NETWERK IBP IN HET MBO

Kennisnet SURF saMBO-ICT

Benchmark IBP-E 2021

resultaten van de de onderdelen Informatiebeveiliging, Privacy en Examinering, bespreking van de Peer review 2021 en de pilot met het nieuwe toetsingskader Informatiebeveiliging volgens het NBA-model

10 december 2021

Resultaten Benchmark IBP-E 2021

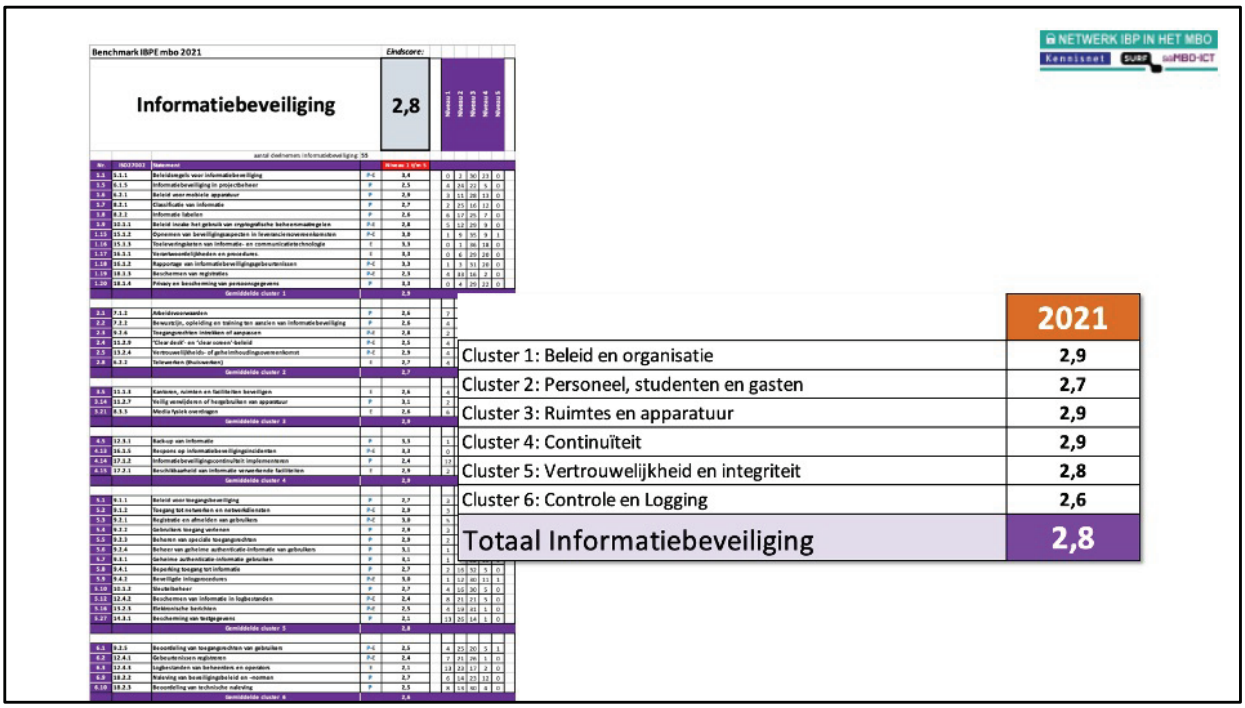
	2015	2016	2017	2018	2019	2020	2021
Cluster 1: Beleid en organisatie	1,7	1,8	2,0	2,4	2,6	2,9	**2,9**
Cluster 2: Personeel, studenten en gasten	1,7	1,7	1,9	2,3	2,3	2,6	**2,7**
Cluster 3: Ruimtes en apparatuur	2,1	2,2	2,3	2,5	2,6	2,9	**2,9**
Cluster 4: Continuïteit	2,0	2,1	2,3	2,5	2,6	2,8	**2,9**
Cluster 5: Vertrouwelijkheid en integriteit	2,0	2,0	2,2	2,4	2,4	2,8	**2,8**
Cluster 6: Controle en Logging	1,6	1,6	1,8	2,1	2,1	2,4	**2,6**
Totaal score Informatiebeveiliging	1,9	1,9	2,1	2,4	2,5	2,8	**2,8**
Totaal score Privacy (Pluscluster 7)	-	1,5	1,9	2,3	2,5	2,8	**2,9**
Totaal score Examinering (Pluscluster 8)	-	-	-	2,1	2,5	2,8	**2,8**
Percentage deelnemende instellingen	**29%**	**46%**	**77%**	**95%**	**95%**	**97%**	**98%**

De resultaten van Benchmark IBP-E 2021

Sinds 2015 meet de mbo-sector de volwassenheid van de informatiebeveiliging met een zelfassessment. Daarvoor gebruiken de instellingen een toetsingskader dat in de onderwijssector is ontwikkeld en gebaseerd is op de ISO 27001-norm voor informatiebeveiliging. In 2016 is een toetsingskader voor privacy toegevoegd en sinds 2018 wordt ook de volwassenheid op het gebied van (digitale) examinering gemeten. Het toetsingskader Informatiebeveiliging bevat 101 statements, verdeeld over 6 clusters. Het onderdeel Privacy telt 21 statements en het onderdeel Examinering bestaat uit 18 statements, die vooral te maken hebben met de digitale aspecten van de examinering.

De volwassenheid wordt gemeten aan de hand van het Capability Maturity Model. Dit model meet de volwassenheid op een schaal van 1 tot 5. De sector heeft afgesproken dat 2 het minimaal wenselijke niveau is en niveau 3 het ambitieniveau. Niveau 3 wordt in het algemeen beschouwd als een goede balans tussen veiligheid en kosten van de informatiebeveiliging.

