 4.3 uit cluster 4 *"Ter bescherming tegen malware zijn beheersmaatregelen voor detectie, preventie en herstel geïmplementeerd."* scoren ook 6 van de 21 (29%) van de respondenten hoger.

Maatregel 4.5
En ook voor maatregel 4.5 uit cluster 4 *"Regelmatig worden back-up kopieën van informatie, software en systeemafbeeldingen gemaakt."* scoren 6 van de 21 (29%) van de respondenten hoger.

3. Cyberdreigingsbeeld 2017

In het *Cyberdreigingsbeeld 2017 – sector onderwijs en onderzoek*[6] zijn zeven dreigingen onderkend die relevant zijn voor de sector onderwijs en onderzoek:

Type Dreiging	**Manifestatie van dreiging**	**Risico**		
Type Dreiging	Gebeurtenis	Onderwijs	Onderzoek	Bedrijfsvoering
1. Verkrijging en openbaarmaking van data	• Onderzoeksgegevens worden gestolen • Privacygevoelige informatie wordt gelekt en gepubliceerd • Blauwdruk van opstelling onderzoeksinstellingen komt in verkeerde handen • Fraude door verkrijgen van data over toetsen en opgaven	MIDDEN	HOOG	HOOG
2. Identiteitsfraude	• Student laat iemand anders examen maken • Student doet zich voor als andere student of medewerker om inzage te krijgen in tentamens • Activist doet zich voor als onderzoeker • Student doet zich voor als medewerker en manipuleert studieresultaten	HOOG	MIDDEN	LAAG
3. Verstoring ICT	• DDoS-aanval legt IT-infrastructuur plat • Kritieke onderzoeksdata of examendata worden vernietigd • Opzet van onderzoeksinstellingen wordt gesaboteerd • Onderwijsmiddelen worden onbruikbaar door malware (bijvoorbeeld eLearning of het netwerk)	MIDDEN	MIDDEN	MIDDEN
4. Manipulatie van digitaal opgeslagen data	• Studieresultaten worden vervalst • Manipulatie van onderzoeksgegevens • Aanpassing van bedrijfsvoering data	HOOG	LAAG	LAAG
5. Spionage	• Onderzoeksgegevens worden afgetapt • Via een derde partij wordt intellectueel eigendom gestolen • Controleren van buitenlandse studenten door staten	LAAG	HOOG	LAAG
6. Overname en misbruik ICT	• Opstelling van onderzoeksinstellingen overgenomen • Systemen of accounts worden misbruikt voor andere doeleinden (botnet, mining, spam)	LAAG	MIDDEN	MIDDEN
7. Bewust beschadigen imago	• Website wordt beklad • Social media account wordt gehackt	LAAG	LAAG	LAAG

Tabel 9: relevante dreigingen voor de sector onderwijs en onderzoek

Cluster 2 – *Personeel, gasten en studenten* en cluster 6 – *Controle en logging* scoren het laagst in deze benchmark. Dat heeft invloed op de dreigingen uit het Cyberdreigingsbeeld die gemitigeerd zouden kunnen worden met maatregelen uit die clusters.

“Manipulatie van digitaal opgeslagen data” is een dreiging met een hoog risico voor het onderwijsproces. Maatregelen om dat risico te verminderen zijn onder meer het beheer van identiteiten en toegangsrechten uit cluster 2, en het controleren van toegangsrechten van gebruikers en het verzamelen van loggegevens uit cluster 6. Deze maatregelen scoren in het algemeen laag, waarmee deze dreiging in beperkte mate wordt tegengegaan.

[6] https://www.surf.nl/binaries/content/assets/surf/nl/kennisbank/2017/201712_surf_cyberdreigingsbeeld_2017.pdf

Hetzelfde geldt voor “Identiteitsfraude”. Deze dreiging wordt onder andere verminderd door maatregelen uit cluster 2 en cluster 6 die betrekking hebben op beheer van identiteiten en toegangsrechten en de controle daarop. Verder is bewustwording (cluster 2) belangrijk om de risico’s op het gebied van identiteitsfraude onder de aandacht van medewerkers en studenten te brengen.