In 2021 heeft 98% van de mbo's deelgenomen aan deze benchmark. Ze komen gemiddeld genomen voor elk van de drie onderdelen dicht in de buurt van het ambitieniveau van 3.0.



Scores van de zes clusters Informatiebeveiliging

De 101 statements uit het toetsingskader Informatiebeveiliging zijn onderverdeeld in zes clusters. Cluster 1 gaat vooral over beleidsmaatregelen, cluster 2 over personele aspecten, cluster 3 over ruimten en apparatuur, cluster 4 over continuïteit van de ict-infrastructuur, cluster 5 over toegangsbeveiliging en de betrouwbaarheid van de gegevens en cluster 6 over controle en logging.

Vergeleken met vorig jaar zien we een bescheiden groei in de clusters 2, 4 en 6, waarbij de onderlinge verschillen minder groot worden, met name cluster 6; controle en logging trekt iets bij.

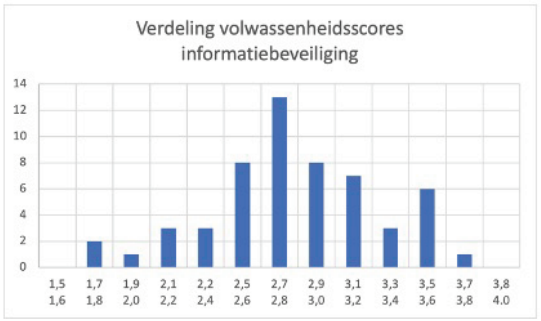
Grote verschillen in volwassenheid IB

Top 10

Cluster 1: Beleid en organisatie	3,7
Cluster 2: Personeel, studenten en gasten	3,4
Cluster 3: Ruimtes en apparatuur	3,5
Cluster 4: Continuïteit	3,5
Cluster 5: Vertrouwelijkheid en integriteit	3,5
Cluster 6: Controle en Logging	3,1
Informatiebeveiliging totaal	**3,5**

Laatste 10

Cluster 1: Beleid en organisatie	2,3
Cluster 2: Personeel, studenten en gasten	2,0
Cluster 3: Ruimtes en apparatuur	2,1
Cluster 4: Continuïteit	2,2
Cluster 5: Vertrouwelijkheid en integriteit	2,1
Cluster 6: Controle en Logging	2,0
Informatiebeveiliging totaal	**2,1**



Grote verschillen in volwassenheid binnen het onderdeel Informatiebeveiliging
Als we kijken naar de verdeling van de scores binnen het onderdeel informatiebeveiliging dan zien we grote verschillen in volwassenheid: de top 10 scoort gemiddeld een volwassenheidsniveau van 3,5 en de laatste 10 een 2,1 gemiddeld. De modus, de meest voorkomende waarde is een 2,8. Twee instellingen halen het minimum van 2 niet en 21 van de 55 instellingen voldoen aan het binnen de sector overeengekomen ambitieniveau van 3,0

Benchmark IBPE mbo 2021

Privacy

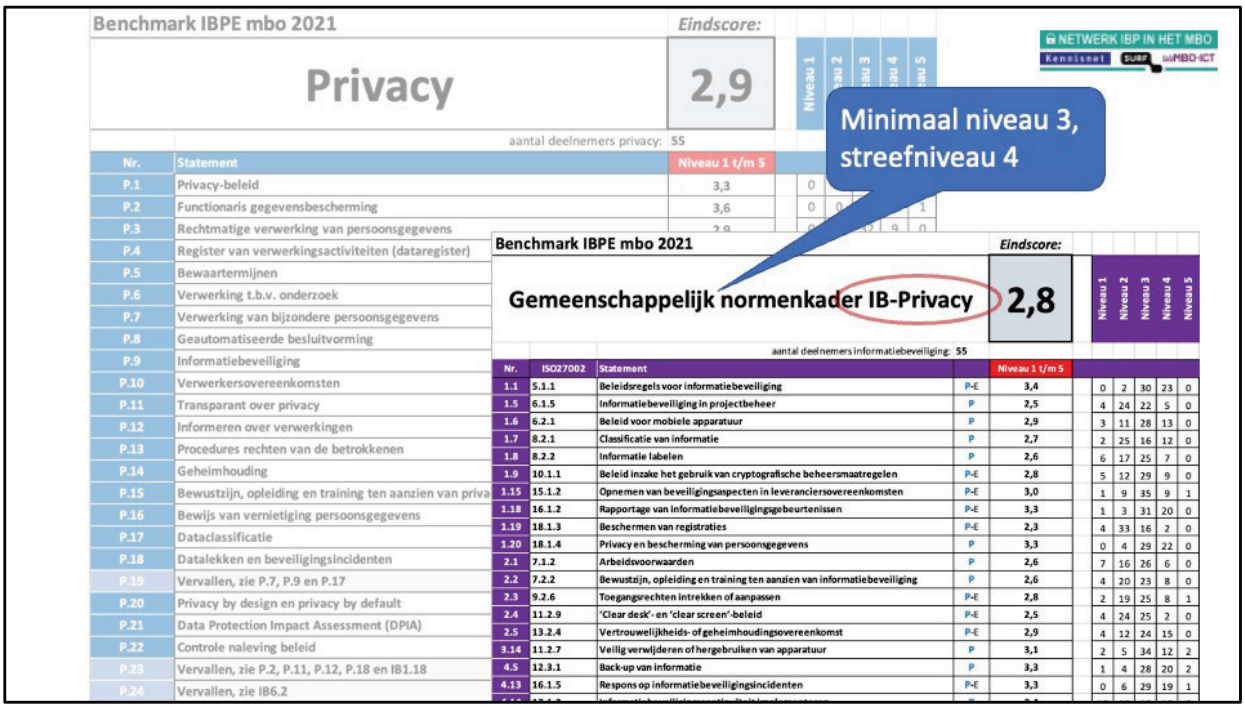
Eindscore: **2,9**

aantal deelnemers privacy: 55

Nr.	Statement	Niveau 1 t/m 5	Niveau 1	Niveau 2	Niveau 3	Niveau 4	Niveau 5
P.1	Privacy-beleid	3,3	0	4	29	21	1
P.2	Functionaris gegevensbescherming	3,6	0	0	22	32	1
P.3	Rechtmatige verwerking van persoonsgegevens	2,9	0	14	32	9	0
P.4	Register van verwerkingsactiviteiten (dataregister)	2,9	0	17	28	9	1
P.5	Bewaartermijnen	2,3	1	35	18	1	0
P.6	Verwerking t.b.v. onderzoek	2,4	13	14	23	5	0
P.7	Verwerking van bijzondere persoonsgegevens	2,7	5	14	28	8	0
P.8	Geautomatiseerde besluitvorming	2,7	9	8	30	8	0
P.9	Informatiebeveiliging	2,8	4	13	29	9	0
P.10	Verwerkersovereenkomsten	3,1	0	8	32	15	0
P.11	Transparant over privacy	3,1	0	10	31	14	0
P.12	Informeren over verwerkingen	2,9	0	15	28	12	0
P.13	Procedures rechten van de betrokkenen	3,0	0	12	32	11	0
P.14	Geheimhouding	2,8	2	19	20	14	0
P.15	Bewustzijn, opleiding en training ten aanzien van privacy	2,7	1	18	32	4	0
P.16	Bewijs van vernietiging persoonsgegevens	2,9	1	12	31	11	0
P.17	Dataclassificatie	2,9	1	14	30	10	0
P.18	Datalekken en beveiligingsincidenten	3,4	0	3	27	23	0
P.19	Vervallen, zie P.7, P.9 en P.17						
P.20	Privacy by design en privacy by default	2,6	3	20	29	3	0
P.21	Data Protection Impact Assessment (DPIA)	2,6	2	22	29	2	0
P.22	Controle naleving beleid	3,1	0	13	26	16	0
P.23	Vervallen, zie P.2, P.11, P.12, P.18 en IB1.18						
P.24	Vervallen, zie IB6.2						

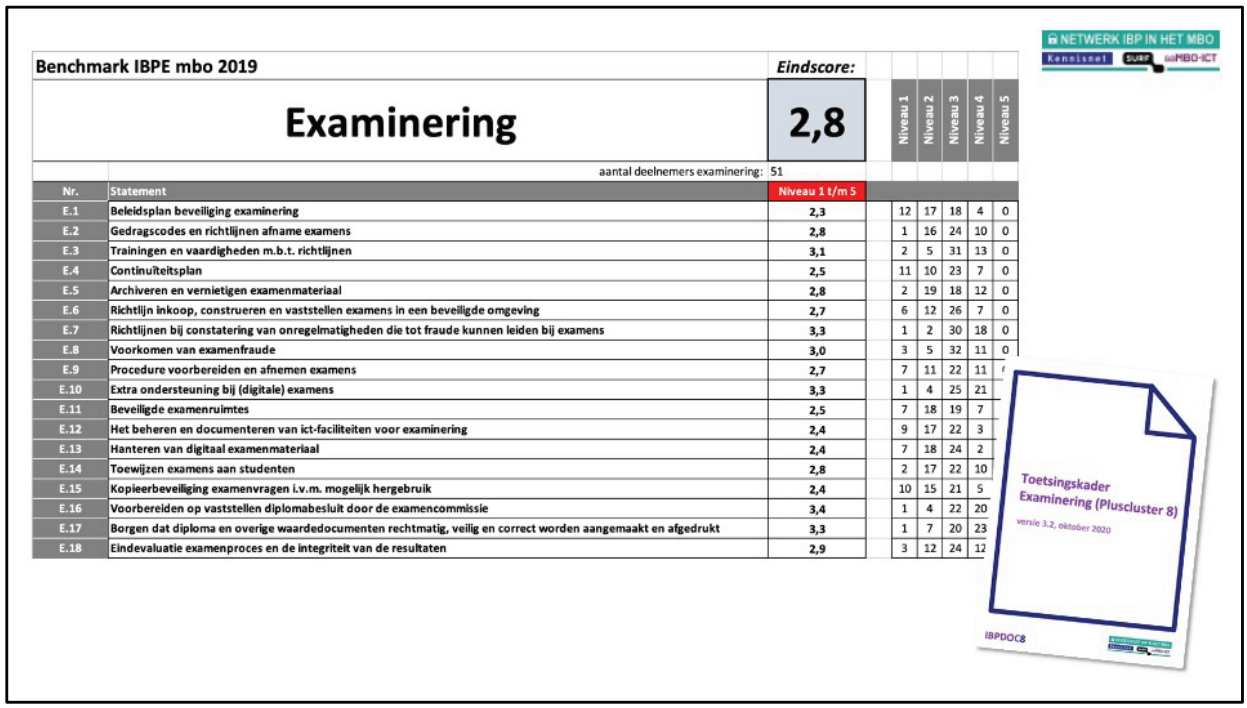
Resultaten cluster Privacy

Het onderdeel Privacy wordt beoordeeld aan de hand van het in de eigen sector ontwikkelde toetsingskader Privacy. Dit cluster bevat 21 statements met betrekking tot de volwassenheid van de organisatie op het gebied van privacymanagement. De score voor het Privacycluster stijgt gemiddeld licht ten opzichte van 2020, van 2,8 naar 2,9. Een belangrijk statement als P.5, met betrekking tot de bewaartermijnen blijft nog steeds achter. De meerderheid scoort dit statement op niveau 2, wat erop duidt dat er wel beleid is (aan de hand van een documentair structuur plan bijvoorbeeld) maar dat het daardwerkelijk naleven van dat beleid nog niet goed lukt.