“Verkrijging en openbaarmaking van data” is een van de dreigingen met een hoog risico voor onderzoek. De maatregelen uit cluster 2 om dit risico te mitigeren zijn het beheer van identiteiten en toegangsrechten en ook bewustwording. Door de lage score in dit cluster blijft dit risico hoog.
Daarnaast wordt “spionage” als een dreiging met een hoog risico gezien voor onderzoek. Omdat dit risico moeilijk valt te kwantificeren zijn bewustwording (cluster 2) en logging (cluster 6) van groot belang. De lage score voor deze maatregelen maakt dat spionage een moeilijk grijpbare dreiging is, waarvan het risico hoog blijft.

Voor de bedrijfsvoering is ook weer “verkrijging en openbaarmaking van data” een dreiging met een hoog risico. De impact van manifestatie van dit risico is wellicht nog hoger geworden nu de AVG[7] van kracht is geworden. Vooral bewustwording (cluster 2) is hier belangrijk, maar ook het beheer van identiteiten en toegangsrechten (cluster 2) en logging (cluster 6) spelen een belangrijke rol om dit risico te verlagen.

[7] Algemene Verordening Gegevensbescherming, die vanaf 25 mei 2018 van kracht is en hoge boetes mogelijk maakt wanneer organisaties persoonsgegevens die verwerkt worden, niet goed beschermen.

4. Overzicht beheersmaatregelen – status ten opzichte van de baseline

Legenda: score is significant onder de baseline (--), onder de baseline (-), gelijk aan de baseline (=) of beter dan de baseline (+)

4.1. Cluster 1: Beleid & Organisatie

1.1	Ten behoeve van informatiebeveiliging is een reeks beleidsregels gedefinieerd en goedgekeurd door de directie.	-
1.2	De beleidsregels voor informatiebeveiliging zijn gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	--
1.3	Het beleid voor informatiebeveiliging wordt met geplande tussenpozen of als zich significante veranderingen voordoen, beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.	--
1.4	Alle verantwoordelijkheden bij informatiebeveiliging zijn gedefinieerd en toegewezen.	-
1.5	Informatiebeveiliging komt aan de orde in projectbeheer, ongeacht het soort project.	-
1.6	Beleid en ondersteunende beveiligingsmaatregelen zijn vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.	--
1.7	Informatie is geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.	-
1.8	Om informatie te labelen is een passende reeks procedures ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	-
1.9	Ter bescherming van informatie is een beleid voor het gebruik van cryptografische beheersmaatregelen ontwikkeld en geïmplementeerd.	--
1.10	Ter bescherming van informatie zijn er tools of applicaties aanwezig waarmee het beleid voor het gebruik van cryptografische beheersmaatregelen wordt geïmplementeerd.	--
1.11	Apparatuur, informatie en software wordt niet zonder toestemming vooraf van de locatie meegenomen.	+
1.12	Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, zijn formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht.	-
1.13	Er zijn overeenkomsten vastgesteld voor het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.	-
1.14	De eisen die verband houden met informatiebeveiliging zijn opgenomen in de eisen voor nieuwe informatiesystemen en voor uitbreidingen van bestaande informatiesystemen.	+
1.15	Alle relevante informatiebeveiligingseisen zijn vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt.	+

1.16	Overeenkomsten met leveranciers bevatten eisen die betrekking hebben op de informatiebeveiligingsrisico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie.	+
1.17	Directieverantwoordelijkheden en -procedures zijn vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.	-
1.18	Informatiebeveiligingsgebeurtenissen worden zo snel mogelijk via de juiste leidinggevende niveaus gerapporteerd.	-
1.19	Registraties worden in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.	-
1.20	Privacy en bescherming van persoonsgegevens worden, voor zover van toepassing, gewaarborgd in overeenstemming met relevante wet- en regelgeving.	-
1.21	Conflicterende taken en verantwoordelijkheden zijn gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.	-