Gemeenschappelijk normenkader IB - Privacy

In het toetsingskader Informatiebeveiliging zijn een aantal statements gemarkeerd als extra relevant voor de bescherming van de privacy. We noemen dat het gemeenschappelijk normenkader IB en Privacy en je zou willen dat de volwassenheid voor deze statements minimaal op 3 maar bij voorkeur op 4 zou uitkomen. Maar dat zien we in de resultaten niet terug, integendeel: deze voor de bescherming van de privacy belangrijke statements scoren hetzelfde als de gehele set van IB-statements.



Benchmark IBPE mbo 2019

Examinering

Eindscore: **2,8**

aantal deelnemers examinering: 51

Nr.	Statement	Niveau 1 t/m 5	Niveau 1	Niveau 2	Niveau 3	Niveau 4	Niveau 5
E.1	Beleidsplan beveiliging examinering	2,3	12	17	18	4	0
E.2	Gedragscodes en richtlijnen afname examens	2,8	1	16	24	10	0
E.3	Trainingen en vaardigheden m.b.t. richtlijnen	3,1	2	5	31	13	0
E.4	Continuïteitsplan	2,5	11	10	23	7	0
E.5	Archiveren en vernietigen examenmateriaal	2,8	2	19	18	12	0
E.6	Richtlijn inkoop, construeren en vaststellen examens in een beveiligde omgeving	2,7	6	12	26	7	0
E.7	Richtlijnen bij constatering van onregelmatigheden die tot fraude kunnen leiden bij examens	3,3	1	2	30	18	0
E.8	Voorkomen van examenfraude	3,0	3	5	32	11	0
E.9	Procedure voorbereiden en afnemen examens	2,7	7	11	22	11	
E.10	Extra ondersteuning bij (digitale) examens	3,3	1	4	25	21	
E.11	Beveiligde examenruimtes	2,5	7	18	19	7	
E.12	Het beheren en documenteren van ict-faciliteiten voor examinering	2,4	9	17	22	3	
E.13	Hanteren van digitaal examenmateriaal	2,4	7	18	24	2	
E.14	Toewijzen examens aan studenten	2,8	2	17	22	10	
E.15	Kopieerbeveiliging examenvragen i.v.m. mogelijk hergebruik	2,4	10	15	21	5	
E.16	Voorbereiden op vaststellen diplomabesluit door de examencommissie	3,4	1	4	22	20	
E.17	Borgen dat diploma en overige waardedocumenten rechtmatig, veilig en correct worden aangemaakt en afgedrukt	3,3	1	7	20	23	
E.18	Eindevaluatie examenproces en de integriteit van de resultaten	2,9	3	12	24	12	

NETWERK IBP IN HET MBO

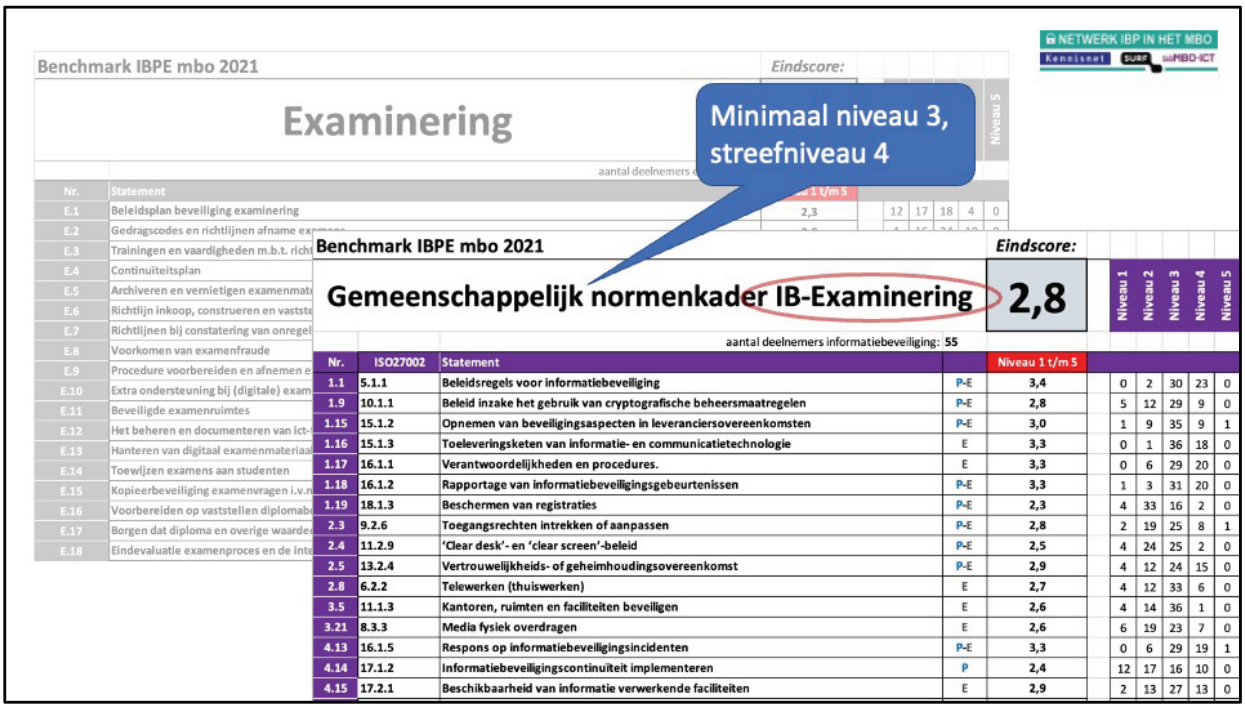
Toetsingskader Examinering (Pluscluster 8)

versie 3.2, oktober 2020

IBPDOC8

Resultaten cluster Examinering

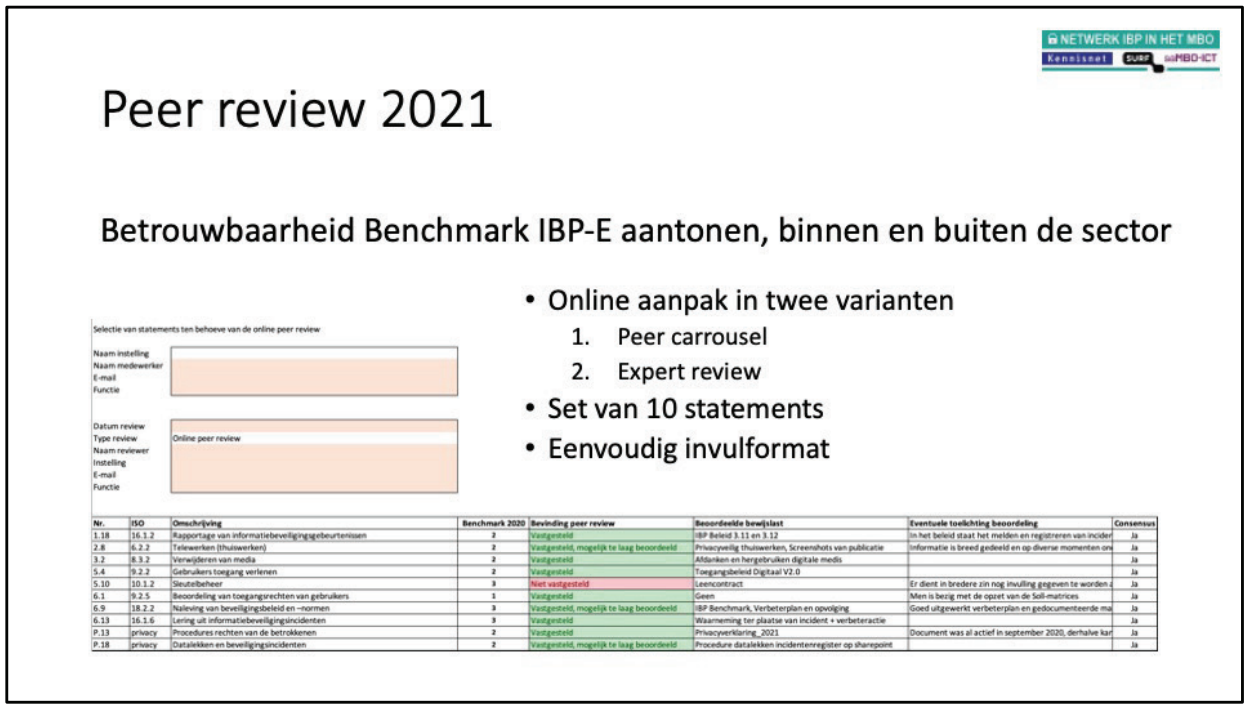
Sinds 2018 scoort de mbo-sector ook de volwassenheid van digitale aspecten van de examinering. Aan dit onderdeel hebben 51 van de 55 benchmarkinvullers meegedaan. In veel instellingen ontbreekt een beleidsplan voor de beveiliging van het (digitale) examineringsproces, waarbij aangetekend moet worden dat dit beleid deels ook kan zijn meegenomen in bijvoorbeeld het handboek examinering. Andere statements die wat achter blijven hebben te maken met het hebben van een continuiteitsplan (E.4), met het planmatig omgaan met ict-faciliteiten (E.12) en het hanteren van digitaal examenmateriaal (E.13), inclusief de beveiliging tegen kopieren van digitaal examenmateriaal (E.15).



Nr.	ISO27002	Statement		Niveau 1 t/m 5	Niveau 1	Niveau 2	Niveau 3	Niveau 4	Niveau 5
1.1	5.1.1	Beleidsregels voor informatiebeveiliging	P-E	3,4	0	2	30	23	0
1.9	10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	P-E	2,8	5	12	29	9	0
1.15	15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	P-E	3,0	1	9	35	9	1
1.16	15.1.3	Toeleveringsketen van informatie- en communicatietechnologie	E	3,3	0	1	36	18	0
1.17	16.1.1	Verantwoordelijkheden en procedures.	E	3,3	0	6	29	20	0
1.18	16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	P-E	3,3	1	3	31	20	0
1.19	18.1.3	Beschermen van registraties	P-E	2,3	4	33	16	2	0
2.3	9.2.6	Toegangsrechten intrekken of aanpassen	P-E	2,8	2	19	25	8	1
2.4	11.2.9	'Clear desk'- en 'clear screen'-beleid	P-E	2,5	4	24	25	2	0
2.5	13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst	P-E	2,9	4	12	24	15	0
2.8	6.2.2	Telewerken (thuiswerken)	E	2,7	4	12	33	6	0
3.5	11.1.3	Kantoren, ruimten en faciliteiten beveiligen	E	2,6	4	14	36	1	0
3.21	8.3.3	Media fysiek overdragen	E	2,6	6	19	23	7	0
4.13	16.1.5	Respons op informatiebeveiligingsincidenten	P-E	3,3	0	6	29	19	1
4.14	17.1.2	Informatiebeveiligingscontinuïteit implementeren	P	2,4	12	17	16	10	0
4.15	17.2.1	Beschikbaarheid van informatie verwerkende faciliteiten	E	2,9	2	13	27	13	0