4.2. Cluster 2: Personeel, studenten en gasten

2.1	De contractuele overeenkomst met medewerkers en contractanten vermeldt hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie.	-
2.2	Alle medewerkers van de organisatie en, voor zover relevant, contractanten krijgen een passende bewustzijnsopleiding en -training en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.	--
2.3	De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten worden bij beëindiging van hun dienstverband, contract of overeenkomst verwijderd, en bij wijzigingen worden ze aangepast.	-
2.4	Er is een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen' beleid voor informatie verwerkende faciliteiten ingesteld.	-
2.5	Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen, zijn vastgesteld en worden regelmatig beoordeeld en gedocumenteerd.	-
2.6	Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie wordt geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.	-
2.7	Verificatie van de achtergrond van alle kandidaten voor een dienstverband wordt uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en staat in verhouding tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's.	--

4.3. Cluster 3: Ruimtes & apparatuur

3.1	Er dienen beveiligingsmaatregelen te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beperken.	-

3.2	Media worden overeenkomstig formele procedures op een veilige en beveiligde manier verwijderd als ze niet langer nodig zijn.	-
3.3	Beveiligingszones zijn gedefinieerd en worden gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatie verwerkende faciliteiten bevatten.	-
3.4	Beveiligde gebieden zijn beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	-
3.5	Voor kantoren, ruimten en faciliteiten is fysieke beveiliging ontworpen en deze wordt toegepast.	-
3.6	Tegen natuurrampen, kwaadwillige aanvallen of ongelukken is fysieke bescherming ontworpen en deze wordt toegepast.	-
3.7	Voor het werken in beveiligde gebieden zijn procedures ontwikkeld en deze worden toegepast.	+
3.8	Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, worden beheerst, en zo mogelijk afgeschermd van informatie verwerkende faciliteiten om onbevoegde toegang te vermijden.	+
3.9	Apparatuur is zodanig geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.	-
3.10	Apparatuur is beschermd tegen stroomuitval en andere storingen door onderbreking van nutsvoorzieningen.	+
3.11	Voedings- en telecommunicatiekabels die voor dataverkeer of ondersteunende informatiediensten worden gebruikt, zijn tegen interceptie of beschadiging beschermd.	-
3.12	Apparatuur wordt op correcte wijze onderhouden, om de continue beschikbaarheid en integriteit ervan te waarborgen.	-
3.13	Bedrijfsmiddelen die zich buiten het terrein bevinden worden beveiligd waarbij rekening wordt gehouden met de verschillende risico's van werken buiten het terrein van de organisatie.	-
3.14	Alle onderdelen van de apparatuur die opslagmedia bevatten, worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven.	-
3.15	De klokken van alle relevante informatie verwerkende systemen binnen een organisatie of beveiligingsdomein worden gesynchroniseerd met één referentietijdbron.	+

4.4. Cluster 4: Continuïteit

4.1	Veranderingen in de organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging worden beheerst.	-
4.2	Ontwikkel-, test- en productieomgevingen zijn gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.	-
4.3	Ter bescherming tegen malware zijn beheersmaatregelen voor detectie, preventie en herstel geïmplementeerd.	+
4.4	Er zijn geschikte procedures ingevoerd om het bewustzijn van de gebruikers omtrent bescherming tegen malware te vergroten.	-

4.5	Regelmatig worden back-up kopieën van informatie, software en systeemafbeeldingen gemaakt.	+
4.6	Gemaakte back-ups worden regelmatig getest conform het overeengekomen back-up beleid.	-
4.7	Om het op operationele systemen installeren van software te beheersen zijn procedures geïmplementeerd.	-
4.8	Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt wordt tijdig verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden wordt geëvalueerd en er worden passende maatregelen genomen om het risico dat ermee samenhangt aan te pakken.	-
4.9	Voor het door gebruikers installeren van software zijn regels vastgesteld en geïmplementeerd.	-
4.10	Organisaties stellen beveiligde ontwikkelomgevingen vast en beveiligen deze passend voor verrichtingen op het gebied van systeemontwikkeling en integratie, die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling.	+
4.11	Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging worden beheerd, rekening houdend met de kritikaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's.	-
4.12	Informatiebeveiligingsgebeurtenissen worden beoordeeld en er wordt geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten.	-
4.13	Op informatiebeveiligingsincidenten wordt gereageerd in overeenstemming met de gedocumenteerde procedures.	-
4.14	De organisatie heeft processen, procedures en beheersmaatregelen vastgesteld, gedocumenteerd en geïmplementeerd om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen en handhaaft deze.	-
4.15	Informatie verwerkende faciliteiten worden met voldoende redundantie geïmplementeerd om aan beschikbaarheidseisen te voldoen.	-