Gemeenschappelijk normenkader IB - Examinering

Ook voor het onderdeel Examinering geldt dat in het toetsingskader Informatiebeveiliging een aantal statements zijn gemarkeerd als extra relevant, in dit geval voor voor de bescherming van de digitale examinering. Voor dit gemeenschappelijk normenkader IB en Examinering zou de gemiddelde volwassenheid fors boven het overall streefniveau van 3,0 uit moeten komen. Dat zien we echter niet terug in de cijfers: het gemiddelde van deze set statements is gelijk aan het totaal voor informatiebeveiliging.



De peer review meet de betrouwbaarheid van de Benchmark IBP-E
De benchmark is een zelfassessment. Dit betekent dat onnauwkeurigheden kunnen ontstaan door verschillen in kennis en ervaring van de respondenten, de mate van aandacht waarmee ze het assessment doorlopen en interpretatieverschillen over de bewijslast voor de statements. Om zicht te krijgen op onnauwkeurigheden en er lering uit te trekken, en de betrouwbaarheid van de benchmark te onderbouwen voeren we een peer review uit, als logische vervolgstap op de Benchmark IBP-E.

Bij de peer review 2021 is de benchmark IBP van 2020 onderzocht aan de hand van een deelverzameling van 10 statements: 8 IB-statements en 2 statements uit het privacy cluster. De peer review is begin 2021 online uitgevoerd door 39 instellingen, in twee varianten:

1. peer carrousel;
   instelling A reviewt instelling B, B reviewt C enzovoort.
2. expert review;
   de beoordeling wordt uitgevoerd door een externe auditor, de instelling zelf voert geen audit uit.

Peer review 2021

- Op basis van de Benchmark IBP-E 2020
- 39 instellingen (23 peer reviews, 16 expert reviews)

Nr.	ISO	Omschrijving	Gem. score	% vastgesteld	% mogelijk te laag
1.18	16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	3,4	97	0
2.8	6.2.2	Telewerken (thuiswerken)	2,6	100	13
3.2	8.3.2	Verwijderen van media	3,1	90	10
5.4	9.2.2	Gebruikers toegang verlenen	2,9	90	8
5.10	10.1.2	Sleutelbeheer	2,6	92	10
6.1	9.2.5	Beoordeling van toegangsrechten van gebruikers	2,4	90	3
6.9	18.2.2	Naleving van beveiligingsbeleid en –normen	2,7	100	26
6.13	16.1.6	Lering uit informatiebeveiligingsincidenten	3,0	97	10
P.13	privacy	Procedures rechten van de betrokkenen	3,0	95	0
P.18	privacy	Datalekken en beveiligingsincidenten	3,4	97	5
		totaal	**2,9**	**95**	**8**

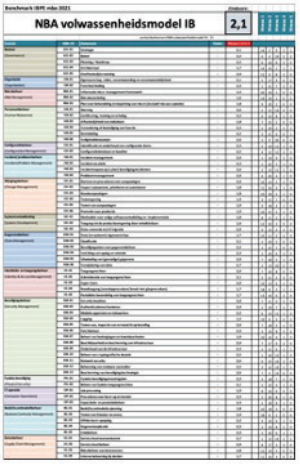
Conclusies Peer review 2021
De uitkomst van de peer review is dat 95% van de onderzochte statements kon worden vastgesteld. Bij 8% van de onderzochte statements gaf de reviewer aan dat op basis van de beoordeelde bewijs- last het statement mogelijk hoger beoordeeld had kunnen worden.
Deze uitkomsten zijn marginaal hoger dan de vorige editie, in 2020 werd 94% van de statements vastgesteld.

Daarmee kan worden onderbouwd dat de Benchmark IBP 2020 door de gereviewde instellingen correct werd ingevuld en het daarmee een bruikbaar instrument is om de volwassenheid op het gebied van IBP te meten.

NETWERK IBP IN HET MBO

NBA-volwassenheidsmodel Informatiebeveiliging

- Minder gericht op technische maatregelen
- Sterker gericht op de governance van de informatiebeveiliging
- Beter toegerust op huidige situatie met clouddiensten
- Risico-gebaseerde aanpak
- Geaccepteerd model (NOREA), dus mogelijkheid om interne/externe auditors te betrekken
- Model dient meerdere doelen
  - Instelling: handreiking, roadmap om te groeien in volwassenheid
  - Sector: als toetsingskader voor de benchmark IB
- We sluiten hiermee weer aan bij het HO en trekken weer samen op met SURF



Naar een nieuw toetsingskader voor Informatiebeveiliging

In 2021 is de discussie op gang gekomen om in navolging van het hoger onderwijs over te stappen op een nieuw toetsingskader voor informatiebeveiliging. Het gaat dan om het Volwassenheidsmodel voor Informatiebeveiliging dat is ontwikkeld door de Nederlandse Beroepsorganisatie voor Accountants (NBA). In het kort het NBA kader. Het is geen norm (zoals ISO 27001) maar een hulpmiddel voor interne- en externe auditors om de gewenste volwassenheid -gelet op de risico's- in kaart te brengen. Vervolgens wordt bepaald waar de organisatie staat en wat er moet gebeuren om het gewenste niveau van informatiebeveiliging te bereiken. Het is daarmee veel meer dan een toetsingskader voor de benchmark IB; het is voor de individuele instelling daarnaast ook een gids om beter in control te komen op het gebied van cyberveiligheid.

Om deze overstap te onderbouwen is in 2021 een pilot benchmark gedaan met het NBA-toetsingskader, daaraan hebben 31 mbo-instellingen deelgenomen. In december 2021 zijn in het Netwerk IBP de ervaringen met het NBA-model geëvalueerd en op basis daarvan zal in 2022 de overstap gemaakt worden naar het NBA-model als toetsingskader voor het onderdeel Informatiebeveiliging. Dit heeft verder geen invloed op de onderdelen Privacy en Examinering, die blijven in 2022 ongewijzigd.

Scores pilot NBA-toetsingskader IB

					2021
1	**Bestuur**	(Governance)	GO	5	**2,2**
2	**Organisatie**	(Organisation)	OR	2	**2,2**
3	**Risicobeheer**	(Risk Management)	RM	3	**1,6**
4	**Personeelsbeheer**	(Human Resources)	HR	6	**2,3**
5	**Configuratiebeheer**	(Configuration Management)	CO	2	**2,4**
6	**Incident/probleembeheer**	(Incident/Problem Management)	IM	4	**2,3**
7	**Wijzigingsbeheer**	(Change Management)	CH	6	**1,9**
8	**Systeemontwikkeling**	(System Development)	SD	3	**1,8**
9	**Gegevensbeheer**	(Data Management)	DM	6	**2,2**
10	**Identiteits- en toegangsbeheer**	(Identity & Access Management)	ID	5	**1,9**
11	**Beveiligingsbeheer**	(Security Management)	SM	13	**2,2**
12	**Fysieke beveiliging**	(Physical Security)	PH	2	**2,2**
13	**IT operatie**	(Computer Operations)	OP	3	**2,2**
14	**Bedrijfscontinuiteitbeheer**	(Business Continuity Management)	BC	5	**2,0**
15	**Ketenbeheer**	(Supply Chain Management)	SC	4	**2,1**
Totaal score NBA-toetsingskader Informatiebeveiliging					**2,1**

Percentage deelnemende instellingen (31)	**55%**

Vergelijking NBA met het huidige ISO-toetsingskader
Het is interessant om het NBA-model te vergelijken met het bestaande toetsingskader IB en daaraan gekoppeld de uitkomsten van de benchmark IB. De ervaring leert dat een derde van de NBA-statements zonder meer wordt afgedekt door bestaande bewijslast uit het huidige toetsingskader en voor een derde van de statements moet er aanvullend nog iets worden geregeld. De resterende een derde van de NBA-statements is nieuw en vraagt de komende tijd aandacht. Het gaat dan om de ‘blinde vlekken’ van het huidige ISO-gebaseerde kader op het gebied van governance, risicomanagement en leveranciersmanagement.

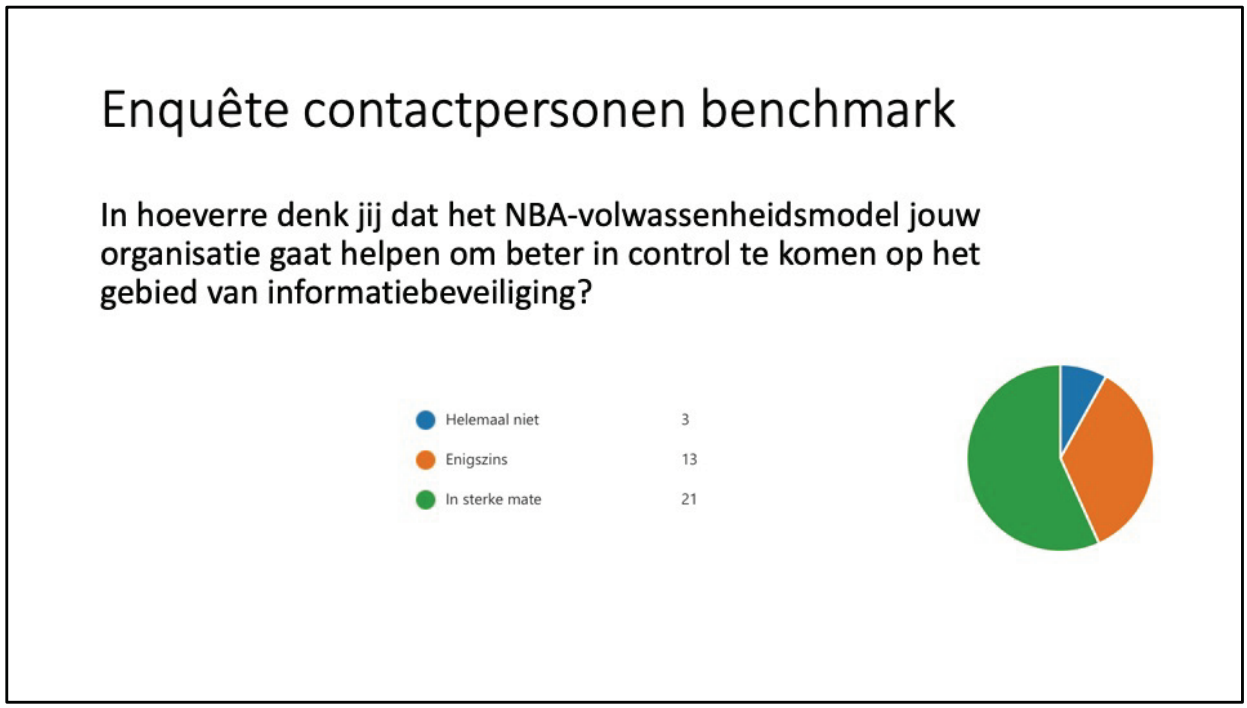
De pilot met het NBA-toetsingskader laat zien dat het volwassenheidniveau, zonder aanvullende maatregelen op dit gebied, volgens deze nieuwe meetlat van 2,8 naar een gemiddelde van 2,1 terugvalt. Op zich is dat geen probleem, de benchmark is immers geen doel op zich, we zien het vooral als een oproep aan de instellingen om werk te maken van de tot nu toe onderbelichte aspecten van informatiebeveiliging. Omdat het model sterk risico-gebaseerd is, is voor de hogere volwassenheidsniveaus betrokkenheid van het senior-management vereist. Betrokkenheid van het CvB wordt de komende periode een belangrijke succesfactor.