4.5. Cluster 5: Toegangsbeveiliging & integriteit

5.1	Een beleid voor toegangsbeveiliging is vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.	-
5.2	Gebruikers krijgen alleen toegang tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.	-
5.3	Een formele registratie- en afmeldingsprocedure is geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	+
5.4	Een formele gebruikerstoegangsverleningsprocedure is geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.	-
5.5	De toewijzing en het gebruik van speciale bevoegdheden zijn beperkt en worden beheerst.	-

5.6	Het toewijzen van geheime authenticatie-informatie wordt beheerst via een formeel beheersproces.	-
5.7	Van gebruikers wordt verlangd dat zij zich bij het gebruiken van geheime authenticatie-informatie houden aan de praktijk van de organisatie.	-
5.8	Toegang tot informatie en systeemfuncties van toepassingen is beperkt in overeenstemming met het beleid voor toegangsbeveiliging.	-
5.9	Indien het beleid voor toegangsbeveiliging dit vereist, wordt toegang tot systemen en toepassingen beheerst door een beveiligde inlogprocedure.	-
5.10	Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels tijdens hun gehele levenscyclus is een beleid ontwikkeld en geïmplementeerd.	-
5.11	Er wordt gebruik gemaakt van tools om cryptografische sleutels tijdens hun gehele levenscyclus adequaat te beheren.	-
5.12	Logfaciliteiten en informatie in logbestanden worden beschermd tegen vervalsing en onbevoegde toegang.	--
5.13	Netwerken worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	-
5.14	Beveiligingsmechanismen, dienstverleningsniveaus en beheer eisen voor alle netwerkdiensten zijn geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.	-
5.15	Groepen van informatiediensten, -gebruikers en -systemen zijn op netwerken gescheiden.	-
5.16	Informatie die is opgenomen in elektronische berichten wordt passend beschermd.	-
5.17	Informatie die deel uitmaakt van transacties van toepassingen wordt beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.	-

4.6. Cluster 6: Controle & logging

6.1	Eigenaren van bedrijfsmiddelen beoordelen toegangsrechten van gebruikers regelmatig.	-
6.2	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, worden gemaakt, bewaard en regelmatig beoordeeld.	-
6.3	Activiteiten van systeembeheerders en -operators worden vastgelegd en de logbestanden worden beschermd en regelmatig beoordeeld.	--
6.4	Uitbestede systeemontwikkeling staat onder supervisie van en wordt gemonitord door de organisatie.	-
6.5	Tijdens ontwikkelactiviteiten wordt de beveiligingsfunctionaliteit getest.	--
6.6	Voor nieuwe informatiesystemen, upgrades en nieuwe versies worden programma's voor het uitvoeren van acceptatietests en gerelateerde criteria vastgesteld.	-
6.7	Organisaties monitoren, beoordelen en auditen regelmatig de dienstverlening van leveranciers.	--
6.8	De organisatie heeft procedures gedefinieerd voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen en past deze toe.	--
6.9	De directie beoordeelt regelmatig de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	-
6.10	Informatiesystemen worden regelmatig beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.	-

4.7. Conclusie

4.7.1. Aantal deelnemers

In 2017 hebben 21 instellingen meegedaan met de SURFaudit-benchmark, 3 meer dan in 2015, maar 4 minder dan in 2013. De doelstelling van 40 deelnemende instellingen is in 2017 nog niet behaald.

4.7.2. Veel scores nog onder baseline

Bij de benchmark 2017 zijn de scores voor ieder cluster nog onder de baseline uitgekomen. In vergelijking met de benchmark 2015, zijn de resultaten voor 2017 in cluster 1, 2, 4 en 5 hoger en voor de clusters 3 en 6 lager uitgekomen.

4.7.3. Cluster 3 en cluster 6

Cluster 3 en cluster 6 zijn verslechterd ten opzichte van de benchmark 2015.