Scores pilot NBA-toetsingskader IB

- Statements NBA zijn via ISO27002 gemapt op huidige toetsingskader
- Vergelijking met scores oud/nieuw op clusterniveau
  - scores op basis van de 31 deelnemende mbo's

Benchmark Informatiebeveiliging 2021	Toetsingskader MBO	Toetsingskader NBA	Vergelijking
Totaal informatiebeveiliging	2,9	2,1	-0,8
Cluster 1: Beleid en organisatie	3,1	2,0	-1,1
Cluster 2: Personeel, studenten en gasten	2,8	2,3	-0,5
Cluster 3: Ruimtes en apparatuur	3,0	2,3	-0,6
Cluster 4: Continuïteit	3,0	2,1	-0,9
Cluster 5: Vertrouwelijkheid en integriteit	2,9	2,2	-0,8
Cluster 6: Controle en Logging	2,6	1,9	-0,7

Vergelijking van het huidige- en het NBA-toetsingskader op clusterniveau
Het NBA-volwassenheidsmodel is evenals ons huidige toetsingskader gebaseerd op de ISO 27001/2 norm. Op die manier zijn de statements volgens het NBA-model te mappen op de clusters van het huidige toetsingskader. We hebben op deze manier de clustergemiddelden vergeleken van de 31 deelnemers aan deze pilot. Op die manier zien we meer gedetailleerd waar aandachtspunten naar boven komen: vooral in het cluster 'Beleid en organisatie' vallen we sterk terug omdat hierin een aantal nieuwe aandachtpunten terugkomen vanuit de NBA-domeinen 'Bestuur' en 'Risicobeheer'. Wat ook meespeelt is dat het NBA-model voor de hogere volwassenheidsniveaus in dit cluster aantoonbare betrokkenheid van het senior management (lees CvB) vraagt.

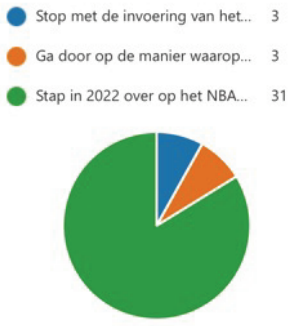


Enquête contactpersonen benchmark
Na het invullen van de Benchmark vullen de contactpersonen (meestal diegenen die de benchmark invullen) een korte enquête in, met vragen over de onwikkelingen op het gebied van IBP. Dit jaar hebben we onder andere gevraagd naar de ervaringen met het NBA-model. Vrijwel alle respondenten zijn van mening dat het nieuwe NBA-volwassenheidsmodel gaat helpen om beter in control te komen op het gebied van informatiebeveiliging.

Enquête contactpersonen benchmark

Op welke manier zie jij de overgang naar het NBA-toetsingskader voor je?

- Stop met de invoering van het NBA-model en behoud het bestaande ISO-gebaseerde toetsingskader
- Ga door op de manier waarop we het nu hebben gedaan: gebruik het NBA-model naast het huidige ISO-toetsingskader en baseer de benchmark op het huidige ISO-toetsingskader
- Stap in 2022 over op het NBA-toetsingskader voor de benchmark en stop met het huidige ISO-toetsingskader



De meerderheid wil in 2022 overstappen op het nieuwe NBA-toetsingskader
Op de vraag of en hoe we zouden moeten overstappen naar het nieuwe toetsingskader antwoordt 84% die overstap in 2022 te willen maken. Tijdens onze netwerkbijeenkomst IBP van 9 december 2021 hebben we deze uitkomsten besproken en deze conclusie ook in breder verband getrokken. Overigens wel met een aantal kanttekeningen:

1. Het is belangrijk om het scholingsprogramma dat in het najaar van 2021 is uitgevoerd voort te te zetten in 2022 en het daarbij ook op andere stakeholders te richten, zoals lijnmanagers.
2. De kracht van dit nieuwe toetsingskader / volwassenheidsmodel is dat het de hele organisatie raakt en saMBO-ICT / MBO Digitaal kan de verbindende rol spelen richting de andere netwerken, zoals het netwerk Informatiemanagement, het CIO-, het CSC- en het FSR-netwerk.
3. De bestuurlijke betrokkenheid wordt gezien als de belangrijkste succesfactor, dus het onderwerp cyberveiligheid moet ook in 2022 prominent op de agenda van de bestuurders, onder meer via regio- en ALV-bijeenkomsten.