De minst scorende maatregelen in cluster 3 (3.1 en 3.13) hebben betrekking op mobiele apparatuur en gebruik van apparatuur buiten de organisatie. Kennelijk is de controle op mobiele apparaten verminderd of is men zich meer bewust geworden van de risico's, waardoor deze maatregelen strenger beoordeeld worden.

De laagst scorende maatregelen in cluster 6 (6.5 en 6.8) hebben betrekking op het testen van beveiligingsfunctionaliteit bij het ontwikkelen van software respectievelijk het verzamelen van bewijsmateriaal tijdens een forensisch onderzoek. Voor beide maatregelen geldt dat veel respondenten ze op CMM-niveau 1 of 2 scoren, dus kennelijk zijn ze nog niet ingebed in de organisatie.

Heel cluster 6 scoorde altijd al significant onder de baseline en behoeft meer aandacht van SURF en de instellingen.

4.7.4. Aantal maatregelen scoren boven baseline

Een aantal maatregelen scoort hoger dan de baseline. De meeste daarvan zijn maatregelen die van oudsher al door de IT-afdelingen worden uitgevoerd, zoals de uitrol van antivirussoftware en het maken van back-ups.

4.7.5. Vooruitblik naar 2019

Op grond van de gezamenlijk uitgesproken intentie van de instellingen om informatieveiligheid op een hoger plan te brengen zouden meer instellingen aan de benchmark moeten meedoen. Dan ontstaat een representatiever beeld hoe we er als sector voor staan. Zowel SURF als SCIPR moeten daarvoor stappen zetten; de *maturitywerkgroep* zal hiervoor ideeën aandragen. De over het algemeen lichte stijging van de scores is positief, maar een aantal clusters scoort lager dan voorheen. Die moeten meer aandacht krijgen de komende tijd.

Enkele security officers hebben aangegeven dat, naarmate ze vaker meedoen, ze ook strenger gaan scoren. Dit verklaart ten dele de lagere score van sommige maatregelen bij een aantal instellingen. Verder moet de scope van de benchmark duidelijker gedefinieerd worden, zodat de instellingen hetzelfde meten en de onderlinge resultaten beter vergelijkbaar zijn. Ook peerreview kan daaraan een bijdrage leveren door de kwaliteit en consistentie van de beoordeling te verhogen.

In de loop van 2018 zal de benchmark tool in productie worden genomen, waarmee het uitvoeren van benchmarks minder tijd in beslag zal nemen, de resultaten sneller verwerkt kunnen worden en de ondersteuning voor peerreviews veel beter zal zijn.

Bijlage Mediaanscore

Mediaan en gemiddelde zijn twee manieren om een algemeen beeld te krijgen van hoe een groep als geheel scoort.

Gemiddelde

- Instelling A: 5
- Instelling B: 4,5
- Instelling C: 3
- Instelling D: 4
- Instelling E: 3,5
- Instelling F: 4
- Instelling G: 4

Tel alle individuele scores bij elkaar op en deel door het aantal.

Het totaal van de 7 instellingen is 28, dus het gemiddelde is 28 / 7 = 4.

Stel dat instelling D heel laag heeft gescoord, bijvoorbeeld 1, dan zakt het gemiddelde naar 25 / 7 = 3,6. Hiermee heeft één behoorlijk afwijkende score in deze (relatief kleine) groep dus een flink effect op het gemiddelde (10% lager).

Mediaan

Zet alle scores in een opklimmende reeks en bepaal welke waarde in het midden ligt, zodat er evenveel scores lager als hoger zijn dan deze mediaan:

3 – 3,5 – 4 – **4** – 4 – 4,5 – 5 → de middelste 4 is de mediaanscore.

Als instelling D een 1 scoort in plaats van 4, wordt het opklimmende rijtje 1 – 3 – 3,5 – **4** – 4 – 4,5 – 5. De mediaanscore blijft 4, want er zijn nog steeds evenveel scores hoger als lager dan 4.

Het effect van één instelling die behoorlijk afwijkt van de rest van de groep, de uitschieter, is zo uit het groepsbeeld geëlimineerd.